

Análisis de empresas de TI en materia de seguridad de datos personales para fomentar la figura de encargado de acuerdo a la LFPDPPP

Reporte correspondiente a recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en el sector de tecnologías de información para dar cumplimiento a la LFPDPPP

Julio, 2012

Contenido

INTRODUCCIÓN	4
I. MARCO LEGAL.....	6
I.1 Marco constitucional.....	6
I.2 Legislación secundaria.....	8
I.3 La figura del encargado	15
II. CONTEXTO JURÍDICO INTERNACIONAL.....	16
II.1 ONU	17
II.2 APEC.....	22
II.3 OCDE.....	24
II.4 UNIÓN EUROPEA	31
III. ESTÁNDARES INTERNACIONALES.....	36
III.1 MEJORES PRÁCTICAS Y ESTÁNDARES.....	36
III.1.1 CMMI.....	36
III.1.2 COBIT	55
III.1.3 ISO 27001	64
III.1.4 ITIL	90
III.1.5 NIST	103
III.1.6 PCI/DSS.....	135
III.2 ÁMBITO INTERNACIONAL.....	142
III.2.1 Europa.....	142
III.2.1.1 España.....	142
III.2.1.2 Reino Unido	154
III.2.2 América.....	169
III.2.2.1 Estados Unidos.....	169
III.3 CONCLUSIONES SOBRE MEJORES PRÁCTICAS Y ESTÁNDARES INTERNACIONALES.....	184
IV. MARCO PROGRAMÁTICO.....	199
V. ANÁLISIS DE LOS RESULTADOS DE LA ENCUESTA-SONDEO EN LÍNEA DE LAS EMPRESAS DEL SECTOR DE TI.....	205

V.1 METODOLOGÍA.....	205
V.2 ANÁLISIS DESCRIPTIVO.....	210
V.2.1 Clasificación de las empresas.....	210
V.2.2 Prácticas organizacionales de privacidad y seguridad de la información.....	211
V.2.3 Tipo, Existencia y Práctica de Medidas de seguridad.....	212
V.2.4 Tratamiento de Datos Personales en el denominado Cómputo en la Nube.....	219
V.2.5 CONCLUSIONES DEL ANÁLISIS DE LOS RESULTADOS DE LA ENCUESTA-SONDEO EN LÍNEA.....	220
VI. RECOMENDACIONES Y PROPUESTA DE MEDIDAS CORRECTIVAS	223
VII. PROPUESTA DE POLÍTICAS PÚBLICAS.....	296
7.1 Objetivos.....	296
7.2 Líneas de Acción.....	297
7.3 Previsión de Recursos.....	301
7.4 Instrumentos de Política.....	302
7.5 Responsables Institucionales de la Ejecución.....	304
ANEXOS.....	309
ANEXO 1.....	310
ENCUESTA-SONDEO EN LÍNEA.....	310
ANEXO 2.....	324
RESULTADOS Y ESQUEMA ESTADÍSTICO DE LA ENCUESTA-SONDEO EN LÍNEA.....	324
RESUMEN EJECUTIVO.....	377

INTRODUCCIÓN

El presente reporte tiene como propósito condensar en una propuesta concreta los estudios realizados en sus diversas etapas del proyecto **“ANÁLISIS DE EMPRESAS DE TI EN MATERIA DE SEGURIDAD DE DATOS PERSONALES PARA FOMENTAR LA FIGURA DEL ENCARGADO DE ACUERDO A LA LFPDPPP”** encomendado a la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) por parte de la Secretaría de Economía en el marco del Proyecto de Desarrollo de la Industria de las Tecnologías de la Información (PROSOFT 2.0).

Se trata del quinto y último reporte relativo a “Recomendaciones y medidas correctivas para una práctica de medidas de seguridad en protección de datos personales en el sector de las TI para dar cumplimiento a la LFPDPPP”, conforme a los Términos de Referencia de este proyecto¹.

Es importante señalar que esta propuesta toma en consideración, como marco referencial, diversas previsiones jurídicas contenidas en la Constitución Política de los Estados Unidos Mexicanos, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento, así como otras normas de carácter nacional o internacional que autorizan al Gobierno Federal a realizar las actividades que constituyen las políticas públicas y que, a su vez, limitan la discrecionalidad en la actuación de los que elaborarán y ejecutarán medidas correctivas a que se refiere este estudio.

Del proceso de recolección de información y análisis de los datos realizado en las entregas o reportes previos, el estudio ha permitido racionalizar

¹ TORS. Apartado “Metodología de Trabajo” inciso f), pág. 14

objetivos, estrategias, prioridades, previsiones, medidas, instrumentos o herramientas y demás conceptos que integran una propuesta, tanto de recomendaciones y medidas correctivas como de políticas públicas.

Cabe señalar que la elaboración de esta propuesta se apega a los lineamientos de la Ley de Planeación y que forma parte de una estrategia, tanto para impulsar el desarrollo de las TI como para fomentar la cultura de protección de datos personales. Por lo tanto, las recomendaciones y medidas que aquí se plantean señalan los principales resultados que se deben obtener para desarrollar las habilidades y fomentar el uso de buenas prácticas en el sector de TI para poder brindar certeza a las empresas que las subcontraten bajo la figura de encargado.

Finalmente se debe señalar que el ámbito de este reporte se circunscribe a empresas del sector de TI², lo que no impide que se aplique a otro tipo de actividades económicas.

² http://dof.gob.mx/nota_detalle.php?codigo=5182928&fecha=23/03/2011

I. MARCO LEGAL

Antes de iniciar el desarrollo de la propuesta de medidas correctivas así como de las recomendaciones sobre políticas públicas, es importante considerar el marco normativo que la sustenta, toda vez que en México existen disposiciones que norman los diversos aspectos de la protección de datos personales, así como de la generación de políticas públicas en esta y otras materias.

I.1 Marco constitucional

En primer lugar, la Constitución Política de los Estados Unidos Mexicanos establece una serie de principios desde que el 20 de julio de 2007 aparecieron publicadas en el Diario Oficial de la Federación reformas al artículo 6, cuyo texto –dirigido al tratamiento de datos personales por el Estado- establece:

Artículo 6o. La manifestación de las ideas...

Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

Una vez concretada la tutela de los datos en posesión del Gobierno, el 30 de abril de 2009 se publicó en el DOF la adición de una fracción XXIX-O al artículo 73 de la Constitución, para facultar al Congreso a legislar sobre la

protección de datos personales en posesión de los particulares, tema que solamente se regía por criterios de confidencialidad.

Dicha enmienda constitucional estableció lo siguiente:

Artículo 73. El Congreso tiene facultad:

XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.

Pero como derecho (humano) expreso, la protección de datos personales en posesión de los particulares quedó plasmada en la Constitución Federal, cuando se reformó en junio del 2009 su artículo 16 que, en lo conducente, establece:

Artículo 16. Nadie puede ser molestado en su persona...

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros.

I.2 Legislación secundaria

Al amparo de ese marco previsto en la Constitución, fue publicada en el Diario Oficial de la Federación del 5 de julio del año 2010 la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)**, en la cual se prevén criterios jurídicos relativos a la figura del encargado, como coparticipe en el tratamiento de datos personales, así como principios en materia de seguridad.

Los dispositivos relativos a ambos temas (encargado y seguridad) son, principalmente, los siguientes:

Artículo 3. Para los efectos de esta Ley, se entenderá por:

IX. Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

XIX. Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

Artículo 19. Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Artículo 20. Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.

Artículo 36. Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.

El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

Artículo 39. El Instituto (IFAIPD) tiene las siguientes atribuciones:

V. Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable;

Artículo 58. Los titulares que consideren que han sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento a lo dispuesto en la presente Ley por el responsable o el encargado, podrán ejercer los derechos que estimen pertinentes para efectos de la indemnización que proceda, en términos de las disposiciones legales correspondientes.

Artículo 63. Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:

XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.

Artículo 67. Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

A efecto de proveer a la exacta observancia de la citada LFPDPPP, se publicó en el Diario Oficial de la Federación el **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, acerca del cual se hacen comentarios en el apartado 1.3 de este documento.

Al tiempo que existe un marco especial sobre la protección de datos personales, la **Ley Federal de Protección al Consumidor** publicada en el Diario de la Federación del 21 de diciembre del 2011 regula cuestiones que ahora, en un contexto jurídico más definido sobre privacidad y el derecho a la autodeterminación informativa, tiene gran relevancia para el rol que juegan las empresas de Tecnologías de la Información en materia de seguridad de datos personales, cuando asumen el papel del encargado en el tratamiento de estos.

En efecto, dicha Ley establece lo siguiente:

ARTÍCULO 16. Los proveedores y empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella. De existir dicha información, deberán ponerla a su disposición si ella misma o su representante lo solicita, e informar acerca de qué información han compartido con terceros y la identidad de esos terceros, así como las recomendaciones que hayan efectuado. La

respuesta a cada solicitud deberá darse dentro de los treinta días siguientes a su presentación. En caso de existir alguna ambigüedad o inexactitud en la información de un consumidor, éste se la deberá hacer notar al proveedor o a la empresa, quien deberá efectuar dentro de un plazo de treinta días contados a partir de la fecha en que se le haya hecho la solicitud, las correcciones que fundadamente indique el consumidor, e informar las correcciones a los terceros a quienes les haya entregado dicha información.

Para los efectos de esta ley, se entiende por fines mercadotécnicos o publicitarios el ofrecimiento y promoción de bienes, productos o servicios a consumidores.

ARTÍCULO 17. En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría.

El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.

ARTÍCULO 18. La Procuraduría (PROFECO) podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por correo electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito.

ARTÍCULO 18 BIS. Queda prohibido a los proveedores y a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el artículo anterior. Los proveedores que sean objeto de publicidad son corresponsables del manejo de la información de los consumidores cuando dicha publicidad la envíen a través de terceros.

Por otra parte, la **Ley de Protección y Defensa al Usuario de Servicios Financieros** publicada en Diario Oficial de la Federación del 18 de enero de 1999, contempla desde antes de la LFPDPPP del 2010, que debe existir una política empresarial a favor de la tutela de los datos personales de los usuarios de los servicios financieros, conforme al criterio siguiente:

Artículo 8o. La Comisión Nacional (CONDUSEF), con la información que le proporcionen las autoridades competentes y las Instituciones Financieras, establecerá y mantendrá actualizado un Registro de Prestadores de Servicios Financieros, en los términos y

condiciones que señala esta Ley. Lo anterior, sin perjuicio de los demás registros que corresponda llevar a otras autoridades.

Asimismo, la Comisión Nacional establecerá y mantendrá actualizada una Base de Datos de comisiones que le sean reportadas y que comprenderá sólo las comisiones vigentes que efectivamente cobren, misma que se dará a conocer al público en general, por el medio de difusión que la Comisión Nacional considere pertinente.

La Comisión Nacional establecerá y mantendrá actualizado, un Registro de Usuarios que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Queda prohibido a las Instituciones Financieras utilizar información relativa a la base de datos de sus clientes con fines mercadotécnicos o publicitarios, así como enviar publicidad a los clientes que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el párrafo anterior. Las Instituciones Financieras que sean objeto de publicidad son corresponsables del manejo de la información de sus clientes cuando dicha publicidad la envíen a través de terceros.

Los usuarios se podrán inscribir gratuitamente en el Registro Público de Usuarios, a través de los medios que establezca la Comisión Nacional, la cual será consultada por las Instituciones Financieras.

Las Instituciones Financieras que incumplan lo dispuesto por el presente artículo, se harán acreedoras a las sanciones que establece esta Ley.

I.3 La figura del encargado

Siendo objeto de este estudio el papel que le corresponde al denominado “encargado” en el campo del tratamiento de datos personales en posesión de particulares, es pertinente tener presente que la LFPDPPP establece en su artículo 3, fracción IX, que se trata de *“la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable”*.

Por su parte, el Reglamento de dicha Ley aclara en su artículo 49 que:

Figura del encargado

Artículo 49. El encargado es la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Acerca de sus obligaciones, también dispone:

Obligaciones del encargado

Artículo 50. El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:

- I. Tratar únicamente los datos personales conforme a las instrucciones del responsable;
- II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
- III. Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables;

IV. Guardar confidencialidad respecto de los datos personales tratados;

V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y

VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.

Los acuerdos entre el responsable y el encargado relacionados con el tratamiento deberán estar acordes con el aviso de privacidad correspondiente.

Y respecto a la relación entre el responsable y el encargado, el Reglamento invocado señala:

Relación entre el responsable y el encargado

Artículo 51. La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.

II. CONTEXTO JURÍDICO INTERNACIONAL

El marco legal no se agota en el orden jurídico nacional, sino que existe una serie de instrumentos internacionales que inciden en el respeto de los principios previstos en el artículo 6 de la LFPDPPP, como son los derivados de organismos internacionales.

Es de señalar que la Organización Mundial de la Propiedad Intelectual (OMPI-WIPO); la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL); la Organización para la Cooperación y el Desarrollo Económico (OCDE-OECD); el Área de Libre Comercio de las Américas (ALCA) y la Cámara de Comercio Internacional (CCI-ICC) han venido formulando propuestas de buenas prácticas, al igual que la Red Iberoamericana de Protección de Datos.³

II.1 ONU

Primeramente es relevante la Resolución 45/95 de la Organización de las Naciones Unidas⁴ que, en lo conducente establece:

Principios rectores aplicables a los ficheros computarizados de datos personales. (Resolución 45/95 de 14 de diciembre, de la Asamblea General de las Naciones Unidas (documento E/CN.4/1990/72.20 de febrero de 1990))

Directrices para la regulación de los archivos de datos personales informatizados

Adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990.

Los procedimientos para llevar a la práctica las normas relativas a los archivos de datos personales informatizados se dejan a la iniciativa de cada Estado, con sujeción a las siguientes orientaciones:

³ <http://www.redipd.org/>

⁴ http://www.informatica-juridica.com/anexos/Principios_rectores_aplicables_ficheros_computarizados_datos_personales_Resolucion_45_95_14_diciembre_Asamblea_General_Naciones_Unidas.asp

A. PRINCIPIOS RELATIVOS A LAS GARANTÍAS MÍNIMAS QUE DEBEN PREVER LAS LEGISLACIONES NACIONALES

Principio de legalidad y lealtad

La información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas.

Principio de exactitud

Las personas responsables de la compilación de archivos, o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que los mismos se mantengan de la forma más completa posible, con el fin de evitar errores de omisión, así como de actualizarlos periódicamente o cuando se use la información contenida en un archivo, mientras están siendo procesados.

Principio de especificación de la finalidad

La finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada, con el fin de que posteriormente sea posible garantizar que:

Todos los datos personales recogidos y registrados sigan siendo pertinentes y adecuados para los fines especificados;

Ninguno de los referidos datos personales sea utilizado o revelado, salvo con el consentimiento de la persona afectada, para fines incompatibles con aquellos especificados;

El periodo durante el que se guarden los datos personales no supere aquel que permita la consecución de los fines especificados.

Principio de acceso de la persona interesada

Cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costes o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios. Debe preverse un recurso, en caso necesario, ante la autoridad supervisora especificada más abajo en el principio 8. El coste de cualquier rectificación será soportado por la persona responsable del archivo. Es conveniente que las disposiciones relacionadas con este principio se apliquen a todas las personas, sea cual sea su nacionalidad o lugar de residencia.

Principio de no discriminación

Sin perjuicio de los casos susceptibles de excepción restrictivamente contemplados en el principio 6, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.

Facultad para hacer excepciones

Las excepciones a los principios 1 a 4 solamente pueden ser autorizadas en caso de que sean necesarias para proteger la seguridad nacional, el orden público, la salud pública o la moralidad, así como, entre otras cosas, los derechos y libertades de otros, especialmente de personas que estén perseguidas (cláusula humanitaria), siempre que tales excepciones estén especificadas de forma explícita en una ley o norma equivalente promulgada de acuerdo con el sistema jurídico interno, que expresamente establezca sus límites y prevea las salvaguardas adecuadas.

Las excepciones al principio 5, relativo a la prohibición de la discriminación, además de estar sujetas a las mismas salvaguardas que las prescritas para las excepciones a los principios 1 a 4, solamente podrán autorizarse dentro de los límites establecidos en la Carta Internacional de Derechos Humanos y en el resto de instrumentos aplicables en el campo de la protección de los derechos humanos y la prevención de la discriminación.

Principio de seguridad

Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, como la pérdida o destrucción accidental, como humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos.

Supervisión y sanciones

El derecho de cada país designará a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios arriba establecidos. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica. En caso de violación de lo dispuesto en la ley nacional que lleve a la práctica los principios anteriormente mencionados, deben contemplarse condenas penales u otras sanciones, junto con los recursos individuales adecuados.

Flujo transfronterizo de datos

Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca salvaguardas similares para la protección de la intimidad, la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que no existan salvaguardas recíprocas, no deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad.

Campo de aplicación

Los presentes principios deben hacerse aplicables, en primer lugar, a todos los archivos informatizados públicos y privados, así como, mediante extensión optativa y sujeta a los ajustes correspondientes, a los archivos manuales. Pueden dictarse disposiciones especiales, también optativas, para hacer aplicable la totalidad o parte de los principios a los archivos relativos a personas jurídicas, especialmente cuando contengan alguna información relativa a individuos.

B. APLICACIÓN DE LAS DIRECTRICES A ARCHIVOS DE DATOS PERSONALES MANTENIDOS POR ORGANIZACIONES INTERNACIONALES GUBERNAMENTALES

Las presentes directrices serán de aplicación a los archivos de datos personales que mantengan las organizaciones internacionales gubernamentales, sujetas a cualquier ajuste que sea preciso para tener en cuenta cualquier diferencia que pueda existir entre archivos para fines internos, como aquellos que conciernen a la gestión de personal, y archivos para fines externos, relativos a terceros que tengan relaciones con la organización.

Cada organización debe designar a la autoridad legalmente competente para supervisar la observancia de estas directrices.

Cláusula humanitaria: puede preverse específicamente una excepción a estos principios cuando la finalidad del archivo sea la protección de los derechos humanos y las libertades fundamentales de la persona afectada, o la ayuda humanitaria. Debe preverse una excepción similar en la legislación nacional para las organizaciones internacionales gubernamentales cuyo acuerdo organizativo no impida la puesta en práctica de la referida legislación nacional, así como para las organizaciones internacionales no gubernamentales a las que sea aplicable esta ley.

II.2 APEC

La Organización para la Cooperación Económica en Asia-Pacífico (APEC) ha emitido criterios sobre la regulación de los proveedores en los servicios de Internet y en lo relacionado al tráfico de los flujos de información.

Las Economías de APEC aprobaron en la reunión de Sidney, Australia, en 2007, el APEC Data Privacy Pathfinder, diseñado al interior del Sub-grupo de Privacidad⁵. Este acuerdo consiste en un conjunto de compromisos dirigidos a desarrollar el Sistema de Reglas de Privacidad Transfronterizas (CBPRs).

El objetivo de este sistema de protección de datos es incentivar a las organizaciones a que desarrollen sus propias reglas de privacidad que regulen el flujo de información personal internacional. Los países integrantes de APEC han reconocido que las organizaciones, (empresas, compañías, etc.) tienen un gran interés en la protección de la información personal de sus clientes y que muchas de las compañías ya han diseñado procedimientos y prácticas empresariales para asegurarse que la información personal se encuentra protegida.

Para lograr sus objetivos, el APEC Data Privacy Pathfinder tiene como propósito el desarrollo de nueve proyectos⁶, agrupados en cuatro categorías que corresponden a los objetivos primarios del CBPRs:

Autoevaluación (Proyecto 1. Guía de autoevaluación para las empresas).

Revisión del cumplimiento (Proyecto 2. Criterios de reconocimiento de los agentes responsables del sector público o privado; Proyecto 3. Proceso de revisión de cumplimiento de los CBPRs; y Proyecto 4. Directorios y contactos de los agentes responsables y organismos).

Reconocimiento/aceptación (Proyecto 5. Directorio de las autoridades de protección de datos personales y privacidad);

⁵ El Sub-Grupo de Privacidad de APEC fue creado en 2003 dentro del Grupo de Manejo de Comercio Electrónico (ECSG) de APEC para abordar todos los temas relacionados con privacidad. El grupo se reúne dos veces al año y reporta sus avances al ECSG quien en última instancia reporta directamente a los Ministros de APEC.

⁶ Fuente: APEC Data Privacy Pathfinder: Project Work Plan, 2007/SOM3/ECSG/DPS/004.

Resolución de conflictos y aplicación (Proyecto 6. Formato para la realización de acuerdos de cooperación y Proyecto 7. Formato para el manejo de quejas transfronterizas).

II.3 OCDE

La Organización para la Cooperación y el Desarrollo Económico (OCDE) ha asumido la tarea de atender asuntos sobre los actos ilícitos en torno al Internet, así como para establecer estándares sobre privacidad y protección de datos personales. Como producto de su trabajo, resultan interesantes sus Lineamientos para la Protección al Consumidor en el Contexto del Comercio Electrónico del año 1999.

De los dispositivos de la OCDE, debemos destacar las Directrices Relativas a la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales⁷, que conforme al siguiente resumen prevén:

PRIMERA PARTE – Generalidades

Definiciones

Como guía para estas directrices:

- “controlador de datos” es una segunda parte que, de acuerdo con la legislación nacional, tiene competencia para determinar los contenidos y el uso de datos personales independientemente de si dicha parte o un agente en su nombre los recoge, guarda, procesa o divulga;
- “datos personales” son cualquier información relacionada con un individuo identificado o identificable (sujeto de los datos);
- “flujo transfronterizo de datos personales” es el movimiento de datos personales a través de fronteras nacionales.

⁷ <http://www.oecd.org/dataoecd/16/51/15590267.pdf> Resumen elaborado por el propio organismo © OCDE 2002

Alcance de las directrices

Estas directrices aplican a datos personales del sector público o privado que, debido a la forma en que se procesan, a su naturaleza o al contexto en que se usan, suponen un peligro para la privacidad y las libertades individuales.

Estas directrices no se deberían interpretar como medio para evitar:

- la aplicación de diferentes medidas protectoras a diferentes categorías de datos personales dependiendo de su naturaleza y el contexto en el que se recogen, almacenan, procesan o divulgan;
- la exclusión de la aplicación de las directrices de datos personales que obviamente no entrañan riesgo alguno para la privacidad ni las libertades individuales; o bien,
- la aplicación de las directrices sólo al procesamiento automático de datos personales.

Las excepciones a los principios de los capítulos dos y tres de estas directrices, como las relacionadas con la soberanía y seguridad nacional y el orden público, deberían ser:

- la menor cantidad posible y
- de conocimiento público.

En el caso concreto de países federales, la observancia de estas directrices se podría ver afectada por la distribución de competencias.

Estas directrices se deberán considerar como estándares mínimos que se puedan complementar con otras medidas de protección de la privacidad y de las libertades individuales.

SEGUNDA PARTE - Principios básicos de aplicación nacional

Principio de limitación de recogida

Deberán existir límites para la recogida de datos personales y cualquiera de estos datos deberá obtenerse con medios legales y justos y, siempre que sea apropiado, con el conocimiento o consentimiento del sujeto implicado.

Principio de calidad de los datos

Los datos personales deberán ser relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, exactos, completos y actuales.

Principio de especificación del propósito

El propósito de la recogida de datos se deberá especificar a más tardar en el momento en que se produce dicha recogida, y su uso se verá limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, especificando en cada momento el cambio de objetivo.

Principio de limitación de uso

No se deberá divulgar, poner a disposición o usar los datos personales para propósitos que no cumplan lo expuesto en el apartado 9⁸, excepto:

⁸ Los efectos para los cuales se recojan los datos personales deberían especificarse en el momento de la recogida, a más tardar, y la posterior utilización quedar limitada al cumplimiento de tales efectos o de aquellos otros que no sean incompatibles con los mismos y que se especifiquen en cada ocasión en que

- si se tiene el consentimiento del sujeto implicado o
- por imposición legal o de las autoridades.

Principio de salvaguardia de la seguridad

Se emplearán salvaguardias razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos.

Principio de transparencia

Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales. Se deberá contar con medios ágiles para determinar la existencia y la naturaleza de datos personales, el propósito principal para su uso y la identidad y lugar de residencia habitual de quien controla esos datos.

Principio de participación individual

Todo individuo tendrá derecho a:

- que el controlador de datos u otra fuente le confirme que tiene datos sobre su persona;
- que se le comuniquen los datos relativos a su persona
 - en un tiempo razonable;
 - a un precio, si existiese, que no sea excesivo;
 - de forma razonable; y

se cambie la finalidad.

http://www.agpd.es/portaleswebAGPD/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-proteccion-de-privacidad-Trad..pdf

- de manera inteligible;
- que se le expliquen las razones por las que una petición suya según los subapartados⁹ (a) y (b) haya sido denegada, así como poder cuestionar tal denegación; y
- expresar dudas sobre los datos relativos a su persona y, si su reclamación tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan.

Principio de responsabilidad

Sobre todo controlador de datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

TERCERA PARTE - Principios básicos de aplicación internacional: restricciones en el libre flujo y la legitimidad

Los países miembros deberán considerar las implicaciones que el procesamiento nacional y la reexportación de datos personales puedan tener para otros países miembros.

Los países miembros deberán seguir todos los pasos razonables y apropiados para asegurar que el flujo transfronterizo de datos personales, incluido el tránsito a través de un país miembro, se realice de forma ininterrumpida y segura.

⁹ a) Recabar, del controlador de los datos o de otro modo, confirmación de si el controlador tiene o no tiene datos correspondientes a la misma; b) hacer que se le comuniquen los datos correspondientes a ella dentro de un plazo razonable, por una cuota en su caso, que no sea excesiva, de manera razonable y de una forma que le resulte fácilmente inteligible.
Ibid., p. 5.

Los países miembros deberán abstenerse de restringir el intercambio transfronterizo de datos personales con otros países miembros, excepto cuando el país receptor todavía no observe de forma sustancial estas directrices o cuando la reexportación de tales datos burle la legislación nacional sobre privacidad. Un país miembro también podrá imponer restricciones a ciertas categorías de datos personales sobre las que rijan normativas específicas, contenidas en su legislación nacional sobre privacidad, que por su naturaleza no tienen una protección equiparable en el país receptor.

Los países miembros deberán evitar la elaboración de leyes, políticas y prácticas destinadas a proteger la privacidad y las libertades individuales que pudieran crear obstáculos al flujo transfronterizo de datos personales excediendo los requisitos para tal protección.

CUARTA PARTE - Implantación nacional

A la hora de implantar en el ámbito nacional los principios expuestos en los capítulos dos y tres¹⁰, los países miembros deberán crear procedimientos o instituciones legales, administrativos o de otro tipo para garantizar la protección de la privacidad y las libertades individuales en relación con los datos personales. Los países miembros deberán poner especial empeño en:

- adoptar una legislación nacional adecuada;

¹⁰ Ibid., pp. 4-6.

- impulsar y apoyar la autorregulación, ya sea mediante códigos de conducta o de otro modo;
- brindar los medios razonables para que los individuos ejerzan sus derechos;
- sancionar adecuadamente y ofrecer soluciones en caso de fallos con el fin de cumplir las medidas de implantación expuestas en los capítulos dos y tres¹¹; y
- asegurar que no haya discriminación desleal hacia el sujeto de los datos.

QUINTA PARTE - Cooperación internacional

Si así se solicitara, los países miembros deberán dar a conocer a otros países miembros detalles sobre la observancia de los principios expuestos en estas directrices. Deberán asegurarse además de que los procedimientos para el flujo transfronterizo de datos personales, y de protección de la privacidad y las libertades individuales sean sencillos y compatibles con los de otros países miembros que cumplen estas directrices.

Los países miembros deberán establecer procedimientos para facilitar:

- el intercambio de información relacionada con estas directrices
- la cooperación en cuestiones procesales y de investigación

Los países miembros deberán orientar su trabajo hacia la elaboración de principios, nacionales e internacionales, que

¹¹ Ibid., pp. 4-6.

gobiernen la legislación aplicable en materia de flujos transfronterizos de datos personales.

II.4 UNIÓN EUROPEA

La Unión Europea ha sido muy activa en la creación de reglas para fortalecer las actividades de protección de datos personales en el ámbito del *e-commerce*. En particular, la Directiva 95/46/CE en materia de protección de datos personales, instituye un orden regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE).

En específico, la Directiva 95/46/CE se ha resumido en los términos siguientes:¹²

La presente Directiva se aplica a los datos tratados por medios automatizados (base de datos informática de clientes, por ejemplo), así como a los datos contenidos en un fichero no automatizado o que vayan a figurar en él (ficheros en papel tradicionales).

La Directiva no se aplicará al tratamiento de datos:

- efectuado por una persona física en el ejercicio de actividades exclusivamente particulares o domésticas;
- aplicado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, tales como la seguridad pública, la defensa o la seguridad del Estado.

¹² http://europa.eu/legislation_summaries/information_society/data_protection/114012_es.htm

La Directiva tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Dichos principios se refieren a:

La **calidad** de los datos: los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.

La **legitimación** del tratamiento: el tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento de forma inequívoca o si el tratamiento es necesario para:

- la ejecución de un contrato en el que el interesado sea parte, o
- el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
- proteger el interés vital del interesado, o
- el cumplimiento de una misión de interés público, o
- la satisfacción del interés legítimo perseguido por el responsable del tratamiento.

Las **categorías** especiales de tratamiento: deberá prohibirse el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Esta disposición va acompañada de reservas que se aplicarán, por ejemplo, en caso de

que el tratamiento sea necesario para salvaguardar el interés vital del interesado o para la prevención o el diagnóstico médico.

La **información** a los afectados por dicho tratamiento: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) a la persona de quien se recaben los datos que le conciernan.

El **derecho de acceso** del interesado a los datos: todos los interesados deberán tener el derecho de obtener del responsable del tratamiento:

- la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos;
- la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones.

Las **excepciones y limitaciones**: se podrá limitar el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado.

El **derecho del interesado a oponerse** al tratamiento: el interesado deberá tener derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento. También deberá tener la posibilidad de oponerse, previa petición y sin gastos, al tratamiento de los datos respecto de los cuales se prevea un tratamiento destinado a la prospección. Por último, deberá ser informado antes de que los datos se comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación.

La confidencialidad y la seguridad del tratamiento: las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento. Por otra parte, el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.

La notificación del tratamiento a la autoridad de control: el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.

Las legislaciones nacionales deben prever un **recurso judicial** para los casos en los que el responsable del tratamiento de datos no

respete los derechos de los interesados. Además, las personas que sufran un perjuicio como consecuencia de un tratamiento ilícito de sus datos personales tendrán derecho a obtener la reparación del perjuicio sufrido.

Se autorizará la transferencia de datos personales de un Estado miembro a un tercer país que garantice un nivel de protección adecuado; por el contrario, no se autorizará la transferencia a terceros países que no dispongan de tal nivel de protección, salvo contadas excepciones.

La Directiva pretende facilitar la elaboración de códigos de conducta nacionales y comunitarios que contribuyan a una correcta aplicación de las disposiciones nacionales y comunitarias.

Cada Estado miembro designará una o varias autoridades públicas independientes encargadas de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros en aplicación de la presente directiva.

Se crea un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales, que estará compuesto por representantes de las autoridades de control nacionales, por representantes de las autoridades de control de las instituciones y organismos comunitarios y por un representante de la Comisión.

Igualmente, se debe considerar la Directiva 1999/93/CE del Parlamento Europeo y del Consejo¹³ por el que se establece un marco regulatorio para la firma electrónica.

¹³ <http://www.boe.es/doue/2000/013/L00012-00020.pdf> (Fecha de consulta 8 de noviembre de 2011).

III. ESTÁNDARES INTERNACIONALES

Otro aspecto que es necesario considerar, es el relativo a los estándares que se han ido produciendo en el entorno mundial para fomentar la práctica de medidas de seguridad de la información y protección de datos personales, y sobre todo en el sector de las TI.

En entregas previas a esta versión final del estudio, se analizaron varios casos de estándares internacionales que pueden servir de referencia al caso mexicano, el cual se encuentra en proceso de implementación de la LFPDPPP y su Reglamento.

Por lo anterior, se presenta a continuación un resumen de las mejores prácticas y estándares internacionales en materia de seguridad de la información.

III.1 MEJORES PRÁCTICAS Y ESTÁNDARES

III.1.1 CMMI

III.1.1.1 Antecedentes

En la década de los 30, Walter Shewhart comenzó a trabajar en la mejora de procesos, desarrollando principios de control estadístico de calidad. Enseguida, W. Edwards Deming, Philip Crosby y Joseph Juran afinaron dichos principios. Por su parte, Watts Humphrey, Ron Radice y otros comenzaron a extender los controles estadísticos de calidad, aplicándolos en el software de IBM y del SEI (Software Engineering Institute de Carnegie Mellon University).

Capability Maturity Model Integration (CMMI por sus siglas en inglés) fue creado por el equipo de trabajo de CMMI y posteriormente fue publicado por el SEI. En este proyecto participaron expertos del gobierno, la

industria y del propio SEI. La finalidad era mejorar el Software Capability Maturity Model (SW-CMM) desarrollado en 1991.¹⁴ El objetivo inicial se encaminó en resolver la problemática que significaba la utilización de diversos modelos. Esto era realmente un problema, pues los modelos se construían a partir de diferentes y variadas arquitecturas y acercamientos. Así pues, se inició un proceso de selección y tamización de modelos, con la finalidad de analizarlos y combinarlos, y de esta forma crear un solo marco de mejora. Al concretar un marco uniforme para las organizaciones, se alcanzaría sin duda una amplia mejora en los procesos de TI.

Ahora bien, inicialmente CMMI era un modelo que combinaba tres modelos: a) madurez y capacidad para software (SW-CMM) v2.0 borrador C, b) capacidad de sistema de ingeniería (SECM) (EIA 2002a) y c) integrado de capacidad y madurez de desarrollo de producto (IPD-CMM) v0.98.

El primer modelo CMMI (V1.02) fue diseñado para empresas de desarrollo que buscaban la mejora de procesos a nivel empresarial, de tal forma que en el año 2000 se lanzó el modelo CMMI original, o sea, método de entrenamiento y valoración. Éste incorporaba ingeniería del software e ingeniería de sistemas. Cabe señalar que también fue diseñado para apoyar la integración futura de otras disciplinas. Dos años más tarde se lanzó la versión 1.1 y cuatro años después la versión 1.2.

Durante el lanzamiento de la versión 1.2 se contempló la creación de otros dos modelos. Consecuentemente el nombre original de CMMI cambió, dando un giro conceptual que pondera el desarrollo y la

¹⁴ Véase <http://www.sei.cmu.edu/cmmi/why/CMMI-Timeline.cfm> revisado el 4 de febrero 2012, 22:00 hrs.

implementación de constelaciones. Pero ¿qué es una constelación? Este concepto se refiere a la colección de componentes de CMMI utilizados para construir los modelos, por un lado, y al material de capacitación y los documentos de evaluación relacionados para un área de interés, por el otro.

En el 2007 se lanzó el modelo CMMI para adquisiciones, el cual comenzó como versión 1.2; dos años más tarde se lanzó el CMMI para servicios, y también comenzó como versión 1.2.

La versión 1.3 se lanzó en noviembre de 2010, aplicándose en el modelo de adquisición. Enseguida, en el 2011, se aplicó en los modelos de desarrollo y de servicio. Los tres modelos tienen como objetivo asegurar la consistencia entre ellos, así como proporcionar material con mayor madurez.

Lo cierto es que el CMMI es un conjunto de mejores prácticas que proporciona los elementos esenciales para tener procesos efectivos. Además, permite identificar las fortalezas y debilidades de las organizaciones. Más aún, el CMMI abona el terreno para que se realicen los cambios necesarios en una organización, transformando las debilidades en fortalezas.

III.1.1.2 Utilización y estructura

Los modelos CMMI son un conjunto de mejores prácticas que ayudan a mejorar la eficiencia, eficacia y calidad dentro de grupos de trabajo, proyectos y divisiones. En suma, contribuye al mejoramiento en todas las áreas de una organización. Este modelo es tan versátil que puede ser utilizado tanto por organizaciones pequeñas como grandes en cualquier

sector, por ejemplo, electrónico, servicios de salud, seguros, finanzas, transporte, entre otros más.

Actualmente existen tres modelos de CMMI:

- Desarrollo
- Adquisición
- Servicios

CMMI para el desarrollo

Es un modelo de referencia que abarca actividades tanto para la esfera de desarrollo de productos como para la esfera de servicios. Incluye los siguientes aspectos: gestión de proyectos, gestión de procesos, ingeniería de sistemas, ingeniería de hardware y de software, y procesos de soporte utilizados para el desarrollo y mantenimiento. Este modelo no especifica un flujo en particular del proceso, ni establece un número de productos que deban ser desarrollados por día o por mercado. Más bien establece que –los proyectos y organizaciones– tengan procesos en el ámbito de las prácticas relacionadas con el desarrollo.

Dicho con otras palabras, este modelo busca que los requerimientos del cliente sean integrados en el producto o servicio final. El paso siguiente es analizar el trabajo de desarrollo, de manera que se pueda diseñar correctamente un producto o servicio. Es importante asegurarse que éste considere las necesidades del usuario final y las especificaciones formuladas durante el diseño.

El CMMI para el desarrollo puede implementarse en organizaciones de varios sectores, por ejemplo, aeroespacial, hardware, software, defensa, telecomunicaciones, banca, por mencionar algunos.

CMMI para adquisición

Modelo diseñado para negocios que se centran en trabajar con proveedores, ya sea para armar un producto o entregar un servicio. Asimismo integra la creación de solicitudes efectivas y acuerdos con los proveedores, recolectando y comunicando de forma efectiva los requerimientos a los proveedores. De ahí, pues, que se puedan monitorear las actividades y componentes, asegurando que el trabajo de los proveedores sea consistente con las necesidades del usuario final.

CMMI para servicios

Modelo diseñado para negocios que se enfocan en establecer, administrar y entregar servicios. Se caracteriza por analizar a detalle la planeación y administración de la capacidad y disponibilidad del servicio, el manejo de quejas y problemas, la planeación de las interrupciones del servicio, y la toma de decisiones sobre cuáles servicios proporcionar. Además, revisa y se asegura de que todo esté en su lugar en el momento de prestar un servicio (personal, procesos, consumibles y equipo).¹⁵

Este tipo de modelo es muy recomendable para empresas que proporcionan servicios de capacitación, logística, mantenimiento, consultoría, recursos humanos, salud, servicios de TI, investigación, por mencionar algunos giros.

Cada uno de los modelos incluye tres categorías de componentes:

- Requeridos: imprescindibles para lograr la mejora en el proceso de un área determinada. Particularmente las metas específicas y genéricas.

¹⁵Véase <http://www.sei.cmu.edu/library/assets/whitepapers/Which%20CMMI%20Model%20Is%20for%20You.pdf>, revisado el 4 de febrero 2012, 23:00 hrs.

- Esperados: describen las actividades más importantes. Particularmente las prácticas específicas y genéricas.
- Informativos: ayudan a los usuarios del modelo a entender los componentes requeridos y esperados, por ejemplo, subprácticas, notas, referencias, etc.

Cabe mencionar que estos tres modelos tienen la misma estructura y comparten elementos comunes, conocidos como áreas de proceso. Dichas áreas incluyen 16 temas centrales, que aplican en el contexto de cada una de éstas. Ciertamente al ser implementados de manera colectiva, satisfacen una serie de metas que se consideran importantes en el proceso de mejora de esa área. Los temas que tratan son los siguientes:

- Análisis causal y resolución (CAR)
- Administración de la configuración (CM)
- Análisis de decisiones y resolución (DAR)
- Administración Integrada de Proyecto (IPM)
- Medición y análisis (MA)
- Definición de procesos organizacionales (OPD)
- Enfoque del proceso organizacional (OPF)
- Administración del desempeño organizacional (OPM)
- Desempeño del proceso organizacional (OPP)
- Formación organizativa (OT)
- Monitoreo y control del proyecto (PMC)
- Planeación del proyecto (PP)
- Aseguramiento de la calidad del proceso y del producto (PPQA)
- Administración cuantitativa del proyecto (QPM)
- Administración de requerimientos (REQM)
- Administración de riesgo (RSKM)

No obstante cada uno de los modelos tiene áreas de procesos específicos.¹⁶

CMMI para adquisición

- Desarrollo de requerimientos para adquisición (ARD)
- Desarrollo de solicitud y acuerdo del proveedor (SSAD)
- Administración del acuerdo (AM)
- Administración de adquisición técnica (ATM)
- Verificación de la adquisición (AVER)
- Validación de la verificación (AVAL)

CMMI para desarrollo

- Integración del producto (PI)
- Desarrollo de requerimientos (RD)
- Administración de requerimientos (REQM)
- Administración del acuerdo del proveedor (SAM)
- Solución técnica (TS)
- Validación (VAL)
- Verificación (VER)

CMMI para servicios

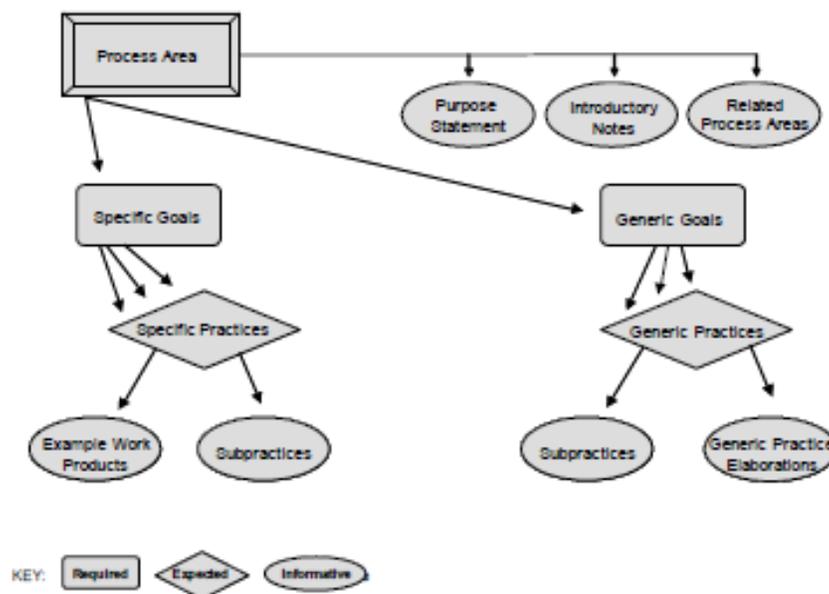
- Administración de la capacidad y disponibilidad (CAM)
- Prevención y solución de incidentes (IRP)
- Administración del contrato del proveedor (SAM)
- Continuidad del servicio (SCON)
- Entrega del servicio (SD)

¹⁶ Véase <http://www.sei.cmu.edu/cmmi/solutions/pas.cfm>, revisado el 5 de febrero 2012, 1:30 hrs; y <http://www.sei.cmu.edu/library/abstracts/webinars/25sep2008.cfm>, revisado el 4 de febrero de 2012, 23:30 hrs.

- Desarrollo del sistema de servicios (SSD)
- Transición del sistema de servicios (SST)
- Administración estratégica del servicio (STSM)

III.1.1.2.1 Componentes del Modelo CMMI

Para entender cabalmente los componentes de este modelo presentamos a continuación el siguiente diagrama:



Si lo que se quiere es implementar cualquiera de los modelos mencionados, se tiene que establecer –antes que nada– niveles. De esta forma podremos identificar la ruta a seguir para satisfacer las necesidades de mejora de los procesos.

El modelo CMMI maneja dos rutas de mejora y utiliza dos representaciones diferentes:

- Representación continua. Permite a las organizaciones mejorar de forma incremental los procesos que corresponden a un área o áreas de proceso individual seleccionadas por la organización. Este

tipo de representación utiliza niveles de capacidad, que se enumeran del 0 al 3, tal y como se muestra a continuación:

Nivel 0	Incompleto
Nivel 1	Realizado
Nivel 2	Administrado
Nivel 3	Definido

- Representación por etapas. Permite a las organizaciones mejorar un conjunto de procesos relacionados, tratando de forma incremental conjuntos sucesivos de áreas de proceso. Este tipo de representación utiliza niveles de madurez, los cuales van del 1 al 5, tal y como se muestra a continuación:

Nivel 1	Inicial
Nivel 2	Administrado
Nivel 3	Definido
Nivel 4	Administrado cuantitativamente
Nivel 5	En optimización

III.1.1.3 SSE-CMM¹⁷

III.1.1.3.1 Antecedentes

La iniciativa SSE-CMM (Systems Security Engineering Capability Model 3.0) dio inicio en 1993 como un esfuerzo de la NSA sobre la búsqueda del trabajo existente sobre Modelos de Madurez de Capacidad (CMM).

¹⁷ Véase <http://www.sse-cmm.org/docs/ssecmmv3final.pdf> pág. 29, Capability-maturity-model-derive-security-requirements_1005[1].pdf, revisado el 9 de febrero de 2012, 12:30hrs; y SSE-CCM.pdf, p. 2, revisado el 9 de febrero de 2012, 13:15 hrs.

Pretendía investigar las necesidades de un modelo de capacidad y madurez especializado para la ingeniería de seguridad.

El SEI de la Universidad Carnegie Mellon –como se menciona al principio del documento— es uno de los creadores de los Modelos de Madurez de Capacidad. El SSE-CMM se desarrolló a partir del Sistema de Ingeniería (SE-CMM), el objetivo era que la ingeniería de seguridad se convirtiera en una disciplina definida, madura y medible.

Cabe destacar que el SSE-CMM es una compilación de mejores prácticas de ingeniería de sistemas. Y uno de sus conceptos rectores plantea que para desempeñar bien una actividad particular, de manera repetible, es imprescindible que ciertos procesos estén siempre presentes, ponderando la importancia de los objetivos de la actividad y de los logros.

III.1.1.3.2 Utilización y estructura

Este modelo se divide en tres áreas básicas,¹⁸ a saber:

- **Riesgo.** Se refiere a la identificación y priorización de los peligros inherentes al producto o servicio desarrollado. Los riesgos son evaluados por la probabilidad de una amenaza, vulnerabilidad y el impacto potencial de un incidente no deseado. En este caso las áreas de procesos incluyen actividades que aseguren que la organización del proveedor esté analizando las amenazas, vulnerabilidades, impactos y riesgos asociados.
- **Ingeniería.** Esta área de proceso trabaja en conjunto con otras disciplinas de la ingeniería para determinar e implementar soluciones a los problemas presentados.
- **Aseguramiento.** Establece el grado de confianza sobre las soluciones de seguridad que se requieren, generando confianza en los clientes.

¹⁸ Estas áreas –que están interconectadas—pueden considerarse de forma separada.

La meta principal de este modelo es separar –de manera clara– las características básicas del proceso de ingeniería de seguridad de las características de administración e institucionalización. Para lograr este cometido se han planteado dos dimensiones: dominio y capacidad.

Ahora bien, un dominio consiste en todas las prácticas que –de manera colectiva– definen la ingeniería de seguridad. Este proceso se conoce como *prácticas base*; existen 129 de estas prácticas, organizadas en 22 áreas de procesos. Además, 61 *prácticas base* están organizadas en 11 áreas de procesos, que cubren las principales áreas de ingeniería de seguridad. A continuación las enlistamos:

- PA01 Administrar los controles de seguridad
- PA02 Evaluar el impacto
- PA03 Evaluar el riesgo de la seguridad
- PA04 Evaluar la amenaza
- PA05 Evaluar la vulnerabilidad
- PA06 Construir el argumento del aseguramiento
- PA07 Coordinar la seguridad
- PA08 Supervisar la postura de seguridad
- PA09 Proveer la entrada de seguridad
- PA10 Especificar las necesidades de seguridad
- PA11 Verificar y validar la seguridad

Las 68 restantes, organizadas en 11 áreas de procesos, están dirigidas a los dominios del proyecto y de la organización. A continuación las enlistamos:

- PA12 Asegurar la calidad
- PA13 Administrar la configuración
- PA14 Administrar el riesgo del proyecto
- PA15 Monitorear y controlar el esfuerzo técnico

- PA16 Planear el esfuerzo técnico
- PA17 Definir el proceso de ingeniería de sistemas de la organización
- PA18 Mejorar el proceso de ingeniería de sistemas de la organización
- PA19 Administrar la evolución de la línea de producción
- PA20 Administrar el ambiente de soporte de la ingeniería de sistemas
- PA21 Proporcionar las habilidades y conocimiento actuales
- PA22 Coordinarse con proveedores

Por su parte, la dimensión de capacidad representa prácticas que indican la capacidad de administración e institucionalización del proceso. Dichas prácticas son conocidas como *prácticas genéricas*, ya que aplican a una amplia gama de dominios, y representan actividades que deben ser desempeñadas como parte de la elaboración de prácticas base. Lo cierto es que las prácticas son actividades que aplican a todos los procesos, y están encaminadas a la administración, medición y aspectos de institucionalización de un proceso. Por lo regular son utilizadas durante una evaluación para determinar la capacidad de una organización en el desempeño de un proceso.

Las prácticas genéricas están agrupadas en áreas lógicas llamadas 'Características Comunes', las cuales, a su vez, se organizan en cinco niveles de capacidad, que miden el aumento de la capacidad organizacional. A diferencia de las prácticas base de la dimensión de dominio, las prácticas genéricas de una dimensión de capacidad están ordenadas con base en la madurez.

De ahí, pues, que las características comunes estén diseñadas para describir cambios importantes en la forma principal de una organización

que esté encaminada a desarrollar procesos de trabajo. La característica que se localiza en el nivel 1 es la menos común.

A continuación se muestran los atributos de madurez de la ingeniería de sistemas, necesarios para alcanzar cada nivel:

Nivel 1

1.1 Las prácticas base son desempeñadas

Nivel 2

2.1 Planeación del desempeño

2.2 Disciplina del desempeño

2.3 Verificación del desempeño

2.4 Monitoreo del desempeño

Nivel 3

3.1 Definir un proceso estándar

3.2 Desempeñar el proceso definido

3.3 Coordinar el proceso

Nivel 4

4.1 Establecimiento de metas de calidad medible

4.2 Administrar objetivamente el desempeño

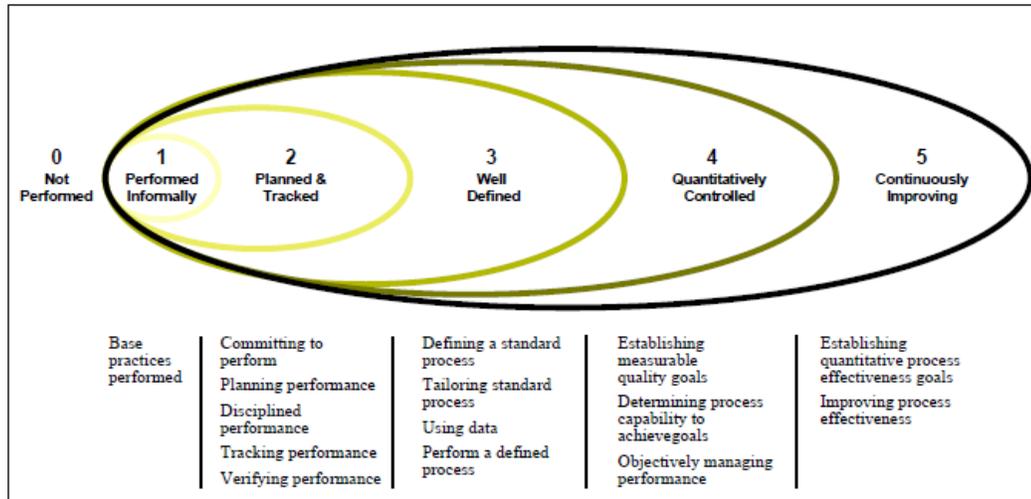
Nivel 5

5.1 Mejorar la capacidad organizacional

5.2 Mejorar la efectividad del proceso

Las características comunes y los niveles de capacidad son importantes para evaluar y mejorar la capacidad de proceso de una organización.

Diagrama de niveles de capacidad¹⁹



Nivel 1. Desempeñado informalmente: las prácticas base del área de proceso son generalmente desempeñadas, pero el desempeño puede no estar rigurosamente planeado ni monitoreado.

Nivel 2. Planeado y monitoreado: el desempeño de las prácticas base están planeadas y monitoreadas y éste es verificado de acuerdo a ciertos procedimientos específicos.

Nivel 3. Bien definidas: las prácticas base son desempeñadas de acuerdo a un proceso bien definido, utilizando procesos documentados y aprobados, y versiones adaptadas de estándares.

Nivel 4. Cuantitativamente controlado: mediciones detalladas de desempeño que son recolectadas y analizadas.

Nivel 5. Mejora continua: las metas cuantitativas de desempeño –para procesar eficacia y eficiencia– son establecidas; este nivel se sustenta en las metas de negocio de una organización.

¹⁹ Véase <http://www.sse-cmm.org/docs/ssecmmv3final.pdf>, pp. 33-44, revisado el 9 de febrero 2012, 18:00 hrs; y SSE-CCM.pdf pp. 8-9, revisado el 12 de febrero de 2012, 20:00 hrs.

III.1.1.4 Modelos que aplican para la protección de datos personales²⁰

La seguridad de la información puede ser concebida, dentro del modelo CMMI de desarrollo y de servicios, como un tipo de requerimiento. Sin embargo, el SSE-CMM en sus 11 áreas de procesos de ingeniería de seguridad lo establece de forma específica.

A continuación presentamos las áreas de proceso:

PA01 Administrar los controles de seguridad

- Prácticas base

BP.01.01 Establecer responsabilidades y rendición de cuentas de los controles de seguridad y comunicarlos a todos en la organización.

BP.01.02 Administrar la configuración de los controles de seguridad del sistema.

BP.01.03 Administrar la conciencia sobre seguridad, capacitación y programas de educación para todos los usuarios y administradores.

BP.01.04 Administrar el mantenimiento periódico y la administración de los servicios de seguridad y mecanismos de control.

PA02 Evaluar el impacto

- Prácticas base

BP.02.01 Identificar, analizar y priorizar las capacidades operacionales, de negocio o de misión categorizadas por el sistema.

BP.02.02 Identificar y definir las características de los activos del sistema que soportan las capacidades clave o los objetivos de seguridad del sistema.

BP.02.03 Seleccionar el impacto métrico a utilizarse para esta valoración.

BP.02.04 Identificar la relación entre las métricas seleccionadas para esta valoración y los factores de conversión métricos si se requieren.

²⁰ Véase <http://www.sse-cmm.org/docs/ssecmmv3final.pdf>, pp. 117-197, revisado el 13 febrero 2012, 20:00hrs; y SSE-CCM.pdf, pp. 2-5, revisado el 13 febrero 2012, 20:00hrs.

BP. 02.05 Identificar y caracterizar los impactos.

BP. 02.06 Monitorear los cambios actuales en los impactos.

PA03 Evaluar el riesgo de la seguridad

- Prácticas base

BP.03.01 Seleccionar los métodos, técnicas y criterios a través de los cuales los riesgos de seguridad para el sistema en un ambiente definido son analizados, valorados y comparados.

BP.03.02 Identificar amenazas/vulnerabilidades/impactos triples (exposiciones)

BP.03.03 Evaluar el riesgo asociado con la ocurrencia a una exposición.

BP.03.04 Evaluar la incertidumbre total asociada con la exposición del riesgo.

BP.03.05 Ordenar los riesgos por prioridad

BP.03.06 Monitorear los cambios actuales en el espectro del riesgo y cambios en sus características.

PA04 Evaluar la amenaza

- Prácticas base

BP.04.01 Identificar las amenazas aplicables provenientes de un recurso natural.

BP.04.02 Identificar las amenazas aplicables provenientes de fuentes artificiales, tanto de manera accidental o deliberada.

BP.04.03 Identificar las unidades de medida apropiadas así como los rangos aplicables en un ambiente específico.

BP.04.04 Evaluar la capacidad y motivación del agente amenaza para eventos de amenaza provenientes de fuentes artificiales.

BP.04.05 Evaluar la probabilidad de ocurrencia de un evento amenaza.

BP.04.06 Monitorear los cambios actuales en el espectro de amenazas y cambios en sus características.

PA05 Evaluar la vulnerabilidad

- Prácticas base

BP.05.01 Seleccionar los métodos, técnicas y criterios a través de los cuales las vulnerabilidades del sistema de seguridad en un ambiente definido sean identificadas y categorizadas.

BP.05.02 Identificar las vulnerabilidades del sistema de seguridad.

BP.05.03 Juntar información relacionada con las propiedades de las vulnerabilidades.

BP.05.04 Evaluar la vulnerabilidad del sistema y agregar vulnerabilidades que sean resultado de vulnerabilidades específicas y combinaciones de éstas.

BP.05.05 Monitorear cambios actuales en las vulnerabilidades aplicables y cambios a sus características.

PA06 Construir el criterio de aseguramiento

- Prácticas base

BP.06.01 Identificar los objetivos de protección de la seguridad.

BP.06.02 Definir una estrategia de seguridad para ocuparse de todos los objetivos de protección.

BP.06.03 Identificar y controlar la evidencia de protección (controles de seguridad).

BP.06.04 Analizar la evidencia de protección (evidencia de seguridad).

BP.06.05 Proveer un argumento de aseguramiento de seguridad que demuestre que las necesidades del cliente son conocidas.

PA07 Coordinar la seguridad

- Prácticas base

BP.07.01 Definir los objetivos de coordinación de ingeniería de seguridad.

BP.07.02 Identificar los mecanismos de coordinación para la ingeniería de seguridad.

BP.07.03 Facilitar la coordinación de la ingeniería de seguridad.

BP.07.04 Utilizar los mecanismos identificados para coordinar decisiones y recomendaciones relacionadas a la seguridad.

PA08 Supervisar el nivel de seguridad

- Prácticas base

BP.08.01 Analizar los registros de eventos para determinar la causa de un evento, cómo procedió y eventos futuros parecidos.

BP.08.02 Monitorear cambios en amenazas, vulnerabilidades, impactos, riesgos y el ambiente.

BP.08.03 Identificar incidentes relevantes de seguridad.

BP.08.04 Monitorear el desempeño y efectividad funcional de controles de seguridad.

BP.08.05 Revisar el nivel de seguridad del sistema para identificar los cambios necesarios.

BP.08.06 Manejar la respuesta de incidentes relevantes de seguridad.

BP.08.07 Asegurar que los dispositivos relacionados con el monitoreo de seguridad sean protegidos adecuadamente.

PA09 Proveer la entrada de seguridad

- Prácticas base

BP. 09.01 Colaborar con diseñadores, desarrolladores y usuarios para asegurar que las partes apropiadas tienen un entendimiento común de las necesidades de entrada de seguridad.

BP.09.02 Determinar las limitaciones y consideraciones de seguridad requeridas para tomar decisiones de ingeniería informadas.

BP.09.03 Identificar soluciones alternativas a la seguridad relacionadas con problemas de ingeniería.

BP.09.04 Analizar y priorizar las alternativas de ingeniería usando limitantes y consideraciones de seguridad.

BP.09.05 Proveer una guía relacionada de seguridad a los otros grupos de ingeniería.

BP.09.06 Proveer una guía relacionada de seguridad a los usuarios y administradores del sistema operacional.

PA10 Especificar las necesidades de seguridad

- Prácticas base

BP.10.01 Obtener un entendimiento de las necesidades de seguridad del cliente.

BP.10.02 Identificar las leyes, políticas, estándares, influencias externas y limitantes que regulan el sistema.

BP.10.03 Identificar el propósito del sistema para determinar el contexto de seguridad.

BP.10.04 Capturar un punto de vista orientado a seguridad de alto nivel de la operación del sistema.

BP.10.05 Capturar metas de alto nivel que definan la seguridad del sistema.

BP.10.06 Definir un conjunto consistente de declaraciones que definan la protección que será implementada en un sistema.

BP.10.07 Obtener el consentimiento de que los requisitos específicos del sistema concuerdan con las necesidades del cliente.

PA11 Verificar y validar la seguridad

- Prácticas base

BP.11.01 Identificar la solución para ser verificada y validada.

BP.11.02 Definir el acercamiento y el nivel de rigor para verificar y validar cada solución.

BP.11.03 Verificar que la solución implementa los requerimientos asociados con el nivel previo de abstracción.

BP.11.04 Validar la solución mostrando que esta satisface las necesidades asociadas con el nivel previo de abstracción, en última instancia satisfaciendo las necesidades de seguridad operativa del cliente.

BP.11.05 Capturar los resultados de verificación y validación para los otros grupos de ingeniería.

III.1.2 COBIT

III.1.2.1 Antecedentes

CobiT quiere decir Control Objectives for Information and Related Technology por sus siglas en inglés, y fue creado en 1992 por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA) y el Instituto de Administración de las Tecnologías de la Información (ITG).

Pero, ¿qué es exactamente CobiT? Se puede decir que es un conjunto de prácticas para mejorar el manejo de la información tanto en la esfera financiera como en la tecnológica. Su función principal consiste en brindarle ayuda a todas aquellas organizaciones que deseen mapear sus procesos informáticos, con base en las mejores prácticas recopiladas por ISACA. De ahí, pues, que CobiT sea implementado regularmente por compañías que realizan auditorías de sistemas de información. Cabe destacar que estas auditorías pueden aplicarse desde un punto de vista financiero o desde un punto de vista de las Tecnologías de Información (TI).²¹

Ciertamente CobiT es un marco de referencia para establecer un rumbo seguro y confiable de las Tecnologías de Información, pero también sirve como una herramienta que da soporte a la Alta Dirección, permitiéndole reducir la brecha existente entre las necesidades de control, las cuestiones técnicas y los riesgos propios de un negocio. Asimismo, CobiT

²¹ Véase Seguridad de la Información en Colombia, Alineando CobiT 4.1, ITIL V3 e ISO 27002 para beneficio del negocio <http://seguridadinformacioncolombia.blogspot.com/search/label/cobit>, revisado el 23 de enero de 2012, 13:00hrs.

ha permitido el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones: enfatiza el cumplimiento normativo, ayuda a éstas a maximizar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de CobiT.²²

La versión de CobiT utilizada hasta los primeros meses de 2012 ha sido la 4,1. Sin embargo, ISACA ha anunciado que lanzará la versión 5 en el segundo trimestre de 2012. Ahora bien, CobiT 5 empleará como plataforma a COBIT 4,1 –ampliando desde luego sus capacidades y bondades— pero estableciendo puentes con otros marcos referenciales importantes, estándares y recursos, por ejemplo, ITIL, ISO, ISF, la OCDE, AICPA y el NIST, e integrando otras guías de ISACA como Val IT, Riesgo TI (Risk IT), el Marco de la Garantía de las TI y el Modelo de Negocio para la Seguridad de la Información (BMIS); todo ello de acuerdo a una imagen que le de cohesión y unidad a la nueva versión CobiT 5. Sin duda, la nueva versión CobiT5 favorecerá a las empresas, logrando una mayor confianza y fiabilidad en sus sistemas de información.²³

III.1.2.2 Utilización y estructura

El principal objetivo de CobiT es ofrecer confianza en los sistemas de información y –valga la redundancia— en la información que éstos generan a la Alta Dirección. Lo cierto es que ayuda a entender cómo dirigir y cómo gestionar el uso de los sistemas de información. Los proveedores de sistemas requieren de un “Código de buenas prácticas”, y no cabe duda que CobiT es una herramienta muy útil para la elaboración de un código de esta naturaleza. En definitiva, CobiT provee de los

²² Véase ISACA, “COBIT Framework for IT Governance and Control”, <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>, revisado el 23 de enero de 2012, 14:30hrs.

²³ Véase ISACA, “ISACA Invites Public Comment on COBIT 5 Exposure Draft” <http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-Invites-Public-Comment-on-COBIT-5-Exposure-Draft.aspx>, revisado el 27 de enero de 2012, 19:00hrs.

instrumentos pertinentes para la supervisión de todas las actividades relacionadas con TI.

Cobit ofrece las siguientes ventajas:

- Este sistema se sustenta en los estándares y las mejores prácticas de la industria informática a nivel mundial. Gracias a su aceptación, CobiT se ha convertido en un marco de referencia en las actividades de TI –al menos en los gobiernos de los países más desarrollados—. Puesto en marcha, CobiT asegura que TI se encuentre debidamente alineado con las metas del negocio y orienta su desarrollo para obtener ventajas competitivas.
- Una de sus bondades es brindar un lenguaje común que abre puertas a los ejecutivos de negocios para comunicar sus metas, objetivos y resultados a los auditores, TI y otros profesionales.
- Adecúa las mejores prácticas y herramientas con el propósito de monitorear y gestionar las actividades de TI. El uso de sistemas por lo regular necesita de una gestión equilibrada, y CobiT cumple con ese objetivo.
- Mediante sus ciclos de vida CobiT apoya a los ejecutivos en el entendimiento de los procesos de gestión y de inversión en TI. Es un sistema que ha desarrollado métodos viables que aseguran las bondades y beneficios que representa las tecnologías de información.

Existe una gran distancia entre las compañías que gestionan adecuadamente sus recursos TI y las que no. De ahí, pues, la importancia de utilizar un sistema como CobiT: por un lado, desarrolla políticas transparentes y buenas prácticas para la gestión de TI; por el otro, su marco referencial maneja los riesgos de gestión inherentes a TI,

permitiendo el cumplimiento, la continuidad, la seguridad y la privacidad que se requieren en el ámbito informático.

El reconocimiento, aceptación e implementación de CobiT –como herramienta de gestión a escala internacional– son, sin duda, una señal de la seriedad que puede tener una organización al hacer uso de él. Ciertamente es un instrumento que ayuda a empresas y profesionales de TI a demostrar su competitividad ante las demás compañías. De la misma manera que encontramos procesos genéricos de muchos tipos de negocios, también encontramos estándares y buenas prácticas en la utilización de TI, que las compañías deben seguir y respetar –sobre todo cuando se sustentan en tecnologías de información–. En pocas palabras, CobiT ofrece un marco de referencia adecuado –con estándares viables y buenas prácticas– para desarrollar una buena gestión organizacional.

Al identificar e implementar los principios relevantes de CobiT, seguramente se conseguirá una gestión exitosa de los recursos de sistemas. Así pues, los resultados serán sumamente positivos para toda organización enfocada en TI.

A continuación enlistamos algunos de los beneficios más importantes en la implementación de CobiT en TI:

- Transparencia y certidumbre en el ciclo de vida de costos de TI.
- TI entregará información de calidad, en menor tiempo.
- TI brindará servicios de calidad, por lo tanto, los proyectos apoyados en TI serán exitosos.
- Los requerimientos de seguridad y privacidad serán identificados fácilmente, por lo tanto, el monitoreo del sistema y sus resultados será igualmente sencillo.
- Los riesgos inherentes a TI serán gestionados con mayor efectividad.

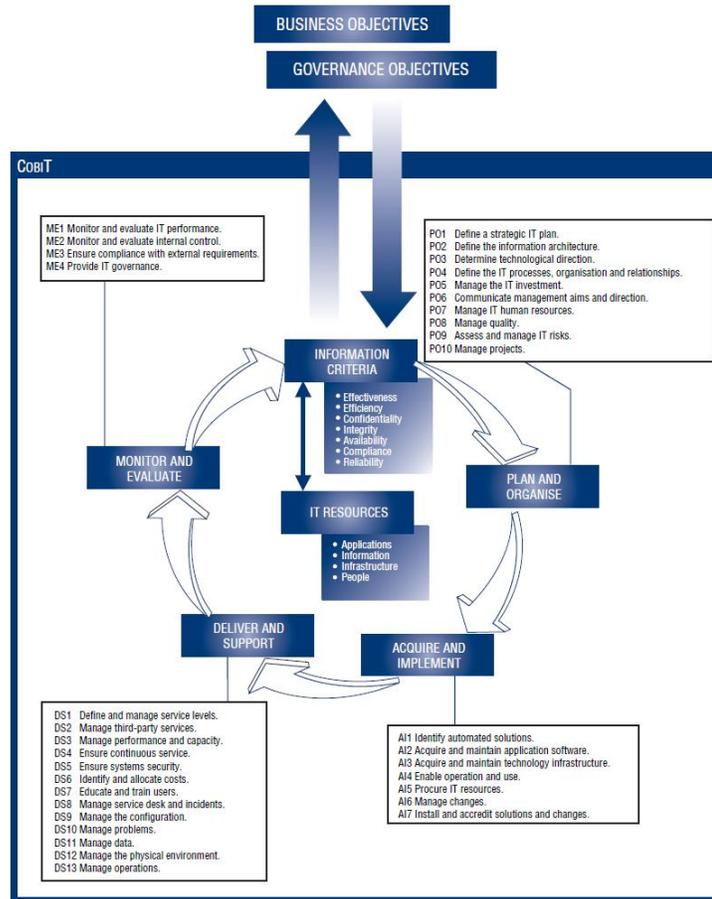
- El cumplimiento de regulaciones implícitas a TI serán una práctica normal dentro de su gestión.

Es importante denotar que el marco de referencia CobiT en su versión 4 (hasta julio de 2010) incluye lo siguiente:²⁴

- Marco de referencia: esclarece el método de organización de CobiT para la gestión de TI; de tal suerte que señala los objetivos de control y buenas prácticas del negocio por dominios y procesos de TI, vinculándolos directamente con los requerimientos del negocio. Este marco de referencia contiene un total de 34 niveles de objetivos de control, uno por cada proceso de TI, agrupados en cuatro dominios: Planeamiento y Organización, Adquisición e Implementación, Desarrollo y Soporte, y Monitoreo y Evaluación.
- Descripción de procesos: abarca todas las áreas y responsabilidades de TI –de principio a fin—, incluyendo a cada uno de los 34 procesos de TI.
- Objetivos de control: provee objetivos de gestión sustentados en las mejores prácticas para los procesos de TI.
- Directrices de gestión: incluye herramientas que ayudan en la asignación de responsabilidades. Además, mide desempeños.
- Modelos de madurez: proporciona perfiles de los procesos de TI, describiendo para cada uno de ellos un estado actual y uno futuro.

²⁴ Véase Seguridad de la Información en Colombia, Alineando CobiT 4.1, ITIL V3 e ISO 27002 para beneficio del negocio <http://seguridadinformacioncolombia.blogspot.com/search/label/cobit>, revisado el 23 de enero de 2012, 13:00hrs.

Diagrama de la Estructura de CobiT 4.1²⁵



III.1.2.3 Dominios y Objetivos de control que aplican para la protección de datos personales de acuerdo a CobiT 4.1²⁶

- Dominio: Planear y Organizar (PO)
 - PO1. Definir un Plan Estratégico de Tecnología de Información
 - Identificar los riesgos de TI asociados a la información

²⁵ Idem.

²⁶ Fuente: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/02-CobiTPromotorSeguridadInformacionHaciaGobiernoTI.pdf, revisado el 20 de enero de 2012, 14:00hrs.

- PO2. Definir la Arquitectura de la Información
 - Establecer Dueños de la información
 - Clasificar la información con base en: Sensibilidad / Confidencialidad, Criticidad / Disponibilidad
 - Administrar la integridad de la información
- PO4. Definir los Procesos de TI, su Organización y sus Relaciones
 - Identificar responsabilidades con base en: Riesgos, Seguridad y Cumplimiento
- PO9. Analizar y Administrar los Riesgos
 - Análisis de riesgos
 - Identificación de vulnerabilidades y amenazas
 - Manejo del riesgo: Mitigar, Evitar, Compartir y Aceptar
 - Mantenimiento y monitoreo
- Dominio: Adquirir e Implementar (AI)
 - AI2. Adquirir y Mantener Software de Aplicación
 - AI3. Adquirir y Mantener la Arquitectura Tecnológica
 - AI4. Facilitar la Operación y el Uso
 - Trasferir el conocimiento a todos los niveles de la organización
 - AI5. Proveer los Recursos de TI
 - Acuerdos de confidencialidad
 - Responsabilidad sobre la seguridad y la propiedad intelectual
 - AI6. Administrar los Cambios
 - Procedimientos para los cambios
 - Análisis de impacto, priorización y autorización

- Cambios de emergencia
- AI7. Instalar y Acreditar Soluciones y Cambios
 - Plan y ambiente de pruebas
 - Conversión de datos y sistemas
 - Puesta en marcha
- Dominio: Entregar y Soportar (DS)
 - DS1. Definir y Administrar los Niveles de Servicio
 - Acuerdos de Nivel de Servicio: Disponibilidad, Seguridad y Confiabilidad
 - DS2. Administrar Servicios Administrados por Terceros
 - Administrar los riesgos de los proveedores
 - DS3. Administrar el Desempeño y la Capacidad
 - Disponibilidad de los recursos de TI
 - DS4. Asegurar el Servicio Continuo
 - Identificación de recursos críticos de TI
 - Desarrollo, implementación y pruebas del plan de continuidad
 - Recuperación y reinicio de las operaciones
 - DS5. Garantizar la Seguridad de los Sistemas
 - Administración de la seguridad de TI
 - Planeación de seguridad de TI
 - Administración de identidad
 - Administración de usuarios
 - Prueba y monitoreo a la seguridad
 - Definición de incidentes de seguridad
 - Protección de las tecnologías de seguridad
 - Seguridad en la red
 - Intercambio de datos sensitivos
 - DS8. Administrar la Mesa de Servicio y los Incidentes
 - DS9. Administrar la Configuración

- DS10. Administrar Problemas
 - Identificar y administrar los problemas
 - Seguimiento y solución de los problemas
 - Integración de la administración de incidentes, configuración y problemas
- DS11. Administrar los Datos
 - Sistemas de administración de medios
 - Definición de sistemas de almacenamiento, respaldos y recuperación
 - Definición de periodos y acuerdos de retención de datos
 - Acuerdos y procedimientos de destrucción de datos
 - Requerimientos de seguridad para la administración de datos
- DS12. Administrar el Ambiente Físico
 - Planos y selección del sitio
 - Medidas de seguridad física
 - Acceso físico
 - Protección contra factores ambientales
- DS13. Administrar las Operaciones
 - Monitoreo de la Infraestructura de TI
 - Documentos sensitivos y dispositivos de salida
 - Mantenimiento Preventivo
- Dominio: Monitorear y Evaluar (ME)²⁷
 - ME1. Monitorear y Evaluar el Desempeño de TI
 - ME2. Monitorear y Evaluar el Control Interno
 - ME3. Asegurar el Cumplimiento con Requerimientos Externos
 - ME4. Proporcionar Gobierno de TI

²⁷ Los objetivos de control relativos a este dominio revisan la efectividad de los controles de seguridad que permiten la autorregulación y la vigilancia del cumplimiento de regulaciones externas, así como contar con un esquema corporativo de gobierno de TI sobre el control y la seguridad de la información.

III.1.3 ISO 27001

III.1.3.1 Antecedentes

ISO/IEC 27001 es un estándar internacional de gestión de seguridad de la información que permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad de la información en un nivel adecuado para la propia organización. El objeto principal es proteger la información para que no caiga en manos incorrectas o se pierda para siempre.²⁸ Cabe señalar que el parámetro de protección se establece con base en un nivel aceptable de riesgo en las operaciones del negocio.

Este ISO se publicó el 15 de octubre de 2005 y es la norma principal de la serie, pues contiene los requisitos del sistema de gestión de seguridad de la información (SGSI). Su origen se remonta a la BS 7799-2:2002, que ya quedó anulada. Ahora bien, es la norma a través de la cual se certifican – por auditores externos– los Sistemas de Gestión de Sistemas de Información de las organizaciones. En su Anexo A enumera –en forma de resumen– los objetivos de control y los controles que desarrolla la ISO 27002:2005, con la finalidad de que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. Lo cierto es que no es obligatoria la implementación de todos los controles enumerados en dicho anexo, sin embargo, una organización deberá argumentar sólidamente la no aplicabilidad de los controles no utilizados.²⁹

III.1.3.2 Utilización y estructura

El ISO/IEC 27000 es un conjunto de estándares desarrollados –o en fase de desarrollo– por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un

²⁸ Véase http://www.bureauveritas.com.pe/Home2/Our-Services/Certification/iso_27001.pdf, Revisado el 31 de enero de 2012, 13:30hrs.

²⁹ Véase <http://www.iso27000.es/iso27000.html>, revisado el 31 de enero de 2012, 13:30hrs.

marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, ya sea pública o privada, grande o pequeña.

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001. Asimismo, ISO continúa desarrollando otras normas dentro de la serie 27000 que sirven de apoyo a las organizaciones en la interpretación e implementación de la ISO/IEC 27001. Desde luego esta última es la norma principal y única certificable dentro de la serie.

Para entender cabalmente la utilización y estructura de la ISO/IEC 27000 es necesario reseñar cada una de las ISOs:

ISO/IEC 27003

Se publicó el 1 de febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

ISO/IEC 27004

Se publicó el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

ISO/IEC 27006

Se publicó –en segunda edición– el 1 de diciembre de 2011 (la primera edición salió a la luz el 1 de marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (requisitos para la acreditación de entidades que operan certificación/registro de SGSIs), que añade a ISO/IEC 17021 (requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

ISO/IEC 27007

Se publicó el 14 de noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

ISO/IEC TR 27008

Se publicó el 15 de octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

ISO/IEC 27010

En fase de desarrollo, se contempla su publicación en 2012. Es una norma en dos partes, que consistirá en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores.

ISO/IEC 27011

Se publicó el 15 de diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones, basada en ISO/IEC 27002. Está publicada también como norma ITU-T X.1051.

ISO/IEC 27013

En fase de desarrollo, se contempla su publicación en 2012. Consistirá en una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

ISO/IEC 27014

En fase de desarrollo, se contempla su publicación en 2012. Consistirá en una guía de gobierno corporativo de la seguridad de la información.

ISO/IEC 27015

En fase de desarrollo, se contempla su publicación en 2013. Consistirá en una guía de SGSI para organizaciones del sector financiero y de seguros.

ISO/IEC TR 27016

En fase de desarrollo, se contempla su publicación en 2013. Consistirá en una guía de valoración de los aspectos financieros de la seguridad de la información.

ISO/IEC 27017

En fase de desarrollo, se contempla su publicación en 2013. Consistirá en una guía de seguridad para Cloud Computing.

ISO/IEC 27031

Se publicó el 1 de Marzo de 2011. No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777.

ISO/IEC 27032

En fase de desarrollo, se contempla su publicación en 2012. Consistirá en una guía relativa a la ciberseguridad.

ISO/IEC 27033

Parcialmente desarrollada. Norma dedicada a la seguridad en redes, que se compone de siete partes: 27033-1, conceptos generales (publicada el 15 de diciembre de 2009); 27033-2, directrices de diseño e implementación de seguridad en redes (prevista para 2012); 27033-3, escenarios de referencia de redes (publicada el 3 de diciembre de 2010); 27033-4, aseguramiento de las comunicaciones entre redes mediante *gateways* de seguridad (prevista para 2012); 27033-5, aseguramiento de comunicaciones mediante VPNs (prevista para 2013); 27033-6, convergencia IP (prevista para 2013); y 27033-7, redes inalámbricas (prevista para 2013).

ISO/IEC 27034

Parcialmente desarrollada. Norma dedicada a la seguridad en aplicaciones informáticas, que se compone de cinco partes: 27034-1, conceptos generales (publicada el 21 de noviembre de 2011); 27034-2, marco normativo de la organización (prevista para 2013); 27034-3, proceso de gestión de seguridad en aplicaciones (prevista para 2013); 27034-4, validación de la seguridad en aplicaciones (prevista para 2013); 27034-5, estructura de datos de protocolos y controles de seguridad de aplicaciones (prevista para 2013).

ISO/IEC 27035

Se publicó el 17 de agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información.

ISO/IEC 27036

En fase de desarrollo, se contempla su publicación en 2013. Consistirá en una guía en cuatro partes de seguridad en las relaciones con los proveedores: 27036-1, visión general y conceptos; 27036-2, requisitos comunes; 27036-3, seguridad en la cadena de suministro TIC; 27036-4, seguridad en *outsourcing* (externalización de servicios).

ISO/IEC 27037

En fase de desarrollo, se contempla su publicación en 2012. Consistirá en una guía de identificación, recopilación y custodia de evidencias digitales.

ISO/IEC 27038

En fase de desarrollo, se contempla su publicación en 2013. Consistirá en una guía de especificación para seguridad en la redacción digital.

ISO/IEC 27039

En fase de desarrollo, se contempla su publicación en 2013. Consistirá en una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).

ISO/IEC 27040

En fase de desarrollo, se contempla su publicación en 2014. Consistirá en una guía para la seguridad en medios de almacenamiento.

ISO 27799

Se publicó el 12 de junio de 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002; todo ello en relación a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

ISO 27001:2005



Diagrama de dominios³⁰

III.1.3.3 Sistema de Gestión de la Seguridad de la Información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. En consecuencia, la gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por lo tanto, garantizar que los riesgos de la seguridad de la información sean

³⁰ Véase http://www.tcps.com/vermas/iso_27001.htm, revisado el 9 de febrero de 2012, 12:00hrs.

conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente, medible y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En las siguientes secciones se desarrollarán los conceptos fundamentales de un SGSI según la norma ISO 27001.

El Anexo A contiene los dominios descritos a continuación:

- A.5 Política de seguridad
- A.6 Organización de la seguridad de la información
- A.7 Gestión de activos
- A.8 Seguridad relacionada con el personal
- A.9 Seguridad física y del entorno
- A.10 Gestión de comunicaciones y operaciones
- A.11 Control de acceso
- A.12 Adquisición, desarrollo y mantenimiento de los sistemas de la información
- A.13 Gestión de los incidentes de seguridad de la información
- A.14 Gestión de la continuidad del negocio
- A.15 Cumplimiento

A.5 Política de seguridad

Este grupo está constituido por dos controles y es justamente el primer caso que se puede poner de manifiesto sobre el mencionado "desconcepto" sobre lo que uno piensa que es un control. En efecto, aquí se puede apreciar claramente la complejidad que representa el diseño, planificación, preparación, implementación y revisiones de una Política de Seguridad.

La Política de Seguridad se divide en dos documentos:

a) Política de seguridad (nivel político o estratégico de la organización). Es la mayor línea rectora, la alta dirección. Define las grandes líneas a seguir y el nivel de compromiso de la dirección con ellas.

b) Plan de Seguridad (nivel de planeamiento o táctico). Define el "cómo". Es decir, baja a un nivel más de detalle, para dar inicio al conjunto de acciones o líneas rectoras que se deberán cumplir.

Dichos documentos han servido como base metodológica en el desarrollo de los SGSI. En realidad se trata de lo que proponen los RFCs (Request For Comments), o sea, Política de Seguridad RFC - 2196 Site Security Handbook y también la anterior RFC-1244 (que si bien queda obsoleta por la primera, es muy ilustrativa). Ambas plantean una metodología muy eficiente de retroalimentación, que parte desde el nivel más alto de una organización hasta llegar al nivel de detalle. Gracias a ello se puede comparar las decisiones tomadas y reingresar las conclusiones al sistema, evaluando los resultados y modificando las deficiencias. Se trata de un ciclo permanente y sin fin, cuya característica fundamental es la constancia y la actualización de conocimientos.

Este dominio propone los siguientes pasos:

- La política es el marco estratégico de la organización, en otras palabras, es el más alto nivel. El análisis de riesgo y el grado de exposición determinan el impacto que puede producir los distintos niveles de clasificación de la información que se posee. Una vez que se han determinado estos conceptos, se pasa al 'cómo', esto es, al Plan de Seguridad. Y este último –si bien no está directamente relacionado con las normas ISO en la RFC– se ha considerado por la similitud que tiene en la elaboración de procedimientos de detalle para cada actividad que se implementa y por su excelente metodología.

- Una “Política de Seguridad” bien planteada, diseñada y desarrollada cubre la gran mayoría de los aspectos que hacen falta para un verdadero SGSI.

A.6 Organización de la seguridad de la información

Este grupo abarca once controles y se subdivide de la manera siguiente:

-Organización Interna. Compromiso de la Dirección, coordinaciones, responsabilidades, autorizaciones, acuerdos de confidencialidad, contactos con autoridades y grupos de interés en temas de seguridad y revisiones independientes.

- Partes externas. Riesgos relacionados con terceros, gobierno de la seguridad respecto a clientes y socios de negocio. Ahora bien, lo más importante de este subgrupo es lo siguiente:

a) Organizar y mantener actualizada la cadena de contactos (internos y externos), con el mayor detalle posible (personas, responsabilidades, activos, necesidades, acuerdos, riesgos, etc.).

b) Derechos y obligaciones de cualquiera de los involucrados.

Lo más conveniente es diseñar e implementar una base de datos, que permita –de forma amigable– el alta, baja y/o modificación de cualquiera de estos campos. Enseguida debe redactarse la documentación inicial de responsables: derechos y obligaciones (para el personal tanto interno como ajeno) y el conjunto de medidas a adoptar con cada uno de ellos. Una vez hecho esto se debe documentar la metodología de actualización, auditabilidad y periodicidad de los informes referidos.

A.7 Gestión de activos

Este grupo cubre cinco controles y se encuentra subdividido de la siguiente manera:

- Responsabilidad en los recursos. Inventario y propietario de los recursos, empleo aceptable de los mismos.

- Clasificación de la información. Guías de clasificación y denominación, identificación y tratamiento de la información.

Este grupo es eminentemente procedimental y no aporta nada nuevo al ámbito ya conocido en seguridad de la información: todo recurso deberá estar perfectamente inventariado con el máximo detalle posible; se deberá documentar el “uso adecuado de los recursos”; y toda la información deberá ser tratada de acuerdo a su nivel.

Vale la pena mencionar que el problema que aqueja a la mayoría de las empresas –con un parque informático considerable– es la actualización de su sistema de inventario. A su vez, esto dificulta la asignación de la “propiedad” de los recursos que apoyan el proceso de negocio. Lo cierto es que este aspecto debe abordarse “sí o sí”, pues es imposible pensar en seguridad, si no se sabe fehacientemente lo que se posee y si no se conoce cada elemento que queda desactualizado o aún no ha sido inventariado.

No cabe duda que las mejores metodologías son las que permiten conservar vigente el estado de la red, de manera que podamos inventariar lo que se “escucha”. Así pues, se hace un empleo lógico y completo de los elementos de red o seguridad (IDSs, firewalls, routers, sniffers, etc.), aprovechando la actividad cotidiana de escucha y tratamiento de tramas para mantener “vivo” el estado de la red. En pocas palabras, se podrá saber cuáles direcciones de la “Home Net” se encuentran activas y cuáles no. Se aprovecha esta funcionalidad para

almacenar y enviar datos a un repositorio adecuado, el cual será el responsable de mantener el inventario actualizado.³¹

Este grupo de objetivos de control puede ser alineado con los esfuerzos de la organización sobre la creación y mantenimiento de una “base de datos de cambios y configuración” (CCMDB por sus siglas en inglés), dentro de las iniciativas de gestión de servicios informáticos.

A.8 Seguridad relacionada con el personal

Este grupo cubre nueve controles y se encuentra subdividido de la siguiente forma:

- Antes del empleo. Responsabilidades y roles, verificaciones curriculares, términos y condiciones de empleo.
- Durante el empleo. Administración de responsabilidades, preparación, educación y entrenamiento en seguridad de la información, medidas disciplinarias.
- Finalización o cambio de empleo. Finalización de responsabilidades, devolución de recursos y revocación de derechos.

Actualmente este grupo debe ser el gran ausente en la mayoría de las organizaciones. Se trata de un serio trabajo a realizar entre RRHH y los responsables de Seguridad de la Información de la organización.

El punto de partida es la redacción de la documentación necesaria para la contratación de personal y la revocación de sus contratos (por solicitud, cambio o despido). Antes bien, deberán quedar claras las acciones a seguir para los diferentes perfiles de la organización; todo ello de acuerdo a la responsabilidad de manejo de la información que tenga un puesto determinado. Como se pueda apreciar, tanto la contratación como el cese

³¹ Sobre este tema, se propone la lectura de dos artículos publicados hace tiempo en Internet que se denominan “Metodología Nessus-Snort” y “Matriz de Estado de Seguridad”, si bien los mismos deben ser actualizados al día de hoy, de ellos se puede obtener una clara imagen de cómo se puede realizar esta tarea y aprovechar las acciones de seguridad para mejorar el análisis de riesgo y el inventario.

de un puesto son actividades propias de esta área. Y cada paso deberá ser coordinado según la documentación confeccionada –así no se pasará por alto ningún detalle—, pues son justamente estas pequeñas omisiones las que generan una alta dependencia técnica de personas con un perfil peligroso para la organización; o se dan casos de personas que, al tiempo de haberse ido, mantienen accesos o permisos que no se debieran ser, provocando fuga de información.

A.9 Seguridad física y del entorno

Este grupo cubre trece controles y se encuentra subdividido de la siguiente manera:

- Áreas de seguridad. Seguridad física y perimetral; control físico de entradas; seguridad de locales, edificios y recursos; protección contra amenazas externas y del entorno; seguridad en áreas de trabajo, acceso público, y de entrega y carga.

- Seguridad de elementos. Ubicación y protección de equipos y elementos de soporte a los equipos; seguridad en el cableado y mantenimiento de equipos; seguridad en el equipamiento fuera de la organización; seguridad en la redistribución o reutilización de equipamiento, borrado de información y/o software.

Uno de los mejores resultados que se pueden obtener en la organización de una infraestructura de seguridad de la información, está en estructurarla con base en niveles. Tal vez no sea necesario hacerlo con el detalle de los siete niveles del modelo ISO/OSI, pero sí por lo menos de acuerdo al modelo TCP/IP que algunos consideran de cuatro niveles (integrando, cuando se puede, el ámbito físico con el de enlace) y otros de cinco niveles.

Sin duda, es correcto considerar separadamente el nivel físico con el de enlace, pues presentan vulnerabilidades muy diferentes. Ahora bien, si se presenta el modelo de cinco niveles, es posible organizar una estructura de seguridad que contemple medidas y acciones por cada nivel.

A.10 Gestión de comunicaciones y operaciones

Este grupo trata de asegurar que la explotación de la infraestructura se realice de forma segura y controlada, se supervise su estado y se reporten las incidencias. Para ello, define varios objetivos de control: procedimientos y responsabilidades operacionales; gestión de servicios de terceros; planificación y aceptación de sistemas; protección contra códigos maliciosos; copias de seguridad; gestión de la seguridad de red; gestión de dispositivos de almacenamiento; control sobre el intercambio de información entre sociedades; control de los servicios de comercio electrónico; y monitorización de sistemas.

Este dominio detalla más controles técnicos que organizativos respecto a dominios anteriores. Las garantías que brinda son disponibilidad, confidencialidad, integridad y conservación de la información.

Con su implementación se establecerán responsabilidades y procedimientos para la gestión y operación de todos los medios de tratamiento de información. Esto incluye la elaboración de instrucciones apropiadas de operación y procedimientos de respuesta ante incidencias. Cuando sea adecuado, se activará un sistema de segregación de tareas, de tal suerte que se reduzca el riesgo de un mal uso de la infraestructura –deliberado o por negligencia—. Además, tomará prevenciones para detectar la introducción de algún software dañino.

En este orden de ideas debe señalarse que el software propio y los recursos de tratamiento de información son vulnerables a la introducción de algún software dañino como virus informáticos, gusanos de la red,

caballos de Troya y bombas lógicas. Los usuarios deben conocer los peligros que tiene el software dañino o no autorizado, y se deberán implantar controles y medidas especiales para detectar o evitar su introducción en puestos de trabajo. En particular es esencial que se tomen precauciones para detectar o evitar los virus informáticos en los ordenadores personales. Se establecerán procedimientos rutinarios hasta conseguir una estrategia viable que respalde la información, por ejemplo, haciendo copias de respaldo, ensayando su oportuna restauración, registrando eventos o fallos, y monitorizando el entorno de los equipos cuando proceda.

La gestión de seguridad en las redes que incide en la Administración requiere sin duda de una atención especial. La estrategia de seguridad debe concretarse mediante controles y medidas adicionales que protejan los datos sensibles que circulan por las redes públicas. Lo cierto es que deben establecerse los controles necesarios de tal suerte que se impida la suplantación del emisor, modificación o pérdida de la información transmitida, tanto en las comunicaciones con sistemas situados en las redes internas, como con aquellos sistemas externos. Este mecanismo debe ser independiente de las plataformas, protocolo o aplicaciones que las soporten. Así pues, se establecerán los procedimientos adecuados para proteger los documentos, soportes informáticos (discos, cintas, etc.), datos de entrada o salida, y documentación del sistema frente a daño, robo y acceso no autorizado.

A.11 Control de acceso

Este dominio cubre uno de los aspectos más importantes y evidentes respecto a la seguridad: la problemática del control de acceso a los sistemas de información. Para ello plantea los siguientes objetivos de control: requisitos del negocio para el control de acceso, gestión de los accesos de los usuarios, responsabilidades del usuario, control de acceso

de red, control de acceso del sistema operativo, control de acceso a las aplicaciones y a la información y teletrabajo, y movilidad en el ámbito de la Administración. Las garantías que cubre este dominio son autenticidad y confidencialidad y, además, es el control base que asegura una buena trazabilidad. De ahí, pues, que los permisos de acceso a las redes, a los sistemas y a la información se otorguen con ciertos candados, pues los usuarios deben acceder únicamente a los recursos e información necesarios para el desempeño de sus funciones.

Más aún, este dominio contempla el establecimiento de procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios. Dichos procedimientos pueden cubrir todas las etapas del ciclo de vida del acceso a usuarios, desde el registro inicial de usuarios hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios. Muchas veces encontramos que no hay un verdadero control de acceso y manejo de la información. En consecuencia, deberá ponerse mayor atención al control de la asignación de derechos de acceso privilegiado.

Todos los accesos realizados a las aplicaciones informáticas que sirven de soporte a la tramitación telemática por los usuarios registrados llevarán asociado un proceso de identificación, autenticación y autorización. Se establecerán mecanismos de registro, monitorización de acceso y uso de los sistemas. Las credenciales de acceso de cada usuario serán personales e intransferibles. Toda persona registrada que disponga de credenciales de acceso será responsable de mantener su confidencialidad y asegurar su correcto uso. Se establecerán los mecanismos necesarios en los sistemas para impedir la visualización de las credenciales por parte de terceras personas.

Ahora bien, considerando que una protección efectiva necesita la cooperación de los usuarios autorizados, los usuarios deberán ser

conscientes de sus responsabilidades en el mantenimiento de la efectividad de las medidas de control de acceso, en particular las que se refieren al uso de contraseñas y a la seguridad del material puesto a su disposición.

Es evidente que el acceso a los servicios –ya sea a través de redes externas o internas– deberá controlarse, de modo tal, que se asegure que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios. En este tenor se desprenden algunas directrices en los mecanismos y controles del dominio:

- Mecanismos adecuados de autenticación para los usuarios y los equipos.
- Control de los accesos de los usuarios a los servicios de información. El acceso remoto a las aplicaciones informáticas que sirven de soporte a la tramitación telemática desde redes públicas, debe garantizar la confidencialidad de la información que se transmite, así como la identidad de los usuarios autorizados a hacer uso del servicio de acceso remoto mediante mecanismos de autenticación fuerte.

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de la información

Este dominio pretende garantizar que la seguridad se integre en los sistemas de información desde su desarrollo. Para ello ha establecido varios objetivos de control: requisitos de seguridad que afectan a los sistemas de información (sean adquiridos o desarrollados), correcto procesamiento de las aplicaciones, controles criptográficos, seguridad en los sistemas de ficheros, seguridad en los procesos de desarrollo, y soporte y gestión de vulnerabilidades técnicas. En pocas palabras trata de cubrir las garantías de disponibilidad, confidencialidad e integridad.

Así pues, los proyectos de desarrollo que se inicien en la Administración y afecten directamente a las aplicaciones informáticas que sirven de soporte a los procesos del negocio, tendrán que llevarse a cabo considerando *requisitos específicos de seguridad durante todo su ciclo de vida*. El desarrollo y mantenimiento de las aplicaciones dentro del ámbito especificado, deberá incluir los controles y registros apropiados que garanticen la correcta implementación de las especificaciones de seguridad. Para lograrlo se tendrá que considerar las mejores prácticas de seguridad en la programación.

Es sustancial señalar que cuando ciertas medidas y controles no proporcionen la protección adecuada, se usarán sistemas y técnicas criptográficas –cifrado, firma digital, no-repudio– para proteger la información sometida a riesgo.

La información residente en las aplicaciones informáticas que sirven de soporte a los procesos del negocio, debe protegerse contra modificaciones no autorizadas, empleando mecanismos que aseguren la integridad de la misma (relacionada con el control de acceso).

Definitivamente es muy importante proveer de las guías, estándares, recomendaciones y procedimientos necesarios para facilitar la inclusión de la seguridad durante las etapas del ciclo de vida de desarrollo, por ejemplo, con el uso de controles criptográficos, gestión de claves, programación segura, etc. Los entornos que forman parte del ciclo de vida de desarrollo informático, tienen que separarse o segmentarse en todos y cada uno de los sistemas. Asimismo, y con la finalidad de evitar el acceso o divulgación de datos que residan en los entornos, es importante controlar el intercambio de datos reales entre el entorno de producción y el resto de éstos. Lo cierto es que en los entornos de pruebas, infraestructura o desarrollo para aplicaciones, se requiere de juegos de datos de prueba, que estén disponibles y preparados específicamente, de

tal manera que las relaciones entre datos y personas se puedan disociar o enmascarar.

A.13 Gestión de los incidentes de seguridad de la información

Este dominio trata de garantizar que los eventos y debilidades en la seguridad, asociados a la TI y las aplicaciones soporte de la e-Administración, sean comunicados y difundidos. De esta manera se podrán realizar las acciones correctivas de forma oportuna y correcta, dirigiéndose principalmente a cubrir las garantías de disponibilidad, confidencialidad e integridad.

Conlleva la exigencia de informar con la mayor celeridad posible (ante cualquier debilidad que se observe o se sospeche). Para cumplir este objetivo hay que establecer los procedimientos y cauces adecuados (canales de gestión conocidos).³²

Para ello, se requiere de la aplicación de una metodología sólida en la gestión de incidentes de seguridad (establecer responsabilidades y procedimientos) y el empleo de procesos y técnicas para la recolección de evidencias. Cabe señalar que este dominio pondera mecanismos que permiten la monitorización de las incidencias de seguridad, cuantificación y costos asociados de las mismas, así como la recopilación de evidencias.

Ante todo, es fundamental establecer procedimientos formales para informar y priorizar eventos de seguridad. Todo el personal afectado deberá conocer los procedimientos para informar de los diferentes tipos de eventos y debilidades que pudieran impactar en la seguridad de las aplicaciones informáticas, que sirven de soporte a la tramitación telemática. Con base en lo anterior, se estructurarán responsabilidades y procedimientos formales para manejar los eventos de seguridad y

³² Este punto está ligado con el apartado 8.4 (sobre la seguridad ligada a recursos humanos), que se refiere específicamente a la concienciación, formación y capacitación en seguridad de la información.

debilidad de forma expedita y eficaz; se establecerá un proceso formal de mejora continua sobre toda la gestión de incidentes de seguridad; y se recopilarán las evidencias necesarias de cada incidente, cumpliendo en todo momento con la legalidad vigente.

A.14 Gestión de la continuidad del negocio

Este dominio trata de asegurar la disponibilidad de la TI que soporta las aplicaciones del negocio en caso de una interrupción no planeada y no tolerable. El objetivo es establecer un plan de acción para minimizar los efectos de esta interrupción (desastre). Las garantías que este dominio cubre son la integridad, la disponibilidad y la conservación de la información, reduciendo el tiempo de no disponibilidad a niveles aceptables. Todo ello desde el punto de vista de la actividad del dueño del proceso de negocio que es soportado por la TI afectada. De ahí que sea necesaria una combinación de controles de carácter organizativo, tecnológico y procedimental, tanto preventivos como de recuperación.

A.15 Cumplimiento

El objetivo de este dominio es evitar el incumplimiento en la esfera legal, por ejemplo, en algún cuerpo de leyes, obligaciones estatutarias, reglamentarias o contractuales o en cualquier requisito de seguridad. En efecto, el diseño, el uso, la operación y la gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad estatutarios, reglamentarios y contractuales y, por lo tanto, deberá asegurarse que los sistemas cumplan con las normas y políticas de seguridad de la organización.³³

³³ <http://seguridadinformacioncolombia.blogspot.com/2010/05/iso-27001-e-iso-27002-dominio-15.html>, revisado el 2 febrero de 2012, 13:27hrs.

III.1.3.4 Otros estándares

Las normas publicadas bajo la serie ISO 27000 son estándares alineados con el conjunto de normas publicadas por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), ya sean actuales o futuras, y que son desarrolladas mediante comités técnicos específicos.

Aquellas organizaciones que estén empleando algún estándar o conjunto de buenas prácticas en seguridad de la información, pero con modelos de gestión diferentes a éste, obtendrán el beneficio de una adaptación y certificación en la norma ISO 27001 con un menor esfuerzo.

En relación a la seguridad de la información, gestión del riesgo, continuidad de negocio y materias relacionadas, se incluye a continuación una selección de los estándares y métodos de referencia más conocidos y relevantes.

ISO / IEC 27005:2011

Recientemente se publicó ISO / IEC 27005:2011. Norma que proporciona un marco para la implementación de un enfoque de gestión de riesgos para la gestión de amenazas a los sistemas de gestión de seguridad.

No cabe duda que los riesgos de seguridad de la información representan una amenaza considerable para las empresas. Esto ha sido así si se considera la posibilidad de pérdida financiera, pérdida de los servicios de redes esenciales, o pérdida de reputación y confianza de los clientes. La gestión de riesgos es uno de los elementos clave en la prevención del fraude online, robo de identidad, daños a los sitios web,

pérdida de datos personales y muchos otros incidentes de seguridad informática.

Es una norma esencial para aquellos que quieran gestionar sus riesgos de manera efectiva y, en particular, para cumplir con la gestión de la información de seguridad popular mediante el sistema estándar ISO / IEC 27001. La gestión de riesgos es fundamental para la dirección de cualquier negocio. Y esta norma ayuda aconsejando y asesorando a las organizaciones sobre el por qué, qué y el cómo de la gestión de riesgos de seguridad de la información. La finalidad es apoyar en los objetivos de sus políticas y directrices de gobierno.

En esta edición, el marco descrito en la norma ISO / IEC 27005 ha sido revisado y actualizado para reflejar el contenido de los documentos de gestión de riesgos:

- ISO 31000:2009, Gestión de riesgos - Principios y directrices
- ISO / IEC 31010:2009, Gestión de riesgos - Técnicas de evaluación de riesgos

Ahora bien, la ISO / IEC 27005:2011 no establece ningún método específico para la gestión de riesgos de seguridad. Depende de cada organización el definir su enfoque de gestión de riesgos, en función, por ejemplo, del alcance del sistema de gestión de seguridad. Esto se logra de acuerdo al contexto de gestión de riesgo o al contexto del sector de la industria o empresa.³⁴

³⁴ <http://www.continuitycentral.com/news05868.html>, revisado el 2 de febrero de 2012, 13:56hrs.

III.1.3.5 Dominios que aplican para la protección de datos personales

Debido a que la ISO/IEC 27001 es el estándar internacional de seguridad de la información, la aplicabilidad en la protección de datos personales se encuentra en todos los dominios.

Dominios	Objetivos de control
A.5 Política de seguridad	<ul style="list-style-type: none"> • Política de seguridad de la información
A.6 Organización de la seguridad de la información	<ul style="list-style-type: none"> • Organización Interna • Terceros
A.7 Gestión de activos	<ul style="list-style-type: none"> • Responsabilidad sobre los activos • Clasificación de la información
A.8 Seguridad relacionada con el personal	<ul style="list-style-type: none"> • Antes del empleo • Durante el empleo • Cese del empleo o cambio de trabajo
A.9 Seguridad física y del entorno	<ul style="list-style-type: none"> • Áreas Seguras • Seguridad de los equipos
A.10 Gestión de comunicaciones y operaciones	<ul style="list-style-type: none"> • Responsabilidad y procedimientos de la operación • Gestión de la provisión de servicios por terceros • Planificación y aceptación del sistema

Dominios	Objetivos de control
	<ul style="list-style-type: none"> • Protección contra el código malicioso y descargable • Copias de seguridad • Gestión de la seguridad de las redes • Manipulación de los soportes • Intercambio de Información • Servicios de Comercio electrónico • Supervisión
<p>A.11 Control de acceso</p>	<ul style="list-style-type: none"> • Requisitos de negocio para el control de acceso • Gestión de acceso de usuario • Responsabilidades de usuario • Control de acceso a la red • Control de acceso al sistema operativo • Control de acceso a las aplicaciones y a la información • Ordenadores portátiles y teletrabajo
<p>A.12 Adquisición, desarrollo y mantenimiento de los sistemas de la información</p>	<ul style="list-style-type: none"> • Requisitos de seguridad de los sistemas de información • Tratamiento correcto de las aplicaciones • Controles criptográficos • Seguridad de los archivos del sistema

Dominios	Objetivos de control
	<ul style="list-style-type: none"> • Seguridad en los procesos de desarrollo y soporte • Gestión de la vulnerabilidad técnica
<p>A.13 Gestión de los incidentes de seguridad de la información</p>	<ul style="list-style-type: none"> • Notificación de eventos y puntos débiles de seguridad de la información • Gestión de incidentes y mejoras de seguridad de la información
<p>A.14 Gestión de la continuidad del negocio</p>	<ul style="list-style-type: none"> • Aspectos de seguridad de la información en la gestión de la continuidad del negocio
<p>A.15 Cumplimiento</p>	<ul style="list-style-type: none"> • Cumplimiento de los requisitos legales • Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico • Consideraciones sobre las auditorías de los sistemas de la información

Cabe señalar que en el dominio A.15 Cumplimiento, Objetivo de control "Cumplimiento de los Requisitos Legales" se encuentra el Control 15.1.4 relativo a la Protección de datos y privacidad de la información de carácter personal de forma específica.

III.1.1.4 ITIL³⁵

III.1.1.4.1 Antecedentes

ITIL significa Information Technology Infrastructure Library por sus siglas en inglés, y se refiere al conjunto de directrices (Mejores Prácticas) y de módulos mediante los cuales podemos establecer un mejor aprovechamiento de los recursos informáticos de una entidad u organización, desde una perspectiva de servicios. Ciertamente ITIL ha trazado el camino del 'cómo' obtener mayor beneficio de las tecnologías informáticas.³⁶

La Biblioteca de Infraestructura de Tecnologías de Información fue desarrollado por una agencia estatal británica durante los años ochenta: la Central Computing and Telecommunications Agency (CCTA). Sin embargo, se puso en marcha hasta los años noventa cuando –a iniciativa del gobierno inglés– se reunió a varias empresas exitosas para ponderar las mejores prácticas que éstas utilizaban. El propósito había sido el de mejorar la deficiente calidad de los servicios de TI adquiridos por el gobierno y, a su vez, reducir los costos de estos servicios.

El núcleo de este procedimiento se sustentó en la configuración de servicios de TI de forma focalizada y orientada al cliente. Para ello se fijó de manera clara y expedita las responsabilidades dentro de los procesos de TI. Enseguida se introdujeron procesos efectivos, orientados hacia los beneficios del cliente. Lo cierto es que se atenuaron las cuestiones técnicas, tradicionalmente valoradas por las organizaciones de TI, en beneficio de la calidad del servicio. Las recomendaciones que arrojó ITIL tienen sin duda una validez general. Las exigencias de las empresas y organizaciones analizadas en el transcurso de su elaboración fueron

³⁵ La información de este apartado se obtuvo en <http://www.overti.es/procesos-itsm/procesos-itol-v3.aspx>,

revisado 2 febrero de 2012, 13:56 horas.

³⁶ Es importante señalar que las Tecnologías de Información entrañan disciplinas informáticas entrelazadas y mutuamente dependientes.

semejantes, independientemente del tamaño o el sector de las mismas, de ahí su generalidad.

Es importante señalar que desde 1989 Office of Government Commerce (OGC), dependiente del gobierno británico, ha editado una colección de libros que corresponde a los trabajos desarrollados por ITIL. En consecuencia ésta es una marca registrada de la OGC.

Con el paso de los años ITIL se ha convertido en norma estándar para la *Gestión de Servicios de TI*. Los responsables de TI, al tomar consciencia de la importancia de este tipo de gestión de servicios, desarrollaron una terminología conjunta que ha sido de gran valía. En situaciones en las que el servicio de la infraestructura de TI tiene que ser externalizado, la homogeneización de los términos se vuelve una condición imprescindible para su aplicación. Más aún, gracias a la homologación terminológica de ITIL es posible definir las relaciones necesarias entre clientes y proveedores.

En 2007 se editó una nueva versión de ITIL totalmente revisada y mejorada: "ITIL Versión 3 (ITIL V3)". ITIL V3 ha recogido las experiencias de las versiones anteriores, dimensionando al mismo tiempo el giro de cada empresa. ¿Cuál ha sido la ventaja? Principalmente que cada empresa u organización logre una mejoría en las políticas organizacionales de TI, consiguiendo así ventajas sobre la competencia.

Ahora bien, el 14 de diciembre de 2005 se estableció ISO/IEC 20000 como estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información). La serie 20000 proviene de la adopción de la serie BS 15000 desarrollada por la entidad de normalización británica, o sea, la British Standards Institution (BSI).

III.1.4.2 Utilización y estructura

Entre las funciones principales de ITIL encontramos: a) promover la visión de TI como proveedor de servicios; b) alinear la organización de TI con el negocio de la empresa; c) estandarizar los procesos de gestión de servicios de TI; d) promover el uso de conceptos comunes para mejorar la comunicación; e) servir de base para la certificación de las personas y las empresas; f) estandarizar los procesos, roles y sus relaciones; g) entender de qué manera se puede automatizar la gestión.

Este sistema consta de cinco publicaciones básicas que reproducen conjuntamente el Ciclo de Vida del Servicio (ITIL Service Lifecycle):

- Estrategia del Servicio (Service Strategy)
- Diseño del Servicio (Service Design)
- Transición del Servicio (Service Transition)
- Operación del Servicio (Service Operation)
- Perfeccionamiento Continuo del Servicio (Continual Service Improvement)

III.1.4.2.1 Estrategia del Servicio (SS)

La SS establece las políticas y estrategias encaminadas a mejorar los servicios ya existentes. Para tal efecto, implementa una serie de lineamientos, a saber: evaluación de la estrategia, utilidad del servicio y garantía, portafolio de servicios, catálogo de servicios, factores económicos del servicio (ROI, Financiero, portafolio de Servicios, administración de la demanda) y modelo del servicio.

Es importante señalar que la SS se enfoca en el estudio y posibilidades del mercado. Esto lo ha logrado a través de una búsqueda de servicios innovadores que satisfagan al cliente. Cabe preguntarse ¿cómo lo logra? En primer lugar toma en cuenta la viabilidad de su puesta en marcha; en

segundo lugar es un sistema que analiza las mejoras potenciales para los servicios ya existentes; y en tercer lugar establece una política de verificación de los contratos con base en las nuevas ofertas de proveedores antiguos y proveedores potenciales, incluyendo por supuesto la renovación o revocación de los contratos vigentes.

La SS distingue cuatro procesos:

- Gestión Financiera
- Generación de la Estrategia
- Gestión de la Demanda
- Gestión de la Cartera de Servicios (SPM)

Debemos dimensionar la importancia de la fase de Estrategia del Servicio, pues ésta es la columna vertebral del **Ciclo de vida del servicio**. Su principal objetivo es convertir la **Gestión del Servicio** en un activo estratégico.

Para conseguir este objetivo es imprescindible determinar en primera instancia qué servicios deben ser prestados y por qué han de ser prestados desde la perspectiva del cliente y el mercado.

III.1.4.2.2 Diseño del Servicio (SD)

El SD se encarga de diseñar, desarrollar y administrar los servicios de información. Entre los tópicos que se trabajan aquí encontramos:

- Administración de Niveles de Servicio
- Administración del Catálogo de Servicios
- Administración de Disponibilidad
- Administración de continuidad de TI
- Administración de Seguridad de la Información
- Administración de Proveedores

- Transición del Servicio. La transición del servicio implica el envío de productos que se desplazan a la producción en el entorno actual. Entre los tópicos que se trabajan en el TS destacan: Gestión de Cambios, Gestión de Activos y Configuraciones, Administración del Conocimiento, Administración de versiones y desarrollos, Soporte, Testeo y Evaluación.

El siguiente paso, una vez identificado un posible servicio, consiste en analizar su viabilidad. Para ello se toman factores tales como infraestructura disponible, capacitación del personal y se planifican aspectos como seguridad y prevención ante desastres. Además, en la puesta en marcha se toman en consideración la reasignación de cargos (contratación, despidos, ascensos, jubilaciones, etc.), la infraestructura y el software a implementar.

Ciertamente los servicios en ITIL han sido definidos como un medio que aporta valor al cliente, sin que éste deba asumir los riesgos y costes específicos de su prestación.

A continuación enumeramos los procesos de gestión:

- Gestión del Catálogo de Servicios
- Gestión del Nivel de Servicio (SLM)
- Gestión de la Capacidad
- Gestión de la Disponibilidad
- Gestión de la Continuidad del Servicio TI (ITSCM)
- Gestión de la Seguridad de la Información
- Gestión de Proveedores

III.1.4.2.3 Transición del Servicio (ST)

La ST se refiere a la administración del día a día de la operación. A continuación enlistamos los tópicos que se incluyen en esta fase:

- Administración de Eventos
- Administración de requerimientos
- Administración de Incidentes
- Administración de Problemas

La misión de la fase de Transición del Servicio es hacer que los productos y servicios definidos en la fase de **Diseño del Servicio** se integren en el entorno de la producción y sean accesibles a los clientes y usuarios autorizados.

Sus principales objetivos se resumen de la siguiente manera:

- Supervisar y dar soporte a todo el proceso de cambio del nuevo servicio o, en su defecto, del servicio modificado.
- Garantizar que los nuevos servicios cumplan con los requisitos y estándares de calidad estipulados en las fases de Estrategia y Diseño.
- Minimizar los riesgos intrínsecos asociados al cambio, reduciendo el posible impacto sobre los servicios ya existentes.
- Mejorar la satisfacción del cliente respecto a los servicios prestados.
- Comunicar el cambio a todos los agentes implicados.

Los procesos que se han desarrollado en la ST son los siguientes:

- Planificación y Soporte de la Transición
- Gestión de Cambios

- Gestión de Configuración y Activos del Servicio SACM
- Gestión de Entregas y Despliegues
- Validación y pruebas del servicio
- Evaluación
- Gestión del Conocimiento

III.1.4.2.4 Operación del Servicio (SO)

La fase de Operación del Servicio es, sin duda, la más crítica entre todas. La percepción que los clientes y usuarios tengan de la calidad de los servicios prestados depende en última instancia de una correcta organización y coordinación de todos los agentes involucrados.

Ahora bien, las otras fases del Ciclo de Vida del Servicio tienen como objetivo último que los servicios sean correctamente prestados, aportando el valor y la utilidad requerida por el cliente con los niveles de calidad acordados. Evidentemente de nada sirve una correcta estrategia, diseño y transición del servicio, si falla la 'entrega' del producto final.

Los principales objetivos de la fase de Operación del Servicio incluyen:

- Coordinar e implementar todos los procesos, actividades y funciones necesarias para la prestación de los servicios acordados con los niveles de calidad aprobados.
- Dar soporte a todos los usuarios del servicio.
- Gestionar la infraestructura tecnológica necesaria para la prestación del servicio.

Uno de los aspectos esenciales en la Operación del Servicio es equilibrar la estabilidad con la capacidad de respuesta.

La estabilidad es necesaria pues, por un lado, los clientes muestran resistencia al cambio y al mismo tiempo requieren disponibilidad. Por otro lado, las necesidades de un negocio cambian rápidamente y eso requiere rapidez en las respuestas.

Por lo regular, los cambios que se dan de acuerdo a una correcta planificación, no tienen que afectar a la estabilidad del servicio. Sin embargo, esto requiere la colaboración de todos los agentes implicados en la Operación del Servicio, que deben aportar el *feedback* necesario.

Para evitar los problemas de inestabilidad es conveniente adoptar una actitud proactiva, que permita dar respuestas a las nuevas necesidades del negocio de una forma progresiva. La actitud reactiva provoca que los cambios sólo se implementen cuando la organización TI se ve obligada a responder a estímulos externos. Así pues, lo reactivo trae como consecuencia un estado de “urgencia”, que obstaculiza los cambios correctamente planificados.

No cabe duda que es muy importante encontrar un equilibrio entre los procesos de gestión internos –orientados a administrar y mantener la tecnología y recursos humanos necesarios para la prestación del servicio— y las demandas externas de los clientes.

La organización TI no debe comprometerse en la prestación de servicios para las entidades que no tengan la capacidad tecnológica suficiente o los recursos humanos necesarios, ni tampoco caer en el error de aumentar excesivamente la infraestructura TI –encareciendo innecesariamente el costo de los servicios prestados—

A continuación enlistamos los procesos de la SO:

- Gestión de Eventos
- Gestión de Incidencias/Incidentes
- Gestión de Peticiones

- Gestión de Problemas
- Gestión de Accesos
- Service Desk (Centro de Servicio al Usuario) (Función)
- Gestión Técnica (Función)
- Gestión de la Operación de TI (Función)
- Gestión de Aplicaciones (Función)

III.1.4.2.5 Mejora Continua del Servicio (CSI)

Esta fase se centra en los elementos inherentes a los procesos de identificación e introducción de mejoras en la gestión de servicios TI, ocupándose también de cuestiones relacionadas con la retirada de servicios. Indudablemente CSI se traduce en mejoras del servicio a través de su ciclo de vida.

A continuación enlistamos los procesos de la CSI:

- Medición del Servicio
- Proceso de mejora de CSI
- Informes de Servicio

Es conveniente señalar que en ITILv2 sólo se hablaba de la función de Service Desk. Ahora, en ITILv3, se agregaron las siguientes funciones: Función de Administración de Operaciones de TI; Función de Administración de Aplicaciones; Función de Administración Técnica; y Función del Service Desk.

Es cierto que ITILv2 alineaba TI con el negocio, pero en ITIL v3 las TI se han integrado al negocio. El objetivo ha sido sincronizar todo aquello que la empresa necesita con lo que puede hacer.

Transición a la V.3

V2	V3
Alinear T.I. al Negocio	Integración de T.I. al Negocio
Administración de la cadena de Valor	Integración con la red de Valor
Catálogo de Servicios Lineal	Portafolio de Servicios Dinámico
Colección Integrada de Procesos	Administración Holística del Ciclo de Vida del Servicio

El mejoramiento continuo del servicio sólo se puede alcanzar mediante el continuo monitoreo y medición de todas las actividades y procesos que han sido involucrados en la prestación de los servicios TI, a saber:

- Conformidad: los procesos se adecúan a los nuevos modelos y protocolos.
- Calidad: se cumplen los objetivos preestablecidos en tiempo y forma.
- Rendimiento: los procesos son eficientes y rentables para la organización TI.
- Valor: los servicios ofrecen el valor esperado y se diferencian de los de la competencia.

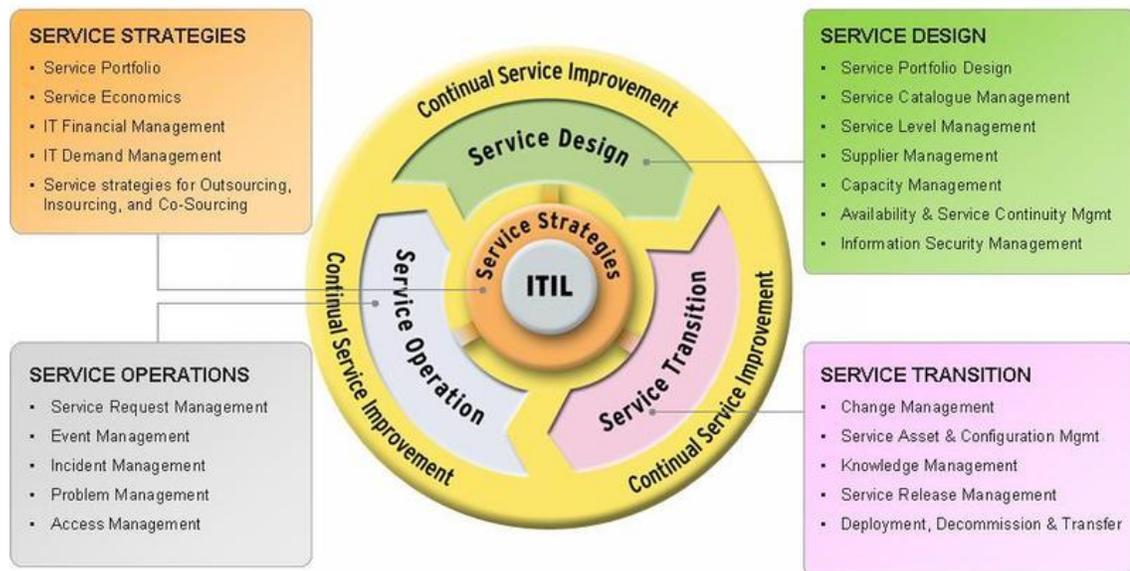
Los principales objetivos de la fase de Mejora Continua del Servicio se resumen de la siguiente manera:

- Recomendar mejoras para todos los procesos y actividades involucrados en la gestión y prestación de los servicios TI.
- Monitorizar y analizar los parámetros de seguimiento de Niveles de Servicio y contrastarlos con los SLAs en vigor.
- Proponer mejoras que aumenten el ROI y VOI asociados a los servicios TI.
- Dar soporte a la fase de estrategia y diseño para la definición de nuevos servicios y procesos/ actividades asociados a los mismos.

Los resultados de esta fase del ciclo de vida han de verse reflejados en Planes de Mejora del Servicio que incorporen toda la información necesaria, de tal suerte que se consiga:

- Mejorar la calidad de los servicios prestados.
- Incorporar nuevos servicios que se adapten mejor a los requisitos de los clientes y el mercado.
- Mejorar y hacer más eficientes los procesos internos de la organización TI.

Diagrama³⁷



III.1.4.3 Procesos de ITIL que aplican para la protección de datos personales

Estrategia del Servicio (SS)

- Generación de la Estrategia
- Gestión de la Cartera de Servicios (SPM)

Fase de Diseño del Servicio (SD)

- Gestión del Catálogo de Servicios
- Gestión de la Disponibilidad
- Gestión de la Continuidad del Servicio TI (ITSCM)

³⁷ Véase

http://blog.lontra.com/shared/image.html?/photos/uncategorized/2007/10/17/itilv3_blog_pic.jpg,
revisado el 25 de enero de 2012, 21:16hrs.

- Gestión de la Seguridad de la Información
- Gestión de proveedores

Transición del Servicio (ST)

- Gestión de Cambios
- Gestión de Configuración y Activos del Servicio SACM

Operación del Servicio (SO)

- Gestión de Eventos
- Gestión de Incidencias/Incidentes
- Gestión de Peticiones
- Gestión de Problemas
- Service Desk
- Gestión de Accesos

Mejora Continua (CSI)

- Proceso de mejora de CSI

III.1.4.4 Procedimientos de ITIL que aplican para la protección de datos personales

Considerando que ITIL cubre los servicios de TI en todas sus fases, se puede decir que los cinco libros contienen procedimientos útiles, que aplican para la protección de la información. Ahora bien, para cubrir los temas de protección de datos personales –de forma detallada– se encuentran los siguientes procedimientos:

- SS 2.6 Funciones y procesos a través del ciclo de vida
- ST 6.3 Modelos organizacionales para apoyar la transición de servicios

- SO 6.6 Roles y responsabilidades en la operación del servicio
- SD 4.7.5.2 Clasificación de proveedores y mantenimiento de la base de datos de proveedores y contratos
- SD 4.7.5.4 Gestión y desempeño de proveedores y contratos
- SD 4.2.5.9 Desarrollar contratos y relaciones
- SD 4.7.5.5 Renovación y/o término de contratos
- SD 6.2 Análisis de actividades
- SD 6.4 Roles y responsabilidades
- CSI 6 Organización para la mejora continua del servicio

III.1.5 NIST

III.1.5.1 Antecedentes

NIST –por sus siglas en inglés, *National Institute of Standards and Technology*— es una agencia federal no regulatoria del Departamento de Comercio de los Estados Unidos. Su misión consiste en promover la innovación y la competencia industrial –en ese país— mediante avances en metrología, estándares y tecnología de forma que mejoren la seguridad económica y la calidad de vida de los norteamericanos.³⁸ El Instituto fue fundado el 3 de marzo de 1901, como la Oficina Nacional de Estándares (National Bureau of Standards)³⁹ y en 1988 cambió su nombre a NIST.

Los laboratorios de NIST se centran en tres áreas focalizadas en su misión: ciencia de medición (Medición Física, Medición de Materiales),

³⁸ Véase http://www.nist.gov/public_affairs/general_information.cfm, revisado el 20 de febrero de 2012, 11:00hrs.

³⁹ Véase <http://www.100.nist.gov/>, revisado el 20 de febrero de 2012, 12:00hrs.

tecnología (Tecnología de la Información, Ingeniería) e Instalaciones de Usuarios Nacionales (Centro NIST para la Investigación del Neutrón, Centro de Nanociencia y Nanotecnología).⁴⁰

II.5.2 Publicaciones Especiales de la Serie 800

Se establecieron en 1990 con el fin de presentar publicaciones para la seguridad informática y la Tecnología de la Información. La serie 800 reporta sobre investigación de Tecnologías de la Información (ITL), directrices y esfuerzos alcanzados en seguridad informática, así como sus actividades colaborativas con la industria, gobierno y organizaciones académicas.⁴¹

La tabla que a continuación se muestra enlista algunas de las publicaciones especiales que, debido a su contenido, aplican para la figura de encargado y la protección de datos personales.

⁴⁰ Véase http://www.nist.gov/public_affairs/factsheet/overview-brochure.cfm, revisado el 20 de febrero de 2012, 11:30hrs

⁴¹ Véase <http://csrc.nist.gov/publications/PubsSPs.html>, revisado el 20 de febrero de 2012, 11:40hrs.

Número de la Publicación	Fecha	Título
NIST SP 800-12	Octubre de 1995	Introducción a la Seguridad Informática: El Manual NIST
NIST SP 800- 14	Septiembre de 1996	Principios y Prácticas Generalmente Aceptadas para la Seguridad de los Sistemas de Tecnologías de la Información
NIST SP 800-39	Marzo de 2011	Administración del Riesgo en la Seguridad de la Información
NIST SP 800-122	Abril de 2010	Guía para la Protección de la Confidencialidad de Información de Identificación Personal
NIST SP 800-144	Diciembre de 2011	Directrices en Seguridad y Privacidad en Cómputo en la Nube de tipo Público

Algunas de las Publicaciones Especiales (SP) que aplican directamente para el tema de la seguridad y protección de los datos personales se describirán brevemente a continuación:

NIST SP 800-12⁴²

INTRODUCCIÓN A LA SEGURIDAD DE TECNOLOGÍAS DE INFORMACIÓN

Manual de NIST

Este documento proporciona un marco referencial en seguridad de Tecnologías de Información (incluyendo hardware, software e información); maneja importantes conceptos, consideraciones de riesgo de seguridad de la información y la interrelación de los controles de seguridad.

Menciona los 8 principios de seguridad de Tecnologías de Información (TI) descritos en el NIST 800-14 y la importancia de definir roles y responsabilidades en las organizaciones.

El mayor esfuerzo de este manual se enfoca a los controles de seguridad de acuerdo a su naturaleza.

Clasificación de Controles

- *Controles administrativos*

Son técnicas y mecanismos que maneja la administración de las organizaciones (directores, gerentes). En general se enfocan a la gestión del programa de seguridad de TI y a la administración del riesgo de la organización.

- Política de seguridad de tecnologías de información

⁴² Véase <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>, revisado el 20 de febrero de 2012, 14:00hrs.

- Administración del programa de seguridad de TI
- Administración del Riesgo en la seguridad de TI
- Planeación y seguridad en el ciclo de vida de la seguridad de TI
- Aseguramiento

- *Controles operativos*

Son los controles enfocados a ser ejecutados e implantados por las personas (lo contrario a los sistemas) en sus actividades diarias (procesos, procedimientos). Estos controles generalmente incrementan la seguridad de un sistema en particular (o de un grupo de sistemas).

- Personal/Usuarios
- Capacidades para contingencias y desastres
- Manejo de incidentes de seguridad de TI
- Concienciación, capacitación y educación
- Consideraciones de seguridad en soporte y operación de TI
- Seguridad física y ambiental

- *Controles técnicos*

Son los controles habilitados por tecnología que implantan por y a través de los sistemas de TI. Sin embargo, la implantación de los controles técnicos siempre requiere de importantes consideraciones operacionales. Estos controles deben ser consistentes con la administración de seguridad (nivel de riesgo definido) dentro de la organización.

- Identificación y autenticación
- Control de acceso lógico
- Auditoría (registro)
- Criptografía (cifrado)

NIST SP 800-14⁴³

PRINCIPIOS Y PRÁCTICAS GENERALMENTE ACEPTADAS PARA LA SEGURIDAD DE LOS SISTEMAS DE TECNOLOGÍAS DE INFORMACIÓN

Este documento proporciona una base para revisar los programas de seguridad de TI. Permite ganar un entendimiento de los requerimientos básicos de seguridad de los sistemas de TI que deben aplicarse en las organizaciones.

Describe 8 principios y 14 prácticas de seguridad.

Principios

- 1) La seguridad de los sistemas de TI soporta la misión de las organizaciones*

El propósito de la seguridad de los sistemas de TI es proteger los recursos valiosos de una organización (información, hardware y software).

A través de la selección y aplicación apropiada de controles, la seguridad apoya a las organizaciones en la misión de proteger sus recursos físicos y financieros, su reputación, su posición legal, sus empleados y otros activos tangibles e intangibles.

⁴³ Véase Generally Accepted Principles and Practices for Securing Information Technology Systems NIST SP 800-14, septiembre de 1996, en <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf> revisado el 17 de febrero de 2012, 13:00hrs.

2) La seguridad de los sistemas de TI es un elemento integral de una buena administración

La información y los sistemas de TI son frecuentemente activos críticos. Proteger los sistemas de TI puede ser tan importante como proteger otros recursos de la organización (financieros, activos físicos, empleados)

3) La seguridad de los sistemas de TI debe ser costo/efectiva

Los costos y beneficios de la seguridad deberán ser examinados cuidadosamente en los aspectos monetarios y no monetarios para asegurarse que el costo de los controles de seguridad no exceda los beneficios esperados.

4) Los dueños/usuarios de los sistemas tienen responsabilidades de seguridad fuera de su organización

Si los sistemas tienen usuarios externos, deberán asegurarse de compartir el conocimiento apropiado acerca de las medidas de seguridad existentes.

5) Los roles y las responsabilidades de la seguridad en los sistemas de TI debe ser explícita

Los roles y responsabilidades de dueños, proveedores y usuarios de los sistemas de TI en relación a la seguridad de los sistemas de TI deberán ser explícitas.

6) La seguridad de los sistemas de TI requiere de un enfoque organizacional e integrado

Para proveer una seguridad efectiva se requiere de un enfoque organizacional que contemple diferentes áreas, inclusive las que se encuentran fuera del entorno de los sistemas de TI.

7) La seguridad de los sistemas de TI debe ser periódicamente revisada

Debido a que el ambiente e infraestructura de TI son muy dinámicos, la tecnología, usuarios, datos, riesgos asociados a los sistemas de información siempre están cambiando. Muchos cambios de este tipo afectan los sistemas de seguridad. Un cambio en el valor o uso de la información generan nuevas amenazas y/o vulnerabilidades.

8) La seguridad de los sistemas de TI es limitado por factores sociales

La capacidad de la seguridad de soportar la misión de la organización, puede verse limitada por varios factores en los que se encuentran factores sociales.

Algunas medidas de autenticación pueden ser consideradas de invasión en algún ambiente o cultura.

Las medidas de seguridad deben ser seleccionadas e implementadas, reconociendo los derechos e intereses de legitimidad de las personas que interactúan con los recursos/activos informáticos.

Prácticas

1) Política

Las organizaciones deben tener diferentes tipos de políticas: las generales y las específicas para cada evento o sistema.

Las políticas deben ser:

- Complementadas
- Visibles
- Soportadas por la administración
- Consistentes

2) Administración del programa

La administración de la seguridad con múltiples niveles brinda muchos beneficios. Cada nivel contribuye al programa de seguridad con diferentes capacidades, responsabilidades y recursos.

3) Administración del Riesgo

El riesgo es la posibilidad de que un evento adverso para la organización ocurra. La administración del riesgo es el proceso de evaluar el riesgo, reducir y mantenerlo a un nivel aceptable.

La administración del riesgo requiere de un análisis y evaluación del riesgo para determinar las mejores acciones para manejarlo. La selección de los controles de seguridad para manejar el riesgo deben ser costo/efectivas.

4) Planeación del ciclo de vida

La seguridad, como tantos otros aspectos de los sistemas de información, deberá ser administrada en todo el ciclo de vida.

Existen diferentes modelos para el manejo del ciclo de vida de los sistemas, la mayoría se compone de 5 fases:

- Inicio
- Desarrollo/adquisición
- Implantación
- Operación
- Terminación

5) Personal/Usuarios

Muchos aspectos de seguridad están relacionados con usuarios, diseñadores, implantadores y administradores. Ningún sistema de TI puede estar asegurado sin un manejo apropiado del acceso de todos los usuarios/personal.

6) *Capacidades para contingencias y desastres*

El plan de contingencia apoya a las organizaciones a continuar sus operaciones en caso de una interrupción no planeada.

7) *Manejo de incidentes de seguridad*

Un incidente de seguridad puede ser el resultado de un virus informático, código malicioso o sistemas de intrusión. El manejo de incidentes da respuesta a códigos maliciosos y amenazas técnicas.

8) *Concienciación y capacitación*

Un efectivo plan de seguridad de concienciación y capacitación requiere:

- Planeación
- Implantación
- Mantenimiento
- Evaluación periódica

9) *Consideraciones de seguridad en la operación y soporte de computadoras*

10) *Seguridad física y ambiental*

Controles de seguridad física y ambiental son implementados para proteger las instalaciones.

11) *Identificación y autenticación*

La Identificación y autenticación (I/A) es un componente crítico en la seguridad, y es la base para los diferentes tipos de control de acceso. Lo cierto es que I/A es una medida técnica que previene el acceso a personas no autorizadas.

12) *Control de acceso lógico*

13) Auditoría

Mantener registros de las actividades por sistema, aplicación o usuario.

14) Cifrado

Es una herramienta importante para proteger la información y es utilizada en varios aspectos de la seguridad de la información.

NIST SP 800-39⁴⁴

ADMINISTRACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

En este documento se establece la importancia que tiene el ejercicio de análisis y administración del riesgo en la gestión de la seguridad de la información.

La seguridad de la información puede ser definida básicamente como la preservación de la confidencialidad, la integridad y la disponibilidad de los sistemas de información. Dependiendo del entorno de las organizaciones, se pueden tener diferentes amenazas que comprometan a los objetivos previamente mencionados. Ante un riesgo concreto las organizaciones deben tener alternativas del manejo del mismo.

El propósito de la publicación especial 800-39, es proporcionar a las organizaciones una guía para la administración del riesgo en la seguridad de la información.

Cabe señalar que el rol de la administración del riesgo de la seguridad de la información en las organizaciones es de tal relevancia que, dependiendo del manejo de la misma, contribuye para alcanzar metas y objetivos estratégicos.

⁴⁴ Véase “Managing Information Security Risk”, NIST Special Publication 800-39; marzo de 2011, en <http://csrc.nist.gov/publications/nistpubs/800-39-SP800-39-final.pdf>, revisado el 16 de febrero de 2012, 11:00hrs.

Para tener una buena administración del riesgo se recomienda lo siguiente:

- Asegurarse de que los Ejecutivos reconozcan la importancia de la administración del riesgo.
- Asegurarse de que el proceso de la administración del riesgo en las organizaciones sea en todos los niveles el mismo.
- Que esta actividad esté contemplada en todos los procesos de negocio.
- Que cada persona en la organización entienda la relación de los riesgos asociados a cada uno de los procesos de negocio.

Ahora bien, cuáles son los **Componentes del Riesgo** en un proceso de administración del mismo:

- Establecer el riesgo
- Valorar el riesgo
- Responder al riesgo
- Monitorear el riesgo

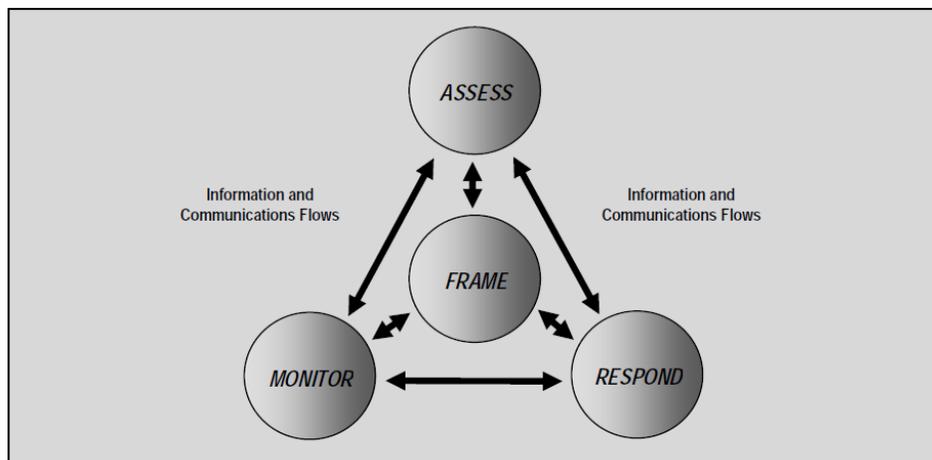


Figura 1: Proceso de Administración del Riesgo

El primer componente tiene como objetivo establecer una estrategia de la administración del riesgo.

El segundo componente tiene como objetivo identificar amenazas, vulnerabilidades internas y externas, y detectar el daño en caso de cumplirse las amenazas.

El tercer componente determina cómo las organizaciones responden al riesgo tomando como base el resultado de la valoración del riesgo.

El cuarto componente determina cómo se monitorea el riesgo para asegurarse que los controles establecidos cumplan con los objetivos planteados.

Adicionalmente a los cuatro componentes de administración del riesgo descritos anteriormente, las organizaciones también deben considerar los riesgos externos, por ejemplo, las relaciones con proveedores, clientes y proveedores de servicios.

Por ello, para integrar el manejo del riesgo a través de toda la organización, esta guía ha establecido que se requiere de un enfoque de tres niveles:

1. Nivel organizacional
2. Nivel de proceso de negocio
3. Nivel de sistemas de información

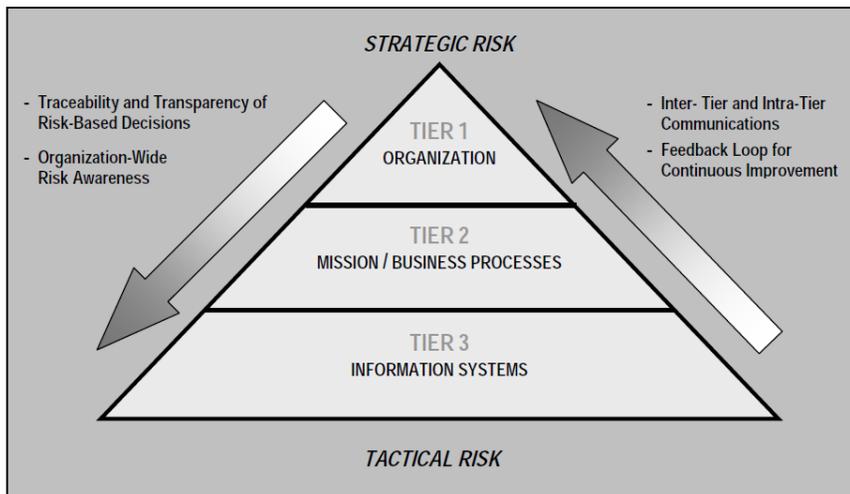


Figura 2: Administración del Riesgo Multiniveles

Nivel 1 Organización

En este nivel se contempla el riesgo desde una perspectiva organizacional, estableciendo e implementando estructuras de gobierno que sean consistentes con la estrategia, metas y objetivos de las organizaciones. Además, deben considerarse los requerimientos definidos por leyes federales, directrices, políticas, regulaciones, estándares y las funciones del negocio.

El gobierno es un conjunto de responsabilidades y prácticas ejecutadas por los responsables de cada organización (ejemplo: el grupo de directores y la administración ejecutiva en una corporación).

En este nivel se definen:

- Estrategia de administración del riesgo
- Estrategia de inversión
- Misión y prioridades del riesgo

Nivel 2 Procesos del Negocio

Se establece el riesgo desde una perspectiva de procesos de negocio a través del diseño, desarrollo e implementación de procesos que soporten las funciones del negocio definidos en el nivel 1.

En este nivel se determinan:

- Los procesos de negocios definidos en la estrategia de administración del riesgo.
- La arquitectura de la empresa incluyendo la de seguridad de la información.

Nivel 3 Sistemas de Información

En este nivel se refleja la estrategia de la administración del riesgo de la organización y cualquier riesgo relacionado con el costo, programa y requerimientos a ejecutar por cada sistema de información, que soportan las funciones de la organización.

Cultura Organizacional

La cultura organizacional se refiere a los valores, creencias y normas que influyen en el comportamiento y acciones de cada miembro de la organización. Es un elemento muy importante dentro de las organizaciones, ya que si la estrategia de administración del riesgo no es consistente con la cultura organizacional, el resultado de la implantación de la estrategia tendría muchas dificultades e inclusive no sería posible implantarla.

NIST SP 800-122⁴⁵

GUÍA PARA LA PROTECCIÓN DE LA CONFIDENCIALIDAD DE INFORMACIÓN DE IDENTIFICACIÓN PERSONAL

(Recomendaciones del Instituto Nacional de Estándares y Tecnología NIST)

Las recomendaciones que se hacen en este documento están dirigidas principalmente a las agencias gubernamentales federales de Estados Unidos y a quienes dirigen negocios en nombre de las agencias. Sin embargo, pueden ser útiles para cualquier organización.

Esta guía sugiere categorizar el nivel de impacto de la confidencialidad de la PII (Información de Identificación Personal) en bajo, moderado y alto, y con base en el daño potencial que pudiera resultar a los titulares de la información y/o la organización si la PII fuera vulnerada, utilizada o divulgada de forma inapropiada. Cada organización deberá decidir qué factores utilizará para determinar los niveles de impacto y crear e implementar la política, procedimientos y controles apropiados.

Algunos ejemplos de estos factores son:

- Identificabilidad
- Cantidad de PII
- Sensibilidad del campo de datos
- Contexto de uso
- Obligaciones para proteger la confidencialidad
- Acceso a y ubicación de la PII

⁴⁵ Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), en <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>, revisado el 7 de febrero de 2012, 13:00 hrs.

Se establece que la PII debe ser protegida a través de una combinación de medidas, incluyendo salvaguardias operativas, salvaguardias específicas de privacidad y controles de seguridad. Existen dos tipos de controles operativos para la protección de PII: a) política y elaboración de procedimiento y b) educación, capacitación y concienciación.

Ciertamente los controles específicos de privacidad, son controles para la protección de la confidencialidad de la PII. Éstos proveen tipos de protección que usualmente no son necesarios para otros tipos de datos. Además, ayudan a las organizaciones a recolectar, mantener, utilizar y difundir datos en diferentes formas, protegiendo la confidencialidad de los datos.

A continuación enlistamos dichos controles:

- Minimizar el uso, obtención y retención de la PII
- Dirigir las evaluaciones de impacto de la privacidad (PIA por sus siglas en inglés): ¿qué información se obtendrá? ¿por qué? ¿con qué fin se utilizará? ¿con quién se compartirá? ¿cómo se resguardará la información? y ¿qué decisiones se tomarán con respecto al sistema de TI o al conjunto de información como resultado de la aplicación del PIA?
- Enmascaramiento de la información
- Disociación de la información

No cabe duda que la NIST SP 800-122 aborda de manera correcta el tema de los controles de seguridad. Y menciona que muy a menudo estos controles ya están implementados en un sistema de la organización para proteger otro tipo de datos procesados, almacenados o transmitidos por el sistema. En ese sentido señala que la NIST SP 800-53 es la que trata la protección general de datos y sistemas.

Algunos controles que pueden ser utilizados para salvaguardar la confidencialidad de la PII y que se encuentran dentro de la NIST SP 800-53 son los siguientes:

- Cumplimiento de acceso (AC-3)
- Separación de funciones (AC-5)
- Privilegio mínimo (AC-6)
- Acceso Remoto (AC-17)
- Colaboración y compartición de información basada en el usuario (AC-21)
- Control de acceso para dispositivos móviles (AC-19)
- Eventos auditables (AU-2)
- Revisión de auditoría, análisis y reporte (AU-6)
- Identificación y Autenticación (Usuarios organizacionales) (IA-2)
- Acceso a medios (MP-2)
- Etiquetado de medios (MP-3)
- Almacenamiento de medios (MP-4)
- Transportación de medios (MP-5)
- Saneamiento de medios (MP-6)
- Transmisión de confidencialidad (SC-9)
- Protección de información almacenada (SC-28)
- Monitoreo de sistema de información (SI-4)

Por otra parte, esta guía plantea en su apartado número 5 “Respuesta a Incidentes para brechas que involucran PII” que las organizaciones deben desarrollar políticas que determinen cuándo y cómo los titulares de la información deben ser notificados; además se pregunta cuándo una brecha debe ser reportada públicamente y cuándo deben proveerse servicios correctivos. Lo cierto es que la administración de incidentes que involucren PII requiere de una coordinación estrecha y vinculante entre todo el personal de la organización. Se deben establecer roles claros y

responsabilidades que aseguren la administración efectiva cuando un incidente ocurra.

La NIST SP 800-61 Revisión 1 describe cuatro fases para el manejo de incidentes de seguridad: preparación; detección y análisis; contención, erradicación y recuperación; y actividad después del incidente. Asimismo, la NIST SP 800-122 proporciona detalles adicionales sobre consideraciones específicas para PII en cada una de estas cuatro fases.

A continuación se describen brevemente las consideraciones antes mencionadas:

Preparación

La preparación requiere el mayor esfuerzo pues establece la etapa para asegurar que la brecha sea manejada apropiadamente. El desarrollo de planes de respuesta para brechas que involucran PII necesita que las organizaciones tomen decisiones acerca de cómo manejar las brechas que involucran PII y las decisiones que deben utilizarse para desarrollar políticas y procedimientos. Estas políticas y decisiones deberán ser comunicadas a todo el personal de la organización a través de capacitación y programas de concienciación. La capacitación deberá incluir ejercicios para simular un incidente y probar si el plan de respuesta es efectivo y si el personal entiende y es capaz de desempeñar sus roles de forma efectiva. Los programas de capacitación también deben informar a los empleados sobre las consecuencias de sus acciones por uso y manejo inapropiado de la PII.

De ahí, pues, que los empleados deban ser provistos de una clara definición de qué constituye una brecha que involucra información personal y qué información necesita ser reportada.

Adicionalmente, las organizaciones tendrán que establecer un Comité o persona responsable de utilizar la política de notificación de una brecha para coordinar la respuesta de la organización.

En este punto deberá considerarse el nivel de impacto de la confidencialidad de la PII para poder determinar en qué circunstancias se requiere que la organización provea asistencia correctiva a los titulares afectados, ya que el nivel de impacto proporciona un análisis de la probabilidad de daño por la pérdida de confidencialidad para cada caso de PII.

Detección y Análisis

Las organizaciones pueden seguir utilizando las tecnologías de detección y análisis actuales, sin embargo, es posible que sea necesario que hagan ajustes a los procesos de manejo de incidentes tales como asegurar que los procesos de análisis incluyan una evaluación de si un incidente involucra PII.

Contención, erradicación y recuperación

Las tecnologías y técnicas existentes para contención, erradicación y recuperación pueden ser utilizadas para brechas que involucren PII. Si es el caso, podría ser necesario que se apliquen cambios a los procesos de manejo de incidentes, por ejemplo, en el desarrollo de pasos adicionales de saneamiento de medios cuando la PII necesite ser borrada de un medio durante la recuperación. La PII no debe ser saneada hasta que se determine si ésta debe ser preservada como evidencia. Adicionalmente, es importante determinar si la PII fue accesada y cuántos registros o individuos fueron afectados.

Actividad después del incidente

La información obtenida a través de la detección, análisis, contención y recuperación debe ser recolectada para compartirla dentro de la organización. Sin duda, esto ayudará a protegerse contra incidentes futuros. El plan de respuesta a incidentes debe ser actualizado continuamente y mejorado con base en las lecciones aprendidas durante cada siniestro. Dichas lecciones deberán indicar también la necesidad adicional de capacitación, controles de seguridad y procedimientos para protegerse contra futuros incidentes.

NIST SP 800-144

DIRECTRICES EN SEGURIDAD Y PRIVACIDAD EN CÓMPUTO EN LA NUBE DE TIPO PÚBLICO

Este documento está dirigido principalmente para las agencias gubernamentales federales de Estados Unidos, sin embargo, se menciona que dichas directrices también pueden ser útiles para organizaciones no gubernamentales.

El propósito de esta guía es proveer una perspectiva general de los servicios de cómputo en la nube de tipo público y los retos en seguridad y privacidad que conllevan.

El cómputo en la nube ha sido definido por el Instituto Nacional de Estándares y Tecnología (NIST) como un modelo para permitir el acceso de red de forma conveniente y bajo demanda a un conjunto compartido de recursos computacionales configurables (ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios). Bajo este esquema, los recursos computacionales configurables pueden ser rápidamente suministrados y liberados con un esfuerzo mínimo de administración o simplemente con la interacción del proveedor de la nube.

Modelos de uso

Existen diferentes modelos del cómputo en la nube, entre los cuales se pueden mencionar los siguientes:

- Nube pública: es aquella en la que la infraestructura y recursos computacionales incluidos están disponibles para el público en general sobre Internet. Le pertenece y es operada por un proveedor de servicios de cómputo en la nube y por definición es externa a la organización del consumidor.
- Nube privada: es aquella en que el ambiente de cómputo es operado exclusivamente para una sola organización. Esta puede ser administrada por la organización o por un tercero, y puede estar hospedada dentro del centro de datos de la organización o fuera de esta. Una nube privada tiene el potencial de proporcionar a la organización un mayor control sobre la infraestructura, recursos computacionales y consumidores que una nube pública.
- Nube comunidad: es similar a la nube privada pero la infraestructura y recursos computacionales son exclusivos para dos o más organizaciones que tienen consideraciones comunes en cuanto a privacidad, seguridad y regulación, en lugar de una sola organización.
- Nubes híbridas: son más complejas debido a que implican una composición de dos o más nubes (privada, comunidad o pública). Cada miembro permanece como una entidad única, pero está ligada a las otras a través de tecnología estandarizada o propietaria que permite la portabilidad de aplicación y datos entre ellos.

Ahora bien, los modelos de uso juegan un importante papel en el cómputo en la nube. Por su parte, los modelos de servicio también representan una importante consideración. A continuación presentamos tres modelos de servicios conocidos y utilizados comúnmente: Software

como un Servicio (SaaS), Plataforma como un Servicio (PaaS) e Infraestructura como un Servicio (IaaS).

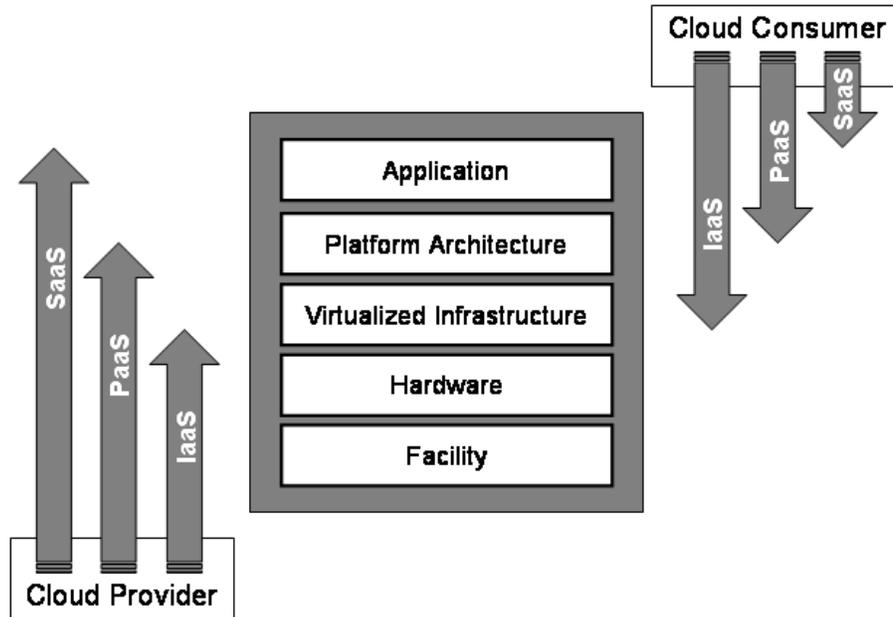


Figura 1: Diferencias en ámbito y control entre modelos de servicio de la nube

El conjunto de objetivos de seguridad y privacidad de una organización es un factor clave para las decisiones sobre servicios de outsourcing de tecnología de información. Particularmente en las decisiones que implican pasar los recursos organizacionales a una nube pública y a los servicios de un proveedor específico. En ese momento los acuerdos de servicio cobran gran relevancia.

Un acuerdo de servicio define los términos y condiciones para el acceso y uso de los servicios ofrecidos por el proveedor de la nube. También establece el periodo de servicio, las condiciones de terminación y la disposición de los datos (tomemos como ejemplo el periodo de preservación, una vez que se da la terminación del mismo).

Así pues, los términos y condiciones completos para un acuerdo de servicio de cómputo en la nube se estipulan usualmente en múltiples documentos, los cuales típicamente pueden incluir un Acuerdo de Nivel de Servicio (SLA), una política de privacidad, una política de uso aceptable o sencillamente términos de uso.

Existen dos tipos de acuerdos de servicio: acuerdos predefinidos no negociables y acuerdos negociados.

Lo cierto es que cuando se utiliza un ambiente de cómputo en la nube se forman áreas de mejora, que traen consigo beneficios de seguridad y privacidad para las organizaciones.

Dichas áreas de mejora son:

- Especialización del personal
- Fortaleza de plataforma
- Disponibilidad de recurso
- Respaldos y recuperación
- Puntos móviles
- Concentración de datos

Sin embargo, los servicios de cómputo en la nube también tienen áreas de preocupación cuando son comparados con ambientes computacionales que se encuentran en centros de datos tradicionales. Algunos de estos puntos de preocupación son los siguientes:

- Complejidad del sistema. Muchos componentes hacen que una nube pública tenga una mayor superficie de ataque
- Ambiente compartido por multi-usuarios
- Servicios que son entregados vía Internet
- Pérdida de control (tanto de aspectos físicos como lógicos)

La NIST SP 800-144 muestra en dos tablas un resumen de recomendaciones, tanto en temas de seguridad y privacidad como de actividades a realizarse para la contratación de un servicio de outsourcing de cómputo en la nube. Éstas se citan a continuación:⁴⁶

Tabla 1: Asuntos sobre Seguridad, Privacidad y Recomendaciones

Áreas	Recomendaciones
Gobierno	<p>Extender las prácticas organizacionales concernientes a las políticas, procedimientos y estándares utilizados para el desarrollo de aplicación y servicio provisionados en la nube, así como el diseño, implementación, pruebas, uso y monitoreo de servicios utilizados o comprometidos.</p> <p>Establecer mecanismos de auditoría y herramientas para asegurar que las prácticas organizacionales se siguen a lo largo del ciclo de vida del sistema.</p>
Cumplimiento	<p>Entender los diferentes tipos de leyes y regulaciones que imponen obligaciones de seguridad y privacidad en la organización y que</p>

⁴⁶ Guidelines on Security and Privacy in Public Cloud Computing, <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>, revisado el 9 de febrero de 2012, 11:00 hrs.

Áreas	Recomendaciones
	<p>impactan potencialmente las iniciativas del cómputo en la nube, particularmente aquellas que involucran la ubicación de los datos, los controles de privacidad y seguridad, la administración de registros y los requerimientos del descubrimiento electrónico (electronic discovery)⁴⁷.</p> <p>Revisar y evaluar la oferta del proveedor de la nube con respecto a los requerimientos organizacionales a ser cumplidos y asegurar que los términos del contrato se ajustan adecuadamente a los requerimientos.</p> <p>Asegurarse de que las capacidades del descubrimiento electrónico (electronic discovery) del proveedor de la nube y los procesos no comprometan la privacidad o la seguridad de los datos y las aplicaciones.</p>

⁴⁷ Se puede definir a “**e-Discovery**” (electronic discovery) como la **etapa de descubrimiento electrónico en la que se busca, localiza y asegura información electrónica con el propósito de ser usada como evidencia**, ya sea que se trate de un caso legal que tramite en el ámbito Civil o Penal, o bien de temas relacionados con el cumplimiento de regulaciones y normas.

Véase <http://www.iaia.org.ar/revistas/elauditorinterno/21/Articulo2.htm>, revisado el 20 de febrero de 2012, 12:00hrs.

Áreas	Recomendaciones
<p>Confianza</p>	<p>Asegurarse de que los acuerdos de servicio tengan suficientes medios para permitir la visibilidad en los controles de seguridad y privacidad y los procesos empleados por el proveedor de la nube, y su desempeño en el tiempo.</p> <p>Establecer derechos claros y exclusivos de la propiedad sobre los datos.</p> <p>Instituir un programa de administración de riesgo que sea suficientemente flexible para adaptarse a la constante evolución y ambiente cambiante de riesgo para el ciclo de vida del sistema.</p> <p>Monitorear continuamente el estado de seguridad del sistema de información para apoyar las decisiones de administración de riesgos que se están presentando en el momento.</p>
<p>Arquitectura</p>	<p>Entender las tecnologías subyacentes que el proveedor de la nube utiliza para prestar los servicios, incluyendo las implicaciones que los controles</p>

Áreas	Recomendaciones
	<p>técnicos involucrados tienen en la seguridad y privacidad del sistema, sobre el ciclo de vida completo del sistema y a través de todos los componentes del sistema.</p>
<p>Identidad y Administración de Acceso</p>	<p>Asegurarse de que los controles adecuados están establecidos para proteger la autenticación, autorización y otras funciones de administración de identidad y acceso, y son adecuados para la organización.</p>
<p>Aislamiento de software</p>	<p>Entender la virtualización y otras técnicas lógicas de aislamiento que el proveedor de la nube emplea en su arquitectura de software multi-usuario y evaluar los riesgos involucrados para la organización.</p>
<p>Protección de datos</p>	<p>Evaluar la conveniencia de las soluciones de administración de datos del proveedor de la nube para los datos de interés para la organización y la habilidad de controlar el acceso a los datos, de proteger los datos almacenados y estáticos, en tránsito y en uso, y el saneamiento de los datos.</p>

Áreas	Recomendaciones
	<p>Tomar en cuenta el riesgo de los datos organizacionales recopilados con aquellos pertenecientes a otras organizaciones cuyos perfiles de amenazas son altos o cuyos datos representan colectivamente un valor significativo.</p> <p>Entender y ponderar completamente los riesgos involucrados en la administración de la llave de cifrado con los mecanismos disponibles en el ambiente de la nube y los procesos establecidos por el proveedor de la nube.</p>
<p>Disponibilidad</p>	<p>Entender las disposiciones contractuales y procedimientos para la disponibilidad, el respaldo de datos y recuperación, y la recuperación en caso de desastre, y asegurar que ellos se ajusten a los requerimientos del plan de continuidad y contingencia de la organización.</p> <p>Asegurarse de que durante una interrupción media o prolongada o un desastre serio, las operaciones</p>

Áreas	Recomendaciones
	<p>críticas puedan ser reanudadas inmediatamente, y que todas las operaciones puedan restituirse finalmente de forma oportuna y organizada.</p>
<p>Respuesta a incidentes</p>	<p>Entender las disposiciones contractuales y procedimientos para la respuesta a incidentes y asegurarse de que se ajustan a los requerimientos de la organización.</p> <p>Asegurarse de que el proveedor de la nube cuenta con un proceso de respuesta transparente establecido, y mecanismos suficientes para compartir información durante y después de un incidente.</p> <p>Asegurarse de que la organización puede responder a incidentes de forma coordinada con el proveedor de la nube de acuerdo con sus respectivos roles y responsabilidades para el ambiente de cómputo.</p>

Tabla 2: Actividades de Outsourcing y Recomendaciones

Áreas	Recomendaciones
<p>Actividades preliminares</p>	<p>Identificar la seguridad, privacidad y otros requerimientos organizacionales que deben reunir los servicios de la nube, como un criterio para seleccionar al proveedor.</p> <p>Analizar los controles de seguridad y privacidad del ambiente del proveedor de la nube y evaluar el nivel de riesgo involucrado con respecto a los objetivos de control de la organización.</p> <p>Evaluar la habilidad del proveedor de la nube y el compromiso para entregar servicios de la nube conforme al calendario objetivo y ajustarse a los niveles de seguridad y privacidad estipulados.</p>
<p>Actividades de inicio y concurrentes</p>	<p>Asegurarse de que los requerimientos contractuales se encuentran registrados explícitamente en el acuerdo de servicio, incluyendo las disposiciones de privacidad y</p>

Áreas	Recomendaciones
	<p>seguridad, y que estas sean aceptadas por el proveedor de la nube.</p> <p>Involucrar a un consultor legal en la revisión del acuerdo de servicio y en cualquier negociación acerca de los términos del servicio.</p> <p>Evaluar continuamente el desempeño del proveedor de la nube y la calidad de los servicios proveídos para asegurar que las obligaciones contractuales están siendo cumplidas y administrar y mitigar el riesgo.</p>
<p>Actividades finales</p>	<p>Avisar al proveedor de la nube sobre cualquier requerimiento contractual que deba ser observado en la terminación.</p> <p>Revocar todos los derechos de acceso físicos y electrónicos asignados al proveedor de la nube y recuperar físicamente los tokens y badges de manera oportuna.</p> <p>Asegurarse que los recursos organizacionales puestos a</p>

Áreas	Recomendaciones
	disposición de o en posesión del proveedor de la nube, bajo los términos del acuerdo de servicio, sean regresados o recuperados en forma utilizable y que la información haya sido suprimida.

III.1.6 PCI/DSS

III.1.6.1 Antecedentes

Payment Card Industry Data Security Standard (PCI-DSS) es un estándar internacional que establece un conjunto de requerimientos de seguridad de la información para proteger los datos de los tarjetahabientes.

El origen de PCI-DSS se remonta al 2004, en un esfuerzo conjunto entre PCI Security Standards Council (PCI SSC) y las principales compañías emisoras de tarjetas de crédito (Visa Internacional, Mastercard Worldwide, American Express, JCB Internacional y Discover Financial Services), para persuadir –o en su caso disuadir– a los comercios, proveedores de servicios y bancos a que implementen sistemas que atenúen los riesgos de fraude con tarjetas de crédito y débito. Esto se lograría mediante la protección de la infraestructura que procesa, transmite o almacena los datos relativos a tarjetahabientes.⁴⁸

III.1.6.2 Utilización y estructura

PCI-DSS fue creado para proteger la confidencialidad, integridad y trazabilidad de los datos relacionados con tarjetas de crédito y débito.

⁴⁸ Véase Implantación y Certificación en el estándar PCI DSS, <http://www.isecauditors.com/es/consultoria-pci-dss.html>, revisado el 8 de febrero de 2012, 11:30hrs.

Las compañías que procesan, guardan o transmiten datos de tarjetas deben cumplir con el estándar. De no hacerlo se arriesgan a la pérdida de sus permisos para procesar las tarjetas de crédito y débito (pérdida de franquicias), enfrentando auditorías rigurosas y pagos de multas. Ciertamente los comerciantes y proveedores de servicios de tarjetas de crédito y débito, deberán validar su cumplimiento al estándar en forma periódica.

Cabe destacar que la validación es realizada por auditores autorizados: Qualified Security Assessor (QSAs). Sólo a las compañías que procesan menos de 80,000 transacciones por año se les permite realizar una autoevaluación a través de un cuestionario provisto por el Consorcio del PCI (PCI SSC).

Versiones de PCI DSS:

PCI DSS Ver 1.0 enero de 2005

PCI DSS Ver 1.1 septiembre de 2006

PCI DSS Ver 1.2 octubre de 2008

La versión actual 2.0 de PCI DSS está diseñada para proporcionar mayor claridad y flexibilidad, y así mejorar la comprensión de las normas y su implementación por parte de los empresarios y comerciantes.

Requerimientos de PCI DSS Versión 2.0

La versión de la norma (2.0) ha especificado 12 requerimientos para el cumplimiento, organizados en 6 secciones relacionadas lógicamente. A éstas se les ha denominado *objetivos de control*.

Los objetivos de control y sus requerimientos son los siguientes:

- Desarrollar y Mantener una Red Segura

- Requerimiento 1: Instalar y mantener una configuración de firewalls para proteger los datos de los propietarios de tarjetas.
- Requerimiento 2: No usar contraseñas del sistema y otros parámetros de seguridad predeterminados provistos por los proveedores.
- Proteger los Datos de los propietarios de tarjetas
 - Requerimiento 3: Proteger los datos almacenados de los propietarios de tarjetas.
 - Requerimiento 4: Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.
- Mantener un Programa de Manejo de Vulnerabilidad
 - Requerimiento 5: Usar y actualizar regularmente un software antivirus.
 - Requerimiento 6: Desarrollar y mantener sistemas y aplicaciones seguras.
- Implementar Medidas sólidas de control de acceso
 - Requerimiento 7: Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información.
 - Requerimiento 8: Asignar una Identificación única a cada persona que tenga acceso a una computadora.
 - Requerimiento 9: Restringir el acceso físico a los datos de los propietarios de tarjetas.
- Monitorear y Probar regularmente las redes
 - Requerimiento 10: Rastrear y monitorear todo el acceso a los recursos de la red y datos de los propietarios de tarjetas.
 - Requerimiento 11: Probar regularmente los sistemas y procesos de seguridad.

- Mantener una Política de Seguridad de la Información.
 - Requerimiento 12: Mantener una política que contemple la seguridad de la información ⁴⁹

Actividades a desarrollar en cada uno de los requerimientos:

Requerimiento 1

- Reglas de configuración de firewall
- Segmentación de la red
- Proceso de control de cambios

Requerimiento 2

- Cambiar el *default* de configuración y acceso de administrador
- Estándares de configuración
- Cifrar los accesos a administrador desde terminales

Requerimiento 3

- Almacenar la información mínima
- No almacenar información sensible después de la autorización
- Enmascarar los números de cuenta cuando son mostrados
- Almacenar el PAN (número de tarjeta) de manera no legible
- Manejo de claves de cifrado

Requerimiento 4

- Cifrar los datos enviados sobre redes públicas
- Nunca enviar el PAN en correo sin cifrado

⁴⁹ Véase https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf, revisado el 13 de febrero de 2012, 10:30hrs.

Requerimiento 5

- Mecanismos de actualización de antivirus

Requerimiento 6

- Manejo de parches y control de cambios
- Proceso de manejo de vulnerabilidades
- Proceso de control de cambios
- Controles en el desarrollo de software
- Desarrollo seguro de software
- Proteger las aplicaciones Web públicas de ataques

Requerimiento 7

- Implementar control de acceso basado en roles de los empleados

Requerimiento 8

- Autenticación con contraseña
- Cifrar las contraseñas durante la transmisión y almacenamiento en todos los componentes del sistema
- Acceso remoto con autenticación de doble factor
- Administración de usuarios, cuentas, contraseñas
- Autenticar y registrar todos los accesos a bases de datos con información de tarjetahabientes

Requerimiento 9

- Cámaras a los sistemas que almacenan, procesan o transmiten datos de las tarjetas
- Procedimientos de control de acceso físico

- Almacenamiento de Backups
- Control de acceso a medios que contienen información de tarjetahabientes
- Manejo y control de medios

Requerimiento 10

- Centralización de registros (logs) de eventos de accesos a datos de tarjetahabientes
- Control de acceso a registros (logs)
- Software de integridad de los archivos de registro (log)
- Reloj único
- Retención de registros de log de 1 año

Requerimiento 11

- Búsqueda de vulnerabilidades cada trimestre
- Prueba de penetración cada año
- Uso de IDS (Intrusion Detection System), IPS (Intrusion Protection System)
- Herramienta de integridad de archivos

Requerimiento 12

- Política para el ambiente de los tarjetahabientes
- Establecer, actualizar y divulgar la política de seguridad
- Responsabilidades
- Programa de Concienciación
- Procedimientos de contratación de personal
- Contratos de terceros para compartir información de tarjetahabientes
- Plan de respuesta a incidentes

- Conexión con terceros
- Evaluación de riesgos del ambiente del tarjetahabiente⁵⁰

III.1.6.3 Objetivos de control y requerimientos que aplican para la protección de datos personales

La información que proporciona el tarjetahabiente para el manejo de las tarjetas de crédito y débito es de carácter personal (datos de identificación, financieros y patrimoniales). De modo que todas las empresas que realicen algún tipo de tratamiento de estos datos tendrán que cumplir con el estándar PCI DSS. Por esta razón, cada uno de los objetivos de control y requerimientos previstos en dicho estándar y descritos anteriormente aplican para la protección de datos personales.

⁵⁰ Véase <http://www.acis.org.co/fileadmin/Conferencias/PresentacionPCI.pdf>, revisado el 13 de febrero de 2012, 13:00hrs.

III.2 ÁMBITO INTERNACIONAL

III.2.1 Europa

III.2.1.1 España

III.2.1.1.1 La Agencia Española de Protección de Datos y la legislación española en materia de seguridad

La Agencia Española de Protección de Datos (AEPD) es la institución encargada de cuidar y fomentar la privacidad y la protección de datos personales de los españoles. Como todos sabemos España es un país que pertenece a la Unión Europea. Esta realidad le da una dimensión muy distinta a la figura de encargado y a las medidas de seguridad de la información en relación a México. Sin embargo, ahondar en el caso español puede ser muy esclarecedor para comprender y mejorar la situación de nuestro país en este tema. Para ello, es necesario tener una visión general sobre lo que su legislación dicta al respecto y conocer –al menos someramente—las publicaciones que ha editado la Agencia sobre mejores prácticas en seguridad.

El estatuto de la AEPD fue aprobado a través del Real Decreto 428/1993 (26 de marzo de 1993), definiendo a la Agencia como un “ente de Derecho público”⁵¹ con personalidad jurídica propia y plena capacidad pública y privada. En este documento se establece como función general de la AEPD: “Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.”⁵²

⁵¹ Artículo 1 del Real Decreto 428/1993, DE 26 DE MARZO, POR EL QUE SE APRUEBA EL ESTATUTO DE LA AGENCIA DE PROTECCIÓN DE DATOS, <http://www.boe.es/boe/dias/1993/05/04/pdfs/A13244-13250.pdf>, revisado el 20 de enero de 2012, 17:00hrs.

⁵² Véase <https://www.agpd.es/portaleswebAGPD/conozca/funciones/index-ides-idphp.php>, revisado el 23 de enero de 2012, 11:00hrs.

No obstante la claridad del párrafo anterior, es pertinente enlistar las funciones concretas de la AEPD:

En relación con los afectados

- Atender a sus peticiones y reclamaciones.
- Información de los derechos reconocidos en la Ley.
- Promover campañas de difusión a través de los medios.

En relación con quienes tratan datos

- Emitir autorizaciones previstas en la Ley.
- Requerir medidas de corrección.
- Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.
- Ejercer la potestad sancionadora.
- Recabar ayuda e información que precise.
- Autorizar las transferencias internacionales de datos.

En la elaboración de normas

- Informar los Proyectos de normas de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD).
- Informar los Proyectos de normas que incidan en materias de protección de datos.
- Dictar Instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD.
- Dictar recomendaciones en materia de seguridad y control de acceso a los ficheros.

En materia de telecomunicaciones

- Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente.

Otras funciones

- Velar por la publicidad en los tratamientos, publicando anualmente una lista de los mismos (CD).
- Cooperación Internacional.
- Representación de España en los foros internacionales en la materia.
- Control y observancia de lo dispuesto en la Ley reguladora de la Función Estadística Pública.
- Elaboración de una Memoria Anual, presentada por conducto del Ministro de Justicia a las Cortes.”⁵³

III.2.1.1.2 Encargado y medidas de seguridad en la legislación española

Con el fin de tener un mejor entendimiento sobre lo relacionado a la figura de encargado y las medidas de seguridad expuestas en la Ley Orgánica 15/1999 (13 de diciembre de 1999), de Protección de Datos de Carácter Personal (LOPD), podemos encontrar que el artículo 3, inciso g, define al encargado del tratamiento de la siguiente manera: “La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo

⁵³ Véase <https://www.agpd.es/portalwebAGPD/conozca/funciones/index-ides-idphp.php>, revisado el 23 de enero de 2012, 11:30hrs.

que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.”⁵⁴

Asimismo, el artículo 9 sobre Seguridad de los datos establece que tanto el responsable como el encargado del tratamiento deberán adoptar medidas de índole técnica y organizativas, que garanticen la seguridad de los datos de carácter personal para evitar su alteración, pérdida, tratamiento o acceso no autorizado. Para ello, se tomará en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos.

Por su parte, el Real Decreto 1720/2007 (21 de diciembre de 2007), aprueba el Reglamento de desarrollo de la LOPD y establece en el Título VIII, Capítulo I, Artículo 80, que las medidas de seguridad exigibles a las bases de datos (ficheros) y tratamientos se deben clasificar en tres niveles: básico, medio y alto.

Cabe señalar que dicho Reglamento establece las medidas de seguridad aplicables a bases de datos y tratamientos, tanto automatizados como no automatizados. Tomando en cuenta que este Reglamento ha sido considerado como apegado a mejores prácticas y estándares internacionales en materia de seguridad de la información, lo presentamos a continuación de manera resumida:

⁵⁴ Véase <http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>, revisado el 16 de enero de 2012, 17:00hrs.

1. FICHEROS (BASES DE DATOS) Y TRATAMIENTOS
AUTOMATIZADOS

NIVEL DE SEGURIDAD	ARTÍCULO	MEDIDAS DE SEGURIDAD
BÁSICO	89	Funciones y obligaciones del personal
	90	Registro de incidencias
	91	Control de acceso
	92	Gestión de soportes y documentos
	93	Identificación y autenticación
	94	Copias de respaldo y recuperación
MEDIO	95	Responsable de seguridad
	96	Auditoría
	97	Gestión de soportes y documentos
	98	Identificación y autenticación
	99	Control de acceso físico
	100	Registro de incidencias
ALTO	101	Gestión y distribución de soportes

NIVEL DE SEGURIDAD	ARTÍCULO	MEDIDAS DE SEGURIDAD
	102	Copias de respaldo y recuperación
	103	Registro de accesos
	104	Telecomunicaciones

2. FICHEROS (BASES DE DATOS) Y TRATAMIENTOS NO AUTOMATIZADOS

NIVEL DE SEGURIDAD	ARTÍCULO	MEDIDAS DE SEGURIDAD
BÁSICO	105	Obligaciones comunes
	106	Criterios de archivo
	107	Dispositivos de almacenamiento
	108	Custodia de los soportes
MEDIO	109	Responsable de seguridad
	110	Auditoría
ALTO	111	Almacenamiento de la información
	112	Copia o reproducción
	113	Acceso a la documentación
	114	Traslado de documentación

III.2.1.1.3 Mejores prácticas y estándares en materia de protección de datos

La Agencia Española de Protección de Datos ha emitido un documento denominado *Guía de Seguridad de Datos*, cuya finalidad es la de facilitar a los responsables de ficheros (bases de datos) y a los encargados de tratamientos de datos personales la adopción de las disposiciones del Reglamento (RLOPD). Dicha guía recoge una serie de mejores prácticas en materia de protección de datos personales.

Ahora bien, respecto a los niveles de seguridad se menciona que la clasificación de los niveles de seguridad se realiza conforme a la naturaleza de la información tratada y a la necesidad de garantizar la confidencialidad y la integridad de la información.

CLASIFICACIÓN⁵⁵

NIVEL ALTO. Ficheros o tratamientos con datos:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;
- recabados con fines policiales sin consentimiento de las personas afectadas; y
- derivados de actos de violencia de género.

NIVEL MEDIO. Ficheros o tratamientos con datos:

- relativos a la comisión de infracciones administrativas o penales;
- que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);

⁵⁵ La clasificación que se muestra fue tomada del apartado “Niveles de seguridad” de la Guía de Seguridad de Datos, la cual se basa en el artículo 80 del Reglamento de la LOPD.

- de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;
- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y
- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.⁵⁶

NIVEL BÁSICO. Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
- se trate de ficheros o tratamientos de estos tipos de datos de forma incidental o accesorio, que no guarden relación con la finalidad del fichero; y
- en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

⁵⁶ Para esta categoría además deberá disponerse de un registro de accesos.

Lo cierto es que las medidas de seguridad son acumulativas de acuerdo al nivel de seguridad exigible. Es decir, para bases de datos que requieran de medidas de seguridad de nivel medio se deberá cubrir también las de nivel básico, y para el nivel alto se deberá de adoptar las medidas de seguridad de nivel básico y de nivel medio.

Dentro de la guía de la AEPD encontramos un cuadro-resumen de medidas de seguridad que es importante considerar. A continuación lo reproducimos:

	Nivel Básico		
	Nivel Medio		Nivel Alto
RESPONSABLE DE SEGURIDAD		El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad).	El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.
PERSONAL	Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. Definición de las funciones de control y las autorizaciones delegadas por el responsable. Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.		
INCIDENCIAS	Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. Procedimiento de notificación y gestión de las incidencias.	SOLO FICHEROS AUTOMATIZADOS Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. Autorización del responsable del fichero para la recuperación de datos.	
CONTROL DE ACCESO	Relación actualizada de usuarios y accesos autorizados. Control de accesos permitidos a cada usuario según las funciones asignadas. Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. Concesión de permisos de acceso sólo por personal autorizado. Mismas condiciones para personal ajeno con acceso a los recursos de datos.	SOLO FICHEROS AUTOMATIZADOS Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	SOLO FICHEROS AUTOMATIZADOS Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. Revisión mensual del registro por el responsable de seguridad. Conservación 2 años. No es necesario este registro si el responsable del fichero es una persona física y es el único usuario. SOLO FICHEROS NO AUTOMATIZADOS Control de accesos autorizados. Identificación accesos para documentos accesibles por múltiples usuarios.

	Nivel Básico	Nivel Medio	Nivel Alto
IDENTIFICACIÓN Y AUTENTICACIÓN	<p>SOLO FICHEROS AUTOMATIZADOS</p> <p>Identificación y autenticación personalizada.</p> <p>Procedimiento de asignación y distribución de contraseñas.</p> <p>Almacenamiento ininteligible de las contraseñas.</p> <p>Periodicidad del cambio de contraseñas (<1 año).</p>	<p>SOLO FICHEROS AUTOMATIZADOS</p> <p>Limite de intentos reiterados de acceso no autorizado.</p>	
GESTIÓN DE SOPORTES	<p>Inventario de soportes.</p> <p>Identificación del tipo de información que contienen, o sistema de etiquetado.</p> <p>Acceso restringido al lugar de almacenamiento.</p> <p>Autorización de las salidas de soportes (incluidas a través de e-mail) Medidas para el transporte y el desecho de soportes.</p>	<p>SOLO FICHEROS AUTOMATIZADOS</p> <p>Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.</p>	<p>SOLO FICHEROS AUTOMATIZADOS</p> <p>Sistema de etiquetado confidencial.</p> <p>Cifrado de datos en la distribución de soportes.</p> <p>Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).</p>
COPIAS DE RESPALDO	<p>SOLO FICHEROS AUTOMATIZADOS</p> <p>Copia de respaldo semanal.</p> <p>Procedimientos de generación de copias de respaldo y recuperación de datos.</p> <p>Verificación semestral de los procedimientos.</p> <p>Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita.</p> <p>Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.</p>		<p>SOLO FICHEROS AUTOMATIZADOS</p> <p>Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.</p>
CRITERIOS DE ARCHIVO	<p>SOLO FICHEROS NO AUTOMATIZADOS</p> <p>El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)</p>		

	Nivel Básico	Nivel Medio	Nivel Alto
ALMACENAMIENTO	SOLO FICHEROS NO AUTOMATIZADOS Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.		SOLO FICHEROS NO AUTOMATIZADOS Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave.
CUSTODIA SOPORTES	SOLO FICHEROS NO AUTOMATIZADOS Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.		SOLO FICHEROS NO AUTOMATIZADOS Sólo puede realizarse por los usuarios autorizados. Destrucción de copias desechadas.
COPIA O REPRODUCCIÓN		Al menos cada dos años, interna o externa. Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. Verificación y control de la adecuación de las medidas. Informe de detección de deficiencias y propuestas correctoras. Análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero.	
AUDITORIA			SOLO FICHEROS AUTOMATIZADOS Transmisión de datos a través de redes electrónicas cifradas.
TELECOMUNICACIONES			SOLO FICHEROS NO AUTOMATIZADOS Medidas que impidan el acceso o manipulación.
TRASLADO DOCUMENTACIÓN			

En relación al documento de seguridad, la AEPD incluye dentro de la misma Guía de Seguridad de Datos un modelo de este documento, cuyo contenido está estructurado de la siguiente forma:

- Ámbito de aplicación del documento.
- Métodos, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos.
- Información y obligaciones del personal.
- Procedimientos de notificación, gestión y respuestas ante las incidencias.
- Procedimientos de revisión.
- Nueve anexos (descripción de ficheros, nombramientos, autorizaciones de salida o recuperación de datos, delegación de autorizaciones, inventario de soportes, registro de incidencias, encargados de tratamiento, registro de entrada y salida de soportes y medidas alternativas).

Además, el Reglamento de la LOPD establece en sus artículos 96, para el caso de ficheros y tratamientos automatizados, y 110, para el caso de ficheros y tratamientos no automatizados, que a partir del nivel medio de seguridad requerido, estos deberán someterse, al menos cada dos años, a una auditoría interna o externa.

Como resultado de las auditorías se deberá generar un informe. Éste será desarrollado por el responsable de seguridad. Enseguida se entregará al responsable del fichero y a disposición de la Agencia Española de Protección de Datos, o en su caso, a las autoridades de control de las entidades autónomas.

Por último, es importante señalar que la Agencia Española de Protección de Datos ha publicado documentos que permiten –tanto a los responsables como a los encargados del tratamiento de bases de datos–

cumplir con las medidas de seguridad para la protección de datos personales. De igual forma, la Asociación Española de Normalización y Certificación (AENOR) ha publicado, entre otras normas relacionadas a la seguridad de la información, las siguientes:

- Desde el 28 de noviembre de 2007: ISO/IEC 27001 como UNE-ISO/IEC 27001: 2007
- Desde el 9 de diciembre de 2009: ISO/IEC 27002 como UNE-ISO/IEC 27002: 2009

III.2.1.2 Reino Unido

III.2.1.2.1 Acto de Protección de Datos (DPA)

La legislación en el Reino Unido se basa en el DPA –por sus siglas en inglés– Data Protection Act 1998 y fue el resultado de los trabajos desarrollados durante el Acto del Parlamento del Reino Unido (APRU). Este documento se refiere a la legislación sobre el procesamiento de datos personales, el cual reemplazó al Acto de Protección de Datos 1984. El APRU entró en vigor el 1 de marzo de 2000.

De acuerdo a lo establecido en el Data Protection Act 1998, capítulo 29, se puede decir que el APRU se creó en la lógica de “adoptar la nueva disposición para la regulación sobre el procesamiento de la información relacionada a los individuos, incluyendo la obtención, posesión, uso o divulgación de esa información”.⁵⁷

El APRU tiene como objetivo promover estándares altos en el manejo de la información personal, así como proteger el derecho de los individuos a la privacidad.

⁵⁷ Véase <http://www.legislation.gov.uk/ukpga/1998/29/section/1>, revisado el 15 febrero 2012, 20:00hrs.

Y el DPA aplica para firmas que posean información sobre personas vivas; principalmente en formato electrónico, pero si es el caso también en papel.

Un aspecto de interés es la figura de **encargado** (Data processor). El encargado –de acuerdo a lo establecido en el DPA 1998— es la figura que procesa los datos personales en representación del verdadero responsable; es importante precisar que esta figura es diferente a la de un empleado del responsable. Sin embargo, los encargados no están sujetos directamente en este Acto.

De ahí, pues, que el encargado realice el procesamiento pertinente en vez de tomar las decisiones sobre el propósito del procesamiento o la forma en que se realiza.

Este Acto manifiesta obligaciones específicas sobre los responsables cuando el procesamiento de los datos personales es efectuado en su nombre por los encargados. Lo cierto es que el responsable tiene la responsabilidad completa –valga la redundancia— de las acciones llevadas a cabo por el encargado.⁵⁸

El Acto contiene una provisión que aplica en estas circunstancias; establece que cuando se tiene un encargado:

- se debe seleccionar un encargado que provea suficientes garantías sobre sus medidas de seguridad para proteger el procesamiento que hará en nombre del responsable;
- se debe revisar razonablemente que esas medidas de seguridad están llevándose a la práctica;

⁵⁸ Véase [Data_protection_act_legal_guidance.pdf](http://www.gillhams.com/dictionary/235.cfm), p. 17, revisado el 15 febrero 2012, 21:00hrs. <http://www.gillhams.com/dictionary/235.cfm>, revisado el 14 febrero de 2012, 19:00hrs y http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx, revisado el 16 de febrero de 2012, 17:30hrs.

- debe existir un contrato por escrito en el cual se establezca lo que el encargado tiene permitido realizar con los datos personales, para lo cual existe un modelo de contrato publicado por el Comité Europeo para la Estandarización.⁵⁹

En la Oficina del Comisionado de Información y en la legislación en materia de seguridad se contemplaba –con base en el Acto de 1984– la figura del Secretario de Protección de Datos. Éste cambiaría su denominación a Comisionado de la Protección de Datos. Con el paso del tiempo se hicieron algunas consideraciones más dentro del Acto de la Libertad de la Información, concretamente en el 2000, provocando que la figura modificara nuevamente su nombre: actualmente se le conoce como Comisionado de la Información.⁶⁰

III.2.1.2.2 La Oficina del Comisionado de Información y la legislación en materia de seguridad

La Oficina del Comisionado de Información (ICO) es una autoridad independiente en el Reino Unido, que se creó para defender los derechos de información de interés público, y para promover la apertura de los organismos públicos y la privacidad de los datos de los individuos.

¿Cuáles serían pues las funciones del Comisionado? A continuación las enlistamos:

- Promover las buenas prácticas y proporcionar información; brindar consejos a las organizaciones sobre cómo permitir el acceso a la información que tienen en su poder; y proteger los datos personales de los individuos.

⁵⁹ Véase http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx, revisado el 16 de febrero 2012, 24:00 hrs.

⁶⁰ Véase http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf revisado el 16 de febrero 2012, 23:00hrs.

- Resolver la problemática en torno a la violación de la información y dar respuesta a las personas que se quejen porque sus derechos fueron violados.
- Aplicar sanciones legales para aquellos que ignoren o no lleven a cabo sus obligaciones.

Es importante destacar que todas las organizaciones que poseen información personal (responsables) deben notificar al ICO, salvo algunas excepciones marcadas por esta Oficina. La notificación se refiere a un proceso en el que el responsable le proporciona detalles al ICO: detalles sobre el procesamiento que está dando a los datos personales. En consecuencia, la ICO tiene la obligación de publicar el perfil de los detalles y el registro de responsables; esta información puede ser revisada por el público en general, y debe incluir el nombre y la dirección de los responsables, y una descripción del tipo de procesamiento que están llevando a cabo con los datos obtenidos.⁶¹

Las obligaciones de la ICO con relación al Acto son las siguientes:

- Dar seguimiento de las buenas prácticas realizadas por los responsables; en particular promover la observancia de los requerimientos establecidos en el Acto para los responsables.
- Difundir la información sobre el Acto y sobre cómo funciona.
- Incentivar el desarrollo de Códigos de Práctica como guía para las mejores prácticas.
- Cooperar con las autoridades extranjeras designadas en la forma prescrita en la sección 54 del Acto y por la Orden 200 de Protección de Datos (S.I. No. 186).

⁶¹ En relación con este tema, se recomienda consultar http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx y http://www.ico.gov.uk/for_organisations/sector_guides/business.aspx.

- Mantener un registro de los responsables que son requeridos para notificar su procesamiento.
- Presentar anualmente ante cada Casa del Parlamento un reporte general del ejercicio de sus funciones consideradas bajo el Acto.
- Presentar ante cada Casa del Parlamento cualquier Código de Práctica elaborado conforme al Acto.
- Procesar a las personas que hayan cometido alguna violación de acuerdo con lo establecido en el Acto.⁶²

III.2.1.2.3 Mejores prácticas y estándares

Lo primero que se tiene que considerar en este punto, es la seguridad de los datos y las medidas de seguridad.

En cuanto a las medidas de seguridad, el DPA ha establecido lo siguiente: "Principio 7: Se deben tomar medidas técnicas y organizacionales apropiadas en contra del procesamiento sin autorización o ilegal de los datos personales así como en contra de pérdida accidental, destrucción o daño a los datos personales".⁶³

Con base en lo anterior se sugiere diseñar un modelo organizacional de seguridad, acorde con el tipo de datos personales que se poseen y acorde también con las contingencias de vulneración a la seguridad de la información. Sin duda, se debe identificar con claridad quién es el responsable de asegurar la seguridad de la información, aunado a un sistema viable de seguridad física y técnica. Si se cuenta con estos elementos se podrá responder de manera efectiva y rápida ante una vulneración o daño.⁶⁴

⁶² Véase Data_protection_act_legal_guidance.pdf, p. 89; y Data Protection Act1998.pdf, p. 50, revisado 15 febrero 2012.

⁶³ Cita tomada de 1_Data Protection Act 1998.pdf, p. 78, revisado el 14 febrero 2012, 18:00hrs.

⁶⁴ Véase http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx, revisado el 16 de febrero de 2012, 23:00hrs.

En este orden de ideas es importante considerar el principio 8: “Los datos personales no deben ser transferidos a un país o territorio fuera del área económica europea, salvo que ese país o territorio garantice un nivel adecuado de protección de los derechos y libertades de los titulares en relación con el procesamiento de los datos personales”.⁶⁵

Tomando en cuenta lo anterior, la ICO ha diseñado notas y códigos de buenas prácticas, que a continuación se muestran:

A) Nota de buenas prácticas de datos personales. Seguridad de Información Personal (Data Protection Good Practice Note Security of Personal Information):

Con el objetivo de aplicar buenas prácticas de seguridad para la información personal, la ICO (Information Commissioner’s Office) desarrolló *Data Protection Good Practice Note Security of personal information*. Este esquema es una nota de buenas prácticas y su objetivo es alertar a las pequeñas y medianas organizaciones sobre las medidas de seguridad que deben tener para proteger la información personal que poseen.

El DPA 1998 requiere que todas las organizaciones tengan la seguridad apropiada para proteger la información personal contra la divulgación ilegal o desautorizada, la pérdida accidental, destrucción o daño de la misma.

Por obvias razones las pequeñas y medianas empresas tienen menos experiencia en seguridad interna. No cabe duda que esta guía les puede

⁶⁵ Idem.

indicar el camino más apropiado para introducirse en el tema de la seguridad de la información. Veamos algunas recomendaciones:⁶⁶

- Revisar que información poseen y determinar que tan valiosa y sensible es dicha información.
- Identificar quién está a cargo de las medidas de seguridad.
- Considerar las medidas siguientes de seguridad:
 - Medidas organizacionales
 - Staff
 - Seguridad Física
 - Seguridad de las computadoras

B) Nota de buenas prácticas para protección de datos personales
(Lista de entrenamiento para pequeñas y medianas empresas) (*Data Protection Good Practice Note*):

Los vacíos en la esfera de seguridad informática es una preocupación pública legítima. Este problema ha ido creciendo en el ámbito del manejo de la información personal. Ahora bien, debido a que los incidentes de seguridad involucran al staff, existe una clara necesidad de que los trabajadores tengan el entendimiento básico sobre el DPA 1998.

En consecuencia, esta guía destaca algunas de las implicaciones prácticas del DPA. Principalmente se dirige al staff de una oficina de pequeñas y medianas empresas.

⁶⁶ Véase

http://www.ico.gov.uk/upload/documents/library/practical_application/trainingchecklist_v1_web_version.pdf, Data Protection Good Practice Note Security of personal information), revisado el 16 febrero de 2012, 21:00 hrs.

Veamos algunas recomendaciones:⁶⁷

- Guardar la información personal de manera segura.
- Conocimiento de las expectativas razonables de los clientes y empleados.
- No proporcionar información personal del cliente vía telefónica.
- Notificación de acuerdo a lo establecido en el DPA.
- Manejar las solicitudes de las personas sobre su información personal.

C) Código de Práctica de compartición de Datos (*Data Sharing Code of Practice*):⁶⁸

Por compartición de datos se entiende la divulgación de datos de una o más organizaciones hacia un tercero. También se refiere a la compartición de datos e información entre diferentes partes de una misma organización.

Este código ha sido elaborado por la ICO y publicado bajo la sección 52 del DPA. Provee consejo práctico para todo tipo de organización –sean públicas, privadas o terceros– que comparten datos y que cubren medidas sistemáticas de compartición de datos, así como requerimientos ad hoc o únicos para compartir datos personales. Cabe mencionar que, aun cuando el DPA establece requerimientos que deben ser considerados cuando se comparten datos, no proporciona las medidas prácticas que se deben llevar a cabo en la compartición de datos.

⁶⁷ Véase http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/training_checklist_v1_web_version.pdf, revisado el 16 febrero de 2012, 21:00 hrs.

⁶⁸ Véase http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/data_sharing.aspx, revisado el 18 febrero de 2012, 21:00 hrs.

Lo cierto es que dicho código está enfocado principalmente hacia la compartición de los datos personales entre responsables. No obstante, existe también en la relación entre responsables y encargados.

El DPA requiere a las organizaciones que tengan medidas organizacionales y técnicas apropiadas para la compartición de datos, por lo que se recomienda lo siguiente:

- Revisar los datos personales que se reciben de otras organizaciones, asegurándose –por un lado– el conocimiento de su origen, y si existen –por el otro– algunas condiciones sobre el uso de éstos.
- Revisar el tipo de datos personales que comparten las organizaciones entre si, asegurándose de conocer quién tiene acceso a éstos y para qué serán utilizados.
- Evaluar si se comparten datos sensibles.
- Identificar quién tiene acceso a la información y qué organizaciones han compartido dicha información.
- Evitar que todo el staff tenga acceso a la información que se comparte con otras entidades. Deben establecerse candados para que sólo el personal autorizado maneje la información.
- Desarrollar estudios y análisis del efecto que provocaría una violación de la seguridad informática en las personas y en la organización.
- Es muy importante que el staff conozca las políticas de seguridad y procedimientos.

Tomando en cuenta todo lo anterior, es pertinente considerar los siguientes ámbitos de seguridad:

- Seguridad Física
- Seguridad Técnica

D) Código de práctica de información personal en línea (*Personal information online code of practice*):⁶⁹

Este código explica el procedimiento de aplicación del DPA para la recolección y uso de datos personales en línea. La recolección puede ser vía PC, consola de juegos, teléfonos móviles, reproductor multimedia o a través de cualquier equipo que se conecte al Internet. Las actividades que cubre son tres:

- Recolección de datos a través de formularios de inscripción en línea.
- Uso de “cookies” o direcciones IP que permitan identificar el contenido de un individuo en particular.
- Uso de la nube para procesar datos personales.

Este Código fue elaborado por la ICO bajo la sección 51 del DPA, con la intención de promover las buenas prácticas. En realidad es la interpretación de la ICO sobre los requerimientos del Acto cuando los datos personales son recolectados y utilizados en línea.

En el caso de la información en línea es difícil establecer la identificación de una persona, pues un equipo puede tener varios usuarios.

En el caso de la prestación de servicios o de contenidos en línea, es posible que un número de responsables –y posiblemente de encargados– actúen de manera conjunta. Por ello, las organizaciones deberán establecer con claridad quién tendrá la responsabilidad legal.

Así pues, es una buena práctica organizacional explicar al público quién y cómo utiliza su información. El editor de sitios web debe asumir la

⁶⁹ Véase

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf revisado el 18 febrero de 2012, 20:00hrs.

responsabilidad sobre la información que colecta y coloca en la red. También es responsabilidad de los terceros la recolección llevada a cabo en un sitio web, pues éstos tienen obligaciones de acuerdo a lo establecido por el DPA.

Ahora bien, en caso que los responsables utilicen un encargado para proveer servicios en su nombre, deberá existir un contrato por escrito en el cual se estipule que se garantizan los rangos de seguridad acordados.

Para resguardar los datos de manera segura, es una buena práctica incorporar desde el inicio procedimientos de seguridad y protección de la privacidad. Esto es, establecer claramente roles y responsabilidades, tener un registro sobre el lugar donde la información es almacenada y dar seguimiento a la forma en que se colecta la información, ya sea vía correo electrónico, sitios web, etc.

No olvidemos que cuando un miembro del staff renuncia o es expulsado de la organización, el acceso a la información debe ser revocado inmediatamente para dicha persona.

E) Cómputo en la nube (*Cloud computing*):⁷⁰

Los servicios de software, plataformas o infraestructura en la nube generalmente los proporciona una red de servidores de una empresa externa. Es decir, son servicios que brinda un tercero a través de internet. Actualmente son muy pocos los casos en que el cómputo en la nube se realice de manera interna.

El uso de la nube es cada vez mayor por todos los beneficios que representa. Sin embargo, también debe considerarse las implicaciones

⁷⁰ En el tema de la nube se recomienda consultar:
http://www.ico.gov.uk/for_organisations/data_protection/overseas.aspx y
<https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>

legales que encierra, aún cuando todavía no existe una ley específica para esta modalidad.

El término cómputo en la nube se refiere a un sistema en la Web que permite a las organizaciones tener acceso a un grupo o red de recursos informáticos. Esto significa que pueden resguardar la información que consideren importante en una nube de cómputo. Ciertamente la información que se suba a la nube es propiedad de la organización, pero el mantenimiento del sistema informático en internet lo hace un tercero. De ahí lo delicado y complejo de este sistema. Existen diversos tipos de cómputo en la nube dependiendo de cómo se ha implementado o el tipo de red que cubre. Sin embargo, todos tienen aspectos legales similares, que en este momento no son muy claros, pues se encuentran en proceso de desarrollo.

El principal reto, desde un punto de vista legal, lo reviste la pérdida de control. En el Reino Unido se han dado casos de pérdida de información en la Web, esto ha impactado la gobernanza de la información y también ha afectado el cumplimiento de la legislación.

En este orden de ideas, las áreas legales clave que se deben considerar son las siguientes:

- Cumplimiento de la seguridad y protección de los datos
- Jurisdicción
- Confidencialidad
- Libertad de información
- Derechos reservados (copyright)
- Igualdad en la legislación
- Ley del contrato

Lo cierto es que al utilizar un servicio en la nube, la institución que lo haga será responsable del cumplimiento del DPA cuando se procesen datos personales. Asimismo el proveedor de la nube será considerado el encargado, de tal suerte que deberá actuar en concordancia con los términos acordados en el contrato. De esta manera se asegura el cumplimiento del DPA. El contrato puede hacerse de manera escrita o electrónica, pero estableciendo que el proveedor del servicio sólo actuará de acuerdo con las instrucciones del responsable y en el mismo nivel de seguridad de éste.

Un aspecto a destacar es la transferencia de datos fuera del área económica europea (EEA). El DPA ha estipulado que no deben transferirse datos fuera del EEA, salvo que se tengan los niveles adecuados de seguridad y protección informática.

Los proveedores de la nube almacenan y mueven datos alrededor de múltiples servidores localizados en diversas jurisdicciones, las cuales pueden estar fuera del EEA. De ser así, se podría provocar una violación al DPA si no se tienen los niveles adecuados de seguridad. Para dar cumplimiento al DPA deberá contarse con un contrato que incluya los términos establecidos en el DPA.

Las relaciones comerciales entre el Reino Unido y EE.UU. son muy importantes. Por eso para validar la información que provenga de los Estados Unidos será suficiente que la organización esté inscrita en el Safe Harbor.

El CSA –por sus siglas en inglés– Cloud Security Alliance ha llevado a cabo varias investigaciones sobre iniciativas relacionadas a la seguridad en la nube, incluyendo una iniciativa para crear estándares que midan la

seguridad del cómputo en la nube. Estas actividades están relacionadas particularmente con el NIST.⁷¹

F) Foro de Seguridad de la Información:⁷²

El ISF –por sus siglas en inglés, Information Security Forum— fue fundado en 1989, como una organización independiente, sin fines de lucro. Se integró mediante la unión de varias organizaciones líderes a nivel mundial. Es un Foro que se dedica a la investigación, aclaración y solución de temas clave sobre seguridad de la información y administración de riesgo a través del desarrollo de mejores prácticas.

El Estándar de buenas prácticas 2011 contempla la perspectiva empresarial para la seguridad de la información. Para tal efecto, ha proyectado una base –muy práctica—que evalúe y en consecuencia mejore los acuerdos de seguridad de la información de una organización. La temática que aborda es de gran actualidad, por ejemplo, el cómputo en la nube y el almacenamiento de datos. De ahí, pues, que pueda emplearse para identificar, monitorear y controlar riesgos de la seguridad de la información de una organización.

Verdaderamente el Estándar 2011 cubre cada aspecto de la seguridad; se divide en cuatro categorías principales:

- Gobernanza de la seguridad
- Requerimientos de seguridad
- Marco de control
- Monitoreo y mejora de la seguridad

⁷¹ Véase <http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2137/Report-on-Cloud-Computing-and-the-Law-for-UK-FE-and-HE--An-Overview-31082011.aspx>, revisado el 18 febrero de 2012, 24:00 hrs.

⁷² Para este apartado se consultó: https://www.securityforum.org/userfiles/public/the-2011-standard-flyer_pub.pdf, revisado el 20 febrero de 2012, 1:30hrs; y <https://www.securityforum.org/downloadresearch/publicdownload2011sogp/>, revisado el 20 febrero de 2012, 1:30 hrs.

Y su aplicación ayuda a:

- facilitar el cumplimiento con el estándar ISO 27001, así como con otros estándares relevantes (ISO, COBIT, NIST, PCI DSS e ITIL);
- validar acuerdos de seguridad de la información con proveedores externos;
- proporcionar una fundación para información sobre evaluación de riesgos;
- construir las bases para políticas, estándares y procedimientos; y
- desarrollar o mejorar acuerdos de seguridad de la información específicos.

Este estándar cubre seis aspectos de la seguridad de la información; cada uno de ellos se relaciona con un tipo de ambiente en particular. Veamos a continuación cuáles son:

- Administración de la seguridad (SM)
- Aplicaciones de negocio críticas (CB)
- Instalaciones computacionales (CI)
- Redes (NW)
- Desarrollo de sistemas (SD)
- Ambiente de usuario final (UE)

El estándar 2011 establece siete formas para asegurar la seguridad de la información:

- Cumplimiento
- Validación del proveedor
- Evaluación del riesgo
- Políticas, estándares y procedimientos
- Conciencia

- Evaluación de la seguridad de la información
- Medidas de seguridad

III.2.2 América

III.2.2.1 Estados Unidos

III.2.2.1.1 Antecedentes

En el ámbito de la protección de datos personales en posesión de los particulares, Estados Unidos de Norteamérica cuenta con regulaciones en materia de privacidad y medidas de seguridad exigibles a los responsables y encargados de datos personales, tanto sectoriales como estatales. Por esta razón, presentamos a continuación una breve descripción de lo que en esta materia contempla tanto la Comisión Federal de Comercio (FTC), el Acto de Privacidad (Privacy Act), el Acto HIPAA (Health Insurance Portability and Accountability Act of 1996) como la legislación de algunos estados que regulan sobre privacidad y protección de los datos personales.

III.2.2.1.2 La legislación norteamericana en materia de seguridad

III.2.2.1.2.1 Ámbito Federal

Acto de Privacidad (Privacy Act)

El PA 1974 establece un código de prácticas justas que regulan la recolección, mantenimiento, uso y divulgación de la información de los individuos que se encuentra en los sistemas de registro de las agencias federales de los Estados Unidos. Este Acto le requiere a las agencias que proporcionen un aviso público de sus sistemas de registros publicándolos en el Registro Federal.

Además, prohíbe la divulgación de la información personal si no existe un contrato en el cual se establezca el consentimiento del individuo, salvo que se encuentre dentro de las excepciones contempladas en el PA.⁷³

El PA está relacionado con el FOIA –por sus siglas en inglés, Freedom of Information Act— y se encarga de lo siguiente:⁷⁴

- Regula las prácticas de almacenamiento y divulgación de registros de las agencias federales de gobierno.
- Permite a los individuos tener acceso sobre sus registros en las agencias federales.
- Requiere que la información personal que se encuentra en los archivos de las agencias sean exactos, completos, relevantes y actuales.
- Requiere que las agencias obtengan la información directamente del sujeto del registro y que la información obtenida sea utilizada para el propósito establecido.
- Provee soluciones para aquellos individuos cuyos derechos hayan sido violados.
- Provee al sujeto para que pueda impugnar la exactitud de la información.
- Reconoce la necesidad legítima de restringir la divulgación de cierta información.
- Requiere que cada agencia federal publique una descripción de cada sistema de registros administrada por una agencia que contenga información personal.
- Restringe la divulgación de información que identifique a una persona de las agencias federales.

⁷³ Véase <http://www.justice.gov/opcl/privacyact1974.htm> revisado el 20 de febrero de 2012, 22:30hrs.

⁷⁴ Véase <http://www.ftc.gov/foia/privactabout.shtm> revisado el 20 febrero de 2012, 21:00 hrs.; y <http://www.ftc.gov/ogc/brfovrw.shtm> revisado el 20 febrero de 2012, 22:00 hrs.

Código de los Estados Unidos de Norteamérica (United States Code)⁷⁵

El USC es la codificación por temas de las leyes generales y permanentes de los Estados Unidos de Norteamérica y se divide en amplios temas divididos en 50 títulos. Es publicado por la Oficina de Revisión Legislativa de la Cámara de Representantes de Estados Unidos.

Dentro del título 15 “Comercio y Negocios” capítulo 94, se considera el tema de la privacidad de la información personal. Hace un análisis en torno a la divulgación de la información personal privada y al acceso fraudulento de la información financiera.

Cada uno de estos subcapítulos se divide a su vez en secciones; en el caso de divulgación de la información trata lo siguiente:

- Protección de información personal privada
- Obligaciones respecto con la divulgación de la información personal
- Divulgación de la política de privacidad de la institución
- Reglamentación
- Ejecución
- Relación con otras disposiciones
- Relación con leyes estatales
- Estudio de la compartición de la información entre filiales financieras

Con relación al tema de la información financiera se refiere a lo siguiente:

- Protección de la privacidad de la información del cliente en instituciones financieras
- Aplicación de las medidas administrativas

⁷⁵ Véase <http://www.law.cornell.edu/uscode/text/15/chapter-94/subchapter-I> revisado el 22 febrero 2012, 24:00hrs.

- Sanción penal
- Relación con leyes estatales
- Agencia de orientación
- Reportes

Acto de Portabilidad y Rendición de Cuentas de la Seguridad de la Salud de 1996⁷⁶ (Health Insurance Portability and Accountability Act of 1996)

En la sección 1173(d) Estándares de seguridad para información de salud se establece que la Secretaría de Servicios de Salud y Humanos, deberá adoptar estándares de seguridad que tomen en cuenta las capacidades técnicas de los sistemas de registro utilizados para mantener la información de salud; los costos de las medidas de seguridad; la necesidad de capacitación de las personas que tengan acceso a la información de salud; el valor de rastros de auditoría en sistemas computarizados de registro; y las necesidades y capacidades de pequeños proveedores del cuidado de la salud y proveedores rurales del cuidado de la salud.

También se solicita garantizar que los centros de atención de la salud, si son parte de una organización más grande, tengan políticas y procedimientos de seguridad que permitan aislar las actividades de los centro con respecto a la información procesada. Este protocolo previene el acceso no autorizado a la información por parte de la organización de mayor tamaño.

Asimismo, se estipula que las personas que mantengan o transmitan información de salud establezcan controles razonables y apropiados de tipo administrativo, técnico y físico. El objeto de ello es:

⁷⁶ Véase https://www.cms.gov/HIPAAGenInfo/04_PrivacyandSecurityStandards.asp#TopOfPage, revisado el 17 de febrero de 2012. 14:00 hrs.

- asegurar la integridad y confidencialidad de la información;
- proteger contra cualquier amenaza o riesgo previsto a la seguridad e integridad de la información y usos no autorizados o divulgación de la información; y
- garantizar el cumplimiento de lo establecido anteriormente por parte de los oficiales y empleados de las personas que mantienen o transmiten información de salud.

Por último, este Acto contempla los tiempos de adopción de los estándares y las penalizaciones generales por incumplimiento de los requerimientos y estándares.

III.2.2.1.2.2 **Ámbito Estatal**

Estándares para la Protección de Información Personal de los residentes de Commonwealth

El estado de Massachusetts cuenta con un reglamento denominado *201 CMR 17.00: Estándares para la Protección de Información Personal de los residentes de Commonwealth*. Este establece disposiciones relativas a los estándares que deben cumplir aquellas personas que posean o traten información personal de algún habitante de la Commonwealth de Massachusetts.

Los objetivos del instrumento mencionado son los siguientes: garantizar la seguridad y confidencialidad de la información de clientes de acuerdo a los estándares de la industria correspondiente; proteger la información contra amenazas o riesgos previstos; y proteger contra el acceso no autorizados o uso de la información que pueda dar como resultado un daño o incomodidad a cualquier consumidor.

Con respecto al deber de proteger la información y los estándares para llevar a cabo la protección de la información personal, este reglamento estipula que los responsables deben desarrollar, implementar y mantener un programa detallado de seguridad de la información, que esté escrito en una o más partes accesibles, y que contenga controles administrativos, técnicos y físicos apropiados. Todo ello de acuerdo a lo siguiente:

- El tamaño, alcance y tipo de negocio de la persona obligada a salvaguardar la información personal;
- la cantidad de recursos disponibles de la persona obligada;
- la cantidad de datos almacenados; y
- la necesidad de seguridad y confidencialidad de la información tanto del consumidor como del empleado.

Por su parte, el artículo 17.03 fracción 2 establece –de forma enunciativa más no limitativa– el contenido del programa de seguridad. Se citan a continuación todos los incisos que deben cubrirse en dicho programa, puesto que estos cumplen con lo contemplado en diferentes modelos y estándares sobre políticas de seguridad.

Contenido del programa de seguridad de la información:

- La designación de uno o más empleados para mantener el programa de seguridad de la información.
- La identificación y evaluación de los riesgos internos y externos previsibles para la seguridad, confidencialidad y/o integridad de cualquier registro electrónico, en papel o en otro tipo de soporte que contenga información personal, y la evaluación y mejoramiento de la efectividad de controles actuales para limitar tales riesgos, incluyendo:
 - capacitación a empleados (temporales y contratados)

- cumplimiento de políticas y procedimientos por parte de los empleados
- medios para detectar y prevenir fallas de los sistemas de seguridad
- El desarrollo de políticas de seguridad para empleados relativos al almacenamiento, acceso y transportación de registros que contengan información personal fuera de las premisas de negocio.
- La imposición de medidas disciplinarias para violaciones de las reglas del programa de seguridad de la información.
- La prevención del acceso a registros que contengan información personal por parte de empleados que han terminado su relación laboral.
- La supervisión de proveedores de servicio mediante:
 - la selección y conservación de proveedores de servicios que sean capaces de mantener medidas de seguridad apropiadas para proteger la información personal conforme al reglamento y cualquier regulación federal aplicable; y
 - solicitar a dichos proveedores de servicios por contrato la implementación y mantenimiento de las mencionadas medidas de seguridad.
- Establecimiento de restricciones razonables en el acceso físico a registros que contengan información personal y almacenamiento de estos registros y datos en instalaciones cerradas con llave, áreas de almacenamiento o contenedores.
- Monitoreo para regular y garantizar que el programa de seguridad de la información esté operando de forma razonablemente calculada y, de esta forma, prevenir el acceso no autorizado o uso no autorizado de información personal. Con ello se elevarán los controles de información para limitar los riesgos.

- Revisión del alcance de las medidas de seguridad al menos una vez al año o cada vez que las prácticas de negocio lo permita. Esto evitará que las prácticas de seguridad o integridad de los registros que contienen información personal se comprometan.
- Documentación de las acciones tomadas conforme a cualquier incidente que implique una brecha de seguridad; y revisión obligatoria después de un incidente de los eventos y acciones tomadas para realizar cambios en las prácticas del negocio relacionadas con la protección de la información personal.

Cabe señalar que el presente reglamento también incluye requerimientos precisos para aquellos responsables o encargados que almacenen o transmitan información de forma electrónica. A continuación presentamos los requerimientos:

- Protocolos seguros de autenticación de usuarios:
 - Control de IDs de usuarios y otros identificadores;
 - Método de asignación y selección de contraseñas o uso de tecnologías de identificación única (biométricos o tokens);
 - Control de contraseñas de datos de seguridad para garantizar que son guardados en una ubicación y/o formato que no comprometa la seguridad de los datos que protegen;
 - Acceso restringido únicamente a usuarios activos o cuentas de usuarios activos; y
 - Bloqueo de acceso de identificación de usuario después de múltiples intentos no exitosos o limitación de acceso para el sistema en particular.

- Medidas de seguridad de control de acceso que:
 - restrinjan el acceso a registros y archivos que contengan información personal para aquellos que requieran dicha información en el desarrollo de sus funciones laborales; y
 - asignen identificaciones únicas además de contraseñas a cada persona que tenga acceso a computadoras, para mantener la integridad de la seguridad de los controles de acceso.
- Cifrado de todos los registros y archivos transmitidos que contengan información personal y viajen a través de redes públicas o sean transmitidos de forma inalámbrica.
- Monitoreo de sistemas para detección de uso no autorizado o acceso a información personal.
- Cifrado de toda la información personal almacenada en laptops u otros dispositivos portátiles.
- Protección por medio de firewalls actualizados y parches para aquellos archivos que contengan información personal y se encuentren en un sistema conectado a Internet, con el fin de mantener la integridad de la información.
- Software de agentes de seguridad del sistema que incluyan protección malware, parches y definición de virus.
- Capacitación de empleados en el uso apropiado de sistemas de seguridad computacionales, ponderando la importancia de la seguridad de la información personal.

Estatutos Revisados de Nevada (Nevada Revised Statutes)⁷⁷

Dentro de los Estatutos Revisados de Nevada (NRS) el capítulo 603A trata específicamente sobre la seguridad de la información personal. Aquí se establece, bajo el título de "Regulación de Prácticas de Negocio" en sus

⁷⁷ Véase <http://www.leg.state.nv.us/nrs/NRS-603A.html>, revisado el 21 de febrero de 2012, 20:00 hrs.

artículos NRS 603A.200 y NRS 603A.210, lo referente a destrucción de ciertos registros y medidas de seguridad, respectivamente.

En cuanto a la destrucción de ciertos registros lo que se menciona es el hecho de que una vez que el negocio no requiera más mantener registros con información personal de sus clientes, éste deberá asegurarse de la destrucción de estos registros y tomar las medidas necesarias para cumplir con esto.

Lo cierto es que se exige que el responsable que mantiene registros con información personal de algún habitante del estado de Nevada implemente y mantenga medidas de seguridad razonables, y cuente con un contrato donde se establezca la protección de estos registros del acceso no autorizado, adquisición, destrucción, uso, modificación o divulgación.

Ahora bien, el artículo NRS 603A.215 estipula que aquellos responsables que acepten tarjetas de pago deberán cumplir con la versión actual del estándar PCI/DSS. En caso de que el responsable no realice esta práctica, entonces no deberá transferir información personal a través de una transmisión electrónica o sin voz diferente al fax, a menos que se cifre⁷⁸ la información con el fin de garantizar la seguridad de la transmisión electrónica.

⁷⁸ Cifrado quiere decir: “La protección de los datos que se encuentren en forma electrónica u óptica, en almacenamiento o en tránsito, utilizando: una tecnología de cifrado que haya sido adoptada por un cuerpo establecido de estándares, incluido, pero no limitado a, los Estándares de Procesamiento de Información Federal publicado por el NIST, la cual procese tales datos de forma indescifrable en ausencia de las llaves criptográficas necesarias para permitir la decodificación de dichos datos.” NRS 603A.215, <http://www.leg.state.nv.us/nrs/nrs-603a.html>, revisado el 21 de febrero de 2012, 20:00 hrs.

Estos Estatutos especifican que no se tendrá responsabilidad de una brecha de seguridad⁷⁹ en los siguientes casos:

- Cuando el responsable de los datos cumpla con lo anteriormente descrito; y
- La brecha no es causada por negligencia o dolo del responsable, sus oficiales, empleados o agentes.

Lo descrito en el párrafo que antecede no aplica para:

- Proveedores de telecomunicaciones ópticas, alámbricas, inalámbricas, análogas, voz sobre protocolo de Internet y otras tecnologías de transmisión digital, y
- Transmisiones de datos sobre canales de comunicación privados para:
 - Aprobación o procesamiento de instrumentos negociables, transferencias de fondos electrónicos o métodos de pago similares; o
 - Emisión de reportes con respecto a cierres de cuentas debido a fraude, sobregiros substanciales, abuso de cajeros automáticos o información referente a un cliente.

El Capítulo 603A también establece los diferentes métodos de divulgación de las brechas de seguridad de los sistemas de datos y las sanciones a las que los responsables se hacen acreedores.

⁷⁹ Esto se traduce en lo siguiente: “La adquisición no autorizada de datos computarizados que comprometen materialmente la seguridad, confidencialidad o integridad de la información personal mantenida por el responsable. El término no incluye la buena fe de la adquisición de la información personal de un empleado o agente del responsable para un propósito legítimo del responsable, mientras que la información personal no sea usada para un propósito no relacionado con el responsable o sujeto a divulgación posterior no autorizada.”, NRS 603A.20 “Breach of the securiry of the system data” defined. <http://www.leg.state.nv.us/nrs/nrs-603a.html>, revisado el 21 de febrero de 2012, 20:00 hrs.

Cabe señalar que otros estados como California, Hawái, Illinois y Vermont, por mencionar algunos, cuentan con legislación en materia de privacidad:

- California: desde el 2001 se estableció la Oficina de California de Protección de Privacidad (California Office of Privacy Protection), la cual provee de información y asistencia tanto a particulares como a negocios sobre temas de privacidad: robo de identidad, protección de menores en línea, privacidad financiera, ciberseguridad y privacidad en dispositivos móviles.⁸⁰
- Hawái: cuenta con la Oficina de Prácticas de Información (Office of Information Practices), la cual promueve un gobierno abierto y transparente, y administra, entre otras cosas, el Sistema de Registros Reportados (Records Report System RSR). Este último es una base de datos computarizada (sin los registros actuales) que describen los más de 29,000 títulos de registros de los diferentes tipos de registros de gobierno por estado y por agencia de condado que pueden tener acceso público.⁸¹
- Illinois: la Asamblea General de Illinois a través del Acto de Protección de Información Personal (815 ILCS 530/) (Personal Information Protection Act) en su apartado Transacciones Comerciales de diversos temas, aborda problemáticas en torno a los valores, préstamos y créditos, interés, ventas, prácticas engañosas, contratos y franquicias, entre otros más.

En particular, los Estatutos dimensionan los contenidos del documento Acto de Protección de la Información Personal en el tema de prácticas engañosas: aquí se incluyen los conceptos de responsable.

⁸⁰ Véase <http://www.privacy.ca.gov/>, revisado el 22 de febrero, 18:00 hrs.

⁸¹ Véase <http://www.state.hi.us/oip/index.html>, revisado el 22 de febrero de 2012, 18:30 hrs.

Sin embargo, no se consideran a las agencias gubernamentales, universidades públicas y privadas, corporaciones públicas y privadas e instituciones financieras, que por algún motivo manejan, recolectan, divulgan o tratan información personal-privada. El documento tampoco considera el concepto de brecha de la seguridad en los sistemas de datos, ni analiza la problemática de adquisición sin autorización de datos informáticos que comprometen la seguridad, confidencialidad o integridad de la información personal que mantiene el responsable; tampoco trata el tema de la información personal no encriptada que incluye nombre y apellido de una persona en combinación con uno o más de los datos relativos al número de seguridad social, número de licencia de manejo, número de tarjeta de crédito, débito o número de cuenta, junto con el código de seguridad o contraseña.

En caso que se presente una vulneración de la seguridad de los datos el responsable deberá dar aviso de dicha brecha al titular que resida en Illinois. Y en caso de ser una agencia estatal deberá anualmente presentar un reporte sobre dichas vulneraciones y sobre las medidas correctivas implementadas para prevenirlas en el futuro.

- Vermont: dentro de los Estatutos de Vermont, en el título 9 Comercio y Negocios capítulo 62 Protección de Información Personal, se establece el Acto de Notificación de Brechas de Seguridad y se define el contenido de dicha notificación.⁸²

⁸² Véase <http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=062&Section=02435>, revisado el 17 de febrero de 2012, 13:20 hrs.

Comisión Federal de Comercio⁸³

FTC –por sus siglas en inglés, Federal Trade Comission— tiene como misión prevenir las prácticas de los negocios que no son competitivas y que son engañosas o desleales para los consumidores.

Dentro de sus metas se encuentran:

- Proteger a los consumidores
- Mantener la competencia
- Mejorar el desempeño

Uno de los organismos que forma el FTC es el Buró de Protección del Consumidor (BCP), el cual tiene como objetivo proteger a los consumidores contra prácticas fraudulentas del mercado. Asimismo, desarrolla reglas para proteger a los consumidores y proporciona información para que tanto consumidores como empresas conozcan sus derechos y responsabilidades.

Dicho Buró tiene siete divisiones, cada una con su área de experiencia correspondiente:

1. Prácticas de publicidad
2. Educación para consumidor y negocios
3. Cumplimiento
4. Prácticas financieras
5. Prácticas de comercialización
6. Planeación e información
7. Protección de la privacidad y de la identidad

La división de protección de la privacidad y de la identidad es de las divisiones más recientes del BCP, y se encarga de temas relacionados con

⁸³ Véase <http://www.ftc.gov/bcp/bcippi.shtm> revisado el 20 febrero 2012, 20:00 hrs.

la privacidad del consumidor, reportes de crédito, robo de identidad y seguridad de la información.

Dicha división se enfoca en las siguientes secciones:

- Sección 5 del FTC Act. Prohíbe actos o prácticas injustas o engañosas, e involucran el uso de la protección de la información personal del consumidor.
- FCRA (Fair Credit Reporting Act). Asegura la exactitud y privacidad de la información guardada por el buró de crédito, así como por otro tipo de agencias.
- Acto Gramm-Leach-Bliley. Requiere a las instituciones financieras que aseguren la seguridad y confidencialidad de la información del cliente.

Es importante señalar que la Comisión Federal de Comercio (FTC) publica el manual "Cómo proteger la información personal: Una guía para negocios", en el cual se incluyen recomendaciones prácticas sobre la protección de datos vulnerables. Las medidas que se deben tomar en cuenta dependen del tamaño de la organización, así como del tipo de información que posee, aunque los principios básicos son los mismos.

Un plan de seguridad de la información debe considerar las siguientes prácticas clave:⁸⁴

- Conocer el inventario. Se refiere a saber qué tipo de información se tiene, el flujo de la misma y la identificación de quién o quiénes tienen acceso a los datos.
- Reducir los archivos. Se refiere a que en el mantenimiento de los archivos únicamente debe estar la información necesaria para el funcionamiento de la organización.

⁸⁴ Véase www.ftc.gov/infosecurity revisado el 16 de febrero de 2012, 14:00 hrs.

- Cerrar con llave. Se refiere a proteger la información que se encuentra tanto en archivos físicos como electrónicos, y a la capacitación de los empleados sobre el tema de seguridad.
- Eliminar lo no necesario. Se refiere a establecer normas para desechar correctamente toda la información que ya no se necesita.
- Planificación. Se refiere al diseño de un plan de acción para prevenir y responder a incidentes y vulneraciones de seguridad.

III.2.2.1.3 Mejores prácticas y estándares en materia de protección de datos

Como se ha presentado a lo largo de este apartado, existen varias organizaciones gubernamentales y privadas que emiten modelos, mejores prácticas y estándares sobre seguridad de la información en Estados Unidos, por ejemplo, la Universidad de Carnegie Mellon (Software Engineering Institute)- CMMI, ISACA- CobiT o NIST.

III.3 CONCLUSIONES SOBRE MEJORES PRÁCTICAS Y ESTÁNDARES INTERNACIONALES

III.3.1 Conclusiones particulares

CMMI (Capability Maturity Model Integration)

- Conjunto de mejores prácticas que proporciona los elementos para tener procesos efectivos que ayudan a mejorar la eficiencia, eficacia y calidad dentro de los grupos de trabajo, proyectos y divisiones. En otras palabras, contribuye al mejoramiento de todas las áreas de una organización.
- La seguridad de la información puede ser concebida, dentro del modelo CMMI de desarrollo y de servicios, como un tipo de requerimiento. Sin embargo, el SSE-CMM (System Security

Engineering Capability Maturity Model) lo establece de forma específica en sus 11 áreas de procesos de ingeniería de seguridad.

CobiT (Control Objectives for Information and Related Technology)

- Conjunto de prácticas para mejorar el manejo de la información tanto en el área financiera como en la tecnológica. Es un marco de referencia para establecer un rumbo seguro y confiable de las tecnologías de información así como una herramienta que da soporte a la alta dirección para reducir la brecha existente entre las necesidades de control, las cuestiones técnicas y los riesgos propios de un negocio.
- Dentro de los beneficios de CobiT se encuentra que los requerimientos de seguridad y privacidad serán más fácilmente identificados, y su implementación podrá ser monitoreada a través de los dominios establecidos en CobiT: Planear y Organizar (PO), Adquirir e Implementar (AI), Entregar y Soportar (DS) y Monitorear y Evaluar (ME).

ISO 27001

- Es el estándar internacional de gestión de seguridad de la información que permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad de la información a un nivel adecuado.
- En su anexo A enumera en forma de resumen los objetivos de control y controles que desarrolló la ISO 27002:2005, con la finalidad de que sean seleccionados por las organizaciones para el

desarrollo de sus Sistemas de Gestión de la Seguridad de la Información (SGSI).

- En la serie ISO 27000 están en fase de desarrollo la ISO/IEC 27017 –que consistirá en una guía de seguridad para Cloud Computing– y la ISO/IEC 27032 –que consistirá en una guía relativa a la Ciberseguridad–.
- Considerando que la ISO/IEC 27001 es el estándar internacional de seguridad de la información, encontraremos en todos los dominios el criterio de aplicabilidad en la protección de datos personales. Cabe señalar que en el dominio A.15 Cumplimiento, Objetivo de Control “cumplimiento de los requisitos legales” se encuentra –de forma específica– el control 15.1.4 relativo a la protección de datos y privacidad de la información de carácter personal.
- El ISO/IEC 27001 es el estándar en seguridad de información certificable, por lo que las empresas de TI que deseen ser consideradas como un proveedor confiable deberán tomarlo en cuenta para su estrategia de seguridad de información.
- La ISO/IEC 27005:2011 es una norma esencial para aquellos que requieran gestionar sus riesgos de manera efectiva y, en particular, para cumplir con la gestión de la información de seguridad mediante el estándar ISO/IEC 27001.

ITIL (Information Technology Infrastructure Library)

- Conjunto de directrices (mejores prácticas) y de módulos mediante los cuales podemos establecer un mejor aprovechamiento de los recursos informáticos de una entidad u organización, desde una

perspectiva de servicios. ITIL ha trazado el camino del “cómo” obtener mayor beneficio de las tecnologías de información.

- Considerando que ITIL cubre los servicios de TI en todas sus fases, los 5 libros que lo conforman contienen procedimientos útiles, que aplican para la protección de la información.

NIST (National Institute of Standards and Technology)

- Su misión consiste en promover la innovación y la competencia industrial en Estados Unidos.
- Los laboratorios NIST se centran en tres áreas focalizadas: ciencia de medición, tecnología (tecnologías de la información, ingeniería) e instalaciones de usuarios nacionales.
- Las publicaciones para la seguridad informática y la tecnología de la información son los especiales de la serie 800.
- Dentro de la serie 800, los más relevantes en el tema de seguridad y de datos personales se encuentran los siguientes:

Número de Publicación (Fecha)	Título	Contenido
NIST SP 800-12 (Octubre de 1995)	Introducción a la Seguridad Informática: El Manual NIST	Se enfoca a los controles de seguridad de acuerdo a su naturaleza, es decir, se hace una clasificación de los mismos (controles administrativos, operativos y

Número de Publicación (Fecha)	Título	Contenido
		técnicos).
NIST SP 800-14 (Septiembre de 1996)	Principios y Prácticas Generalmente Aceptadas para la Seguridad de los Sistemas Tecnologías de la Información	Se describen los 8 principios y 14 prácticas de seguridad.
NIST SP 800-39 (Marzo de 2011)	Administración del Riesgo en la Seguridad de la Información	Proporciona a las organizaciones una guía para la administración del riesgo de la seguridad de la información estableciendo los componentes del mismo (establecer, valorar, responder y monitorear el riesgo).
NIST SP 800-122 (Abril de 2010)	Guía para la Protección de la Confidencialidad de la Información de Identificación Personal	Sugiere categorizar el nivel de impacto de la confidencialidad de la PII (Información de Identificación Personal) en bajo, moderado y alto, y con base en el daño potencial que pudiera resultar a los titulares de la información y/o la

Número de Publicación (Fecha)	Título	Contenido
		<p>organización si esta fuera vulnerada, utilizada o divulgada de forma inapropiada. Adicionalmente, establece que la PII debe ser protegida a través de una combinación de medidas, incluyendo salvaguardias operativas, salvaguardias específicas de privacidad y controles de seguridad.</p>
<p>NIST SP 800-144 (Diciembre de 2011)</p>	<p>Directrices en Seguridad y Privacidad en Cómputo en la Nube de tipo Público</p>	<p>Provee una perspectiva general de los servicios de cómputo en la nube de tipo público y los retos en seguridad y privacidad que conllevan. Asimismo, describe los modelos de uso (nube pública, nube privada, nube comunidad y nubes híbridas) y emite recomendaciones tanto en temas de seguridad y privacidad como de actividades a realizarse para la contratación de un servicio de outsourcing de cómputo en la nube.</p>

PCI/DSS (Payment Card Industry Data Security Standard)

- Estándar internacional que establece un conjunto de requerimientos de seguridad de la información para proteger los datos de los tarjetahabientes.
- Las compañías que procesan, guardan o transmiten datos de los tarjetahabientes deben cumplir con el estándar, de no hacerlo se arriesgan a la pérdida de sus permisos para operar (pérdida de franquicias).
- La información proporcionada por los tarjetahabientes para el manejo de las tarjetas de crédito y débito es de carácter personal (datos de identificación, financieros y patrimoniales), por esta razón, cada uno de los objetivos de control y requerimientos previstos en este estándar aplican para la protección de datos personales.

España

- La Agencia Española de Protección de Datos (AEPD) es la institución encargada de cuidar y fomentar la privacidad y la protección de datos personales en España. A su vez la Península Ibérica pertenece a la Unión Europea, por lo tanto, debe ceñirse a los criterios de ésta.
- La AEPD es un ente de Derecho público con personalidad jurídica propia y plena capacidad pública y privada conforme al Real Decreto 428/1993 del 26 de marzo de 1993.
- El artículo 9 de la Ley Orgánica 15/1999 (LOPD) del 13 de diciembre de 1999 establece que tanto el responsable como el encargado del tratamiento deberán adoptar medidas de índoles

técnica y organizativas, que garanticen la seguridad de los datos de carácter personal para evitar su alteración, pérdida, tratamiento o acceso no autorizado.

- El Reglamento de desarrollo de la LOPD establece que las medidas de seguridad exigibles a las bases de datos (ficheros) y sus tratamientos se deben clasificar en tres niveles: básico, medio y alto.
- La AEPD ha emitido un documento denominado Guía de Seguridad de Datos y la cual recoge una serie de mejores prácticas en materia de protección de datos personales.
- La clasificación de los niveles de seguridad se realiza conforme a la naturaleza de la información tratada y a la necesidad de garantizar la confidencialidad y la integridad de la información.
- Las medidas de seguridad son acumulativas.
- La Guía establece un documento de seguridad, cuyo contenido está estructurado de la siguiente forma:
 - Ámbito de aplicación del documento.
 - Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos.
 - Información y obligaciones del personal.
 - Procedimientos de notificación, gestión y respuestas ante las incidencias.
 - Procedimientos de revisión.
- El Reglamento de la LOPD establece en sus artículos 96 y 110 que a partir del nivel medio de seguridad requerido, las bases de datos

deberán someterse, al menos cada dos años, a una auditoría interna o externa, de la cual se generará un informe que se entregará al responsable de la base de datos y a disposición de la AEPD o a las autoridades de control de las entidades autónomas.

- La Asociación Española de Normalización y Certificación (AENOR) ha publicado entre otras normas relacionadas a la seguridad de la información, las siguientes:
 - Desde el 28 de noviembre de 2007: ISO/IEC 27001 como UNE-ISO/IEC 27001: 2007
 - Desde el 9 de diciembre de 2009: ISO/IEC 27002 como UNE-ISO/IEC 27002: 2009

Reino Unido

- El Reino Unido a través del Data Protection Act 1998 establece que –cuando se tenga un encargado para el tratamiento de datos personales— se deberá seleccionar un encargado que provea suficientes garantías sobre sus medidas de seguridad para proteger el procesamiento que hará en nombre del responsable; se debe revisar que esas medidas de seguridad están llevándose a la práctica y deberá existir un contrato por escrito donde se establezcan las obligaciones del encargado. Existe un modelo de contrato publicado por el Comité Europeo para la Estandarización.
- La Oficina del Comisionado de Información (ICO) es una autoridad independiente en el Reino Unido, que se creó para defender los derechos de información de interés público, y para promover la apertura de los organismos públicos y la privacidad de los datos de los individuos.

- En relación a las medidas de seguridad, el DPA ha establecido lo siguiente: “Principio 7: Se deben tomar medidas técnicas y organizacionales apropiadas en contra del procesamiento sin autorización o ilegal de los datos personales así como en contra de pérdida accidental, destrucción o daño a los datos personales
- Se sugiere diseñar un modelo organizacional de seguridad, acorde con el tipo de datos personales que se poseen y acorde también con las contingencias de vulneración a la seguridad de la información.
- La ICO ha diseñado notas y códigos de buenas prácticas, que a continuación se muestran:
 - Nota de buenas prácticas de datos personales. Seguridad de Información Personal (Data Protection Good Practice Note Security of Personal Information)
 - Nota de buenas prácticas para protección de datos personales (Lista de entrenamiento para pequeñas y medianas empresas) (Data Protection Good Practice Note)
 - Código de Práctica de compartición de Datos (Data Sharing Code of Practice)
 - Código de práctica de información personal en línea (Personal information online code of practice)
 - Cómputo en la nube (Cloud computing)
- El ISF –por sus siglas en inglés, Information Security Forum— se dedica a la investigación, aclaración y solución de temas clave sobre seguridad de la información y administración de riesgo a través del desarrollo de mejores prácticas

- El Estándar de buenas prácticas 2011 contempla la perspectiva empresarial para la seguridad de la información y se divide en cuatro categorías principales:
 - Gobernanza de la seguridad
 - Requerimientos de seguridad
 - Marco de control
 - Monitoreo y mejora de la seguridad

Estados Unidos

- En el ámbito de la protección de datos personales en posesión de los particulares, Estados Unidos de Norteamérica cuenta con regulaciones en materia de privacidad y medidas de seguridad exigibles a los responsables y encargados de datos personales, tanto sectoriales como estatales.
- En el ámbito federal:
 - El Privacy Act de 1974 establece un código de prácticas justas que regulan la recolección, mantenimiento, uso y divulgación de la información de los individuos que se encuentra en los sistemas de registro de las agencias federales de los Estados Unidos.
 - El United States Code (USC) es la codificación por temas de las leyes generales y permanentes de los Estados Unidos de Norteamérica y se divide en amplios temas divididos en 50 títulos. Es publicado por la Oficina de Revisión Legislativa de la Cámara de Representantes de Estados Unidos.

- Dentro del título 15 “Comercio y Negocios” capítulo 94 del USC, se considera el tema de la privacidad de la información personal. Hace un análisis en torno a la divulgación de la información personal privada y al acceso fraudulento de la información financiera.
- En la sección 1173(d) del Health Insurance Portability and Accountability Act of 1996, “Estándares de seguridad para información de salud” se establece que la Secretaría de Servicios de Salud y Humanos, deberá adoptar estándares de seguridad que tomen en cuenta las capacidades técnicas de los sistemas de registro utilizados para mantener la información de salud; los costos de las medidas de seguridad; la necesidad de capacitación de las personas que tengan acceso a la información de salud; el valor de rastros de auditoría en sistemas computarizados de registro; y las necesidades y capacidades de pequeños proveedores del cuidado de la salud y proveedores rurales del cuidado de la salud.
- En el ámbito estatal:
 - El estado de Massachusetts cuenta con un reglamento denominado 201 CMR 17.00: Estándares para la Protección de Información Personal de los residentes de Commonwealth.
 - Los objetivos del instrumento mencionado son los siguientes: garantizar la seguridad y confidencialidad de la información de clientes de acuerdo a los estándares de la industria correspondiente; proteger la información contra amenazas o riesgos previstos; y proteger contra el acceso no autorizado

o uso de la información que pueda dar como resultado un daño o incomodidad a cualquier consumidor.

- Dentro de los Estatutos Revisados de Nevada (NRS) el capítulo 603A trata específicamente sobre la seguridad de la información personal. Aquí se establece, bajo el título de “Regulación de Prácticas de Negocio” en sus artículos NRS 603A.200 y NRS 603A.210, lo referente a destrucción de ciertos registros y medidas de seguridad, respectivamente.
- El artículo NRS 603A.215 estipula que aquellos responsables que acepten tarjetas de pago deberán cumplir con la versión actual del estándar PCI/DSS. En caso de que el responsable no realice esta práctica, tiene la obligación de no transferir información personal a través de una transmisión electrónica o sin voz diferente al fax, a menos que se cifre⁸⁵ la información con el fin de garantizar la seguridad de la transmisión electrónica.
- Cabe señalar que otros estados como California, Hawái, Illinois y Vermont, por mencionar algunos, cuentan con legislación en materia de privacidad.
- Existen varias organizaciones gubernamentales y privadas que emiten modelos, mejores prácticas y estándares sobre seguridad de la información en Estados Unidos, por ejemplo, la Universidad de Carnegie Mellon (Software Engineering Institute)- CMMI, ISACA-CobiT o NIST.

⁸⁵ Cifrado quiere decir: “La protección de los datos que se encuentren en forma electrónica u óptica, en almacenamiento o en tránsito, utilizando: una tecnología de cifrado que haya sido adoptada por un cuerpo establecido de estándares, incluido, pero no limitado a, los Estándares de Procesamiento de Información Federal publicado por el NIST, la cual procese tales datos de forma indescifrable en ausencia de las llaves criptográficas necesarias para permitir la decodificación de dichos datos.” NRS 603A.215, <http://www.leg.state.nv.us/nrs/nrs-603a.html>, revisado el 21 de febrero de 2012, 20:00 hrs.

III.3.2 Conclusiones generales

Los documentos de seguridad de la información, gestión y control de TI, así como la privacidad de datos, que se han ido mencionando en este documento, son una importante fuente de información, pues contienen prácticas que se han aplicado en organizaciones de diversos sectores a nivel mundial.

Las mejores prácticas, normas y estándares internacionales identificados y descritos proporcionan, por un lado, conceptos organizacionales, operacionales y tecnológicos, y por el otro, metodologías y procesos que nos permiten implantar un programa de administración de la seguridad adecuado a las necesidades de cada organización (gubernamental y privada). Asimismo, se han ponderado los requerimientos de privacidad de las diferentes regulaciones.

Los programas de administración de la seguridad no sólo deben implementarse bajo la perspectiva tecnológica de las mejores prácticas y estándares internacionales, sino que es necesario considerar el tema de la seguridad y protección de los datos personales desde una perspectiva organizacional y jurídica conforme a lo establecido en cada país y contexto de negocio.

Es importante considerar para la correcta administración de la seguridad de la información los programas y mecanismos que busquen cumplir con los elementos fundamentales de la seguridad: confidencialidad, integridad y disponibilidad de la información. Todo ello con base en los requerimientos de operación de la organización y su nivel aceptable de riesgo.

Las organizaciones que están empleando algún estándar o conjunto de buenas prácticas en seguridad de información, pero con modelos de

gestión diferentes al ISO 27001, obtendrán el beneficio de una adaptación y certificación de la norma con un menor esfuerzo.

Finalmente, es necesario utilizar la experiencia de otros países en materia de seguridad de datos personales, pues esto servirá de base para establecer una práctica efectiva de medidas de seguridad en protección de datos personales en México.

IV. MARCO PROGRAMÁTICO

Una vez descrito el marco jurídico doméstico e internacional que ampara toda regulación en el tema de la protección de datos personales, se debe señalar que también existe un ambiente programático que sustenta las políticas públicas nacionales o programáticas en la materia que deriva del Plan Nacional de Desarrollo (PND), el cual establece los objetivos nacionales, las estrategias y las prioridades que deberán regir la acción del gobierno.

Su Eje 2 “Economía competitiva y generadora de empleos” es el que incide en el tema que nos ocupa, pues la protección de los datos personales queda regido por los objetivos tendientes a fortalecer el Estado de Derecho y la seguridad pública, garantizando certidumbre legal y jurídica a las personas y a la propiedad.

Derivado del PND, el Programa Sectorial de Economía (en este caso el formulado para el periodo 2007-2012),⁸⁶ establece ejes, objetivos y líneas de acción relevantes para enmarcar políticas públicas en materia de protección de datos personales en el entorno digital.

Dichos conceptos del Programa Sectorial son los siguientes:

2. CONTRIBUCIÓN DEL PROGRAMA SECTORIAL DE ECONOMÍA 2007-2012, A LOS OBJETIVOS DEL PLAN NACIONAL DE DESARROLLO Y METAS DE LA VISIÓN MÉXICO 2030.

⁸⁶ Publicado en el Diario Oficial de la Federación del miércoles 14 de mayo de 2008.

Línea estratégica 2.5.1. Generalizar la utilización de métodos y procesos enfocados a la innovación en las empresas mexicanas

Acciones:

....

g) Fomentar la adopción de tecnologías de información mediante el impulso al comercio electrónico, el equipamiento y el desarrollo de soluciones informáticas y de comunicaciones que atiendan las necesidades de las empresas.

Objetivo rector 2.6. Dar certidumbre jurídica a los factores económicos a través de la adecuación y aplicación del marco jurídico, así como la modernización de los procesos de apertura de empresas.

....

Dada la relevancia de los temas citados anteriormente, la Secretaría de Economía instrumentará con este objetivo distintas acciones, tales como el establecimiento del Sistema de Apertura Rápida de Empresas (SARE) en municipios del país; modernización del registro público de comercio; protección a los derechos de propiedad industrial, así como el combate a actos que constituyan competencia desleal relacionados con ésta; el impulso de una política nacional de normalización que favorezca el desarrollo de la infraestructura técnica y la competitividad; o la promoción del comercio electrónico, el uso de la firma electrónica y los servicios de conservación de mensajes de datos, entre otros.

Línea estratégica 2.6.10. Promover el comercio electrónico y el uso de la firma electrónica y los servicios de conservación de mensajes de datos.

Acciones:

a) Realizar los trabajos necesarios para la acreditación de un mayor número y diversidad de Prestadores de Servicios de Certificación en materia de firma electrónica, la interoperabilidad de certificados de Firma Electrónica Avanzada en la Administración Pública Federal y las administraciones locales y la regulación de los nuevos servicios de firma e identificación electrónica y de otras tecnologías relacionadas. Todo lo anterior para favorecer el desarrollo del comercio electrónico y del gobierno electrónico lo que generará ahorros en transporte, papel, almacenamiento y otros a las empresas, instituciones, comerciantes y personas en general, con seguridad jurídica, en beneficio de la competitividad general y con impacto ecológico favorable.

b) Promover la armonización de la regulación técnica en materia de servicios de firma electrónica avanzada con los estándares internacionales para facilitar el intercambio comercial por Internet, la interoperabilidad con certificados digitales emitidos en otros países para efectos del comercio electrónico y el abatimiento de costos para el reconocimiento recíproco entre los certificados digitales emitidos en México y en el extranjero.

c) Impulsar cambios legislativos y reglamentarios para que la regulación en materia de comercio electrónico permita una ágil y continua actualización para mantenerla al día y en sintonía con los principales avances tecnológicos y las tendencias globales en la materia.

d) Difundir entre particulares y autoridades, principalmente las jurisdiccionales, los mecanismos de seguridad que ofrece la firma

electrónica avanzada y los servicios relacionados para fomentar su uso y su pleno reconocimiento en el ámbito jurisdiccional. El objetivo es abatir costos asociados a litigios sobre la autenticidad de mensajes de datos con efectos en la esfera jurídica de personas físicas y morales.

e) Llevar a cabo acciones de regulación y difusión para que los servicios de firma electrónica avanzada sean accesibles al mayor número de personas por su costo y facilidad de uso.

EJE 3. FOMENTAR EL COMERCIO EXTERIOR Y LA INVERSIÓN EXTRANJERA DIRECTA

Línea estratégica 3.1.7 Uso de tecnologías de la información en las operaciones de comercio exterior.

Acciones:

a) Coordinar el establecimiento de la ventanilla electrónica en materia de comercio exterior (interconectividad de la Administración Pública Federal, trámites vía Internet, Sistema Integral de Información de Comercio Exterior).

b) Promover el uso de tecnologías de información en los procesos internos de las empresas.

c) Desarrollar empresas de comercio exterior (comercializadoras internacionales).

Línea estratégica 3.2.4. Posicionar a México como un oferente en el mercado de servicios de tecnologías de información.

Acciones:

a) Fomentar el establecimiento de sellos de confianza para favorecer el acreditamiento de la oferta mexicana de servicios.

EJE 4. IMPLEMENTAR UNA POLÍTICA SECTORIAL Y REGIONAL PARA FORTALECER EL MERCADO INTERNO.

Objetivo rector 4.1 Impulsar la reconversión y el crecimiento de sectores estratégicos y de alto valor agregado.

Línea estratégica 4.1.3. Desarrollar la industria de servicios de tecnologías de la información (TI).

Acciones:

a) Promover los servicios de TI y procesos de negocio (BPO por sus siglas en inglés, finanzas, nómina, contabilidad, call centers):

- Diseño o ingeniería de productos de software (Software empaquetado, aplicativo, embobinado, entre otros).

- Servicios soportados con TI (Soporte y seguridad de sistemas, implantación y prueba de base de datos, procesamiento de datos, análisis y gestión de riesgos de sistemas, entre otros).

- Subcontratación de procesos de negocio (BPO por sus siglas en inglés).

Si bien es cierto que el Programa Sectorial de Economía no es específico en el planteamiento de políticas públicas en materia de seguridad para la protección de datos personales, no hay duda que sus objetivos sirven de marco para proveer mecanismos o medidas que alienten la seguridad en el tratamiento de los datos por los particulares, sean estos responsables, encargados o terceros. Esto incide –directa e indirectamente- en elevar la competitividad de las empresas mediante el fomento del uso de las tecnologías de información, la innovación y el desarrollo tecnológico en sus productos y servicios; incrementar la participación de México en los flujos de comercio mundial y en la atracción de Inversión Extranjera Directa; y en general, en posicionar a México como un oferente en el mercado de servicios de tecnologías de información.

Se comprende que el Programa en comento no haya determinado líneas de acción exhaustivas para la economía en general, ni para la digital en lo particular, pues cuando fue emitido en mayo del 2008, México no contaba con lo que ahora es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, emitida en el 2010.

V. ANÁLISIS DE LOS RESULTADOS DE LA ENCUESTA-SONDEO EN LÍNEA DE LAS EMPRESAS DEL SECTOR DE TI

Considerando los contextos jurídicos y programáticos que inciden en el tema que nos ocupa, corresponde presentar el análisis de los resultados de la encuesta-sondeo en línea que se elaboró como reporte de la actividad d) de los Términos de Referencia.

Dicho trabajo de investigación estadístico arrojó datos sobre la existencia, tipo, práctica, efectividad y problemas en la implementación de las medidas de seguridad para la protección de datos personales, los cuales se pueden resumir en los siguientes términos:

V.1 METODOLOGÍA

De acuerdo con lo establecido en las Reglas de Operación del Programa para el Desarrollo de la Industria del Software (Prosoft) para el ejercicio fiscal 2011, se señaló como objetivo general el "Contribuir al desarrollo del sector de tecnologías de la información buscando su crecimiento en el largo plazo en el país favoreciendo la competitividad nacional e internacional".

Se han considerado empresas del sector de TI a todas aquellas que realizan alguna de las siguientes actividades económicas:

- a) Desarrollo de software empaquetado
- b) Desarrollo de software de sistema y herramientas para desarrollo de software aplicativo
- c) Desarrollo de software aplicativo
- d) Servicios de consultoría de software
- e) Servicios de análisis de sistemas computacionales
- f) Servicios de diseño de sistemas computacionales

- g) Servicios de programación de sistemas computacionales
- h) Servicios de procesamiento de datos
- i) Servicios de diseño, desarrollo y administración de bases de datos
- j) Servicios de implantación y pruebas de sistemas computacionales
- k) Servicios de integración de sistemas computacionales
- l) Servicios de procesamiento de datos
- m) Servicios de seguridad de sistemas computacionales y procesamiento de datos
- n) Servicios de análisis y gestión de riesgos de sistemas computacionales y procesamiento de datos
- o) Procesos de negocio basados en el uso de sistemas computacionales y comunicaciones
- p) Servicios de valor agregado de análisis, diseño, desarrollo, administración, mantenimiento, pruebas, seguridad, implantación, mantenimiento y soporte de sistemas computacionales, procesamiento de datos y procesos de negocio
- q) Servicios de capacitación, consultoría y evaluación para el mejoramiento de la capacidad humana, aseguramiento de la calidad y de procesos de las empresas del Sector de TI
- r) Servicios de administración de procesos de negocio basados en tecnologías de información que incluyen entre otros centros de llamado, centros de contacto, administración de nóminas, carteras, cobranza, líneas de producción, entre otros.
- s) Desarrollo de software embebido (embedded software)
- t) Medios interactivos basados en tecnologías de información:
 - I) Desarrollo o creación de entretenimiento interactivo
 - II) Servicios especializados de diseño
 - III) Animación
 - IV) Tecnologías de compresión digital
 - V) Efectos visuales
 - VI) Televisión interactiva, y

- u) Cualquiera otra tecnología que el Consejo Directivo determine.

Tomando como base las actividades económicas mencionadas en las Reglas de Operación, se ha considerado un universo de 12,200 empresas para determinar la muestra que representara a dicho sector.

Por lo anterior, se ha establecido un diseño muestral aleatorio probabilístico que considera una muestra de 530 empresas encuestadas a nivel nacional. Cabe destacar que la participación de las empresas nos permitió que esta muestra se incrementara a 564 empresas. También es importante señalar que el nivel de confianza de la encuesta-sondeo en línea es de 95%.

OBJETIVOS PARTICULARES Y CARACTERÍSTICAS DE LA ENCUESTA-SONDEO EN LÍNEA

Los objetivos particulares definidos en los Términos de Referencia del presente proyecto son:

- a) Identificar habilidades y prácticas nacionales e internacionales en materia de seguridad de datos para empresas de TI.
- b) Valorar el grado de uso de prácticas de seguridad de datos personales actual en empresas de TI en México.
- c) Emitir recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en las empresas de TI.

Con el fin de alcanzar los objetivos mencionados anteriormente se diseñó un cuestionario formado por 22 preguntas, que a su vez se dividieron en cinco secciones principales, las cuales se describen a continuación:

- Introducción

En esta sección se da a conocer de manera breve el programa que el Gobierno Federal a través de la Secretaría de Economía impulsa para promover el crecimiento del sector de servicios de TI, teniendo como uno de sus objetivos particulares el fortalecimiento institucional y mejora del marco legal regulatorio y de políticas sectoriales.

Asimismo, se utilizó este apartado para dar a conocer y/o reforzar entre las empresas participantes el contenido de la LFPDPPP con relación al tratamiento de datos personales así como la figura de encargado.

- Clasificación

En esta sección se buscó agrupar a las diferentes empresas que ofrecen servicios de tecnologías de información en la industria, para las cuales la aplicación de la LFPDPPP es relevante y, por supuesto, de acuerdo a la naturaleza de operación, misión, visión y valores.

Por un lado, se realizó una estratificación del personal participante, para garantizar que la apreciación de la problemática considere las implicaciones de negocio y del ambiente tecnológico. Asimismo, se llevó a cabo la identificación del número de empleados de las empresas y el monto de ventas anuales de éstas como lo establece el DOF (el 30 de junio de 2009) con respecto al tamaño de las empresas pertenecientes al sector Servicios de TI.⁸⁷

⁸⁷ Tamaño de las empresas: El sector de TI corresponde al sector Servicios, conforme al Acuerdo por el que se establece la estratificación de las micro, pequeñas y medianas empresas, publicado en el DOF (30 de junio de 2009)

Por otro lado, se buscó detectar la existencia de empresas en el país que ofrezcan servicios de outsourcing en el tratamiento de datos personales. Una empresa con este perfil podría cubrir las características y requerimientos de la figura de encargado.

- Prácticas Organizacionales de Seguridad y Privacidad de la Información

Con este grupo de preguntas se buscó determinar el tipo de prácticas de gestión y operación relativas a la seguridad y privacidad de la información de las empresas, que en conjunto con su naturaleza operativa, puedan ayudar a determinar las áreas de oportunidad en las mismas de cara al cumplimiento de la LFPDPPP.

De igual forma, se podrá identificar la familiaridad que tienen las empresas sobre aquellos elementos de planeación, operación, supervisión y mejora continua de la seguridad, que han sido considerados como mínimos indispensables para garantizar el nivel de privacidad de los datos personales, dentro de los parámetros de suficiencia de la ley.

- Gestión de la Seguridad y Privacidad de la Información, el cual abarcó como temas principales los procesos, roles y responsabilidades, así como la seguridad de los activos informáticos

El objetivo principal de esta sección es determinar la forma en cómo las organizaciones han asignado las responsabilidades de seguridad de la información, así como los mecanismos de

control técnicos, operativos y de proceso encaminados a lograr el nivel de seguridad y privacidad que la operación requiere. A través de estos controles será posible identificar las medidas de seguridad administrativas, técnicas y físicas con las que las organizaciones cuentan.

Los controles incluidos en la evaluación atienden, en gran medida, a un grupo de mecanismos que pueden favorecer las capacidades sobre seguridad y privacidad de la información.

- Tratamiento de Datos en el denominado Cómputo en la Nube

En esta sección se ha buscado identificar los mecanismos de control que las organizaciones han implementado actualmente para la entrega y uso de servicios en un sistema computacional de esta naturaleza. De esta manera se podrá determinar si la industria está preparada para el cumplimiento de la LFPDPPP, manteniendo los niveles de privacidad de las personas sobre su información.

V.2 ANÁLISIS DESCRIPTIVO

V.2.1 Clasificación de las empresas

A partir de lo establecido en las Reglas de Operación del Prosoft 2011 sobre las actividades económicas que forman el sector de las TI, se detectó que menos del 5% de las empresas encuestadas proporcionan algún tipo de outsourcing.

Si se considera el tamaño de la empresa (número de empleados y rango de ventas anuales, tal y como lo estipula el Diario Oficial de la Federación del 30 de junio de 2009), se observa que alrededor del 80% de las

empresas encuestadas se encuentran en la clasificación de micro y pequeña empresa.

Ahora bien, respecto al procesamiento, almacenamiento o resguardo de datos personales –ya sean internos o de clientes– se presentaron los siguientes rangos:

- Del 41% al 45% de las empresas evaluadas procesan datos personales.
- Del 30% al 31% almacenan datos personales.
- Solo el 25% resguarda este tipo de datos.

V.2.2 Prácticas organizacionales de privacidad y seguridad de la información

De las 564 empresas encuestadas se identificó la utilización de las siguientes regulaciones, marcos referenciales, mejores prácticas y/o estándares para implantar seguridad de información dentro de las mismas:

- Ley de Protección de Datos Personales en Posesión de los Particulares
- Requerimientos de operación de la organización
- Ley de Transparencia y Acceso a la Información Pública Gubernamental
- ISO/IEC 27001:2005
- ITIL
- COBIT
- CMM/SSE-CMM
- PCI/DSS

Es importante señalar que el 26% de las empresas evaluadas desconocen qué regulaciones y/o marcos referenciales se utilizan para implementar la seguridad de la información. Únicamente el 39% señaló a la Ley Federal

de Protección de Datos Personales en Posesión de los Particulares como mecanismo de regulación.

V.2.3 Tipo, Existencia y Práctica de Medidas de seguridad

V.2.3.1 Medidas de seguridad administrativa

V.2.3.1.1 Gestión, soporte y revisión de la seguridad de la información a nivel organizacional

En relación a las medidas de seguridad administrativas para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, que se mencionan en el artículo 3 del Reglamento de la LFPDPPP, se identificaron los siguientes aspectos:

1. Objetivos de control
2. Comité de Seguridad
3. Acuerdos contractuales
4. Evaluación de la efectividad de la seguridad de la información

En el primer aspecto, el 27% de las empresas cuenta con una política central y estándares auxiliares de seguridad de información; el 22% considera como lo más relevante la seguridad de recursos humanos; el 15% se basa en los objetivos de control de cumplimiento; y el 11% considera la gestión de incidentes de seguridad de la información como lo más importante.

En el segundo aspecto, el 55% de las empresas encuestadas no cuenta con un Comité de Seguridad que vigile el cumplimiento, monitoreo y mejoramiento de las políticas establecidas.

En el tercer aspecto, el 36% de las empresas no ha definido ni acuerdos contractuales ni cláusulas con sus clientes o proveedores sobre la

responsabilidad del procesamiento e intercambio de información y datos personales.

En los casos en los que se cuenta con acuerdos contractuales: éstos son definidos por el área comercial en combinación con el área jurídica (30%), definidos solamente por el área jurídica (18%) y empresas en las que existe un grupo interdisciplinario de operaciones comercial y jurídico que define los acuerdos mencionados (15%).

En el cuarto aspecto, el 35% de las empresas no poseen indicadores formales de evaluación de la efectividad de la seguridad de la información. Ahora bien, aquellas empresas que sí cuentan con dichos mecanismos realizan reportes de incidentes, evaluaciones de controles generales de TI, reportes de soluciones de vulnerabilidades técnicas realizadas y/o categorización de eventos identificados por la infraestructura.

V.2.3.1.2 Identificación y clasificación de la información

En este rubro sólo el 29% de las empresas encuestadas lleva a cabo una identificación y clasificación de la información como componente de su marco normativo de seguridad. Además, el 29% señaló que el área responsable de definir y administrar los criterios de clasificación de la información es la Dirección General; el 26% mencionó que la responsable de dicha clasificación es el área de seguridad; y sólo el 8% de las empresas asigna dicha actividad al área de datos personales.

Cabe mencionar que en el 27% de los casos no existen criterios formales de clasificación.

V.2.3.1.3 Concienciación, formación y capacitación del personal en materia de protección de datos personales

Otra medida de seguridad administrativa establecida dentro del Reglamento de la LFPDPPP es la concienciación, formación y capacitación del personal en materia de protección de datos personales. El resultado arrojado en esta encuesta muestra que el 33% lleva a cabo la concienciación de su personal a través de correo electrónico, folletos, medios impresos, etc.

El 53% manifestó que la formación y capacitación se realiza por lo menos una vez al año en su organización. Sin embargo, es importante señalar que el 35% de las empresas no recuerda cuándo recibió la última capacitación sobre seguridad y privacidad de la información.

V.2.3.2 Medidas de seguridad físicas

De acuerdo con lo establecido en la fracción VI del Artículo 2 del Reglamento de la LFPDPPP, las medidas de seguridad físicas son un conjunto de acciones y mecanismos que emplean o no la tecnología para la prevención del acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información; protección de equipos móviles portátiles o de fácil remoción situados fuera o dentro de las instalaciones; la provisión a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad; y la garantía de la eliminación de datos de forma segura.

Las medidas de seguridad físicas han sido definidas por las empresas de acuerdo a los siguientes objetivos de control:

- Seguridad física y de instalaciones (25%) que abarca:

- Control y cierre de puertos/puntos de conexión (red, telefonía)
 - Señalización y estandarización de cableado (Cableado de red, de suministro eléctrico, de telefonía, etc.)
 - Control de acceso físico (Biométrico, smartcard, token)
 - Segregación física de espacios (División de áreas, por ejemplo: área de proveedores, área de carga y descarga, etc.)
 - Inventario físico de infraestructura
 - Inmovilización y aislamiento de equipos (Anaqueles cerrados, espacios confinados, etc.)
 - Infraestructura de soporte (Detección de humo, supresión de incendios, detectores de humedad, planta de luz, UPS)
- Inventario de activos de la información (17%) o gestión de activos que incluye:
 - Inventario de activos
 - Propiedad de los activos
 - Uso aceptable de los activos
 - Directrices de clasificación de la información
 - Etiquetado y manipulado de la información

V.2.3.3 Medidas de Seguridad Técnicas

De acuerdo con lo establecido en la fracción VII del Artículo 2 del Reglamento de la LFPDPPP, las medidas de seguridad técnicas se refieren al "Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:

- a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;

- b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- c) Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y
- d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.”

Las empresas encuestadas han definido las medidas de seguridad técnicas dentro de los siguientes objetivos de control:

- Operaciones de cómputo (22%)

Los mecanismos de seguridad implementados para la protección de información y datos personales en el procesamiento de las aplicaciones son básicamente tres: software antivirus, firewalls y sistemas de detección/prevención de intrusiones.

- Control de acceso lógico (20%)

Los mecanismos de seguridad utilizados para el control de acceso –de acuerdo a la respuesta de las empresas encuestadas– son los siguientes: esquema de gestión de identidades y accesos, certificados digitales, smartcards/dispositivos OTP, biométrico y contraseñas.

- Seguridad de desarrollo de aplicaciones (16%)
- Operación de telecomunicaciones (13%)

Lo cierto es que en el ámbito de redes de comunicaciones se utilizan los mismos mecanismos de seguridad que en el procesamiento de las aplicaciones.

V.2.3.4 Problemas en la implantación de las medidas de seguridad para la protección de datos personales

Para que las empresas del sector de servicios de TI logren adoptar mecanismos de privacidad de datos personales en sus esquemas de seguridad de la información –que cumplan con la LFPDPPP, agregando valor a sus procesos de negocio— deberán atenderse las siguientes causas raíz de las brechas y carencias observadas en los resultados de la encuesta-sondeo:

- El 80% de las empresas del sector de TI se encuentran clasificadas como micro y pequeña empresa, en consecuencia, éstas no han conseguido la capacidad para implementar las medidas de seguridad para protección de datos personales. La carencia se debe principalmente a la falta de recursos económicos y humanos.
- La función de seguridad de la información ha sido concebida y asignada de forma permanente a un contexto tecnológico, que se desenvuelve a través de esfuerzos aislados o puntuales de aseguramiento, basados en herramientas específicas de seguridad. En muchos de estos casos, la premisa principal es satisfacer algún requerimiento de auditoría o evaluación, o bien, resolver problemas acotados.
- Se reconoce una falta de experiencia de la industria de servicios de TI para la asimilación de las regulaciones de privacidad sobre el esquema de seguridad de la información, así como para reconocer

las responsabilidades de cada actor especificado en la LFPDPPP y su Reglamento.

- El enfoque de protección que se ha desarrollado a lo largo del tiempo se basa en la infraestructura tecnológica, y no en la sensibilidad, criticidad e importancia de la información para el negocio, y mucho menos con un enfoque de protección de datos personales.
- Se asignan presupuestos y recursos limitados para implantar las iniciativas de seguridad de la información y privacidad de datos personales. Esta carencia se debe a una competencia con otras prioridades de la organización; prioridades que se desprenden recurrentemente del presupuesto asignado a la función de TI. De ahí, pues, que no se logre desarrollar alternativas de seguridad y privacidad en función de los requerimientos organizacionales.
- Las restricciones de recursos han dado como resultado que la mayoría de las organizaciones encuestadas no ejecuten controles fundamentales en la esfera de seguridad, por ejemplo, análisis de riesgos y estrategia de seguridad, estrategia de capacitación y concientización en seguridad y privacidad, gestión de incidentes de seguridad o mejora continua de la seguridad de la información.

La remediación de estas causas raíz no se encuentra en una solución única o finita, sino en un proceso permanente de la organización por incorporar los aspectos de seguridad, privacidad y cumplimiento de la LFPDPPP y su Reglamento como parte de una cultura organizacional.

V.2.4 Tratamiento de Datos Personales en el denominado Cómputo en la Nube

Con base en lo establecido en el Artículo 52 del Reglamento de la LFPDPPP, el cómputo en la nube se entiende como el “modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.”

La encuesta-sondeo detectó que el 53% de las empresas ofrecen o utilizan servicios de cómputo en la nube.

Se revisaron los aspectos que el Reglamento estipula en relación a las empresas que ofrecen servicios de cómputo en la nube. Y se descubrió lo siguiente: la mayoría de los proveedores desconocen o no cubren los aspectos y mecanismos que dicho Reglamento determina para garantizar la debida protección de los datos personales.

En efecto, las empresas que utilizan servicios de cómputo en la nube perciben que la mayoría de sus proveedores no contemplan los aspectos ni mecanismos referidos anteriormente.

V.2.5 CONCLUSIONES DEL ANÁLISIS DE LOS RESULTADOS DE LA ENCUESTA-SONDEO EN LÍNEA

Con base en las respuestas de las empresas encuestadas sobre el tema de seguridad de información y datos personales, es posible plantear las siguientes conclusiones:

- El porcentaje de participación de empresas micro y pequeña, puede indicar que existe una preocupación genuina por los alcances y requerimientos de seguridad y privacidad para la industria por los esfuerzos a desarrollar en su cumplimiento.
- En el caso de la participación de empresas micro por su nivel de ingreso, es importante no restringir el presupuesto para la implantación de mecanismos de control que ayuden a cumplir con las disposiciones de la Ley. El compromiso de privacidad y seguridad de la información de los datos personales no atiende al tamaño del negocio, sino al tipo y sensibilidad de dichos datos que se manejan en sus procesos.
- Se identifican a los servicios de outsourcing de tratamiento de datos personales como un área de oportunidad de negocios para las empresas del sector de TI en México, ya que actualmente solo el 31% lo ofrece.
- Si bien en las empresas existe cierto entendimiento sobre algunos componentes clave para el cumplimiento de la LFPDPPP, estos aún no se están ejecutando.
- Existe una percepción en las empresas evaluadas de que el tema de seguridad de datos personales debe ser resuelto por una función de tecnología de la información (TI).

- Las organizaciones han trabajado en la implementación de controles técnicos preventivos y de detección de brechas de seguridad, pero no en un contexto de privacidad de datos personales.
- La implementación de los controles actuales está basada en gran parte en la experiencia de los responsables de la función de TI.
- La mayoría del presupuesto para esfuerzos de iniciativas de seguridad y privacidad están derivados de los presupuestos de TI.
- La efectividad de las funciones de seguridad y privacidad no están siendo monitoreadas, evaluadas y supervisadas en ningún sentido.
- A partir de algunas de las opiniones de los participantes que respondieron la encuesta-sondeo, es posible identificar que las empresas consideran que este tipo de regulaciones aplica únicamente para empresas grandes.
- Actualmente las empresas no cuentan con un equipo de respuesta de incidentes ni con una bitácora de control de actividades de la infraestructura de procesamiento, aplicaciones, información y datos personales, que permitan tener un control formalizado de estas actividades. Por lo tanto, sería complicado proporcionar evidencia en un proceso legal relativo a brechas de seguridad y afectación de datos personales.
- Considerando la naturaleza de sus servicios y su inercia operativa, el sector de cómputo en la nube debe realizar esfuerzos en la revisión de sus contratos de adhesión, en las características de

entrega de servicios y en su esquema operativo, de tal forma que se adapten a los requerimientos que el Reglamento de la LFPDPPP establece en el artículo 52.

- Es importante señalar que las empresas que no reconocen la utilidad del análisis de riesgos, basan sus políticas de seguridad de la información en esfuerzos puntuales de remediación de desviaciones o decisiones subjetivas de los responsables de estas funciones.
- El Artículo 20 de la LFPDPPP y los Artículos 63 al 66 de su propio Reglamento, reconocen como prioritario la gestión de incidentes de seguridad de la información. En consecuencia, otra área de oportunidad de cara al cumplimiento de la LFPDPPP, se encuentra en el bajo porcentaje de organizaciones que han trabajado en la gestión de incidentes de seguridad de la información.
- La capacitación sobre seguridad y privacidad de la información representa uno de los esfuerzos más relevantes que la industria de servicios de TI debe ejecutar. Por ello, el carácter organizacional de la privacidad de datos personales en el Reglamento de la Ley implica capacitación activa para el personal de la organización que trate datos personales.

VI. RECOMENDACIONES Y PROPUESTA DE MEDIDAS CORRECTIVAS

Con base en el análisis a que se refiere el apartado anterior, del cual se desprenden fortalezas y debilidades sobre la práctica de medidas de seguridad de la información y protección de datos personales en el sector de las TI, es posible emitir recomendaciones y medidas correctivas para dar cumplimiento a la LFPDPPP.

MARCO PRÁCTICO REFERENCIAL DE MECANISMOS DE CONTROL DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La publicación y entrada en vigor de la LFPDPPP, ha generado implicaciones relevantes en el entorno de negocios de los diferentes sectores económicos, puesto que ahora las organizaciones deben incorporar dentro de sus premisas de negocio la garantía de privacidad de los datos personales que utilizan en sus actividades diarias, para lograr el cumplimiento de las disposiciones de la Ley.

Debe destacarse que la generación de este tipo de regulaciones atiende generalmente a una necesidad de la industria y de los individuos involucrados, a partir de la dinámica y madurez (por los productos y servicios que ofrecen) de sus sectores económicos, y no a una imposición subjetiva con el afán de aumentar la complejidad de estas relaciones comerciales.

En las organizaciones se han generado diversas expectativas y premisas con el objetivo de cumplir satisfactoriamente con las disposiciones, a partir de sus esfuerzos actuales en seguridad de la información, sorteando las restricciones de disponibilidad de recursos (económicos, humanos y técnicos) y logrando su misión y objetivos.

Aún cuando el objeto y alcance de esta regulación trae consigo muchos beneficios a los individuos, para las organizaciones que obtienen y utilizan estos datos, representan un esfuerzo adicional y de fondo en el esquema actual de protección de la información que soporta los procesos de negocio. Dicha representación se da en tres factores fundamentales a partir del estado actual de las prácticas de privacidad del sector de TI en nuestro país:

- a) Organización. Implica que se definan los roles y responsabilidades específicos sobre la privacidad de los datos personales al interior de la empresa. El objetivo es cumplir con el nivel de privacidad determinado y los requerimientos de cumplimiento por parte de los responsables, para favorecer el ejercicio de los derechos otorgados a los titulares de los datos personales por la Ley, en tiempo y forma.

De igual forma, es importante ampliar todos los roles y responsabilidades para consolidar una cultura de privacidad de la información.

- b) Procesos. La empresa debe integrar un marco normativo y de procesos (ejecución) para mantener los objetivos de privacidad que establezca, con base en las especificaciones de las regulaciones aplicables. En este sentido, la empresa deberá desarrollar todos los procesos y procedimientos que garanticen que la infraestructura tecnológica y de seguridad de la información, esté alineada con la operación del negocio y requerimientos particulares de la normatividad.
- c) Mecanismos de protección de la información. Los requerimientos especificados en las regulaciones de privacidad de la información,

tienen implicaciones en el marco de control y seguridad de la información en la infraestructura tecnológica. En consecuencia, ésta debe complementarse y renovarse en función de la existencia de datos personales en los procesos de negocio y los recursos informáticos que los soportan, considerando las nuevas formas tecnológicas (ambientes virtualizados, bases de datos y aplicaciones distribuidas, telecomunicaciones, esquemas de cifrado, entre otros) que ha adoptado el negocio, y las nuevas amenazas que podrían propiciar brechas de seguridad (acceso y divulgación no autorizados, pérdida o alteración de los datos personales).

Para el desarrollo e implementación de estos mecanismos de gestión y control sobre los datos personales que mejoren las prácticas actuales de privacidad de las empresas de TI en México, no existe una ruta preestablecida o definida que sea universalmente aplicable para todas las empresas, sino que su definición, implementación, operación y monitoreo dependerán de cada una de ellas a partir de los siguientes factores:

- a) Misión y naturaleza operativa. La cantidad de datos personales y su uso en los procesos de la organización, atiende directamente al objeto de negocio; por lo que en el caso de las empresas dentro del sector de TI, dependerán de los servicios específicos y requerimientos de sus clientes con una naturaleza operativa y compromiso de privacidad con sus propios clientes finales.
- b) Estrategias comerciales. La creación de nuevos productos y servicios de TI en la organización puede llevar a transformar sus procesos, en los cuales se traten datos personales actualmente. En este caso, cada organización tiene una forma diferente de generar estos productos y servicios.

- c) Estructura orgánica, jerárquica y funcional. Se ha señalado la necesidad de definir y asignar formalmente roles y responsabilidades a partir de las disposiciones de la LFPDPPP, considerando los tramos de control de cada organización, las dependencias organizacionales y funciones de cada rol relacionados con la privacidad de los datos personales.
- d) Marco regulatorio aplicable. Además de la LFPDPPP, se deben tener en cuenta regulaciones adicionales que cada uno de los clientes de las empresas de TI deben cumplir, y que podrían tener una incidencia directa sobre seguridad de la información y privacidad de datos personales.
- e) Esfuerzo actual de seguridad de la información. Cada organización tiene un nivel particular de seguridad de la información establecido a partir de sus requerimientos de protección y operación, por lo que las iniciativas de mecanismos de control para garantizar privacidad de datos personales tendrá una plataforma de arranque distinta en cada caso.

No obstante la particularidad mencionada en el desarrollo e implementación de estos mecanismos de control y gestión para la privacidad de datos personales, existen premisas que deben tomarse en consideración sin importar la complejidad, naturaleza y alcance de estos mecanismos, a saber:

- a) Las iniciativas que soportan el diseño y adopción de estos mecanismos de control y gestión de la privacidad, deben estar soportadas por la Alta Dirección de la organización de forma activa, al menos en la asignación de recursos y supervisión de resultados.

- b) Se pueden utilizar mejores prácticas, recomendaciones y estándares internacionales como referencias de los resultados que deben obtenerse al implantar los mecanismos de control, así como especificaciones de diseño e implementación de los mismos. Sin embargo, cada uno de estos mecanismos debe atender obligadamente a los requerimientos de cada organización.⁸⁸

- c) El nivel de seguridad de la información (nivel de riesgo aceptable) de las organizaciones, debe integrar el compromiso de privacidad de la empresa con sus clientes, puesto que un buen esfuerzo de seguridad de la información no implica el nivel de privacidad requerido, aunque la privacidad sí descansa en buena medida en un esquema de seguridad de la información adecuado para la organización.

- d) Resulta indispensable ejecutar esfuerzos permanentes respecto a la capacitación y entrenamiento de todas las personas de la organización sobre seguridad de la información y privacidad de datos, de acuerdo a sus funciones cotidianas dentro de los procesos del negocio.

Considerando el enfoque de estas premisas y el estado actual del entendimiento del sector de TI en México sobre las implicaciones de la LFPDPPP, así como sus prácticas relativas actuales, se proponen las siguientes acciones para atender el alcance de la privacidad de datos personales, expresado en la propia estructura de la Ley, como un tópico organizacional más allá de un contexto tecnológico.

⁸⁸ Véase: Apartado III. Estándares Internacionales

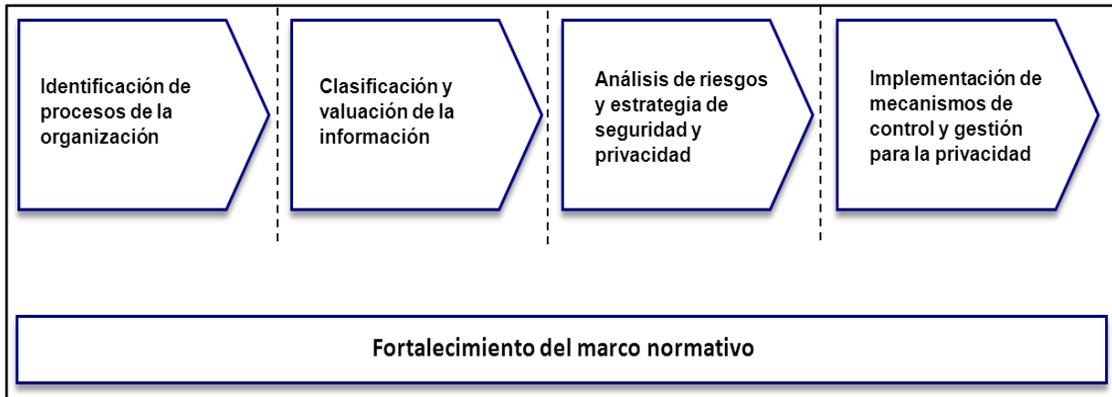


Diagrama de acciones secuenciales para la seguridad de la información y privacidad de datos

Identificación de procesos en la organización

Es recomendable que en este grupo de actividades la organización realice un reconocimiento detallado de todos sus procesos centrales y de soporte, que se presuman relacionados con la obtención y uso de datos personales en el negocio (de acuerdo con los usos establecidos por la LFPDPPP)

El objetivo de la primera fase consiste en que la organización identifique al menos:

- a) El origen de los datos personales en sus procesos y cadenas productivas, cómo se han generado éstos, cómo entran al proceso del negocio y el mecanismo por el que llegan al mismo.
- b) Entidades, funciones y/o roles involucrados en la obtención y usos de los datos personales.
- c) Flujo de los datos personales en los diferentes procesos de la organización, para identificar en dónde comienza y finaliza el compromiso de garantía de privacidad del negocio.

- d) La finalidad del tratamiento de los datos personales en la organización a partir de su presencia en los procesos.
- e) Situaciones de amenaza que puedan afectar la privacidad de los datos personales en los diferentes procesos de la organización.
- f) Escenarios, situaciones o actividades no identificados formalmente en los procesos de la organización, para actualizar la definición formal de estos procesos, así como el contexto del análisis de uso de estos datos.

Clasificación y valuación de la información

En esta fase, se recomienda que la organización realice una valuación de la información que utiliza en todos sus procesos para determinar su importancia con base en sus características de integridad, confidencialidad y disponibilidad, para determinar los mecanismos de control que sean requeridos para cada tipo de información de acuerdo a su clasificación y su valuación.

El personal del negocio (preferentemente el personal responsable del proceso evaluado) determinará los tipos de información y el valor de la misma al proporcionar diferentes percepciones, conocimientos y propósitos, así como los requerimientos de privacidad de los datos personales. La conclusión debe orientarse a una clasificación de la información por su propósito de uso (finalidad), y ser entendible y práctica para la organización.

En este sentido, se propone que se utilicen las siguientes categorías:

De Información

- a) CONFIDENCIAL. El acceso a esta información debe ser altamente restringido y con base en una finalidad justificada. La difusión de esta información requiere de la autorización del responsable del proceso en la organización, o el titular de la misma. Por ejemplo: informes de auditoría, bitácoras y reportes de seguridad, etc.
- b) INTERNA. Información utilizada por los empleados del negocio para la realización de sus funciones; su difusión no causa un daño serio a la organización o a los titulares. Esta información requiere de un acuerdo de confidencialidad y el aviso de privacidad para que sea proporcionada al personal externo o terceros. Ejemplo: políticas, procedimientos, los memorando, los oficios, los directorios telefónicos internos, etc.
- c) PÚBLICA. Es aquella disponible al público para dar a conocer los servicios del negocio, pero sólo existe una persona o función autorizadas en la organización para su difusión.
- d) En caso que la información no tenga una clasificación asignada se considerará como información interna.

De Datos Personales

Tipo de dato ⁸⁹	Ejemplos
Identificación	Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.
Laborales	Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
Patrimoniales	Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

⁸⁹ Clasificación tomada de las “Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales”
http://www.cenni.sep.gob.mx/portales/control_escolar/pdf/legislacion_datos_personales/recomendaciones_sdp.pdf revisado el 14 de julio de 2012, 19:45 hrs.

Tipo de dato ⁸⁹	Ejemplos
<p>Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales</p>	<p>Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.</p>
<p>Datos Académicos</p>	<p>Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.</p>
<p>Tránsito y movimientos migratorios</p>	<p>Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.</p>
<p>Datos Ideológicos</p>	<p>Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas entre otros.</p>
<p>Datos de Salud</p>	<p>Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de</p>

Tipo de dato ⁸⁹	Ejemplos
	aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
Características personales	Tipo de sangre, ADN, huella digital, u otros análogos.
Características físicas	Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
Vida sexual	Preferencia sexual, hábitos sexuales, entre otros.
Origen	Étnico y racial

A partir de las categorías de información definidas y su asociación con el propósito de uso, es indispensable que se definan las acciones mínimas a ejecutar de acuerdo a su categoría y la acción por el propósito de uso. Con base en las necesidades identificadas de las empresas del sector de TI, se recomiendan al menos:

TIPO DE ACCIÓN	CONFIDENCIAL	INTERNA	PÚBLICA
Almacenamiento en medios fijos	Cifrado o Control de acceso físico	Cifrado	Sin Cifrado
Almacenamiento en medios intercambiables	Cifrado	Cifrado	Sin Cifrado
Copiando	Permiso/Conocimiento del responsable del proceso/titular del dato personal	Sin restricciones	Sin restricciones
Faxeando	Cifrado en líneas o recepción atendida	Sin restricciones	Sin restricción
Enviando a través de la red pública	Cifrado	Cifrado	Sin Cifrado
Destrucción	Asegurando su destrucción físicamente	Depositada en basureros ordinarios, pero con procedimientos de destrucción	Depositada en basureros ordinarios
Entregada a Terceros	Autorizar y firmar convenio de confidencialidad y acuerdo de privacidad	Firmar convenio de confidencialidad y aviso de privacidad	Sin restricciones
Etiquetarse los medios electrónicos	Implementar etiquetas internas y externas	No requiere etiqueta	Fecha de liberación y su clasificación como

TIPO DE ACCIÓN	CONFIDENCIAL	INTERNA	PÚBLICA
			PÚBLICA
Etiquetar los logs o bitácoras en hardcopy	En cada página, en las cubiertas inicial y final	No requiere etiqueta	Fecha de liberación y su clasificación como PÚBLICA
Empaquetando para correo interno o externo	Dirigido específicamente a la persona (receptor) y se etiqueta internamente	En sobre sin ninguna etiqueta o marca	En sobre sin ninguna etiqueta o marca
Otorgando derechos de acceso	Sólo los otorga el responsable del proceso o aplicación a partir del acuerdo con el Responsable y/o Titular	Los otorga el propietario	Los otorga el personal autorizado de la organización para su difusión
Registrando en logs o bitácoras	Registrar receptores, las copias que se hacen, las ubicaciones, las direcciones, quienes consultan y quienes modifican, borran o destruyen información	No se registra	No se registra

Asimismo, se deben definir y establecer formalmente las acciones de tratamiento básico de la información de acuerdo a su categoría:

- a) Obtención de la información y datos personales

- b) Inventario de las bases de datos, registros y colecciones de información y datos personales
- c) Comunicación y transmisión de la información y datos personales
- d) Destrucción de la información y datos personales
- e) Seguridad en el transporte de información y datos personales
- f) Almacenamiento de información y datos personales

Los resultados de estas actividades permitirán enfocar de mejor manera los esfuerzos de protección de la información y privacidad de datos personales, con base en la importancia que tenga la información para el negocio de acuerdo a su contexto de uso, puesto que la toma de decisiones sobre prioridades de protección puede basarse en la clasificación asignada.

Análisis de riesgos y estrategia de seguridad y privacidad

El objetivo de este grupo de actividades es que la organización pueda realizar una medición y jerarquización de las situaciones de riesgo de seguridad de la información y privacidad de datos personales, derivados de la forma de operación actual y el uso de la tecnología, con base en su impacto de estos riesgos para el negocio y su nivel de vulnerabilidad asociado, en el ambiente de procesamiento de la información.

De tal suerte que se tengan los elementos suficientes para delimitar una estrategia de seguridad y privacidad, que minimice los riesgos hasta un nivel aceptable para el negocio y el tratamiento por el tipo de dato personal definido por la LFPDPPP, que permita establecer las bases de una arquitectura de seguridad y privacidad de la información que satisfagan los requerimientos actuales y futuros de una operación confiable, segura, repetible y auditable con respecto a la misma Ley.

El alcance de este análisis de riesgos debe centrarse en los procesos, aplicaciones o unidades de análisis (funciones, actividades, servicios de TI, entre otros) relacionados con el uso de datos personales en la organización. En este sentido, se recomienda que los elementos mínimos para su determinación sean:

- a) Valor del activo de información o datos personales para el negocio
- b) Nivel de vulnerabilidad (o efectividad actual de los controles de seguridad y privacidad de la información)
- c) Nivel de impacto al negocio en cada situación de riesgo, suponiendo que ocurran
- d) Probabilidad o posibilidad de las amenazas a la forma actual de operación

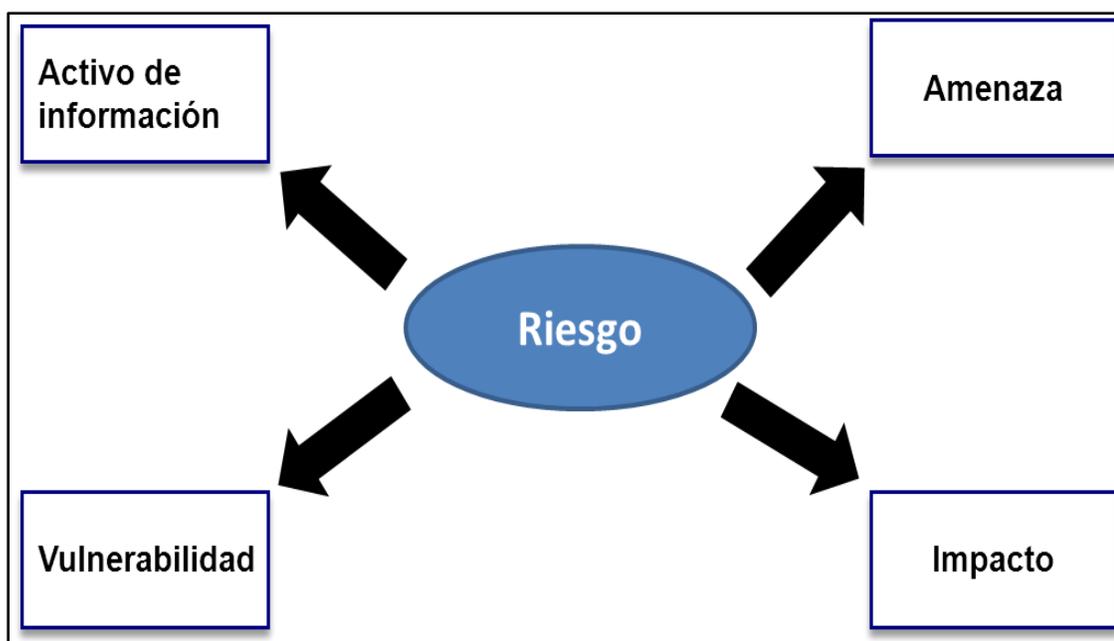


Diagrama de componentes del riesgo de seguridad y privacidad de la información

Para facilitar la ejecución de este ejercicio, es recomendable que puedan crearse categorías representativas para la evaluación, esto es, en vez de

trabajar con catálogos o listados exhaustivos de cada elemento del riesgo a partir de las propuestas de los participantes, éstas pueden ser consolidadas en grupos más genéricos a partir de su relación con las características de la información (integridad, confidencialidad, disponibilidad). Asimismo, se recomienda evitar las escalas de evaluación con graduaciones muy detalladas; en este caso, podría resultar práctico identificar un valor más bajo, un valor más alto, y un grado medio, por lo que una escala con 5 valores es factible.

La organización debe elegir una metodología para el análisis de riesgo, que sea representativa y viable en su naturaleza, es decir, deberá optar entre una metodología cuantitativa (con un requerimiento de números precisos), o bien, una cualitativa (con un fundamento matemático pero basado en percepciones de las mediciones de los elementos del riesgo). En ambos casos se debe garantizar que el análisis de riesgos se ejecute como un ejercicio grupal de evaluación de los elementos del riesgo, cuyos resultados se obtengan de la participación en conjunto de aquellas personas con un rol/responsabilidad en los procesos, evitando evaluaciones subjetivas o aisladas.

A continuación se muestran algunos atributos de los dos tipos de metodologías mencionadas:

Atributo	Cuantitativo	Cualitativo
Requiere cálculos más complejos	X	
Grado de suposición		X
Es fácilmente automatizado	X	

Proporciona un análisis de costo/beneficio	X	
Usa métrica objetiva e independiente	X	
Proporciona las opiniones del personal que mejor conoce los procesos		X
Muestra pérdidas claras que pueden ser acumuladas en el tiempo de un año	X	

Cabe señalar que actualmente las metodologías cuantitativas no son las más utilizadas, puesto que su requerimiento de valores numéricos precisos para cada componente del riesgo, tiende a crear escalas de evaluación poco representativas, basadas en promedios aritméticos o en los límites de estas escalas. En el caso de las metodologías cualitativas, se requieren mecanismos de evaluación menos rígidos que se utilizan con base en la percepción (por conocimiento del negocio y riesgos) de los participantes, y permiten condensar todas las aportaciones.

Es importante mencionar que más allá de la metodología específica de análisis y evaluación de riesgos que el negocio seleccione, el resultado del ejercicio debe permitir una clara identificación de las prioridades de seguridad de la información y privacidad de datos personales con base en la afectación de su misión/objetivos organizacionales, las cuales funcionarán como entrada para la selección de las alternativas de remediación.

Al finalizar el análisis y evaluación de riesgos, el negocio encontrará una lista de aspectos conocidos sobre seguridad de la información y ahora privacidad de datos personales, que deben ser resueltos con las restricciones usuales de recursos humanos, técnicos y económicos. Así pues, se debe desarrollar un enfoque paulatino de resolución con la participación del personal con funciones de seguridad de la información, expertos funcionales del negocio, gestión de tecnología de información y privacidad en la organización.

Cabe mencionar que no se han identificado metodologías para el desarrollo de la estrategia de seguridad de la información y privacidad de datos personales. Sin embargo, un curso de acción mínimo sugerido es:

- 1) Identificar categorías o grupos de mecanismos de control que ayuden a resolver la problemática o prioridades identificadas en la evaluación de riesgos, esto puede realizarse a partir de una lluvia de ideas de los participantes mencionados anteriormente.
- 2) Realizar una evaluación uno a uno, sobre el nivel de contribución del mecanismo de control para resolver la categoría de riesgo (asociación matricial). En este caso, esta contribución no debe ser conceptual del control contra las categorías de riesgo de la priorización obtenida en el análisis de riesgos, sino basada en la efectividad de los controles actuales de seguridad y privacidad de la información.
- 3) Como parte de la asignación del nivel de contribución para resolver el riesgo de los mecanismos de control, debe considerarse la prioridad de la categoría del riesgo con la que se está asociando el control, de tal suerte que un control tenga mayor peso si se relaciona con riesgos más prioritarios para el negocio.

Esta dinámica se puede realizar de forma grupal. El grupo compartirá la información fundamental de la efectividad de los controles actuales, para determinar su nivel de contribución y disminuir el nivel global de riesgo.

De forma similar al análisis y evaluación de riesgo –en este caso, en el resultado final del ejercicio—, la organización encontrará una lista de mecanismos de control y gestión de seguridad de la información y privacidad de datos personales, ordenada por su grado de ayuda al negocio para disminuir el nivel global de riesgo, es decir, no solamente se centrará en resolver los riesgos más importantes, sino que la decisión de desarrollar un control se basará en resolver los riesgos más relevantes para la organización hasta un nivel adecuado y en cumplimiento con la Ley.

Este resultado también permitirá que se determine la secuencia de ejecución de las iniciativas para el desarrollo e implantación de estos controles, estimando los recursos (económicos, humanos y técnicos) necesarios para cada una de ellas.

Implementación de mecanismos de control y gestión para la privacidad de datos personales

El objetivo para las organizaciones en esta última fase de acciones recomendadas, consiste en establecer los mecanismos específicos de control que incrementen la seguridad de la información para garantizar el nivel de privacidad requerido sobre datos personales.

Para lograr una efectividad adecuada de estos controles, la organización debe encontrar un balance de los mismos de acuerdo a lo siguiente:

La posición del control respecto al riesgo. La organización debe optar por controles preventivos, de detección o correctivos. Asumiendo que los preventivos son los más deseables, pero los más costosos o con mayores implicaciones de operación.

La naturaleza del control. La organización debe considerar la implementación de controles administrativos, operativos y técnicos de acuerdo al objetivo de protección en los procesos de negocio y estrategia de seguridad.

La forma de implementación del control. La organización debe decidir para la ejecución de los controles, si se apoyará en mecanismos automatizados, semi automatizados, o bien, manuales. Debe tenerse en cuenta que un control más efectivo es automatizado, y el menos efectivo es aquel cuya implementación es manual.

La combinación de estas características de los controles tiene una incidencia directa en la factibilidad de implementación/operación, efectividad de protección y costo de los controles, por lo que su selección atiende directamente al nivel de riesgo identificado por la organización y su estrategia de seguridad correspondiente.

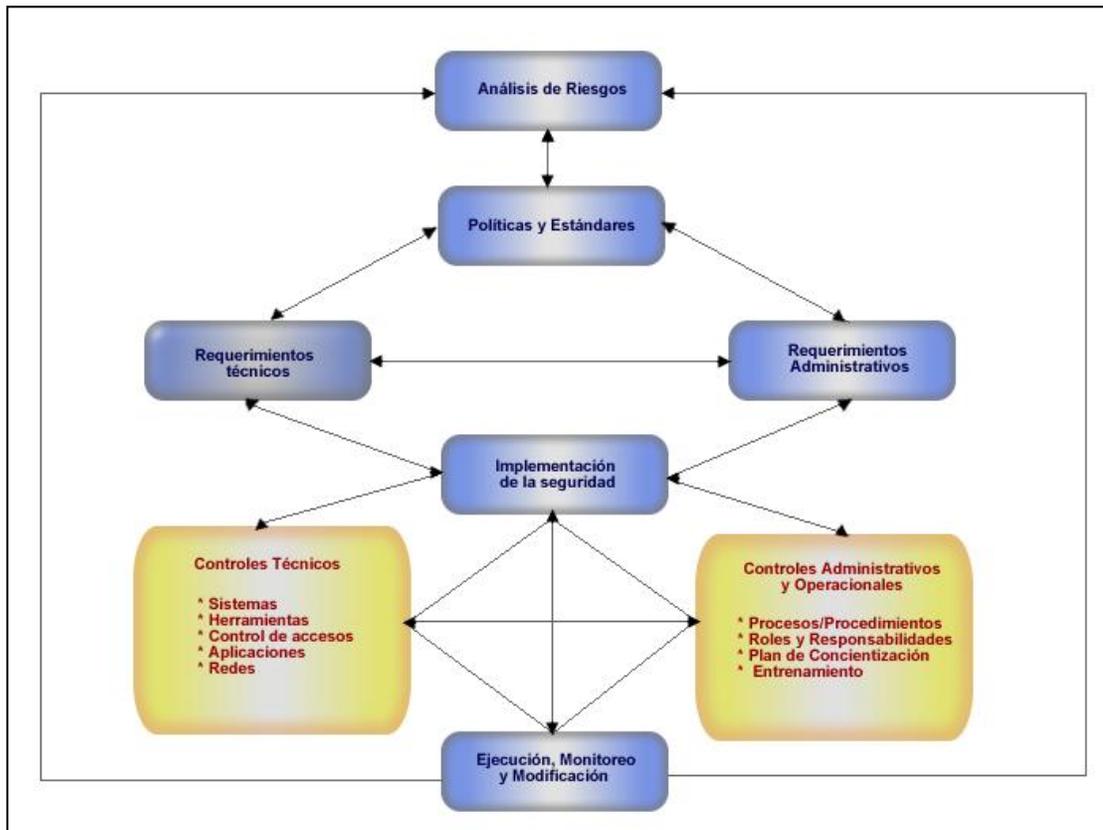


Diagrama de implementación de la normatividad de Seguridad de la Información

En estricto apego a los requerimientos regulatorios establecidos por la LFPDPPP y su Reglamento, se recomienda un grupo mínimo de controles que las organizaciones pueden implementar para cumplirlos:

Controles administrativos

1. Planeación de recursos de procesamiento y seguridad de la información.

El propósito de este mecanismos de control es garantizar que la capacidad instalada y futura de tecnología de información y seguridad estén alineadas con los procesos de la organización, a

partir de soportar sus requerimientos actuales de efectividad y eficiencia, así como su crecimiento natural.

Para que este propósito se cumpla, en la definición de este control debe considerarse al menos:

- a) Determinar las directrices de la organización y expectativas de seguridad y privacidad por parte de los titulares y los responsables. El personal relacionado con actividades funcionales en las áreas de procesamiento de TI y seguridad de la información, debe contemplar las estrategias y objetivos de negocio de la organización para realizar la planeación de la operación de las capacidades actuales.
- b) Alineamiento estratégico. Todas las adquisiciones e instalaciones de recursos de tecnología y seguridad, deben atender a un requerimiento de los titulares y responsables de datos personales.
- c) Medición del desempeño. Efectuar mediciones de la operación de seguridad y procesamiento de TI para determinar si cumplen con los niveles esperados por los titulares y responsables de datos personales.

Asimismo, la función de tecnología y seguridad de la información deberá asegurar el monitoreo continuo de tendencias futuras y condiciones regulatorias, de tal manera que estos factores puedan ser tomados en consideración durante el desarrollo y mantenimiento del plan de alineación de la infraestructura tecnológica.

2. Definición de roles y responsabilidades

Es fundamental que dentro del marco normativo de seguridad y privacidad de la información, se definan las áreas involucradas en la ejecución de los controles y se definan cada uno de los lineamientos corporativos, con base en la función de cada persona involucrada.

En este caso, se recomienda que se identifiquen y definan al menos responsabilidades genéricas relativas a:

- a) Ejecución de la política, procedimiento o control
- b) Supervisión de la política, procedimiento o control
- c) Conocimiento de la política, procedimiento o control
- d) Responsable de la política, procedimiento o control

Para la elaboración y mantenimiento de las políticas, estándares y guías debe indicarse la audiencia a quién está dirigida, esto es, el personal que debe conocer, aplicar y lograr que se cumpla con la normatividad. Los aspectos mínimos que deben asignarse a las audiencias son:

- e) Entender los riesgos y uso de los tipos de información
- f) Seleccionar el nivel de sensibilidad y criticidad de la información
- g) Especificar mecanismos de control suplementarios para proteger la información
- h) Autorizar los requerimientos de acceso a su información
- i) Revisar las listas de control de acceso a su información
- j) Resguardar y mantener posesión física de la información
- k) Seguir las indicaciones del propietario de la información para su manejo y/o procesamiento
- l) Proporcionar reportes periódicos de quiénes tienen acceso

- m) Hacer recomendaciones técnicas y de procedimientos al responsable de la información
- n) Mantener el acceso seguro a las instalaciones de la información
- o) Reforzar los controles especificados por el responsable de los datos personales
- p) Solicitar el acceso a su información
- q) Abstenerse de utilizar información y/o sistemas si no cuenta con la debida autorización
- r) Cumplir con los controles establecidos
- s) Reportar errores y anomalías en la información o en los mecanismos de control
- t) Reportar violaciones al área encargada

Estas responsabilidades deben definirse en primera instancia en el documento central de políticas o estándares, y reflejarse en cada uno de los procedimientos o mecanismos de ejecución.

De la misma manera, dentro de este control deben definirse y asignarse puntualmente las funciones del área o áreas de seguridad de la información y privacidad de datos, tales como:

- a) Evaluación y administración del riesgo
- b) Planes de acción de seguridad y privacidad de la información
- c) Análisis de requerimientos, estándares y tecnología
- d) Identificación de los procesos críticos de la organización
- e) Identificación y selección de proveedores y socios de negocio
- f) Creación de marco normativo de seguridad

Esta definición de roles y responsabilidades debe garantizar una segregación funcional básica que excluya la posibilidad de que un solo individuo responda por un proceso crítico. De igual forma,

deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos.

3. Revisión de contratos y convenios con terceros

A partir de la asignación de roles y responsabilidades, es imperativo que la organización realice una revisión detallada de todo el contexto legal con sus proveedores, socios de negocio y clientes para identificar al menos:

- a) Identificación y clasificación de los datos personales
- b) Requerimientos de seguridad y privacidad
- c) Niveles de servicio informático, seguridad y privacidad
- d) Responsabilidad de mantenimiento del nivel de seguridad
- e) Autorización de subcontratación para tratamiento de datos personales
- f) Tiempos de respuesta ante incidentes y brechas de seguridad
- g) Multas y penalizaciones por desviaciones
- h) Fronteras en la entrega y consumo de servicios informáticos
- i) Obligaciones a las que se encuentra sujeto el responsable en caso de transferencias internacionales

Cada uno de estos rubros debe detallarse en los contratos que rigen los servicios con los responsables de datos personales (de acuerdo a la LFPDPPP).

La ejecución de estas actividades de control requiere de un grupo de trabajo interdisciplinario: área legal, área comercial, área de operación y servicios, área de seguridad de la información y atención a clientes; de tal suerte que se logre un análisis desde todas las perspectivas del servicio que se provee.

4. Capacitación y entrenamiento

Este control debe establecerse como una práctica corporativa para asegurar que el personal reciba orientación al ser contratado, así como entrenamiento y capacitación constante. La finalidad es conservar los conocimientos, habilidades, destrezas y conciencia de seguridad y privacidad al nivel requerido, para la ejecución efectiva de sus tareas. Los programas de educación y entrenamiento dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal deberán ser revisados regularmente.

Se recomienda que la capacitación y entrenamiento se desarrollen bajo una estrategia basada en las carencias reales de entendimiento y prácticas de seguridad de la organización. También se recomienda una estrategia de difusión a través de los canales de comunicación de mayor preferencia entre los propios usuarios, que permita crear una cultura del uso y manejo de los recursos de TI y datos personales, hasta lograr una transformación en su forma de pensar y operar.

Las estrategias sugeridas deberán ejecutarse en fases, de esta forma se alcanzará el nivel de madurez adecuado:

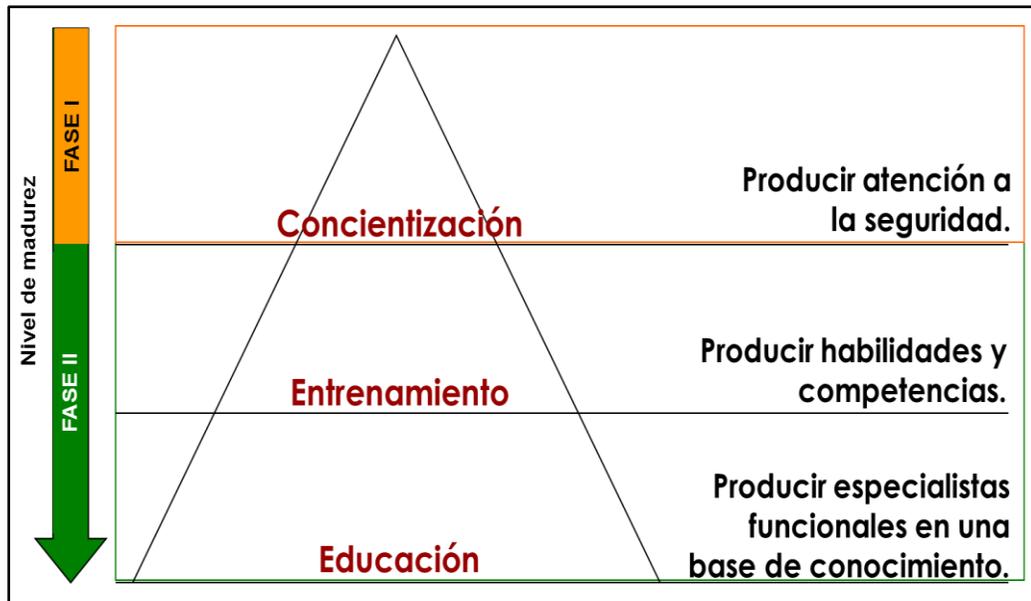


Diagrama de estrategia de concientización y entrenamiento en seguridad de la información y privacidad de datos

De igual forma, es conveniente que la ejecución de estas estrategias –en la creación y divulgación de contenidos– atienda al tipo de función (audiencia) del personal en la organización.

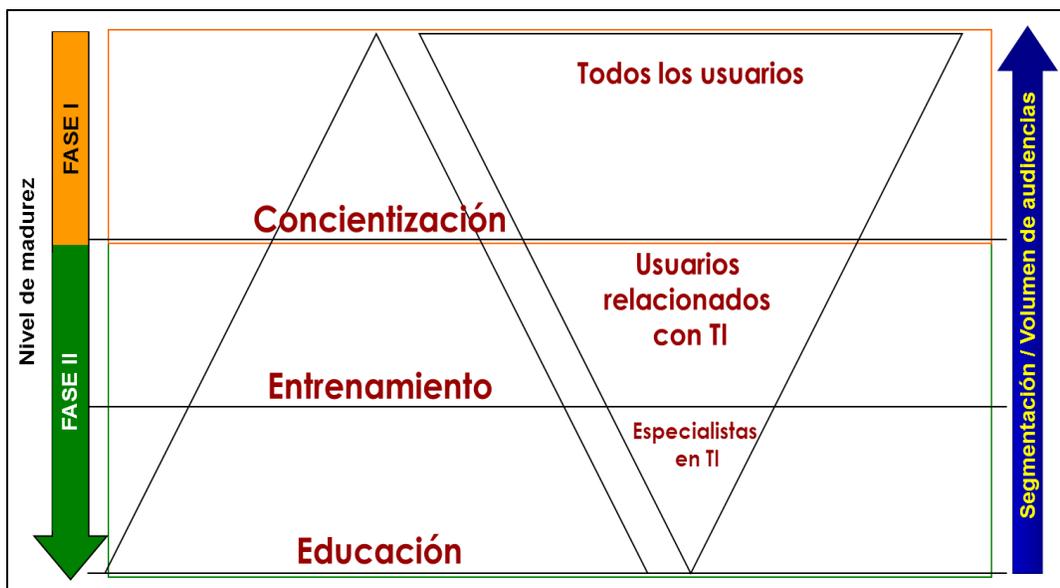


Diagrama de estrategia de concientización y entrenamiento en seguridad de la información y privacidad de datos de acuerdo a las audiencias

Finalmente, cada una de las actividades que se realicen en la definición y ejecución de las estrategias, deberán establecerse como un proceso organizacional formal, que contemple gradualmente el cumplimiento de estos rubros como parte del desempeño laboral de los empleados.

5. Clasificación práctica de la información y datos personales

Como parte de las fases anteriores de estas recomendaciones, se ha establecido la importancia de realizar una clasificación práctica de la información y datos personales dentro de la organización, principalmente, para lograr el tratamiento y nivel de protección adecuado para los datos personales que se utilizan en los procesos de la organización.

En estos controles deben establecerse los mecanismos que permitan clasificar la información en rubros tales como:

- a) Confidencial
- b) Interna
- c) Pública
- d) Datos personales de identificación/laborales
- e) Datos personales patrimoniales, académicos, financieros y sobre procedimientos administrativos seguidos en forma de juicio o jurisdiccionales, de tránsito y movimientos migratorios
- f) Datos personales sensibles (ideológicos, de salud, características personales, características físicas, vida sexual y origen)

Es importante definir cómo asignar la responsabilidad de su aseguramiento en la organización, dentro de los procesos en que se utiliza esta información. Adicionalmente se debe contar con mecanismos que permitan utilizar las funciones de cifrado de datos

y certificados digitales de acuerdo a la clasificación de esta información.

Ahora bien, para el diseño de estos controles pueden tomarse en consideración estas recomendaciones, y las que se han establecido en la fase correspondiente a "Clasificación y valuación de la información", sin menospreciar su establecimiento como un proceso corporativo que contemple actividades de:

- a) Ejecución de los mecanismos de valuación de información
- b) Supervisión de los mecanismos de valuación de información
- c) Conocimiento de los mecanismos de valuación de información
- d) Responsabilidad de los mecanismos de valuación de información

6. Análisis y evaluación de riesgos de seguridad y privacidad de datos

La organización deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de seguridad y privacidad de la información relevante, para el logro de los objetivos del negocio y el cumplimiento de los niveles de privacidad adquiridos con los responsables y titulares (directa o indirectamente). En consecuencia, se formará una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable.

El proceso deberá proporcionar evaluaciones de riesgos, tanto a un nivel global como a niveles específicos de la organización y sus procesos, para nuevos proyectos y para casos recurrentes y con participación multidisciplinaria. Este proceso deberá asegurar que

se realicen reevaluaciones y que la información sobre la evaluación de riesgos sea actualizada con base en auditorías, inspecciones e incidentes identificados.

Como se ha mencionado anteriormente, el análisis y evaluación de riesgos deberá establecerse como un proceso organizacional, considerando al menos los siguientes elementos específicos:

- a) Selección de una metodología de análisis y evaluación de riesgos. deberá establecer un enfoque general para la evaluación de riesgos que defina el alcance y los límites, la metodología que se adoptará para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas.
- b) Identificación de riesgos. La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo y las relaciones causa/efecto entre ellos. Los elementos esenciales de riesgo incluyen activos tangibles e intangibles, valor de los activos, amenazas, vulnerabilidades, protecciones, consecuencias y probabilidad de amenaza. El análisis de riesgos deberá considerar el negocio, regulaciones, aspectos legales, tecnología, relaciones con terceros (socios de negocio y responsables, según la LFPDPPP) y riesgos del factor humano.
- c) Medición de riesgos. El enfoque de la evaluación de riesgos deberá asegurar que la información del análisis de la identificación de riesgos genere como resultado una medida cuantitativa y/o cualitativa del riesgo al cual está expuesta el área examinada. Asimismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización.

- d) Plan de acción contra riesgos identificados (estrategia de seguridad y privacidad). El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos para asegurar que el costo- efectividad de los controles y las medidas de seguridad mitiguen los riesgos en forma continua. El plan de acción contra los riesgos deberá identificar la estrategia de riesgos con el fin de evitar, mitigar o aceptar el riesgo.

Lo cierto es que para el diseño de estos controles se pueden tomar en consideración las recomendaciones apuntadas, y las que se han establecido en la fase correspondiente de "Análisis de riesgos y estrategia de seguridad y privacidad" Por supuesto, sin menospreciar su establecimiento como un proceso corporativo, que contemple actividades de:

- a) Ejecución de los mecanismos de análisis y evaluación de riesgos.
- b) Supervisión de los mecanismos de análisis y evaluación de riesgos.
- c) Conocimiento de los mecanismos de análisis y evaluación de riesgos.
- d) Responsable de los mecanismos de análisis y evaluación de riesgos.

Controles físicos/operativos (gestión técnica de la seguridad de la información y privacidad de datos) y técnicos

1. Gestión técnica de vulnerabilidades

Los objetivos principales de este control son identificar y solucionar las debilidades en el diseño y operación de los diferentes recursos

de infraestructura tecnológica, que podrían ser el punto de partida para una brecha de seguridad de la información, a partir de la corrección de configuraciones, diseño, políticas y estándares relacionados con el activo de información analizado.

Es indispensable realizar un enfoque integral de análisis y evaluación de vulnerabilidades en los siguientes activos de la información:

- a) Bases de datos
- b) Plataformas o sistemas operativos
- c) Aplicaciones
- d) Infraestructura específica de seguridad
- e) Segmentos de red
- f) Ambientes virtualizados

Sin embargo, el proceso de gestión de vulnerabilidades debe permitir corregir las debilidades de control que causan estas vulnerabilidades en los activos de información, por lo que se sugiere instaurar las siguientes fases:

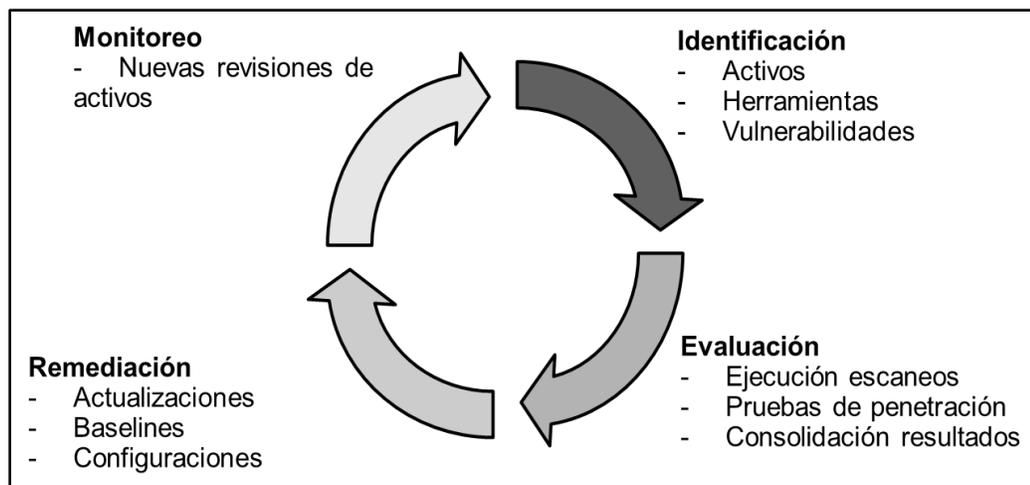


Diagrama del proceso de gestión técnica integral de vulnerabilidades

- a) Identificación. En primera instancia, se debe definir qué activos de la información serán evaluados en cada ciclo, así como las herramientas que serán utilizadas para su análisis y vulnerabilidades potenciales que se están buscando.
- b) Evaluación. A través de herramientas o mecanismos especializados se hace una identificación activa de las debilidades de control en cada capa de activo de la información, que podría ocasionar una brecha de seguridad. En ocasiones puede buscarse explotar la vulnerabilidad para eliminar una identificación falsa (falso positivo), asimismo, se realiza un análisis del contexto y severidad de la vulnerabilidad. con todos los resultados de los demás activos analizados en el ejercicio ponderando su criticidad o sensibilidad por su relación con los datos personales.
- c) Remediación. Se determinan las acciones que corrigen las debilidades de control encontradas en la infraestructura. En este caso se recomienda definir un plan de acción por tipo de acción a ejecutar: actualización del activo por parte del fabricante, ajuste de configuración, creación de nuevas políticas, entre otros.
- d) Monitoreo. Una vez que se han aplicado las correcciones, se deberá reasegurar que las debilidades desaparecieron, o permanecen dentro de los límites tolerables de la organización. Adicionalmente, se pueden agregar listas de activos de la información a revisar en ejercicios futuros.

Como parte de la definición de la gestión de vulnerabilidades técnicas, es importante considerar la definición de métricas de

efectividad del proceso, y fronteras con otros procesos como el análisis de riesgos (utiliza el nivel de vulnerabilidad como insumo para determinar el nivel de exposición a ataques o brechas de seguridad), o aquellos controles que permiten resolver las debilidades de seguridad desde su causa raíz, como muestra la siguiente gráfica.

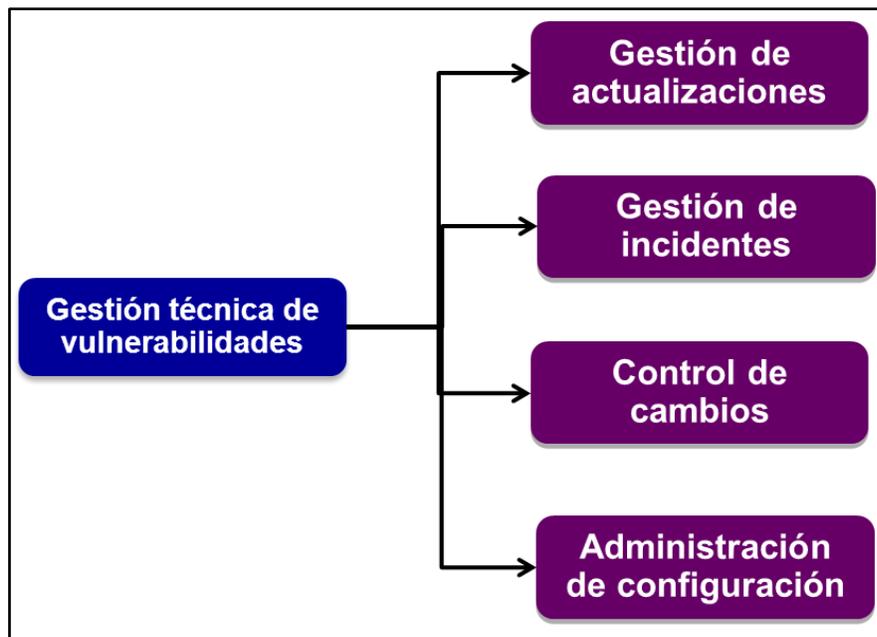


Diagrama de dependencias y relaciones de la gestión técnica de vulnerabilidades

La gestión de vulnerabilidades es un elemento fundamental para evitar incidentes o brechas de seguridad que puedan afectar el nivel de privacidad en aquella infraestructura que procesa datos personales. Todas las actividades realizadas al respecto, podrán resguardarse como evidencia del compromiso de la organización para mantener el nivel de seguridad requerido por tipo de datos personales utilizados.

2. Control de acceso lógico

La organización deberá definir un modelo de control de acceso lógico a los diferentes recursos informáticos en los que se procesen datos personales, de tal suerte que permita cumplir con los principios de identidad, responsabilidad y rastreabilidad, considerando la segregación de funciones.

En la definición de este control, la organización deberá abordar la problemática de la gestión de la identidad digital del usuario y control/monitoreo de sus accesos o actividades en los recursos informáticos. Deberán considerarse al menos, los siguientes aspectos:

- a) Solicitud, autorización y ejecución de la creación, modificación o eliminación de las cuentas de acceso
- b) Sincronización de las identidades digitales en los diferentes recursos de la infraestructura
- c) Centralización de las políticas y reglas sobre identidades digitales y accesos de la infraestructura
- d) Habilitación de alternativas para auto administración de cuentas y contraseñas por parte de los usuarios finales
- e) Aumentar las capacidades técnicas para gestión de bitácoras, pistas de auditoría y monitoreo de las actividades de las cuentas de usuario en la infraestructura crítica

Este modelo debe permitir que todos los usuarios y administradores tengan mecanismos seguros de acceso apegados a los privilegios naturales de su función dentro de la organización. Asimismo,

permite que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente, en forma regular, para identificar y resolver incidentes que involucren actividades no autorizadas. El acceso lógico a la información sobre el registro de recursos de cómputo (seguridad y otras bitácoras) deberá otorgarse tomando como base el principio de menor privilegio.

Algunos de los aspectos mínimos que tendrán que definirse para la operación de este modelo, son:

- a) Identificador único de usuario
- b) Contraseña o método de autenticación (con base en la criticidad o sensibilidad de la información)
- c) Personal que da autorizaciones para los accesos
- d) Mecanismos para el flujo de la identidad digital y accesos (solicitud, modificaciones, creación y eliminación)
- e) Revocación de accesos
- f) Revisión periódica de los privilegios asignados a los usuarios
- g) Bloqueo de cuentas de usuario
- h) Preservación de evidencias de actividades de usuarios
- i) Control de acceso remoto

En la implementación de este control, se pueden requerir diferentes controles tanto de proceso como técnicos de acuerdo a las responsabilidades y actividades de cada usuario.

3. Control de cambios y gestión de las configuraciones

El propósito de estos controles es asegurar que la administración de cambios en los componentes de infraestructura tecnológica y de seguridad, así como el control y la distribución de software sean integrados apropiadamente en un sistema completo de administración de configuración. El sistema utilizado para monitorear los cambios a los sistemas de aplicación deberá soportar el registro y seguimiento de los cambios realizados en los grandes y complejos sistemas de información.

El control de cambios tendrá que establecer parámetros claros a través de una definición de cambios de emergencia y procedimientos. Esto será así cuando se traspasen los procesos normales de análisis de prioridades de la gerencia para su implementación. Los cambios de emergencia deberán ser registrados y autorizados por la gerencia de TI.

Se recomienda considerar los siguientes aspectos en la estructura del control de cambios y gestión de las configuraciones:

- a) Solicitud de un requerimiento
- b) Evaluación de solicitud
- c) Descripción de la solicitud (Análisis de impacto)
- d) Desarrollo
- e) Pruebas
- f) Documentación

- g) Solicitud de migración de componentes
- h) Recepción y validación de documentación y componentes
- i) Programación y coordinación de la migración
- j) Migración al Ambiente de Producción
- k) Validación de componentes
- l) Validación en ambiente de producción

La ejecución de cada una de las actividades de los aspectos antes mencionados, deberá generar una evidencia que se preserve para evaluar la efectividad del proceso, enseguida deberá analizar causas raíz de fallas potenciales e investigar alguna brecha de seguridad relacionada con vulnerabilidades generadas a partir de cambios en los componentes de la infraestructura.

Es fundamental definir las relaciones y dependencias del control de cambios con otros controles relativos a la continuidad del servicio informático. El objetivo es asegurar que todos los activos informáticos se mantengan actualizados con respecto a los requerimientos de operación definidos para satisfacer los acuerdos con los responsables y/o titulares de los datos personales.

4. Cifrado de la información

Como parte de la identificación y clasificación de la información y datos personales, es recomendable que se implemente un esquema de cifrado de datos de acuerdo a su clasificación y ubicación en los activos informáticos.

La organización deberá seleccionar un algoritmo de cifrado cuya fortaleza corresponda al tipo de información y datos personales que procese o almacene, dejando una constancia de este análisis y selección. Es recomendable que se utilice un algoritmo público que esté probado en la industria.

Una vez seleccionado el algoritmo de cifrado, la organización deberá definir el modelo integral de cifrado de la información, considerando de forma mínima los siguientes aspectos:

- a) Escenarios de transferencia de información en diferentes modelos
 - Transferencias de información con entidades y dependencias gubernamentales.
 - Correo electrónico seguro
 - Contraseña tanto en su almacenamiento como en su transferencia
 - Información residente en bases de datos
- b) Fortaleza de la llave por almacenamiento de los datos personales
 - Discos duros en servidores
 - Discos duros externos
 - Esquema de cómputo en la nube
 - Dispositivos móviles de almacenamiento
 - Unidades de almacenamiento virtuales (compartidas)
- c) Identificación del flujo de información en los procesos del negocio, y activos informáticos (redes, almacenamiento, equipos de usuario final, servidores)

- d) Instalación del programa de cifrado para cada tipo de información o dato personal
- e) Resguardo de las llaves de cifrado
- f) Generación y cambio de las llaves de cifrado
- g) Revocación de las llaves de cifrado

La complejidad de este modelo de cifrado tendrá que atender el nivel de operación de la organización, puesto que hay una relación inversamente proporcional entre un cifrado robusto y una operación flexible o rápida. Ahora bien, bajo ninguna circunstancia se recomienda que la organización permita que los usuarios finales instalen algoritmos de cifrado propios o fuera del control de la organización.

5. Respaldos y restauración de la información

El objetivo es implementar una estrategia apropiada de respaldo y recuperación de información y datos personales, para asegurar que ésta incluya una revisión de los requerimientos del negocio (contractuales y legales de acuerdo a la LFPDPPP), así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.

Esta estrategia puede implementarse a partir del establecimiento de procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia definida, y que las copias de respaldo sean verificadas regularmente. Se deberán considerar al menos los siguientes aspectos:

- Determinar la periodicidad de los respaldos considerando al menos los siguientes puntos: requerimientos de operación, requerimientos legales, recuperación por fallas, errores o desastres, requerimientos para DRP, estadísticas, etc.
- Indicar qué información va a ser respaldada; por ejemplo, archivos, programas, etc., especificando la ruta de acceso a esta información.
- Asignar al dueño del aplicativo la responsabilidad de indicar qué información es necesario respaldar.
- Definir requerimientos mínimos de información a ser respaldada por cada aplicación.
- Revisar la integridad de los respaldos identificando que estos se generaron de forma adecuada y de manera integral.
- Realizar pruebas regulares a los medios de almacenamiento de datos, estableciendo periodos de revisión del funcionamiento de los respaldos en función de la importancia de la recuperación de la información.
- Revisar la integridad de la información en los respaldos.
- Revisar los medios de almacenamiento (discos, cintas magnéticas, discos ópticos, etc.) que son reciclados antes de volver a respaldar información, conforme al tiempo de vida especificado por el fabricante.
- Contar con la autorización del área responsable de la información dentro de la organización, para hacer uso de ésta en los medios de almacenamiento.

- Especificar el período mínimo y máximo de retención de la información respaldada.
- Asignar el perfil indicado a la cuenta de usuario para realizar los respaldos y/o para restaurar la información almacenada (cuenta con privilegios para respaldar y restaurar) de acuerdo a su función y responsabilidad.
- Contar con una copia de respaldo adicional de la información crítica. No deberá ser almacenada en el mismo lugar que el respaldo original.
- Resguardar los respaldos en un lugar seguro fuera del centro de cómputo, con condiciones ambientales adecuadas y acceso controlado.
- Registrar en una bitácora los respaldos realizados de información donde se refleje al menos la siguiente información: tipo de respaldo, nombre del que lo realizó, fecha, hora, identificador, lugar de ubicación.
- Resguardar la bitácora donde se registra la información de la realización de los respaldos.
- Etiquetar el respaldo con información necesaria para reconocer el tipo de respaldo, fecha de elaboración, hora, identificador, etc.
- Contar con medios de almacenamiento aceptables que no estén sujetos a una rápida degradación, los cuales almacenarán información por periodos de tiempo largos (más de un año).
- Cifrar los respaldos almacenados Off-Site, de acuerdo al esquema establecido corporativamente.

- Obtener autorización para la sustitución, bloqueo, borrado o destrucción de la información en medios magnéticos.
- Contar con mecanismos seguros para la supresión de información almacenada cuando ya no sea necesaria.
- Contar con un registro de la información suprimida considerando al menos la fecha en que se llevó a cabo, quién lo autorizó, quién lo realizó y qué información se encontraba involucrada.
- Trasladar los respaldos y/o las copias fuera de las instalaciones de la organización únicamente por personal autorizado en contenedores especiales y de forma segura para su traslado.
- Realizar respaldos automáticos de los servidores de área local utilizando el software de respaldo o del mismo sistema operativo.
- Tener un respaldo de la configuración actual como medida de prevención en caso de contingencias y como parte de los procedimientos de Roll-Back, antes de realizar algún cambio.
- Realizar respaldos a los archivos y estructuras de bases datos considerando al menos las bases de datos maestras, índices, formas y vistas así como la información de transacciones (datos de operación del día a día).
- Implementar un control automatizado o manual (librería de programas) que permita centralizar y administrar las versiones respaldadas de los componentes de una aplicación, considerando tener la última versión respaldada disponible solo para el personal autorizado.

- El área responsable de realizar los respaldos a la información puede generar, registrar, recibir y custodiar los archivos de programas y de datos respaldados que sean mantenidos en dispositivos de almacenamiento secundario.
- Registrar en una bitácora las salidas de los respaldos realizados de la información donde se refleje la siguiente información: tipo de respaldo, nombre de la persona que autoriza, que solicita, fecha, hora, identificador, ubicación y motivo.
- Los respaldos podrán someterse a revisiones antivirus, para garantizar que estén libres de infecciones y puedan utilizarse en caso de un ataque de código malicioso.

Los procedimientos de respaldo para los medios relacionados con tecnología de información deberán incluir el almacenamiento apropiado de los archivos de datos, del software y de la documentación relacionada, dentro y fuera de las instalaciones. Los respaldos deberán ser almacenados con seguridad y las instalaciones de almacenamiento deberán ser revisadas periódicamente con respecto a las medidas de seguridad físicas y técnicas requeridas.

El almacenamiento externo de copias de respaldo, documentación y otros recursos tecnológicos de información, catalogados como críticos, debe ser establecido para soportar el plan de recuperación y continuidad del negocio. Los propietarios de los procesos del negocio y el personal de la función de TI deben involucrarse en determinar qué recursos de respaldo almacenados en el sitio alternativo. La instalación de almacenamiento externo debe contar con

medidas ambientales para los medios y otros recursos almacenados; y debe tener un nivel de seguridad suficiente, que permita proteger los recursos de respaldo contra accesos no autorizados, robo o daño. Se debe asegurar que los acuerdos/contratos del sitio alterno son analizados periódicamente.

Para la restauración de los respaldos con datos personales se recomiendan los siguientes aspectos básicos:

- Todo requerimiento de restauración de información respaldada deberá realizarse utilizando un formato formal de solicitud de restauración de información, considerando los siguientes puntos:
 - Nombre y área del solicitante
 - Información a ser restaurada
 - Periodo que comprende el respaldo
 - Fecha de realización del respaldo
 - Lugar de restauración del respaldo
 - Motivo de la restauración

- El formato de solicitud de restauración de respaldo tendrá que ser autorizado por el Responsable.

Recepción de solicitud de restauración de respaldos (operaciones)

- El área responsable de manejar los respaldos de información deberá verificar que la solicitud de información a restaurar esté debidamente formulada y tenga las autorizaciones requeridas.

- El área responsable de manejar los respaldos de información deberá llevar un registro secuencial de todas las solicitudes de restauración de respaldos.
- Se deberá registrar en una bitácora el estatus de terminación de la restauración del respaldo, considerando el nombre de la persona solicitante, lugar donde se ubicará la información a restaurar, estatus del proceso de restauración, nombre del operador que realizó la restauración y la fecha de restauración.
- Se deberá asegurar que el lugar destinado para ser colocada la restauración del respaldo, tenga el suficiente espacio requerido para colocar la información contenida en el respaldo y que se cuente con todos los mecanismos necesarios para su correcta restauración.
- Una vez terminado el proceso de restauración del respaldo se tendrá que notificar al responsable, que solicitó la restauración de la información, el estatus del proceso a través de un documento formal, en donde se solicite su firma de conformidad.

6. Gestión de incidentes/brechas de seguridad

El desarrollo de un componente de control relativo a la gestión de incidentes y brechas de seguridad debe ayudar a la organización a una contención y tratamiento adecuados de aquellos eventos que afecten su esquema de seguridad y privacidad, conforme a los niveles de riesgo establecidos. Asimismo, este componente ayuda a la organización a cumplir los requerimientos de la LFPDPPP que

establecen acciones concretas sobre la comunicación y manejo de las brechas o afectaciones a la privacidad de los datos personales. Es recomendable que la organización apoye su esquema de gestión de incidentes y brechas de seguridad en las capacidades de “Mesa de servicio” (help desk), como un punto de entrada de información sobre las desviaciones, brechas o incidentes de seguridad que puedan afectar la privacidad.

Los elementos mínimos para el desarrollo de este componente de gestión/brechas de seguridad son:

- a) Utilizar un formato para el registro del reporte de incidentes, que contenga al menos la siguiente información:
 - Fecha del reporte
 - Tiempo y duración aproximado del incidente
 - Nombre del sistema
 - Localización física del sistema
 - Tipo de sistema (servidor web, servidor de base de datos, servidor de correo electrónico, aplicación, entre otros)
 - Sistema operativo y dirección IP del equipo
 - Datos afectados
 - Descripción del incidente
 - Información de contacto de la persona que ha reportado el incidente, que contenga al menos: nombre, oficina, teléfono, número de teléfono celular, número de fax y dirección de e-mail
 - Información de contacto del administrador del recurso de información afectado por el incidente, que contenga al menos: nombre, oficina, teléfono, número de teléfono celular, número de fax y dirección de e-mail.

Identificación y reporte de actividades anormales

- b) El reporte de actividades anormales en los equipos y recursos de cómputo deberá realizarse al menos de la siguiente forma:
- Por un reporte de usuario hacia el área de Help Desk
 - Por alerta de una herramienta automatizada de monitoreo a través de correo electrónico, mensajería de sistema operativo o radiolocalizador, hacia el área responsable de tratamiento de incidentes de seguridad y administradores de los recursos afectados
 - Por un reporte del área encargada de la gestión de los recursos afectados de la infraestructura de TI

Reporte de actividades anormales – Help Desk

- c) El encargado del Help Desk deberá clasificar de forma general la naturaleza de la actividad reportada, para determinar si es un incidente menor y, en su caso, atenderlo con los procedimientos establecidos; o bien, si es un incidente considerable, que afecta a los recursos de información, atenderlo mediante la elaboración de un registro especial del evento en el formato especificado para el reporte de actividades anormales.
- d) Se deberá entregar el reporte del incidente –cuando éste sea provocado por causas de operación— al área responsable de

la administración de los recursos o procesos que han presentado el incidente, para su tratamiento.

- e) Se deberá entregar el reporte del incidente –cuando éste sea calificado como incidente de seguridad– al grupo de trabajo responsable del tratamiento de incidentes de seguridad.

Reporte de actividades anormales – Herramientas automatizadas

- f) La notificación de alerta de reporte sobre un incidente que afecte a un recurso de información, deberá contener al menos lo siguiente:
- Fecha del reporte
 - Tiempo de inicio y duración aproximada del incidente
 - Nombre del sistema que presenta el incidente
 - Sistema operativo y dirección IP del equipo donde ocurre el incidente
 - Características del ataque

Determinación del tipo de incidente de operación

- g) El área encargada de la administración del recurso o proceso afectado debe determinar las causas que originaron el incidente.
- h) Se debe corregir el incidente reportado, cuando sus causas sean provocadas por descuidos u omisiones, a través de los procedimientos de mantenimiento correctivo correspondientes.

- i) Cuando se identifiquen las causas del incidente como intencionales o de ataque, se tendrá que entregar el reporte inicial del incidente al grupo de trabajo responsable del tratamiento de incidentes de seguridad, agregando la justificación relacionada.

Determinación del tipo de incidente de seguridad

- j) Cuando el grupo de trabajo responsable del tratamiento de incidentes de seguridad recibe el reporte de un incidente, deberá identificar el tipo del incidente que se está presentando para responder adecuadamente y minimizar sus efectos.
- k) En caso de que el incidente sea originado por un virus informático o código malicioso, se deberá proceder de acuerdo a los procedimientos específicos del tratamiento de virus.
- l) Si no se logra identificar el tipo de incidente, se deberá realizar una investigación del mismo a partir de las características presentadas hasta el momento, en fuentes reconocidas de seguridad informática.
- m) Una vez determinada la presencia de un incidente y sus posibles efectos, se deberá entregar un reporte preliminar de la situación y consecuencias en la operación y seguridad actuales al área responsable de la función de TI en la organización.

- n) El responsable de la función de TI en la organización deberá firmar la autorización del tratamiento del incidente.

Reacción contra incidentes de seguridad

- o) Se tendrá que hacer una determinación general de la forma en que se obtuvo el acceso no autorizado o se desarrolló el incidente y cuántos sistemas se comprometieron.
- p) Se tendrá que efectuar una revisión general de la consistencia de los sistemas de archivos, integridad de bitácoras de transacciones y disponibilidad de los equipos, para determinar el impacto global del incidente.
- q) Se deberá eliminar la sesión de usuario en el sistema, o bien, bloquear la dirección IP que ocasionen el incidente contra el recurso de información.
- r) En caso de que el ataque persista, se deberán deshabilitar los servicios, aplicaciones y puntos de acceso al sistema que se utilicen para provocar el ataque.
- s) Se deberán restablecer los sistemas atacados con la configuración establecida previa al ataque, a partir de un respaldo confiable de la misma.
- t) Se deberán deben corregir las vulnerabilidades explotadas para obtener acceso no autorizado o provocar el ataque al recurso de información, considerando al menos: desactivación de servicios innecesarios para la operación del sistema, instalación de parches de software, cambio de

contraseñas y atendiendo al procedimiento de análisis y corrección de vulnerabilidades.

- u) Si la mitigación de las vulnerabilidades implica un cambio de configuración, instalación de parches de software, cambios de versiones de programas y aplicaciones, entonces se tendrán que realizar de acuerdo con el procedimiento de administración de la configuración y control de cambios.

Seguimiento de incidentes de seguridad

- v) Documentar e informar cada una de las actividades realizadas durante el incidente y su tratamiento a las áreas pertinentes dentro de la organización, procurando –en la medida de lo posible– una clara descripción de la naturaleza de los incidentes, los datos personales comprometidos, las actividades realizadas, su responsable y ejecutor, y los resultados alcanzados.
- w) Analizar la validez de la arquitectura de seguridad actual (políticas, procedimientos, seguridad de sistemas, configuraciones, entre otros) con base en el reporte del incidente, para definir cambios y modificaciones.
- x) Fortalecer los programas de concienciación y entrenamiento de los usuarios con los resultados obtenidos del tratamiento del incidente.

Podrá incluirse adicionalmente una matriz de escalamiento de incidentes, para el tratamiento adecuado de la brecha con base en

su severidad, tiempo de presencia, complejidad de la solución aplicable y áreas de responsabilidad en la solución del incidente.

7. Seguridad física para instalaciones de cómputo

Los resultados de la encuesta-sondeo electrónico realizado a las empresas del sector de TI, reflejan que muchas de éstas son responsables de sus instalaciones donde se ubica la infraestructura para el procesamiento de la información, y en otros casos, se contrata algún tipo de servicios especializado para este fin. En consecuencia, es indispensable observar algunas recomendaciones sobre mecanismos de control que permitan un resguardo apropiado de las instalaciones y recursos físicos de procesamiento de la información.

Controles de acceso físico a las instalaciones de cómputo

- Se recomienda que existan controles de acceso físico a las instalaciones de cómputo, tales como: vigilantes, credenciales de identificación, tarjetas con claves, bitácoras, biométricos, entre otros.
- Controlar los accesos a las instalaciones (edificios) donde se ubica el centro de cómputo.
- Las personas que entran y salen al centro de cómputo deberán registrarse en una bitácora.
- A las personas que entran y salen del centro de cómputo se les deberá asignar un identificador o credencial.

- Crear un plan de visitas al centro de cómputo, o bien, sustentarse con la autorización del personal encargado de su operación y resguardo.
- Todas las personas ajenas a la organización y al centro de cómputo deberán permanecer escoltados durante su estancia y actividades dentro de estas instalaciones.
- Las actividades del personal ajeno al centro de cómputo deberán ser supervisadas permanentemente.
- Se recomienda que al interior del centro de cómputo se cuente con detectores de intrusos o actividades no autorizadas.
- Definir un proceso de manejo de actividades sospechosas y de emergencia dentro del centro de cómputo, alineado con los mecanismos de protección civil de las instalaciones.

Controles ambientales en el centro de cómputo

- Los cuartos donde se mantiene la infraestructura de cómputo deberá estar a la temperatura ambiental recomendada por los fabricantes de la misma (60 – 75 grados Fahrenheit, o 10- 25 grados Celsius).
- Es recomendable que las instalaciones de cómputo cuenten al menos con infraestructura de soporte y operación para enfriamiento y aire acondicionado, detectores de humedad, detectores de humo, sistemas de supresión de incendios, sistema de energía ininterrumpida (UPS), generador eléctrico de respaldo.

- Desarrollar un plan de pruebas periódicas de la infraestructura de soporte y operación de las instalaciones de cómputo tales como sistema de energía ininterrumpida (UPS), generador eléctrico de respaldo, aire acondicionado, sistema de supresión de incendios, entre otros.
- Elaborar un plan de mantenimiento preventivo de la infraestructura de soporte y operación de las instalaciones de cómputo tales como sistema de energía ininterrumpida (UPS), generador eléctrico de respaldo, aire acondicionado, sistema de supresión de incendios, entre otros.
- No se recomienda preservar materiales combustibles dentro del centro de cómputo, ni en distancias cortas fuera del mismo, por ejemplo, palería, cartón, solventes, etc.
- Los cables de telecomunicaciones y energía eléctrica tienen que estar ordenados en ducterías, identificados con etiquetas y dentro de gabinetes con llave.
- Se recomienda desarrollar y ejecutar un plan periódico de revisión del estado de los cables de telecomunicaciones debajo del piso o techo falsos.
- Los cables de energía eléctrica y telecomunicaciones tienen que instalarse en ductos separados (para prevenir interferencias). Asimismo, tienen que identificarse aquellos donde se conectan los equipos del centro de cómputo.
- Instalar un sistema de tierra física adecuado a los tipos de carga e instalaciones de centro de cómputo independiente del resto de las instalaciones.

- Se recomienda elaborar contratos para el suministro de energía ininterrumpida y regulada con la CFE.

Seguridad perimetral de las instalaciones y centro de cómputo

- Establecer perímetros de seguridad física para el centro de cómputo, las instalaciones de la empresa, la cintoteca y almacenes de papelería sensible, a través de rejas, disposición de escritorios, confinamiento de espacios, señalamientos, entre otros.
- Es recomendable que el centro de cómputo no se instale en sótanos ni en los pisos más elevados de las instalaciones de la organización.
- Las instalaciones del centro de cómputo deberán contar con muros completos sólidos de acuerdo a la ubicación del edificio para soportar desastres naturales: inundaciones, terremotos, huracanes, entre otros.
- Los muros de carga del centro de cómputo deberán llegar del techo al piso.
- Las puertas de acceso al centro de cómputo deberán estar protegidas con mecanismos como alarmas, barras, cerraduras.
- Las instalaciones del centro de cómputo deberán mantenerse siempre cerradas y sin señalamientos de su propósito de uso.
- Las áreas vacías deberán ser monitoreadas y cerradas con llave. Asimismo, se deberán crear espacios específicos para carga y descarga de materiales, almacenamiento de

desperdicios, resguardo de combustibles, almacenamiento de papelería, trabajo de terceros o externos.

- Se deberá implementar un plan y proceso que garanticen que el centro de cómputo se mantenga limpio, sin cajas u obstáculos que impidan el libre tránsito de las personas.
- Los mecanismos de seguridad física deberán configurarse a prueba de fallas, de tal suerte que, ante un incidente, el personal pueda evacuar las instalaciones de forma segura. Y a su vez, se impida el acceso no autorizado.
- Se recomienda la existencia de un botiquín de primeros auxilios en la centro de cómputo de acuerdo a las consideraciones de protección de civil e higiene industrial de la organización.

Protección física de equipos y personal

- Se recomienda crear políticas y procedimientos que establezcan un escritorio limpio en la organización, donde el personal resguarde la información y datos personales en medios físicos o impresos.
- De acuerdo al tipo de información en los equipos personales, deberá implementarse un esquema de cifrado a nivel físico en los dispositivos de almacenamiento.

Como se ha mencionado anteriormente, la implementación de estos controles dependerá del nivel de riesgo aceptable y efectividad del ambiente de control actual en cada organización. Los controles

podrán utilizarse para apuntalar los esfuerzos actuales de seguridad de la información para favorecer el cumplimiento de la LFPDPPP.

Para realizar una recomendación mínima como secuencia de implementación de mecanismos de control para dar cumplimiento a la LFPDPPP, se utiliza como criterio el tipo de medidas de seguridad en la infraestructura y procesos de la organización, sobre el tamaño de la empresa dentro del sector de TI en México. Presentamos a continuación el siguiente esquema:

Tipos de medidas de seguridad y privacidad			
	Medidas básicas	Medidas intermedias	Medidas avanzadas
Tamaño de la empresa			
Micro	Definición de roles y responsabilidades. Revisión de contratos y convenios con terceros. Capacitación y entrenamiento. Clasificación práctica de la	(Aplicar los controles de la categoría anterior) Gestión técnica de vulnerabilidades. Gestión de incidentes y brechas de seguridad.	(Aplicar los controles de la categoría anterior) Auditorías internas

Tipos de medidas de seguridad y privacidad	Medidas básicas	Medidas intermedias	Medidas avanzadas
	<p>información y datos personales.</p> <p>Cifrado de la información.</p> <p>Respaldos y restauración de la información.</p>		
Pequeña	<p>Definición de roles y responsabilidades.</p> <p>Revisión de contratos y convenios con terceros.</p> <p>Capacitación y entrenamiento.</p> <p>Clasificación práctica de la información y datos personales.</p>	<p>(Aplicar los controles de la categoría anterior)</p> <p>Gestión técnica de vulnerabilidades.</p> <p>Control de accesos lógicos.</p> <p>Gestión de incidentes y brechas de seguridad.</p>	<p>(Aplicar los controles de la categoría anterior)</p> <p>Auditorías Internas</p>

Tipos de medidas de seguridad y privacidad	Medidas básicas	Medidas intermedias	Medidas avanzadas
	<p>Cifrado de la información.</p> <p>Respaldos y restauración de la información</p>		
Mediana	<p>Definición de roles y responsabilidades.</p> <p>Revisión de contratos y convenios con terceros.</p> <p>Capacitación y entrenamiento.</p> <p>Clasificación práctica de la información y datos personales.</p> <p>Cifrado de la información.</p>	<p>(Aplicar los controles de la categoría anterior)</p> <p>Gestión técnica de vulnerabilidades.</p> <p>Control de accesos lógicos.</p> <p>Gestión de incidentes y brechas de seguridad.</p> <p>Control de cambios y gestión de</p>	<p>(Aplicar los controles de la categoría anterior)</p> <p>Auditorías internas y externas.</p>

Tipos de medidas de seguridad y privacidad	Medidas básicas	Medidas intermedias	Medidas avanzadas	Tamaño de la empresa
	<p>Respaldos y restauración de la información.</p> <p>Análisis y evaluación de riesgos de seguridad y privacidad de datos.</p>	configuraciones.		
Grande	<p>Definición de roles y responsabilidades.</p> <p>Revisión de contratos y convenios con terceros.</p> <p>Capacitación y entrenamiento.</p> <p>Clasificación práctica de la información y</p>	<p>(Aplicar los controles de la categoría anterior)</p> <p>Gestión técnica de vulnerabilidades.</p> <p>Control de accesos lógicos.</p> <p>Gestión de incidentes y brechas de</p>	<p>(Aplicar los controles de la categoría anterior)</p> <p>Auditorías internas y externas.</p>	

Tipos de medidas de seguridad y privacidad Tamaño de la empresa	Medidas básicas	Medidas intermedias	Medidas avanzadas
	datos personales. Cifrado de la información. Respaldos y restauración de la información. Análisis y evaluación de riesgos de seguridad y privacidad de datos.	seguridad. Control de cambios y gestión de configuraciones. Indicadores formales de efectividad.	

Otro criterio que debe ser utilizado en la definición e implantación de controles de seguridad y privacidad de la información –sin perder de vista el propósito de uso de los datos personales de las empresas del sector de TI en México—, son los acuerdos de privacidad/contractuales del Responsable con el Titular de los datos personales, y los términos de la calidad del servicio entre el Encargado y el Responsable. De ahí, pues, que una posible

secuencia de implementación se reduzca a revisar caso por caso con base en toda la secuencia sugerida en este documento.

En la industria de seguridad de la información y privacidad de datos, se puede observar que más allá del tipo de controles y formas de implementación que se seleccionen para establecer un nivel de efectividad mínima, es fundamental que todos los mecanismos de control tengan al menos:

- a) Una política o estándar normativo que los reconozca y defina en la organización, asignando la responsabilidad de cada audiencia relacionada con el control (usuario, cliente, supervisor, entre otros)
- b) Un procedimiento que establezca cómo ejecutar u operar el control.
- c) Un componente de medición de la efectividad o resultados del control, alineado con un sistema de gestión de seguridad de la información, que considere métricas de efectividad alimentadas por el componente de gestión de incidentes/brechas de seguridad.

MEDIDAS CORRECTIVAS PARA LA MEJORA DE LAS PRÁCTICAS DE PRIVACIDAD DE DATOS PERSONALES

Se propone la siguiente asociación de rubros con mecanismos de control genéricos –cuyas características han sido detalladas en la sección anterior— tomando en cuenta la problemática específica en las iniciativas actuales de control de seguridad y privacidad de datos del sector de servicios de tecnologías de información (TI) en México (evaluadas en la

encuesta-sondeo electrónico realizado a las empresas del sector de TI), para implementar un marco de gestión de seguridad de la información que considere la premisa de privacidad de los datos personales dentro de los requerimientos de cumplimiento de la LFPDPPP.

Prácticas organizacionales de seguridad y privacidad de la información

Estado general	Medidas correctivas
<ul style="list-style-type: none"> • Las empresas del sector de TI reconocen ciertos mecanismos como el fundamento para la toma de decisiones sobre el nivel de seguridad de la información y privacidad de datos, tales como: análisis de riesgos, cumplimiento con ejercicios de auditoría, recomendaciones de proveedores, análisis técnicos de vulnerabilidades, entre otros. Sin embargo, su ejecución no se encuentra formalizada ni se reconoce como un componente organizacional con una participación multidisciplinaria. • En este sentido, las organizaciones han comenzado a implantar mecanismos de 	<ul style="list-style-type: none"> • El Análisis y Evaluación de Riesgos de Seguridad y Privacidad se debe establecer como un proceso formalmente definido dentro de las prácticas organizacionales para ajustar la operación del negocio y la calidad de los servicios a los clientes, a partir de identificar las prioridades de protección con un estricto sentido de negocio. • A partir de la identificación de las prioridades de protección y privacidad, las organizaciones deben asignar partidas presupuestales específicas para desarrollar los proyectos de seguridad y privacidad, como parte de un ejercicio

Estado general	Medidas correctivas
<p>seguridad de la información a partir de regulaciones y requerimientos puntuales.</p> <ul style="list-style-type: none"> • Por lo que las asignaciones de presupuesto son limitadas y solamente se realizan, en mayor medida, asignaciones para proyectos aislados específicos. • La ejecución de estos proyectos de controles para seguridad y privacidad son ejecutados como parte de las responsabilidades de la función de Sistemas/Informática/TI del negocio, sin incluir un enfoque y ejecución integrales. • Las organizaciones identifican aquellos rubros generales de control que deben considerarse para desarrollar mecanismos específicos de protección y privacidad, sin embargo, no todos han sido implantados. 	<p>estratégico de planeación de presupuesto, que corresponda al nivel de participación de todas las áreas de la organización en el uso de estos controles en sus procesos.</p> <ul style="list-style-type: none"> • Las organizaciones deben ampliar los roles y responsabilidades sobre seguridad y privacidad para todas las áreas y funciones de su estructura, para que se asienten y ejecuten formalmente. • Se debe definir un procedimiento de estrategia de seguridad y privacidad, que aproveche los resultados del análisis y evaluación de riesgos, para la toma de decisiones sobre los rubros de control que se van a desarrollar en la organización a partir de la prioridad, factibilidad y beneficio de estos controles.

Estado general	Medidas correctivas
<p>Gestión de la seguridad y privacidad de la información</p> <p>“Procesos, roles y responsabilidades”</p>	
<ul style="list-style-type: none"> • Se identifica la existencia de un Comité de Seguridad de la Información que vigila las actividades de aseguramiento y cumplimiento de la privacidad de datos dentro de la organización. • Asimismo, se ha incrementado la participación de roles estratégicos en la clasificación de la información (tipo y prioridad de protección) • Las organizaciones no han ejecutado esfuerzos continuos sobre la capacitación del personal en temas de seguridad y privacidad de la información. • De igual forma, no se han desarrollado esquemas de medición de la efectividad de la función de seguridad y privacidad, por lo que solamente se cuenta con métricas operativas o evaluaciones técnicas esporádicas. 	<ul style="list-style-type: none"> • Las organizaciones deben establecer formalmente (como parte del esfuerzo de asignar roles y responsabilidades), un grupo multidisciplinario que tenga responsabilidades sobre la determinación del nivel de riesgo aceptable, la definición de la estrategia de seguridad, medición de la efectividad de la función de seguridad y operación directa de controles. • Las organizaciones deben incluir a las áreas comerciales, de operación y jurídicas en la definición de los roles y responsabilidades de seguridad y privacidad, con una asignación puntual de la determinación de acuerdos y términos legales, niveles de servicio y desviaciones relativas a brechas de seguridad e incidentes para con proveedores, socios de negocio

Estado general	Medidas correctivas
<ul style="list-style-type: none"> Las implicaciones de los requerimientos de privacidad, no se han considerado en los acuerdos contractuales con proveedores, socios de negocio ni clientes. 	<p>y clientes.</p> <ul style="list-style-type: none"> En el primer esfuerzo de mecanismos de control, las organizaciones deben definir y ejecutar una estrategia integral de concientización sobre seguridad y privacidad de la información, dentro de los parámetros corporativos de comunicación institucional. Como parte de los controles relativos a la gestión de incidentes y brechas, deben derivarse componentes de medición de la efectividad de la función de seguridad, considerando activamente el nivel aceptable de riesgo, y el nivel de seguridad que prevalece en la organización, a partir de medir los componentes del riesgo y el manejo de las brechas de seguridad.

Estado general	Medidas correctivas
<p>Gestión de la seguridad y privacidad de la información</p> <p>“Seguridad de los activos informáticos”</p>	
<ul style="list-style-type: none"> • En mayor medida, las empresas del sector de TI son responsables de sus propias instalaciones donde se encuentra la infraestructura tecnológica para el procesamiento de información. • El enfoque de protección se ha centrado sobre aseguramiento de la infraestructura y no sobre el tipo de información que procesa la organización. • Se identifica un avance considerable en mecanismos de protección relativos a redes de telecomunicaciones, plataformas y equipos de usuario final. • Los esfuerzos actuales de controles de seguridad, no se han desarrollado con requerimientos de privacidad. • La premisa de la selección y características de los mecanismos de control de 	<ul style="list-style-type: none"> • Realizar una revisión detallada sobre las características de sus instalaciones de cómputo para asegurarse que cumplen con los requerimientos de la industria (según estándares aplicables) • En su defecto, solicitar al proveedor de las instalaciones de cómputo, que entregue periódicamente resultados de revisiones o evaluaciones de sus instalaciones. • Desarrollar una estrategia de aseguramiento y privacidad de la información basada en controles preventivos, de detección y correctivos, cuya implementación considere políticas, procedimientos y mecanismos técnicos, que ayuden al cumplimiento de la LFPDPPP y ayuden a alcanzar el nivel de operación requerido

Estado general	Medidas correctivas
<p>seguridad, es la subjetividad/experiencia del personal responsable de la función de seguridad en la organización.</p> <ul style="list-style-type: none"> Existen esfuerzos incipientes sobre el monitoreo preventivo de seguridad a partir de la generación, preservación y explotación, por lo que no se contribuyen a generar métricas de la efectividad de la función de seguridad. 	<p>por la organización (las especificaciones recomendadas para estos controles se pueden encontrar en la sección anterior de este apartado)</p> <ul style="list-style-type: none"> Desarrollar un componente de medición de la efectividad de la función de seguridad de la información. En primera instancia puede considerar capacidades de autorregulación y gradualmente revisiones por terceros.
<p>Tratamiento de datos en el denominado cómputo en la nube</p>	
<ul style="list-style-type: none"> Las organizaciones que ofrecen o consumen servicios de cómputo en la nube, consideran sus implicaciones dentro de su marco normativo de seguridad y privacidad. Sin embargo, los proveedores de estos servicios de cómputo en la nube no tienen un conocimiento pleno sobre las implicaciones de la regulación de privacidad sobre 	<ul style="list-style-type: none"> Desarrollar una estrategia de aseguramiento y privacidad de la información basada en controles preventivos, de detección y correctivos, cuya implementación considere políticas, procedimientos y mecanismos técnicos, que ayuden al cumplimiento de la LFPDPPP y ayuden a alcanzar el nivel de operación requerido por la organización (las

Estado general	Medidas correctivas
<p>la gestión de sus servicios desde el punto de vista de operación, nivel de servicio y legal ante una brecha o desviación de los acuerdos contractuales.</p>	<p>especificaciones recomendadas para estos controles se pueden encontrar en la sección anterior de este apartado).</p> <ul style="list-style-type: none"> • Las organizaciones deben incluir a las áreas comerciales, de operación y jurídicas en la definición de los roles y responsabilidades de seguridad y privacidad, con una asignación puntual de la determinación de acuerdos y términos legales, niveles de servicio y desviaciones relativas a brechas de seguridad e incidentes con proveedores, socios de negocio y clientes.

RECOMENDACIONES ADICIONALES PARA LA MEJORA DE LAS PRÁCTICAS DE PRIVACIDAD DE DATOS PERSONALES

Los resultados del análisis de la encuesta sondeo electrónico realizado a las empresas del sector de TI, permiten identificar que la adopción de los mecanismos de control para lograr el cumplimiento de la regulación dentro de los niveles aceptables de riesgo de las organizaciones, será un esfuerzo considerable para las empresas de dicho sector, ante el estado actual de sus prácticas de gestión de protección y privacidad. Este diagnóstico se basa, en buena medida, en los escasos antecedentes en la industria de este tipo de regulaciones e iniciativas de seguridad sin matices de privacidad.

Para facilitar la adopción de los mecanismos de control que cada organización requerirá a partir de su análisis particular, así como sus características de operación para el cumplimiento de los requerimientos de la LFPDPPP, es importante tener en cuenta además de las mencionadas en el “Marco práctico referencial de mecanismos de control de gestión de seguridad y privacidad de la información”, las siguientes recomendaciones complementarias:

- El esfuerzo para estimar el nivel aceptable de riesgos, y la combinación de controles de seguridad y privacidad en la organización, puede basarse en las referencias documentales de las experiencias en otros países con regulaciones similares. Referencias que han sido incluidas como parte de esta investigación. El uso de éstas no implica copiar o adaptar los elementos que se han desarrollado, sino más bien favorecer la generación de alternativas adecuadas a la realidad operativa de la organización.

- Las empresas del sector de TI deben trabajar en la redefinición de sus servicios para clientes finales, considerando los mecanismos de operación y habilitación tecnológica en que se genera el servicio de TI, y los elementos legales y de calidad del servicio que se acuerdan con los proveedores y clientes. De tal suerte que el modelo de operación atienda estos requerimientos de forma natural; y la seguridad de la información y privacidad de datos se conviertan en atributos naturales de cada servicio ofrecido. Esta recomendación implica que se cambie el enfoque de gestión actual de la infraestructura a un enfoque integral de gestión de servicios informáticos.

Asimismo, se recomienda que dentro de las áreas comerciales de las empresas se defina todo lo relacionado al encargado de acuerdo a la LFPDPPP, considerando entre otros aspectos lo siguiente:

- Objetivo
 - Actividades técnicas a cubrir
 - Beneficios
 - Requerimientos
- Una forma positiva de potenciar los esfuerzos para incrementar la seguridad y privacidad de la información, consiste en que la organización ejecute sus iniciativas de controles dentro de un marco referencial de industria, que pueda ser evaluado de manera independiente (certificación). Así se obtendrá una garantía razonable de la efectividad de la gestión de seguridad considerando los requerimientos de privacidad de las partes interesadas.
 - En apoyo a las actividades de monitoreo y evaluación de efectividad de la función de seguridad dentro de los parámetros de riesgo y privacidad, se recomienda que las organizaciones

implementen un mecanismo de autorregulación. Con ello se dará cumplimiento independiente a la operación de la infraestructura y seguridad, favoreciendo la supervisión y mejora continua en el corto plazo, y a su vez, preparando el marco de seguridad y privacidad para una revisión externa que determine el cumplimiento de la LFPDPPP en la madurez natural de la regulación.

VII. PROPUESTA DE POLÍTICAS PÚBLICAS

Tomando en consideración los elementos apuntados en los apartados anteriores, las recomendaciones y medidas correctivas para una práctica de medidas de seguridad en protección de datos personales en el sector de las TI para dar cumplimiento a la LFPDPPP (en lo relativo a encargados), requiere de un entorno donde las autoridades sectoriales y el IFAIPD encaucen políticas públicas dirigidas tanto al sector público como al privado.

En ese orden de ideas, se propone un esquema programático específico que debe orientarse desde el poder público, conforme a los componentes que a continuación se enuncian.

7.1 Objetivos

Un primer aspecto a considerar es de orden teleológico, es decir, relativo a las finalidades de la política pública a perseguir. Por lo tanto, se requiere definir objetivos concretos y asequibles:

Objetivo General. Impulsar el conocimiento de buenas prácticas nacionales e internacionales en materia de seguridad de datos para el sector de las TI.

Objetivo 1. Generalizar el uso de buenas prácticas en materia de seguridad de datos personales en el sector de TI para poder brindar certeza a las empresas y particulares que las subcontraten bajo la figura de encargado prevista en la LFPDPPP.

Objetivo 2. Desarrollar habilidades sobre prácticas nacionales e internacionales en materia de seguridad de datos para personas físicas o morales relacionadas con el sector de las TI, que operen como encargados en el tratamiento de datos personales en posesión de los particulares.

Objetivo 3. Promover recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en las empresas de TI por parte de las personas físicas o morales, que operen como encargados en el tratamiento de datos personales en posesión de los particulares.

7.2 Líneas de Acción

De cada objetivo específico, en esta sección se proponen líneas de acción específicas.

Objetivo 1. Líneas de Acción:

- a. Identificar las mejores prácticas, tanto nacionales como internacionales, en materia de seguridad de la información y datos personales en el sector de TI.
- b. Difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano.
- c. Concertar con los sectores privado y social, mecanismos de difusión de normas oficiales mexicanas, normas mexicanas y otros estándares relacionados con el tratamiento de datos personales en posesión de los particulares por parte de personas físicas o morales

relacionadas con el sector de las TI, que operen como encargados en el tratamiento de datos personales en posesión de particulares.

- d. Promover un Sistema Nacional de Información público sobre prácticas, normas o estándares nacionales e internacionales en materia de seguridad de datos para el sector de las TI, que ofrezca elementos para implementar mejores prácticas entre las empresas o personas físicas que realicen el tratamiento de datos personales en calidad de encargados.
- e. Identificar la normatividad internacional y nacional relacionada con la TI, especialmente en los rubros de comercio electrónico y seguridad informática, con el fin de crear un contexto informado sobre los marcos regulatorios, programáticos o administrativos que adecuen los servicios de las TI a las mejores prácticas mundiales.
- f. Promover campañas sobre los temas relativos a las obligaciones de los encargados como prestadores de servicios de TI y, en general, sobre procesos y prácticas cualitativos en el ámbito de la protección de datos personales.
- g. Incrementar la divulgación, concienciación y promoción de las regulaciones sobre diferentes temas asociados a la protección de los datos personales en el entorno de las TI.
- h. Promover normas y programas que incorporen al país mejores prácticas y estándares relativos a la seguridad de los procesos electrónicos del tratamiento de datos en el sector privado.

Objetivo 2. Líneas de Acción:

- a. Realizar en forma continua acciones de información sobre el concepto y responsabilidades del encargado como persona física o

jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

- b. Implementar cursos, talleres y demás servicios de capacitación a personas o empresas asociadas al procesamiento de datos, custodia y administración de información, así como aquellos vinculados a la prestación de servicios de TI, Business Process Outsourcing (BPO), redes, aplicaciones o cualquier otra tecnología de la información que permita el intercambio, almacenamiento y/o procesamiento informatizado o por medios físicos de datos por cuenta del responsable.
- c. Capacitar a los responsables sobre los mecanismos para la contratación de un encargado del tratamiento.
- d. Desarrollar programas de formación presencial o a distancia sobre normas, estándares y buenas prácticas dirigidas a los encargados en el tratamiento de datos personales en el entorno digital.
- e. Alinear los programas públicos o privados existentes sobre habilidades digitales, a la comprensión de los temas sobre protección de datos personales en posesión de los particulares.
- f. Informar y capacitar a los organismos empresariales y a sus representaciones en las entidades federativas sobre los aspectos legales de las TI en materia de protección de datos personales, con el propósito de generar una perspectiva informada que permita armonizar, en los ámbitos nacional y regional las mejores prácticas y normas en la materia.

Objetivo 3. Líneas de Acción:

- a. Identificar a las personas o empresas del sector de las TI que realizan actividades como encargados en el tratamiento de datos personales en posesión de los particulares.
- b. Promover la relación de los encargados con sus clientes o con quienes tengan una relación jurídica, mediante la adopción de las disposiciones contractuales a las que se refiere el artículo 51 del Reglamento de la LFPDPPP.
- c. Emitir lineamientos en materia de seguridad física, administrativa y técnica para la prestación de servicios por parte de empresas o personas físicas que operen como encargados en el tratamiento de datos personales en posesión de los particulares.
- d. Promover sistemas de supervisión y vigilancia internos y externos respecto del cumplimiento de los principios de protección de datos personales, incluyendo mecanismos de supervisión independientes que garanticen la imparcialidad.
- e. Difundir manuales sobre medidas preventivas y correctivas para el buen desempeño de los encargados en el ámbito de las TI. Impulsar previsiones referentes a las transferencias internacionales de datos personales, así como sobre las garantías que deberán observarse.
- f. Encauzar el cumplimiento del principio de Responsabilidad, incluyendo lo previsto por el artículo 14 de la Ley, y 47 y 48 del Reglamento, con especial atención en los aspectos de aseguramiento y trazabilidad previstos en el artículo 48 fracciones IX y X del Reglamento de la Ley.

- g. Promover esquemas de autorregulación vinculante para la protección de datos personales en posesión de los particulares, con la participación de los encargados del tratamiento.

7.3 Previsión de Recursos

Se requiere señalar que el éxito de las Políticas Públicas que se promuevan para impulsar el conocimiento de buenas prácticas nacionales e internacionales en materia de seguridad de datos personales para el sector de las TI, con los objetivos y líneas de acción descritas con antelación, radica en que exista infraestructura humana, organizativa y material; que se cuente con recursos financieros; y, sobre todo, que los destinatarios de las mismas, en este caso los particulares que fungen como encargados en el tratamiento de datos personales, sean adecuadamente incentivados a alinearse a estándares, buenas prácticas y, principalmente, a las expectativas institucionales de la industria y de los titulares de los datos.

Al efecto, las dependencias deberán considerar en su respectivo Presupuesto de Egresos anual, partidas para:

- a) Promover dentro de su sector de influencia conforme a la Ley Orgánica de la Administración Pública Federal, el uso de buenas prácticas en materia de seguridad de datos personales en el sector de TI para poder brindar certeza a las empresas y particulares que las subcontraten bajo la figura de encargado prevista en la LFPDPPP, en coadyuvancia con el IFAIPD.
- b) Establecer una unidad administrativa que, además de atender los asuntos de protección de datos personales en posesión de los

particulares desde un punto de vista sectorial, promueva medidas preventivas y correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en las empresas de TI por parte de las personas físicas o morales, que operen como encargados en el tratamiento de datos personales en posesión de particulares.

- c) Realizar estudios o investigaciones sobre estándares de seguridad en el tratamiento de datos personales en posesión de los particulares y a cargo de los encargados.
- d) Crear una base de datos donde voluntariamente se inscriban las empresas y particulares que las subcontraten bajo la figura de encargado prevista en la LFPDPPP.
- e) Establecer acuerdos con la administración del SIEM (Sistema de Información Empresarial Mexicano), para abrir campos que identifiquen a personas o empresas que operen como encargados en el tratamiento de datos personales en posesión de los particulares.

7.4 Instrumentos de Política

Como instrumentos de política, se proponen los siguientes:

- I. El Sistema Nacional de Información de normas, estándares y buenas prácticas en materia de seguridad de datos personales en el sector de TI, cuyo objetivo será orientar e informar a las empresas y particulares que subcontraten servicios de tratamiento bajo la figura de encargado prevista en la LFPDPPP.

- II. El Inventario Nacional de empresas de TI dentro del Sistema de Información Empresarial Mexicano (SIEM).
- III. Las Normas Oficiales Mexicanas, Normas Mexicanas, Lineamientos y Parámetros en materia de seguridad en el tratamiento de datos personales.
- IV. Las medidas, programas, fondos, fideicomisos e instrumentos económicos relativos al desarrollo de la buenas prácticas e implementación de medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en las empresas de TI, por parte de las personas físicas o morales que operen como encargados en el tratamiento de datos personales en posesión de los particulares, los cuales deberán sujetarse a las disposiciones de las Leyes de Ingresos, del Presupuesto de Egresos de la Federación y de la Ley de Presupuesto, Contabilidad y Gasto Público Federal para el ejercicio fiscal que corresponda.
- V. La investigación, desarrollo, innovación y transferencia tecnológica que requieran las empresas del sector de las TI del país en materia de buenas prácticas sobre seguridad en el tratamiento de datos personales.
- VI. Los programas que tengan por objeto promover la construcción de capacidad, competencias sobre de seguridad informática y su certificación.
- VII. Los programas que tengan por objeto promover y realizar campañas permanentes de difusión y eventos especiales orientados al logro de las políticas públicas que impulsen el conocimiento de buenas prácticas nacionales e internacionales en materia de seguridad de datos para el sector de las TI.

- VIII. Los programas que tengan por objeto la implementación y evaluación de medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en las empresas de TI, por parte de las personas físicas o morales que operen como encargados en el tratamiento de datos personales en posesión de los particulares.

7.5 Responsables Institucionales de la Ejecución

Es importante señalar que las dependencias públicas que intervienen en el tema de la protección de datos personales son diversas, tomando en cuenta lo que la LFPDPPP establece en su artículo 40:

Artículo 40. La presente Ley constituirá el marco normativo que las **dependencias** deberán observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda, con la coadyuvancia del Instituto.

Aunado a lo anterior, el artículo 2 fracción I del Reglamento de la LFPDPPP define **dependencias** como: "*Las señaladas en el artículo 26 de la Ley Orgánica de la Administración Pública Federal*".

Por lo tanto, conforme a dichos numerales, las dependencias que intervienen o pueden intervenir en la emisión de la regulación que corresponda a su sector son –además del IFAIPD– las siguientes:

Artículo 26. Para el despacho de los asuntos del orden administrativo, el Poder Ejecutivo de la Unión contará con las siguientes **dependencias**:

Secretaría de Gobernación
Secretaría de Relaciones Exteriores
Secretaría de la Defensa Nacional
Secretaría de Marina
Secretaría de Seguridad Pública
Secretaría de Hacienda y Crédito Público
Secretaría de Desarrollo Social
Secretaría de Medio Ambiente y Recursos Naturales
Secretaría de Energía
Secretaría de Economía
Secretaría de Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación
Secretaría de Comunicaciones y Transportes
Secretaría de la Función Pública
Secretaría de Educación Pública
Secretaría de Salud
Secretaría del Trabajo y Previsión Social
Secretaría de la Reforma Agraria
Secretaría de Turismo
Consejería Jurídica del Ejecutivo Federal

La Secretaría de Economía, enlistada anteriormente, debe cumplir funciones específicas, conforme a las siguientes disposiciones de la LFPDPPP:

Artículo 41. La Secretaría, para efectos de esta Ley, tendrá como función difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano; promoverá las mejores prácticas comerciales en torno a la

protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto.

Artículo 42. En lo referente a las bases de datos de comercio, la regulación que emita la Secretaría, únicamente será aplicable a aquellas bases de datos automatizadas o que formen parte de un proceso de automatización.

Artículo 43. La Secretaría tiene las siguientes atribuciones:

- I. Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial;
- II. Fomentar las buenas prácticas comerciales en materia de protección de datos personales;
- III. Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad en coadyuvancia con el Instituto, a que se refiere la presente Ley;
- IV. Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general a que se refiere el artículo 40, en coadyuvancia con el Instituto;
- V. Fijar los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere el artículo 44 de la presente Ley, incluido la promoción de Normas Mexicanas o Normas Oficiales Mexicanas, en coadyuvancia con el Instituto;
- VI. Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento;

- VII. Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales;
- VIII. Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales;
- IX. Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial, y
- X. Apoyar la realización de eventos, que contribuyan a la difusión de la protección de los datos personales.

En otras palabras, conforme a los ordenamientos invocados, son 19 instituciones públicas, con la coadyuvancia del IFAIPD, las que tienen injerencia en el terreno de las regulaciones sobre privacidad. De aquí que estos 20 organismos en total, deban ser considerados como sujetos responsables de encauzar armónicamente las presentes Políticas Públicas.

Sin perjuicio de lo que establezcan las disposiciones legales aplicables, respecto de la coordinación en la materia entre los sectores público y privado y los distintos órdenes de gobierno, corresponderá a todas las dependencias, en el ámbito de su competencia, conducir, coordinar o participar en la aplicación, otorgamiento y evaluación de las medidas, programas e instrumentos en coadyuvancia con el IFAIPD.

Es importante señalar que la coadyuvancia no está definida en las leyes, por lo que el sentido que debe dársele es de coordinación interinstitucional.



ANEXOS

ANEXO 1

ENCUESTA-SONDEO EN LÍNEA

A partir de la aprobación del cuestionario, el día 9 de abril de 2012, se lanzó la invitación electrónica a las 12,200 empresas que se encontraban en la base de datos de la empresa encuestadora. Dicha invitación se muestra a continuación:



La Secretaría de Economía (SE) y la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de Información (CANIETI), le invitan cordialmente a participar en el estudio “Análisis de empresas de TI en materia de seguridad de datos personales para fomentar la figura de encargado de acuerdo a la LFPDPPP”. El objetivo de esta encuesta es identificar las áreas de oportunidad que permitan a las empresas de TI en México ser consideradas proveedores confiables como encargados del tratamiento de datos personales. Agradecemos el tiempo dedicado a responder la presente.

Participe

Asimismo, la Secretaría de Economía, en apoyo a este proyecto, envió oficio junto con invitación electrónica a diversas asociaciones y cámara (AMITI, AMIPCI Y CANIETI) entre el 17 y el 19 de abril de 2012 con el fin de que la convocatoria fuera mayor.

Los links que se utilizaron para dar acceso a la encuesta-sondeo fueron los siguientes:

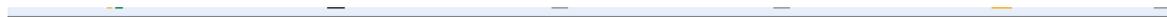
<http://q.elogia.net/qs/ETILFPDPPP/ETILFPDPPP.htm?c=36115049146982012418233317&q=ETILFPDPPP>

<http://q.elogia.net/qs/ETILFPDPPP/ETILFPDPPP.asp?c=#codigo&g=#estudio>

ESTRUCTURA DEL CUESTIONARIO

El diseño html del cuestionario utilizado para la encuesta-sondeo electrónico del proyecto “Análisis de empresas de TI en materia de seguridad de datos personales para fomentar la figura de encargado de acuerdo a la LFPDPPP” constó de 22 pantallas, mismas que se muestran a continuación:

Pantalla 1: Introducción



El Gobierno Federal a través de la Secretaría de Economía (SE) relanzó el Programa de Desarrollo del Sector de Servicios de Tecnologías de Información (PROSOFT 2.0) teniendo como objetivo fundamental crear las condiciones para que nuestro país cuente con un sector de servicios de TI competitivo internacionalmente y asegurar su crecimiento. Uno de los objetivos particulares de este Proyecto es el fortalecimiento institucional y mejora del marco legal, regulatorio y de políticas sectoriales.

Uno de los avances en el marco legal mexicano, que permite dar certeza jurídica en el uso de las TI a los consumidores y otras economías, fue la publicación y entrada en vigor de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su Reglamento.

De acuerdo a la LFPDPPP, se define tratamiento de datos personales como la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio, y la figura de encargado como la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable. En este contexto y con base en los resultados de encuestas en materia de seguridad de la información, se ha identificado como una oportunidad de mercado que dicha figura sea ejecutada por una empresa de TI.

En este tenor, se presenta a continuación un cuestionario que forma parte del Proyecto denominado **Análisis de empresas de TI en materia de seguridad de datos personales para fomentar la figura de encargado de acuerdo a la LFPDPPP** y cuyos resultados nos permitirán conocer el uso de buenas prácticas en materia de seguridad de datos personales en este sector, así como identificar las áreas de oportunidad que permitan a las empresas de TI ser consideradas proveedores confiables y de esta manera fomentar el crecimiento de las mismas.

Por último, se les recuerda que esta encuesta es anónima por lo que sus respuestas no serán asociadas a su empresa bajo ninguna circunstancia.

Continuar

Pantallas 2 a la 4: Sección "Clasificación"

Pantalla 2

I. CLASIFICACIÓN DE EMPRESAS

1. Actividad principal de la empresa: (UNA SOLA RESPUESTA)

- Desarrollo de software empaquetado
- Desarrollo de software a la medida
- Desarrollo de servicios en la nube (cloud computing)
- Servicios de análisis y desarrollo de sistemas computacionales
- Servicios de diseño, desarrollo y administración de bases de datos
- Servicios de seguridad de sistemas computacionales y procesamiento de datos
- BPO (Business Process Outsourcing) Contact center
- BPO (Business Process Outsourcing) Call center
- BPO (Business Process Outsourcing) Knowledge Process Outsourcing
- Multimedia y videojuegos
- Otra, ¿Cuál?

Continuar

Pantalla 3

2. ¿Qué puesto ocupa actualmente en su empresa? (UNA SOLA RESPUESTA)

- Director General
- Director de TI
- Gerente de Seguridad de Información
- Responsable de Auditoría Interna
- Otro, especifique

3. El número de empleados de su empresa es de: (UNA SOLA RESPUESTA)

Seleccione una opción...

4. El rango de ventas anuales (millones de pesos) de su empresa se encuentra en:

Seleccione una opción...

*Tamaño de las empresa: El sector de TI corresponde al sector Servicios, conforme al Acuerdo por el que se establece la estratificación de las micro, pequeñas y medianas empresas, publicado en el DOF (30 de Junio de 2009) http://dof.gob.mx/nota_detalle.php?codigo=5096849&fecha=30/06/2009

Continuar

Pantalla 4

5-¿En el ámbito de sus actividades procesa, almacena o resguarda algún tipo de datos personales? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Procesa datos personales internos (colaboradores y empleados)
- Procesa datos personales de clientes
- Almacena datos personales internos (colaboradores y empleados)
- Almacena datos personales de clientes
- Resguarda datos personales internos (colaboradores y empleados)
- Resguarda datos personales de clientes

6-¿Ofrece servicios de outsourcing para dar tratamiento de datos personales para otras empresas o entidades?

Sí

No

Continuar

Pantallas 5 a la 9: Sección "Prácticas Organizacionales de Seguridad y Privacidad de la Información"

Pantalla 5

II.PRÁCTICAS ORGANIZACIONALES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1.De las siguientes opciones, ¿Qué considera su organización para decidir y dimensionar los niveles de seguridad de la información y protección en su organización? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Análisis de riesgo.
- Resultados de análisis técnicos de vulnerabilidades.
- Observaciones de ejercicios de cumplimiento y auditorías.
- Conocimiento de la organización por parte del departamento TI/Seguridad.
- Recomendaciones de proveedores.
- Otro, especifique

Continuar

Pantalla 6

2. ¿Cuáles son las regulaciones, marcos referenciales (framework), mejores prácticas y/o estándares que ha utilizado su organización para implantar seguridad de la información? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Ley de Protección de Datos Personales en Posesión de los Particulares
- Ley de Transparencia y Acceso a la Información Pública Gubernamental
- PCI/DSS (en cualquiera de sus versiones)
- ISO/IEC 27001:2005
- ITIL (en cualquiera de sus versiones)
- COBIT (en cualquiera de sus versiones)
- CMMI/SSE-CMM
- Requerimientos de operación de su organización
- No sé
- Otra, especifique

Continuar

Pantalla 7

3. ¿Cómo se asignan los recursos para los esfuerzos y operación de seguridad de la información? (UNA SOLA RESPUESTA)

- Derivado del presupuesto de tecnología de información.
- Le asignaron un presupuesto específico para seguridad.
- Le asignaron un presupuesto por cada proyecto.
- No hay recursos asignados para seguridad de la información.
- Otro, especifique

4. ¿Cuál es el ÁREA responsable de la función de seguridad de la información en su organización? (UNA SOLA RESPUESTA)

- Dirección General
- Área de Sistemas/Informática
- Área específica de Seguridad de la Información.
- No se ha definido
- Otra, especifique

Continuar

Pantalla 8

5. ¿Cuáles de los siguientes objetivos de control, se han definido como componentes del marco normativo de seguridad de la información? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Política central y estándares auxiliares de seguridad de la información
- Clasificación de la información
- Inventario de activos de la información
- Seguridad de recursos humanos
- Control de acceso lógico
- Operaciones de cómputo
- Operación de telecomunicaciones
- Seguridad física y de instalaciones
- Gestión de incidentes de seguridad de la información
- Cumplimiento
- Seguridad en desarrollo de aplicaciones
- No tiene un marco normativo de seguridad
- Otro, especifique

Continuar

Pantalla 9

6. ¿Cuáles han sido los objetivos de control que se han implantado o reforzado en la organización como resultado del Análisis de Riesgos de Seguridad de la Información? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Política central y estándares auxiliares de seguridad de la información.
- Mecanismos de seguridad física para instalaciones y centro de datos.
- Seguridad en la infraestructura tecnológica.
- Capacitación y concientización en seguridad y privacidad de la información.
- Revisión de las relaciones contractuales con terceros.
- No se ha realizado análisis de riesgos.
- Otro, especifique

Continuar

Pantallas 10 a la 17: Sección "Gestión de la Seguridad y Privacidad de la Información"

Pantalla 10



III.GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

"Procesos, roles y responsabilidades"

1.¿Cuenta con un Comité de seguridad en su organización que vigile el cumplimiento, monitoreo y mejoramiento de las políticas establecidas? (UNA SOLA RESPUESTA)

Sí

No

2.¿Qué área es responsable de definir y administrar los criterios de clasificación de la información? (UNA SOLA RESPUESTA)

- Dirección General
- Seguridad de la Información
- Áreas de línea de negocio (LOB, por sus siglas en inglés)
- Función de Datos Personales
- No existen criterios formales de clasificación de información.
- Otra, especifique

Continuar

Pantalla 11

3.¿Qué actividades de divulgación y capacitación sobre seguridad y privacidad de la información se desarrollan en su organización? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Concienciación a través de correo electrónico, folletos, medios impresos, etc
- Formación y capacitación semestral en seguridad de la información
- Formación y capacitación anual en seguridad de la información
- No recuerda cuando fue la última capacitación
- Otra, especifique

Continuar

Pantalla 12

4. De las siguientes opciones, ¿Cuál o cuáles toma en cuenta para realizar las evaluaciones de la efectividad de seguridad de la información en su organización? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Reportes de incidentes de seguridad en la infraestructura.
- Evaluaciones de controles generales de TI.
- Reporte de soluciones de vulnerabilidades técnicas realizadas.
- Categorización de eventos identificados por la infraestructura.
- No existen indicadores formales de la efectividad de seguridad.
- Otra, especifique

5. ¿Qué área define los acuerdos contractuales de sus clientes/proveedores sobre la responsabilidad del procesamiento e intercambio de información y datos personales? (UNA SOLA RESPUESTA)

- El área jurídica
- El área comercial y el área jurídica
- Un grupo interdisciplinario de operaciones, comercial y jurídico.
- No se han definido cláusulas de esta responsabilidad.
- Otra, especifique

Continuar

Pantalla 13

III. GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Seguridad de los Activos Informáticos

1. ¿En dónde se encuentra la infraestructura tecnológica que soporta el procesamiento de aplicaciones, información y datos personales de su organización? (UNA SOLA RESPUESTA)

- En una localidad de su organización fuera de las instalaciones/oficinas (centro de datos dedicado)
- En una localidad contratada a un proveedor especializado
- En un área física dentro de las instalaciones/oficinas
- Otra ubicación, especifique

Continuar

Pantalla 14

2. ¿Cuáles son las medidas de seguridad que se han implantado en las instalaciones donde reside la infraestructura de procesamiento de aplicaciones, información y datos personales? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Segregación física de espacios (División de áreas, por ejemplo: área de proveedores, área de carga y descarga, etc).
- Control de acceso físico (Biométrico, smartcard, token).
- Infraestructura de soporte (Detección de humo, supresión de incendios, detectores de humedad, planta de luz, UPS).
- Señalización y estandarización de cableado (Cableado de red, de suministro eléctrico, de telefonía, etc).
- Inmovilización y aislamiento de equipos (Anaqueles cerrados, espacios confinados, etc).
- Inventario físico de infraestructura.
- Control y cierre de puertos/puntos de conexión (Red, telefonía).
- Otra, especifique

Continuar

Pantalla 15

3. ¿Qué tipo de mecanismos de seguridad en la infraestructura emplea su empresa para la protección de información y datos personales? Respecto a:

a. Seguridad de redes y comunicaciones (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Firewalls
- Software antivirus
- Sistemas de detección/ prevención de intrusiones
- Otro, especifique

b. Controles de acceso (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Esquema automático de gestión de identidades y accesos
- Smart cards/Dispositivos OTP
- Certificados digitales
- Matriz de roles y perfiles
- Biométrico
- Otro, especifique

c. Procesamiento en las aplicaciones (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Controles criptográficos
- Revisiones técnicas de código de aplicaciones
- Controles de consulta, extracción y modificación de información en bases de datos
- Sistemas de prevención de fuga de información (DLP-Data Loss/Leak Prevention)
- Otro, especifique

Continuar

Pantalla 16

4. ¿Por qué motivo o motivos su organización llega a realizar las prácticas de respaldo, retención y destrucción de información y datos personales? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Requerimientos fiscales
- Requerimientos contractuales (clientes y proveedores)
- Requerimientos de las áreas de negocio (LOB)
- Experiencia del personal de tecnología de la información
- No lo sabe
- Otro, especifique

5. ¿Cómo ejecutan los análisis de vulnerabilidades de la infraestructura? (UNA SOLA RESPUESTA)

- Con herramientas y personal de la organización
- Su organización contrata a un proveedor especializado
- No se realizan análisis de vulnerabilidades de infraestructura
- No lo sabe
- Otro, especifique

Continuar

Pantalla 17

6. ¿Cómo realiza la revisión y control de bitácoras de actividades (logs) de la infraestructura de procesamiento de aplicaciones, información y datos personales? (UNA SOLA RESPUESTA)

- Con un correlacionador de eventos.
- Con base en consolas de cada dispositivo de seguridad.
- Con revisiones en tiempo real del personal de seguridad.
- Servicios especializados externos de análisis y reporte de seguridad
- No se realiza control formalizado de bitácoras.
- Otro, especifique

7. En caso de contar con un proceso de respuesta a incidentes de seguridad de la información en su empresa, ¿existe un equipo de respuesta a incidentes de seguridad?(UNA SOLA RESPUESTA)

- Sí, depende del área de sistemas.
- Sí, es un equipo multidisciplinario con participación de varias áreas de la organización.
- No
- Sí, otro tipo de equipo. Especifique

Continuar

Pantallas 18 a la 22: Sección "Tratamiento de Datos en el denominado Cómputo en la Nube"

Pantalla 18



IV. TRATAMIENTO DE DATOS EN EL DENOMINADO CÓMPUTO EN LA NUBE

1. ¿Ofrece o utiliza servicios de cómputo en la nube? (UNA SOLA RESPUESTA)

- Ofrece
- Utiliza
- Ninguno

Continuar

Pantalla 19

2. ¿Cuál o cuáles de los aspectos que a continuación se mencionan contempla su organización? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LFPDPPP y su Reglamento.
- Las subcontrataciones que involucran la información sobre la que se presta el servicio son manifestadas al responsable de dicha información.
- Se incluyen condiciones para la prestación del servicio que le autorizan o permiten asumir la titularidad o propiedad de la información sobre la que se presta el servicio.
- Se guarda confidencialidad respecto de los datos personales sobre los que se presta el servicio.

3. ¿Cuál o cuáles de los siguientes mecanismos implementa su organización? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Da a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.
- Permite al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.
- Establece y mantiene medidas de seguridad adecuadas para la protección de los datos personales sobre los que se presta el servicio.
- Garantiza la supresión de los datos personales una vez que se haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos.
- Impide el acceso a los datos personales a personas que no cuenten con privilegios de acceso o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informando de ese hecho al responsable.

Continuar

Pantalla 20

4. ¿Cuál o cuáles de los aspectos que a continuación se mencionan contempla su proveedor de cómputo en la nube? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Tiene y aplica políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LFPDPPP y su Reglamento.
- Transparencia las subcontrataciones que involucran la información sobre la que presta el servicio.
- Se abstiene de incluir condiciones para la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que se presta el servicio.
- Guarda confidencialidad respecto de los datos personales sobre los que se presta el servicio.

5. ¿Cuál o cuáles de los siguientes mecanismos implementa su proveedor de cómputo en la nube? (PUEDE SELECCIONAR MÁS DE UNA OPCIÓN DE RESPUESTA)

- Da a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.
- Le permite limitar el tipo de tratamiento de los datos personales sobre los que presta el servicio.
- Establece y mantiene medidas de seguridad adecuadas para la protección de los datos personales sobre los que presta el servicio.
- Garantiza la supresión de los datos personales una vez que se ha concluido el servicio prestado al responsable, así como la recuperación de los mismos.
- Impide el acceso a los datos personales a personas que no cuenten con privilegios de acceso o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informando de ese hecho al responsable.

Continuar

Pantalla 21

6. Finalmente, ¿le gustaría agregar algún comentario respecto a este estudio?

7. ¿Le gustaría participar en la segunda edición de este importante estudio?, escriba su correo electrónico

Continuar

Pantalla 22

Agradecemos el tiempo que dedicó para contestar este cuestionario.

Finalizar

ANEXO 2

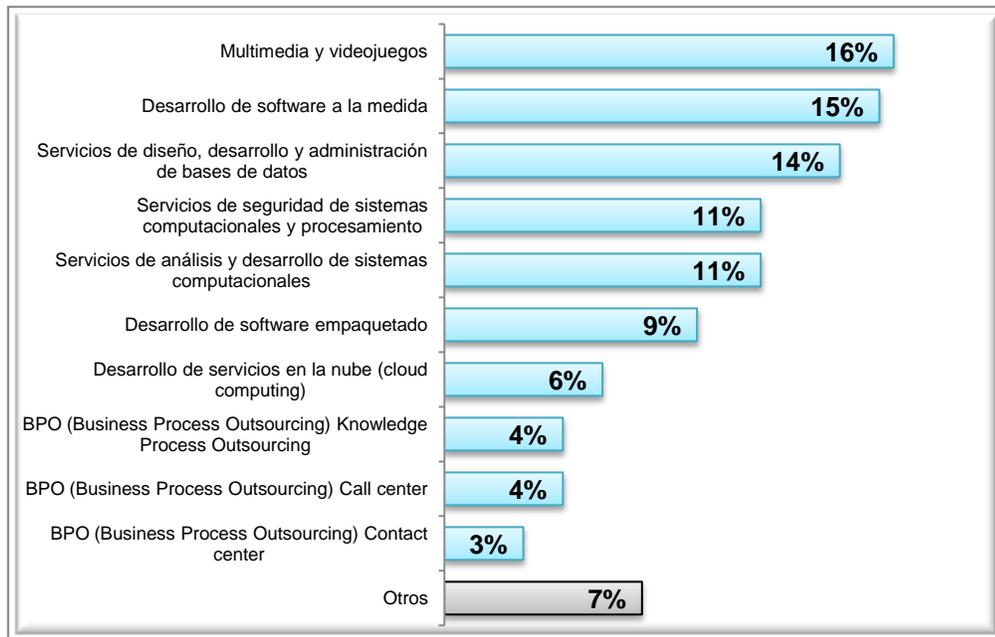
RESULTADOS Y ESQUEMA ESTADÍSTICO DE LA ENCUESTA-SONDEO EN LÍNEA

I. Clasificación

I.1 Actividad principal de la empresa

En la gráfica que se muestra a continuación sobre la distribución de las actividades de las 564 empresas encuestadas, se puede observar lo siguiente:

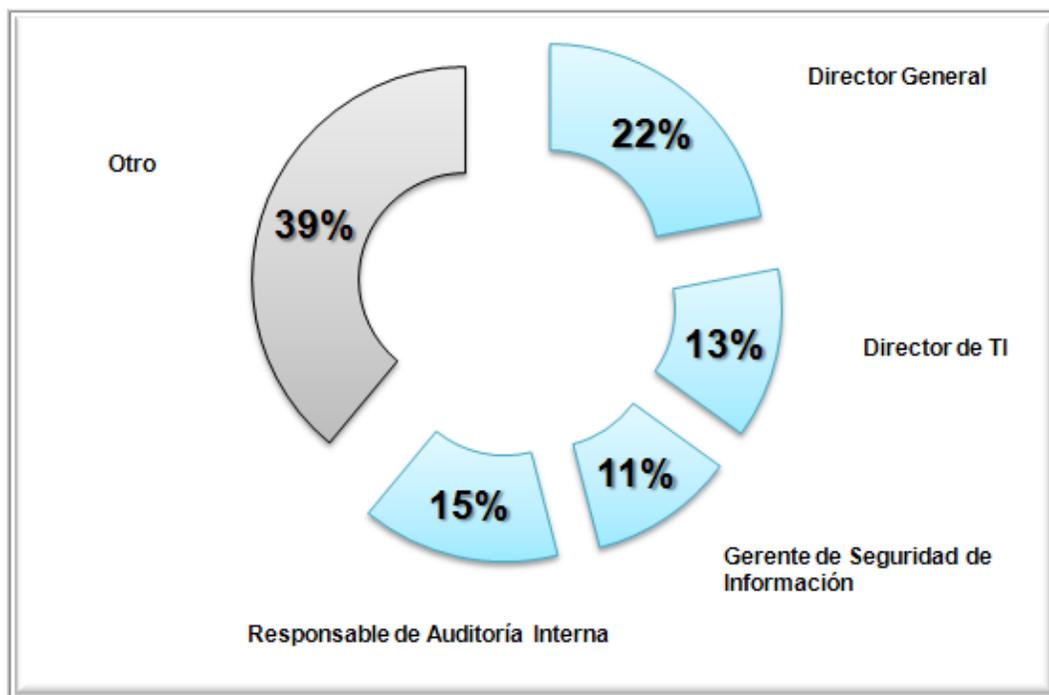
- El 36% de las empresas que respondieron la encuesta-sondeo ofrecen algún tipo de servicio de diseño, desarrollo y administración de bases de datos; seguridad de sistemas computacionales y procesamiento; o bien de análisis y desarrollo de sistemas computacionales.
- El 24% de las empresas tienen como actividad el desarrollo de software a la medida o el empaquetado.
- El 16% de las empresas se dedican a servicios de multimedia y videojuegos.
- El 11% ofrece algún tipo de servicio BPO (Business Process Outsourcing).
- El 7% respondió que su actividad es diseño publicitario on-line, servicios varios on-line y consultoría TI.
- Solo el 6% se dedica al desarrollo de servicios en la nube (cloud computing).



I.2 El cargo o puesto que ocupa la persona que respondió la encuesta-sondeo dentro de la empresa

El 35% de la encuesta-sondeo fue contestada por directores generales y directores de TI, sin embargo, el mayor número de encuestados (39%) fue personal de las empresas que ocupan algún puesto dentro del área de Sistemas o TI:

- Subdirector de Sistemas
- Gerente de Sistemas
- Programador
- Supervisor Administrativo
- Subgerente TI
- Jefe de Área de Sistemas



Tal y como se ve en esta gráfica, el porcentaje de participación de niveles directivos no es muy alta, por lo tanto, detectamos una falta de compromiso y responsabilidad de la alta directiva en temas de seguridad de la información y privacidad de datos personales con un sentido organizacional.

El porcentaje más grande de participantes (39%) en la encuesta-sondeo señala que la responsabilidad en seguridad de la información y privacidad de datos personales, se relega a un plano táctico y operativo, con alcances limitados y esfuerzos acotados dentro de la organización.

I.3 Tamaño de las empresas

Para poder llevar a cabo la clasificación de las empresas encuestadas se tomó como base lo establecido en el Diario Oficial de la Federación (DOF) del 30 de junio de 2009, sobre la estratificación de las micro, pequeñas y medianas empresas, de conformidad con los criterios establecidos en el segundo artículo del **ACUERDO por el que se establece la estratificación de las micro, pequeñas y medianas empresas:**

Estratificación				
Tamaño	Sector	Rango de número de trabajadores	Rango de monto de ventas anuales (mdp)	Tope máximo combinado*
Micro	Todas	Hasta 10	Hasta \$4	4.6
Pequeña	Comercio	Desde 11 hasta 30	Desde \$4.01 hasta \$100	93
	Industria y Servicios	Desde 11 hasta 50	Desde \$4.01 hasta \$100	95
Mediana	Comercio	Desde 31 hasta 100	Desde \$100.01 hasta \$250	235
	Servicios	Desde 51 hasta 100		
	Industria	Desde 51	Desde	250

		hasta 250	\$100.01 hasta \$250	
--	--	--------------	----------------------------	--

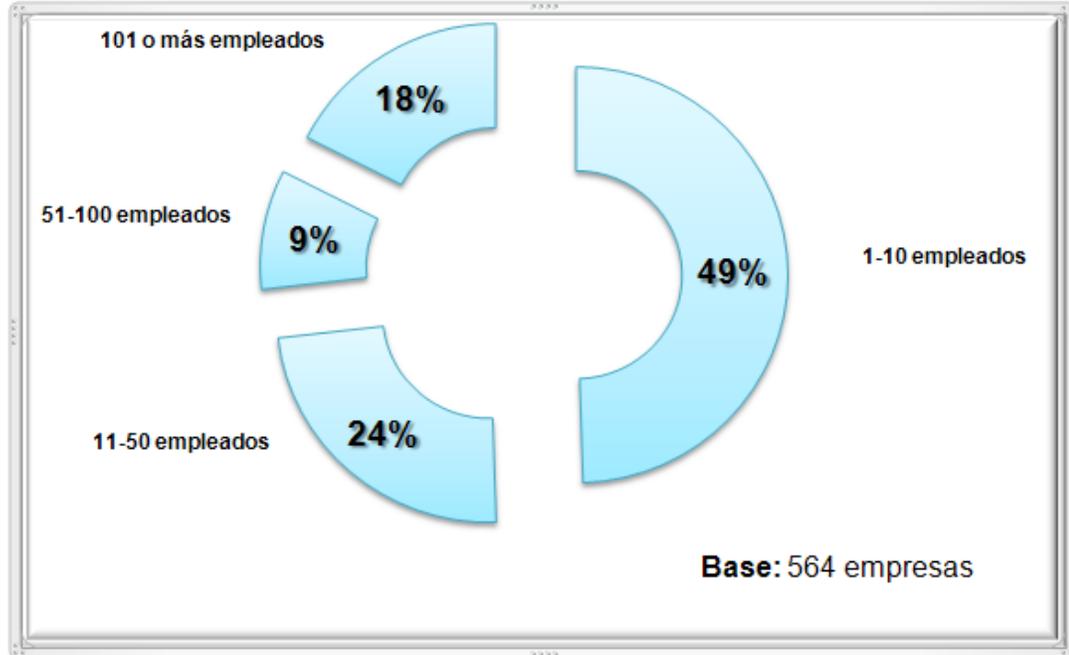
***Tope Máximo Combinado = (Trabajadores) X 10% + (Ventas Anuales) X 90%.**

Para poder conocer el tamaño de las empresas encuestadas se hicieron dos preguntas dentro del cuestionario, una que se refería al número de empleados y otra sobre el rango de ventas anuales en millones de pesos, dando como resultado lo que se muestra en los siguientes sub-incisos:

I.3.1 Número de empleados

De acuerdo a los resultados obtenidos de la encuesta-sondeo en línea, las empresas se pueden clasificar de la siguiente manera:

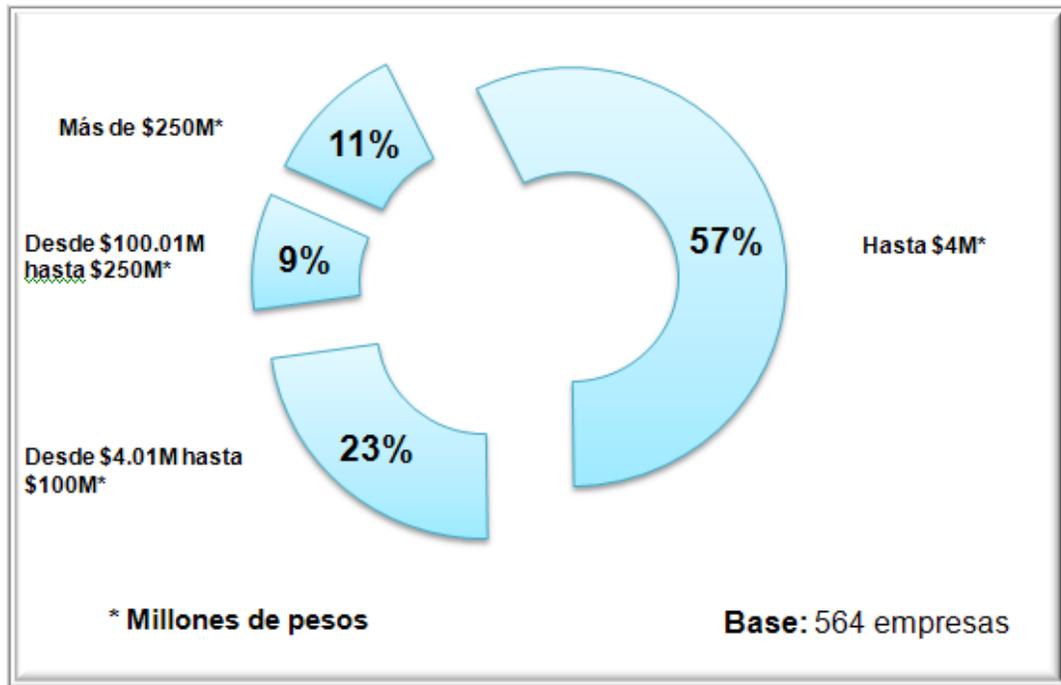
- Micro: 49%
- Pequeña: 24%
- Mediana: 9%
- Grande: 18%



I.3.2 Rango de ventas anuales

Los resultados obtenidos para el rango de venta anuales en millones de pesos son los que se muestran a continuación:

- Micro: 57%
- Pequeña: 23%
- Mediana: 9%
- Grande: 11%

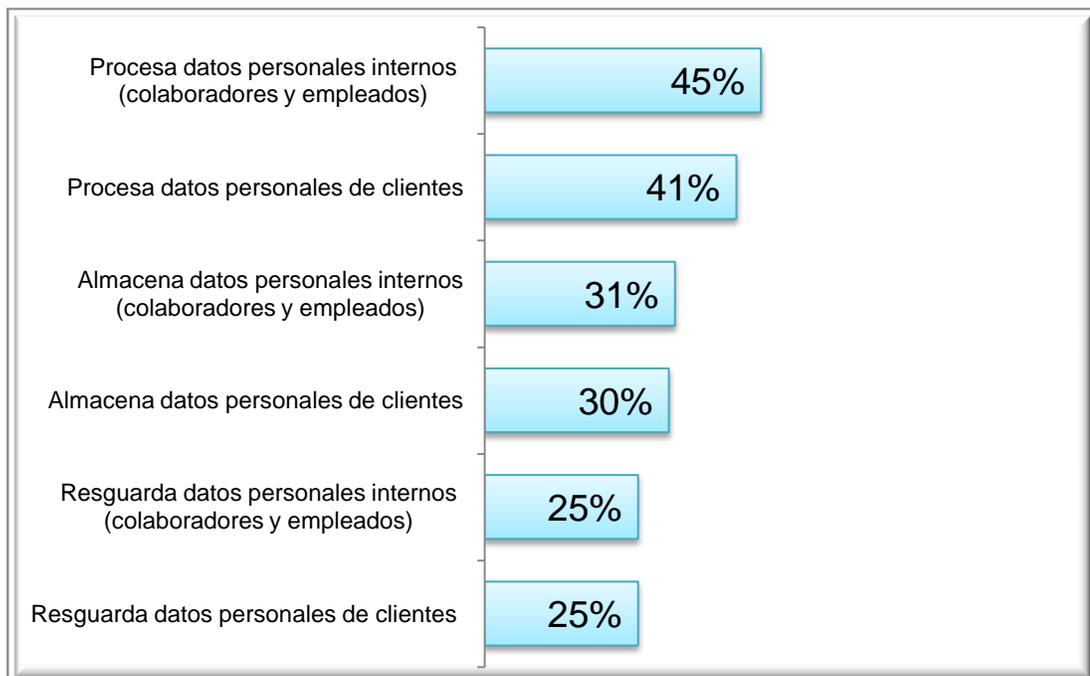


Si comparamos las respuestas obtenidas en la pregunta sobre número de empleados de la empresa y el rango de ventas anuales podemos observar lo siguiente:

- El 8% de las empresas que por el número de sus empleados no entra dentro de la clasificación de micro-empresa, sí podría ser clasificada como tal, si se considera el rango de sus ventas anuales.
- Solo el 11% de las empresas encuestadas presentan las ventas anuales requeridas para ser consideradas grandes empresas, a pesar de que el 18% fueron las empresas que por el número de empleados podrían considerarse grandes empresas.

I.4 Almacenamiento o resguardo de algún tipo de datos personales

Se consideró importante –dentro de la encuesta-sondeo– identificar si las empresas del sector de TI están conscientes de que ellas tratan⁹⁰ datos personales tanto de colaboradores y empleados como de sus clientes, por esta razón se incluyó esta pregunta, obteniendo como resultado lo siguiente:



Mediante las respuestas obtenidas se observa que 4 de cada 10 empresas evaluadas tiene el conocimiento de que realiza procesamiento de datos personales tanto internos como de clientes. Sin embargo, el almacenamiento y resguardo de los datos no se lleva a cabo en la misma proporción.

Es importante señalar que en términos generales las empresas no tienen el conocimiento sobre lo que es el tratamiento de datos personales, pues

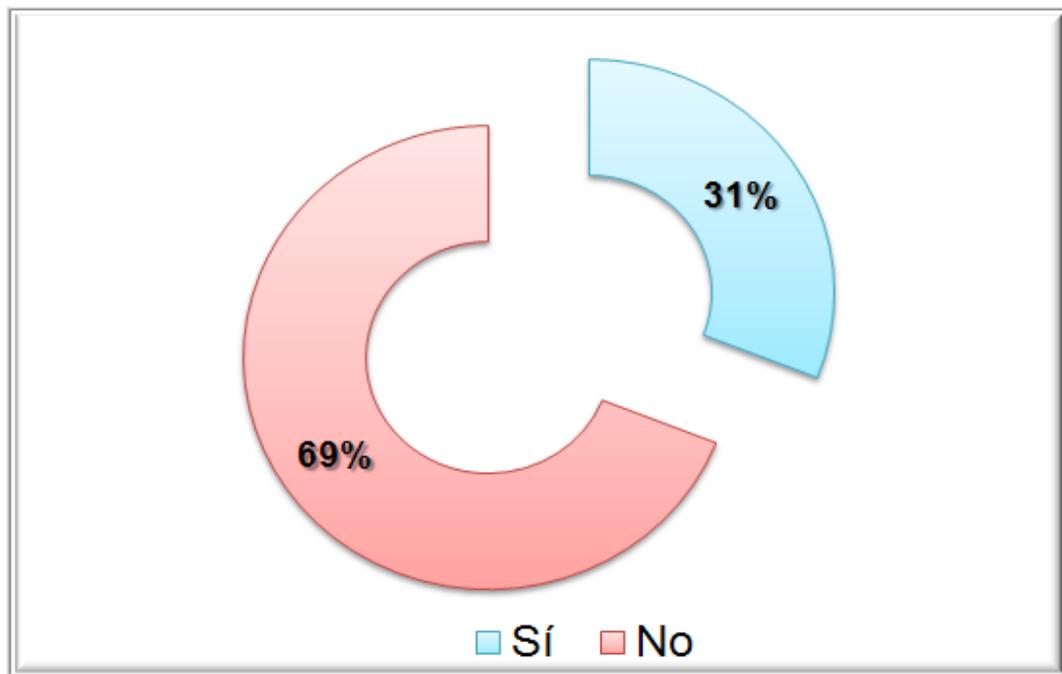
⁹⁰ La LFPDPPP define el tratamiento de datos personales como: “La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.”

aproximadamente 6 de cada 10 empresas no procesa los datos de sus colaboradores y empleados.

I.5 Empresas que ofrecen servicios de outsourcing de tratamiento de datos personales para otras empresas o entidades

Debido a que el presente proyecto tiene como objetivo general: **Desarrollar las habilidades y fomentar el uso de buenas prácticas en materia de seguridad de datos personales en el sector de tecnologías de información, para poder brindar certeza a las empresas que las subcontraten, bajo la figura de encargado prevista en la LFPDPPP**, resultó imprescindible saber si las empresas encuestadas ofrecían o no algún tipo de servicio de tratamiento de datos personales que los convirtiera en encargados.

La respuesta obtenida fue que solo 3 de cada 10 empresas evaluadas ofrece servicios de outsourcing de tratamiento de datos personales.



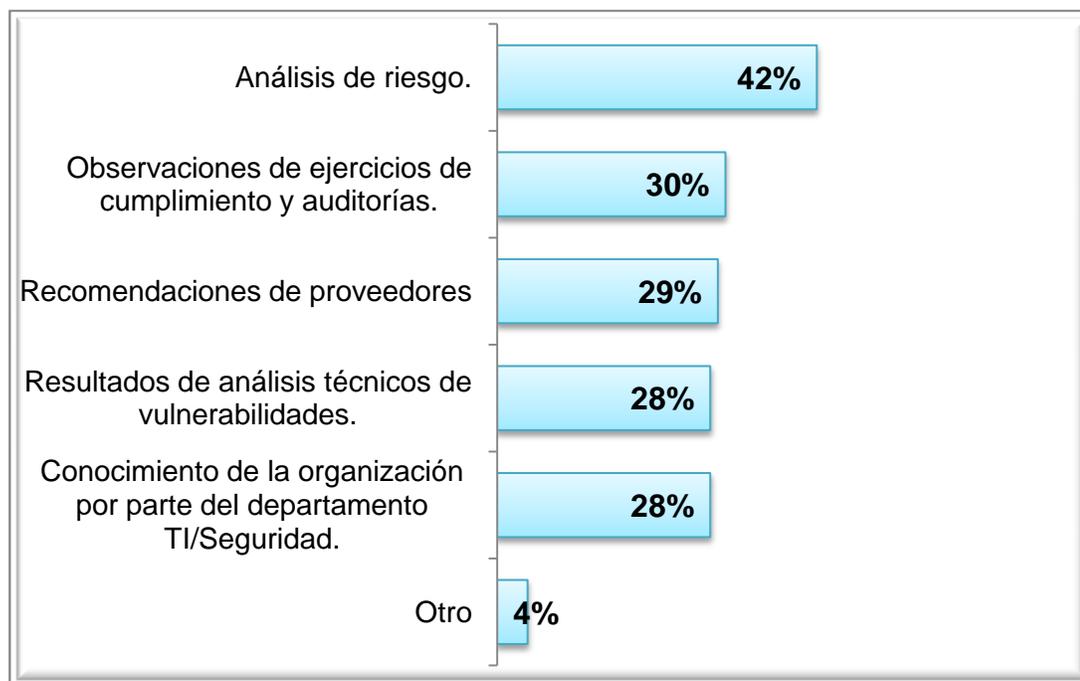
Considerando el tamaño de la oferta de servicios de outsourcing de tratamiento de datos personales (por el porcentaje obtenido), se puede anticipar un nicho de mercado en el sector.

II. Prácticas organizacionales de seguridad y privacidad de la información

II.1 Aspectos que consideran las organizaciones para decidir y dimensionar los niveles de seguridad de la información y protección

Considerando las 564 empresas encuestadas, esta gráfica arroja lo siguiente:

- El 42% de las empresas realizan análisis de riesgos para decidir y dimensionar los niveles de seguridad de la información.
- El 28% de las organizaciones consideran para su estrategia de seguridad de información al departamento de sistemas (TI/Seguridad): puede ser a través de los resultados de análisis técnicos de vulnerabilidades o mediante el conocimiento del área sobre este tema.
- Para decidir dicha estrategia, el 30% de las organizaciones toman en cuenta las observaciones de ejercicios de cumplimiento y auditorías.
- El 4% de las empresas mencionaron basarse en las recomendaciones de clientes.

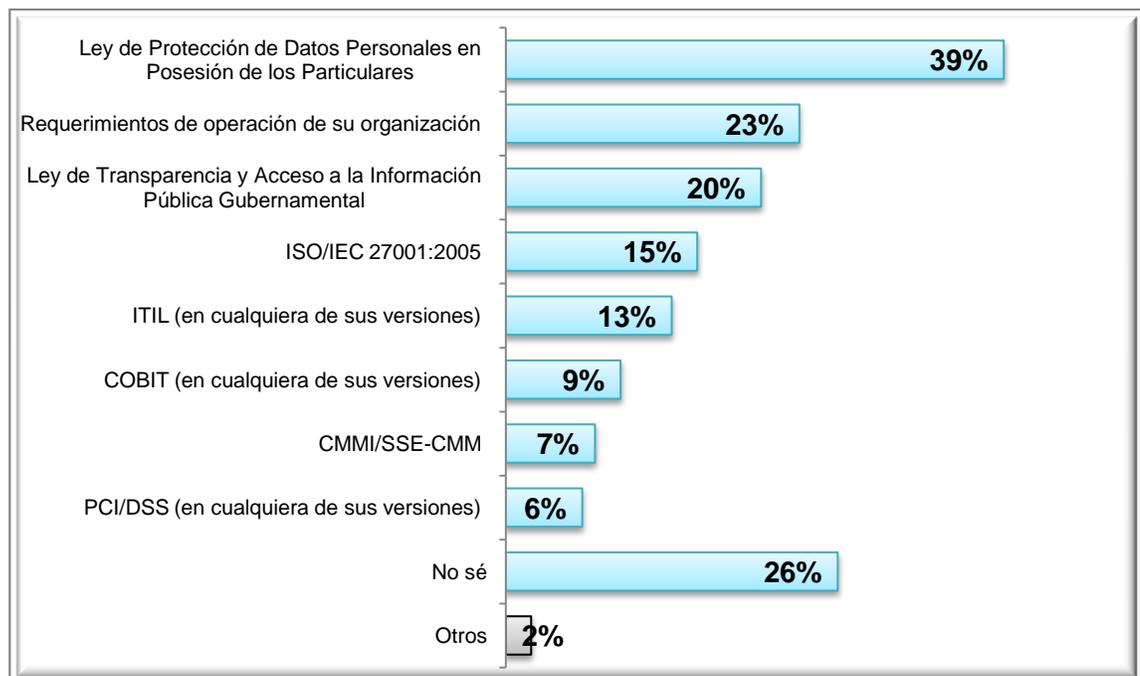


Debe resaltarse que cerca de la mitad de las empresas participantes reconocen al Análisis de Riesgos como un mecanismo fundamental para decidir sus iniciativas y actividades relativas a la seguridad de la información. Lo cierto es que el reconocimiento del Análisis de Riesgo podría facilitar el cumplimiento con la Ley de acuerdo con lo establecido de forma general en el Artículo 19 de la misma, o bien, de manera específica en el Artículo 61 de su propio Reglamento. En este sentido resta corroborar la ejecución real del Análisis de Riesgos en las secciones ulteriores de la encuesta-sondeo.

II.2 Regulaciones, marcos referenciales, mejores prácticas y/o estándares que utilizan las empresas para implantar seguridad de la información

La gráfica relacionada a este tema muestra lo siguiente:

- El 39% de las organizaciones toman como base la Ley Federal de Protección de Datos Personales en Posesión de los Particulares para implantar la seguridad de la información.
- El 50% de las empresas utilizan alguna de las mejores prácticas y estándares internacionales (ISO/IEC 27001-2005, ITIL, COBIT, CMMI/SSE-CMM, PCI/DSS).
- El 26% de las empresas evaluadas no saben qué regulaciones y/o marcos referenciales utilizan para implantar la seguridad de la información.
- El 2% respondió que utilizan estándares internos o no existe práctica de seguridad.

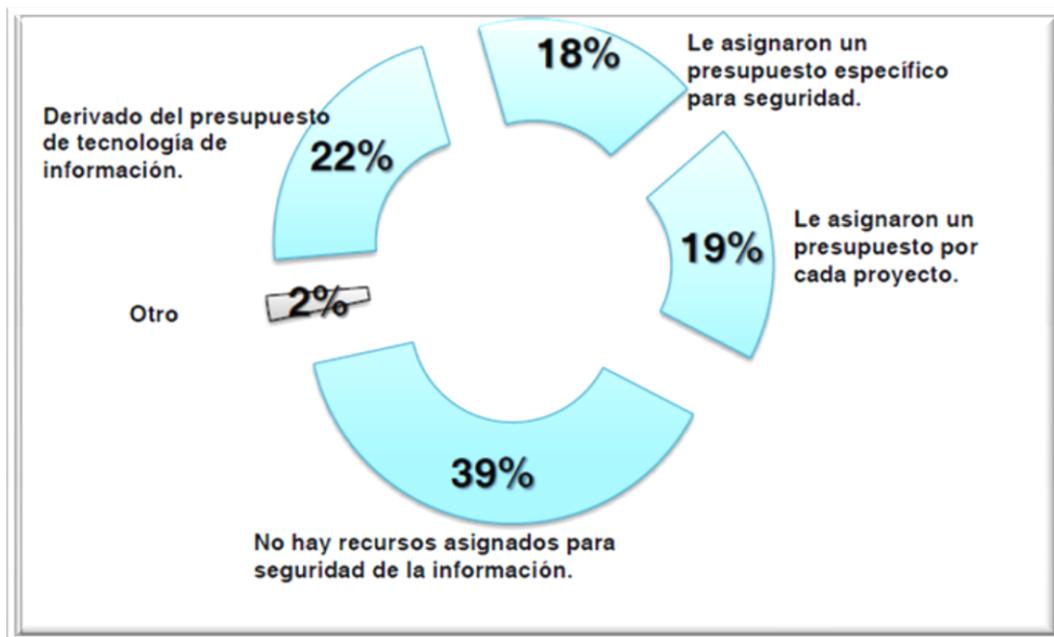


Esta gráfica denota que hay una propensión de la industria de servicios de TI a utilizar referencias estandarizadas o certificables para guiar sus iniciativas de seguridad de la información. Sin embargo, no debe perderse de vista que el porcentaje de empresas que utilizan como referencia la LFPDPPP, podría indicar que las iniciativas tienen un objetivo acotado al cumplimiento de la regulación y no un beneficio organizacional. Esto puede verificarse en las secciones relativas a la implementación de mecanismos de control específicos.

II.3 Asignación de los recursos para los esfuerzos y operación de seguridad de la información

En la gráfica que se muestra a continuación se observa que:

- El 22% de las empresas encuestadas asignan los recursos para la seguridad de la información del presupuesto de tecnología de información.
- El 18% de las organizaciones tienen asignado un presupuesto específico para seguridad.
- Casi 4 de cada 10 empresas evaluadas no asignan recursos en temas de seguridad de la información.



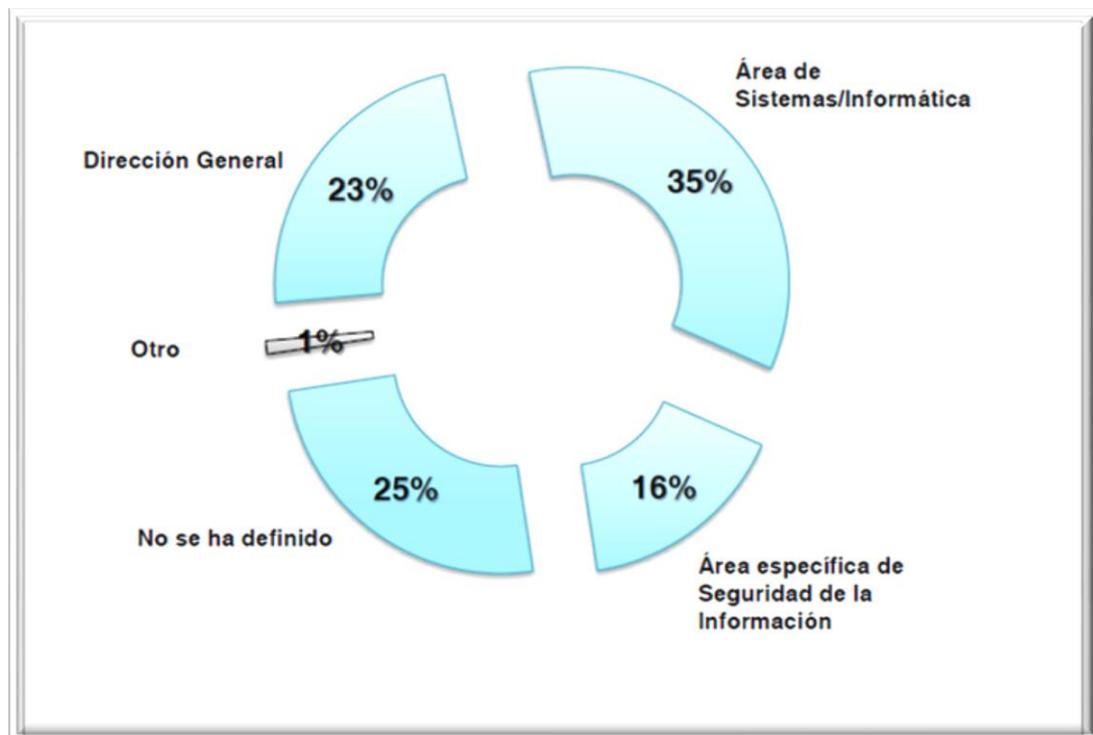
Es pertinente señalar que –de acuerdo a esta gráfica– los presupuestos específicos para seguridad de la información son incipientes para el tipo de iniciativas que han de requerirse para alinearse con una directriz organizacional y lograr el cumplimiento de la LFPDPPP.

Por lo regular no se asigna ningún tipo de recursos a la seguridad de la información; en el mejor de los casos, se dota de recursos con base en un proyecto específico. Este fenómeno es un indicador de la baja prioridad que tiene la seguridad de la información y privacidad de datos personales para las organizaciones, y cuya ejecución es puntual o aislada.

II.4 Área responsable de la función de seguridad de la información

Las respuestas de las 564 empresas encuestadas arrojaron lo siguiente:

- 35 de cada 100 organizaciones evaluadas han asignado como responsable de la seguridad de la información a su área de sistemas.
- El 25% del total de las empresas encuestadas no han definido un responsable de la función de seguridad de la información.
- En el 23% de los casos, la dirección general está involucrada como responsable de la seguridad de la información.
- El 16% de las empresas cuentan con un área específica de seguridad de la información.
- El 1% contestó que el responsable es el área de proyectos o no saben.



En primer lugar, detectamos que un alto porcentaje de las empresas del sector de TI continúan teniendo un enfoque tradicional para atender la función de seguridad de la información, ya sea a través del área de sistemas o de informática. Esta situación podría implicar una adopción más lenta del tema de la privacidad de datos personales como una función organizacional en la que todas las áreas de la misma tienen un rol y responsabilidad activos.

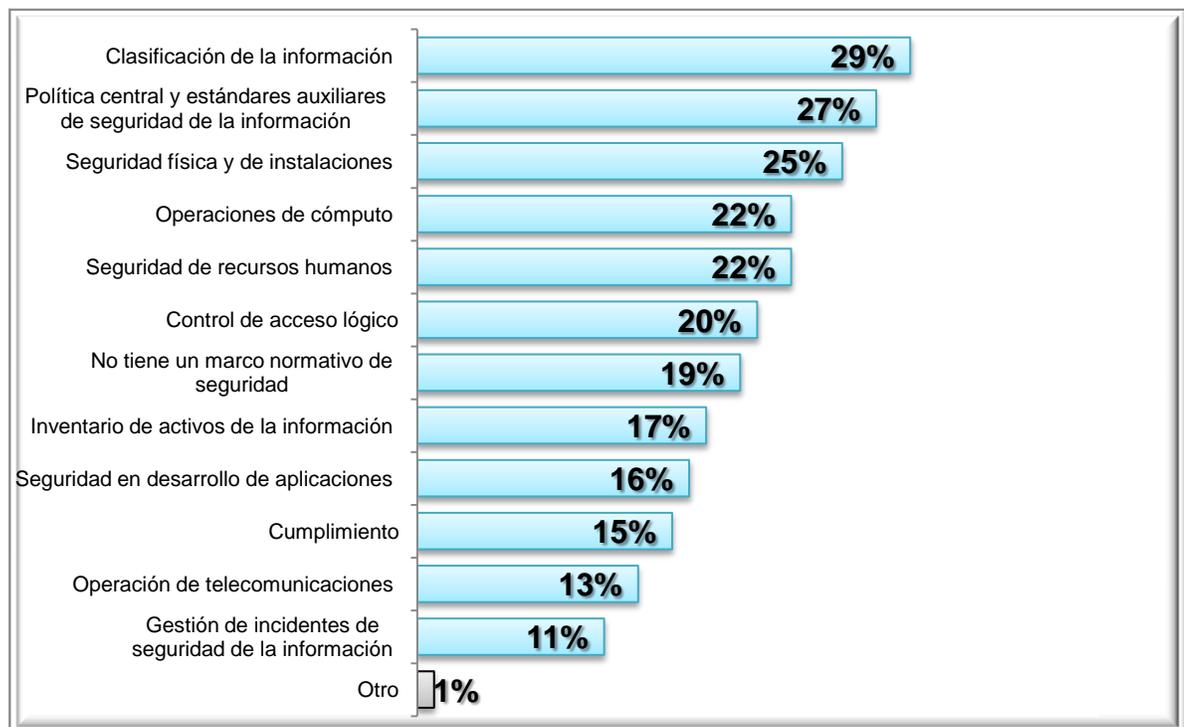
En segundo lugar, vemos que las organizaciones no han asignado formalmente la función de seguridad, cuando en realidad debería ser un aspecto prioritario del negocio.

En tercer lugar, detectamos un aspecto positivo: que la Alta Dirección se involucre directamente en la ejecución de la función de seguridad de la información. Esto permitirá que –de forma natural– se establezca una asignación de responsabilidades hacia los demás niveles jerárquicos.

II.5 Objetivos de control definidos como componentes del marco normativo de la seguridad de la información

En la gráfica que se muestra a continuación se puede observar lo siguiente:

- La mayoría de las empresas evaluadas (29%) considera la clasificación de la información como componente del marco normativo de la seguridad de la información.
- El 27% de las empresas encuestadas considera la política central y estándares auxiliares como componente de su marco normativo.
- Solo el 15% de las empresas encuestadas respondió que utilizan el cumplimiento como el marco normativo.
- Casi 2 de cada 10 empresas evaluadas no posee un marco normativo de seguridad.



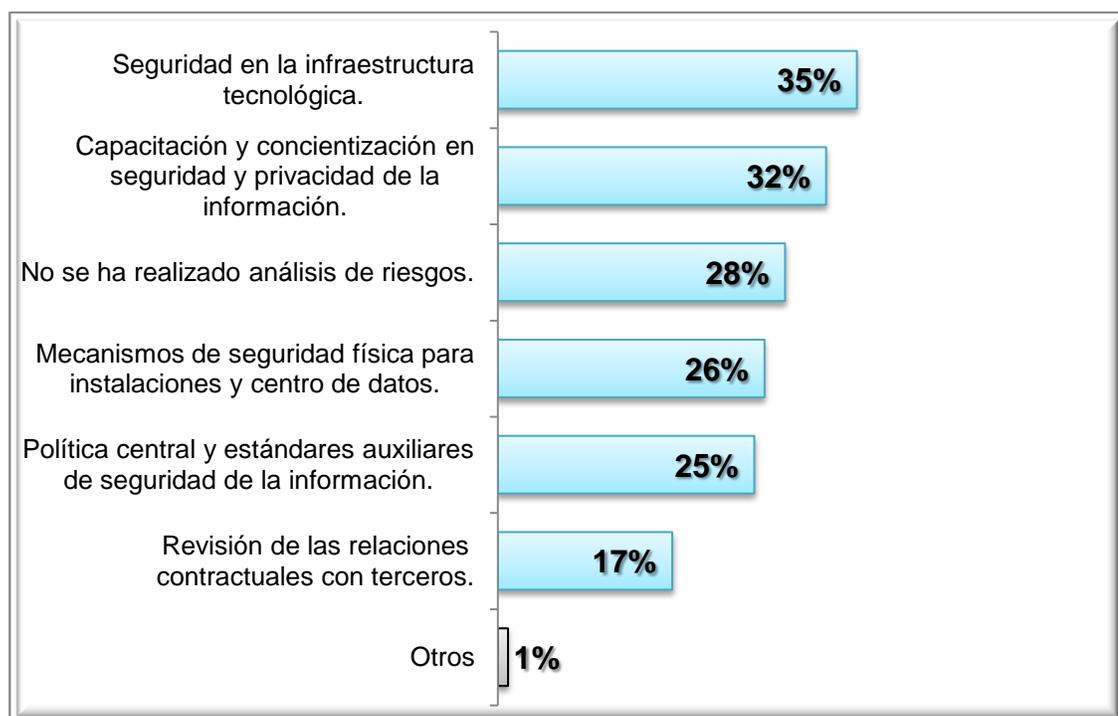
Con base en esta gráfica, observamos que las organizaciones perciben a los mecanismos de control administrativos –con sus políticas y criterios de clasificación de la información— como fundamentales para la operación de la seguridad de la información.

Cabe señalar que actualmente los esfuerzos se han centrado en asegurar instalaciones (seguridad física) e infraestructura (operaciones de cómputo).

II.6 Objetivos de control implantados o reforzados en las organizaciones como resultado del análisis de riesgos de la seguridad de la información

A continuación se muestran los resultados obtenidos sobre los objetivos de control implantados en las empresas que realizan análisis de riesgos:

- El 35% de las empresas evaluadas implantan objetivos de control relacionados a la seguridad en la infraestructura tecnológica.
- El 32% de las empresas utilizan la capacitación y concientización en seguridad y privacidad de la información como objetivos de control para su estrategia de seguridad.
- Solo el 17% de las organizaciones encuestadas consideran como objetivos de control la revisión de las relaciones contractuales con terceros.



En esta gráfica confirmamos las inferencias de las primeras secciones de preguntas, al demostrar que las organizaciones de TI se han enfocado en esfuerzos de seguridad de la infraestructura tecnológica como parte del enfoque tradicional de esta función. Esta situación es un resultado natural de la dependencia de la seguridad de la información del área de sistemas/informática.

Así pues, se ha detectado un alto porcentaje de organizaciones que no han realizado un ejercicio de análisis de riesgos. Esto confirma que –aún cuando se reconoce como un factor fundamental para definir y ejecutar iniciativas de seguridad– las organizaciones se basan únicamente en el conocimiento adquirido a través de su departamento de TI.

Asimismo, el porcentaje de organizaciones que considera sus acuerdos contractuales para implementar controles de seguridad y privacidad de datos personales es bajo.

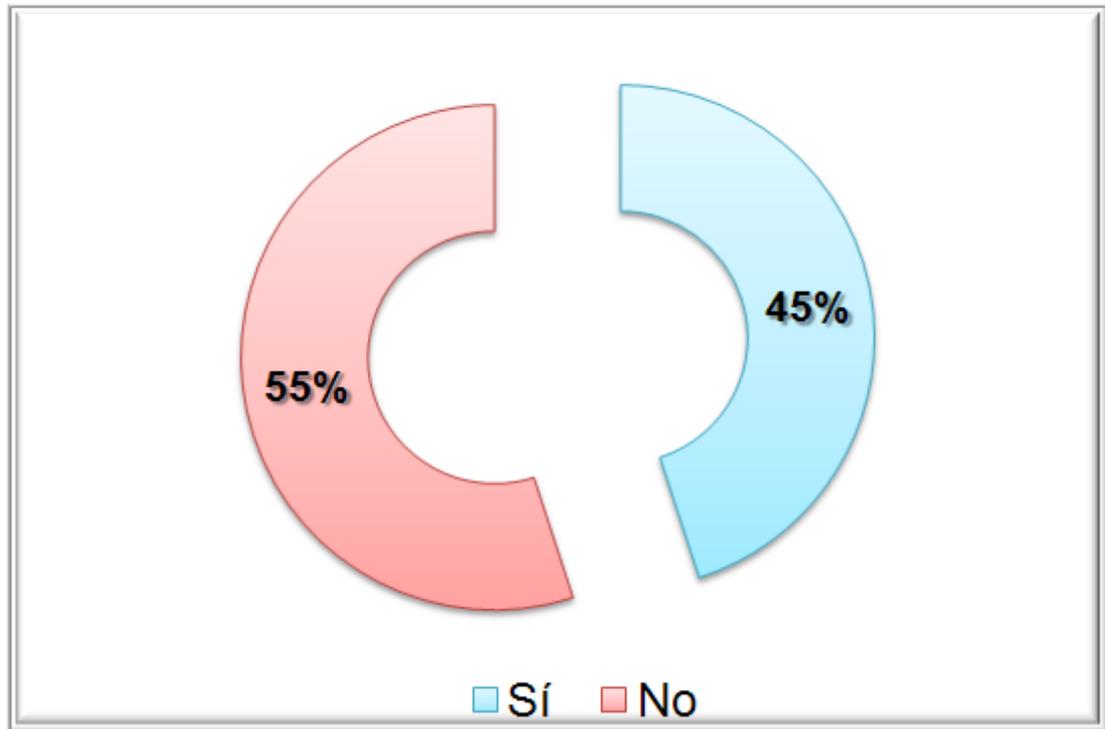
III. Gestión de la seguridad y privacidad de la información

III.1 Procesos, roles y responsabilidades

III.1.1 Comité de seguridad que vigila el cumplimiento, monitoreo y mejoramiento de las políticas establecidas

En esta gráfica se observa lo siguiente:

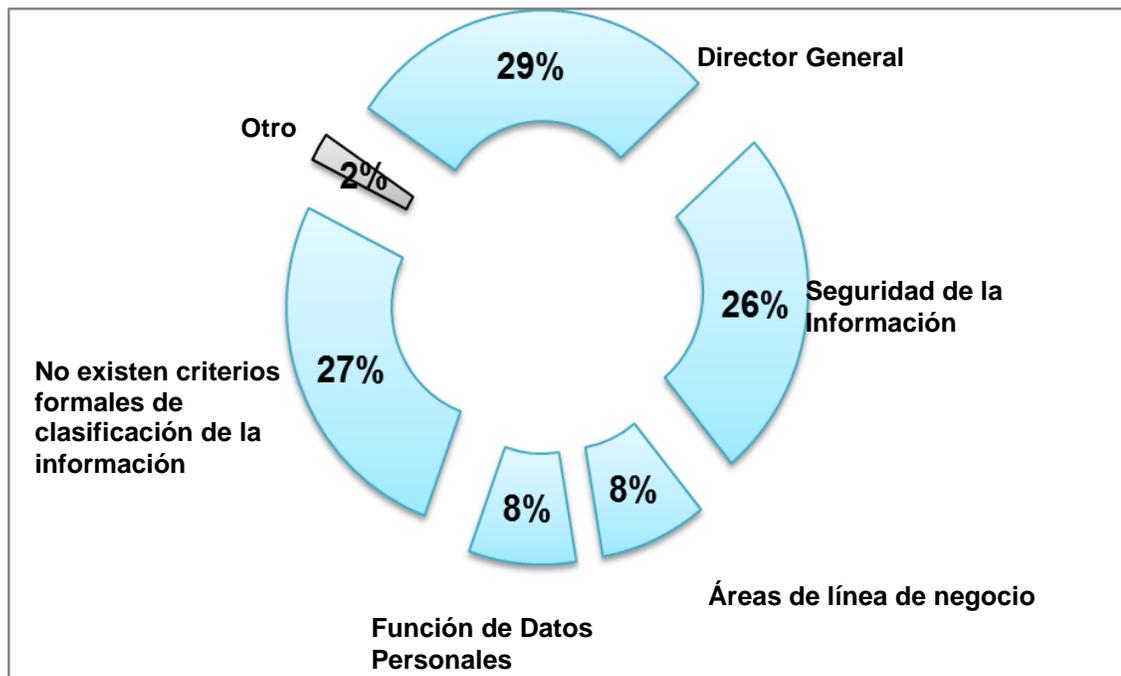
- 55 de cada 100 empresas evaluadas **no cuentan** con un comité de seguridad.
- El 45% de las organizaciones posee un comité de seguridad que vigila el cumplimiento de las políticas de manejo de la información.



III.1.2 Área responsable de definir y administrar los criterios de clasificación de la información

En esta gráfica se observa lo siguiente:

- En 29 de cada 100 empresas encuestadas los criterios de clasificación de información son responsabilidad de la dirección general.
- En el 27% de las empresas no existen criterios formales de clasificación de la información.
- El 26% de las empresas evaluadas, asignan la responsabilidad de clasificación de la información al área de seguridad de la información de forma específica.
- Solo 8 de cada 100 empresas cuentan con la función de datos personales como responsables de la clasificación de la información.



El porcentaje de organizaciones que no han definido un criterio de clasificación de la información (27%) confirma que –aún cuando este control se ha reconocido como básico en la generación de iniciativas de seguridad— no se ejecuta en el esquema actual de operación de seguridad de la información.

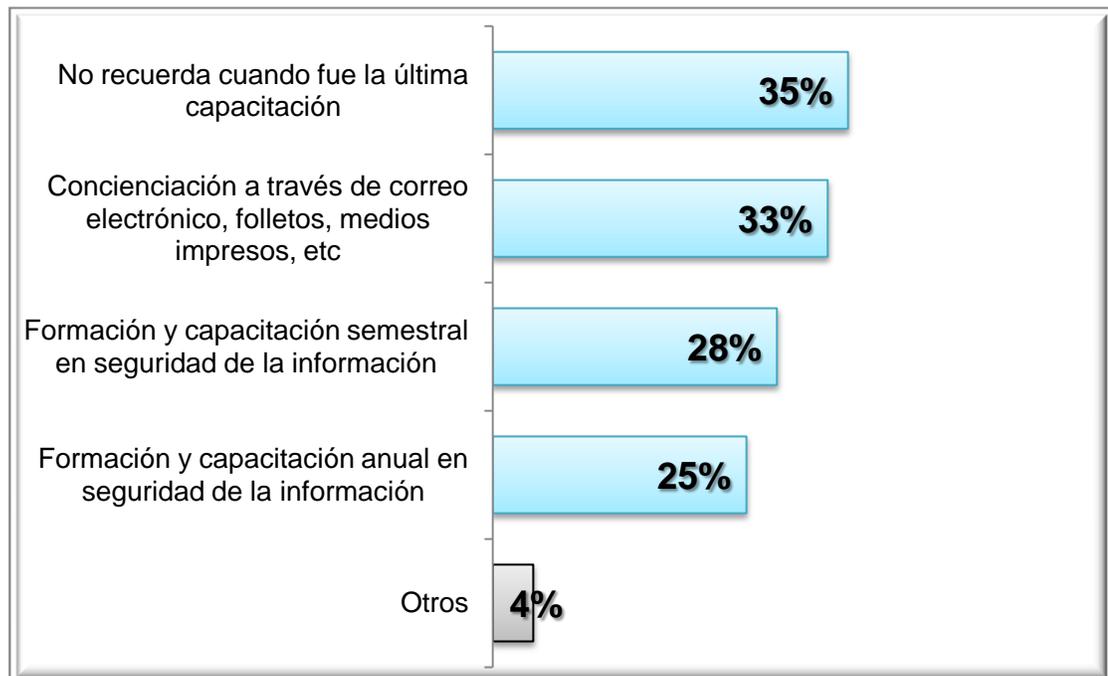
El porcentaje de organizaciones en las que el administrador del criterio de clasificación de la información se encuentra en la Alta Dirección (29%) o en la Seguridad de la Información (26%), demuestra que no se ha logrado una participación activa de la aplicación de estos criterios por parte de los responsables de procesos en datos personales.

Cabe destacar que –aún cuando éste es un mecanismo básico establecido por la el Reglamento de la LFPDPPP— solamente el 8% de las empresas participantes han asignado una función específica de datos personales.

III.1.3 Actividades de divulgación y capacitación sobre seguridad y privacidad de la información

En este tema las empresas evaluadas respondieron lo siguiente:

- El 35% de las empresas evaluadas no recuerdan cuándo fue la última capacitación sobre seguridad y privacidad de la información.
- Más del 50% de las organizaciones toman capacitación en seguridad de la información semestral o anual.
- El 4% respondió que no cuentan con ningún tipo de actividad de divulgación y capacitación sobre seguridad de la información.

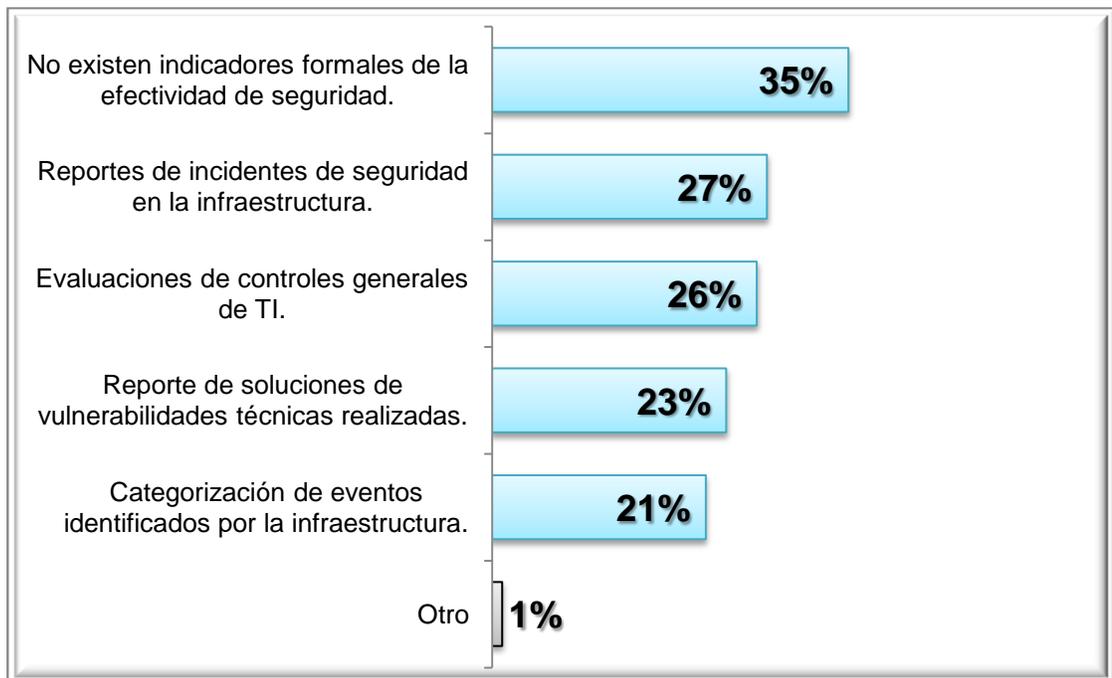


Se reconoció que la capacitación y entrenamiento en seguridad de la información es un elemento fundamental para soportar las iniciativas de seguridad de la información. Sin embargo, el porcentaje de respuesta más alto (35%) nos permite determinar que no se ejecuta como un proceso recurrente en las diversas organizaciones, empresas y negocios.

III.1.4 Actividades que toman en cuenta las organizaciones para realizar las evaluaciones de la efectividad de seguridad de la información

La gráfica siguiente muestra que:

- El 35% de las empresas evaluadas no posee indicadores formales de la efectividad de la seguridad.
- Los controles técnicos son la base de las empresas que sí cuentan con indicadores formales de la efectividad en seguridad.

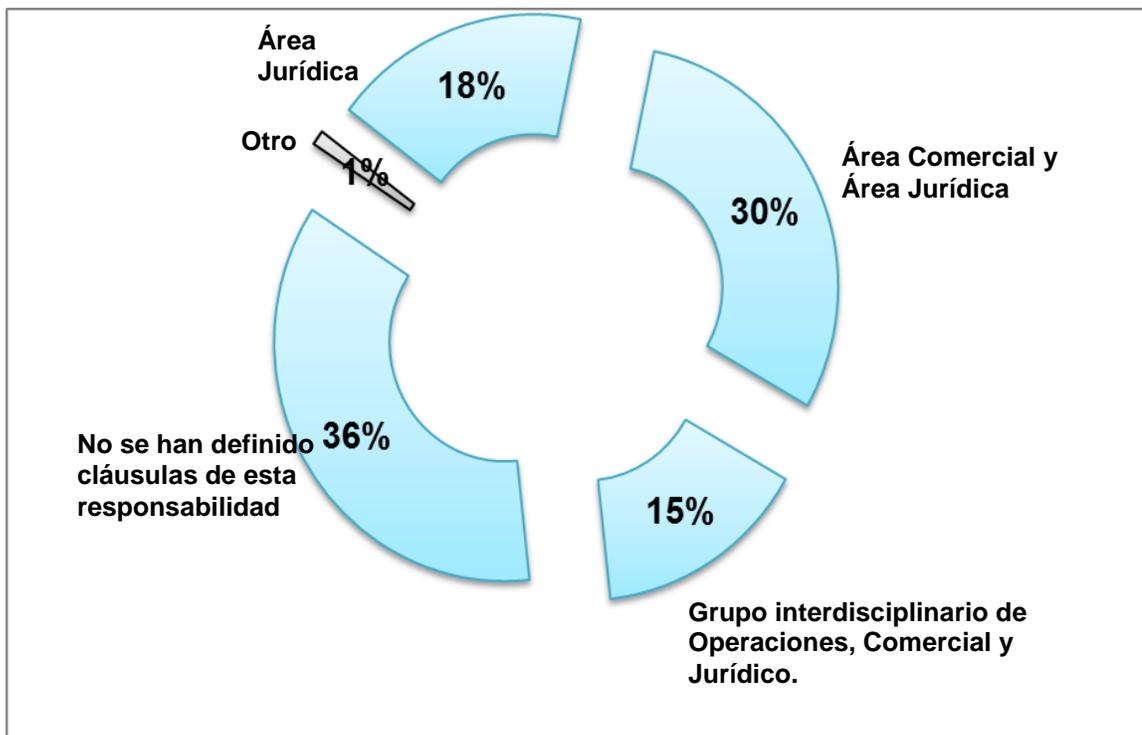


El porcentaje de organizaciones que no tiene una métrica formal de la efectividad en la seguridad de la información (35%), indica que no se cuenta con elementos de mejora continua y aprendizaje sobre las desviaciones de la operación de seguridad. Ahora bien, de acuerdo con el Artículo 82 Fracción V del Reglamento de la Ley, es necesaria una métrica formal para el esquema de autorregulación en la seguridad de la información.

III.1.5 Área que define los acuerdos contractuales de sus clientes/proveedores sobre la responsabilidad del procesamiento e intercambio de la información y datos personales

Las respuestas de las empresas evaluadas sobre este tema indican lo siguiente:

- 36 empresas de cada 100 no han definido cláusulas de esta responsabilidad.
- Para el 48% de las empresas, esta responsabilidad está a cargo del área jurídica (18%) o del área jurídico-comercial (30%).
- Solo el 15% de las empresas evaluadas definen como responsable a un área interdisciplinaria (operaciones, comercial y jurídica).
- Únicamente el 1% de las empresas manifestó que los acuerdos contractuales de sus clientes/proveedores está a cargo del área de sistemas y el área jurídica.



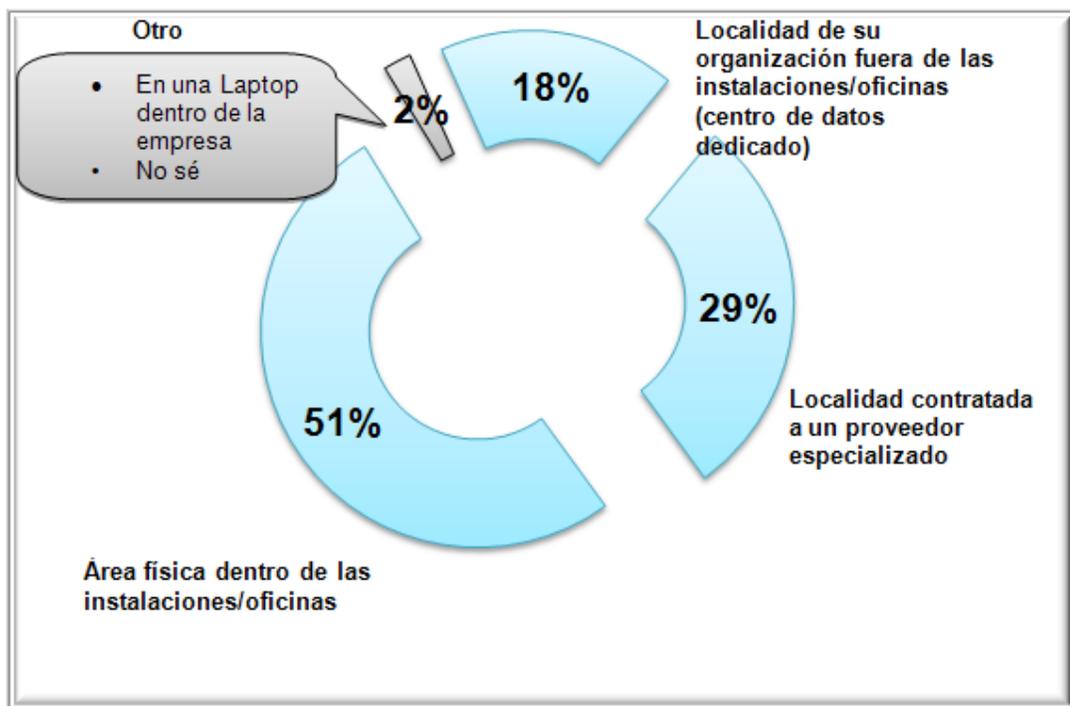
Los resultados de esta pregunta muestran que no se han vinculado de forma completa los acuerdos comerciales/legales/contractuales con el esquema de operación de TI. Este último es el que entrega los servicios a los clientes.

III.2 Seguridad de los Activos Informáticos

III.2.1 Ubicación de la infraestructura tecnológica que soporta el procesamiento de aplicaciones, información y datos personales de la organización

Las respuestas obtenidas de las empresas evaluadas sobre la ubicación de la infraestructura tecnológica con la que cuentan, permite conocer que:

- Más del 50% de las empresas tiene la infraestructura tecnológica dentro de sus instalaciones u oficinas.
- El 29% contrata una localidad a un proveedor especializado.
- El 18% de las empresas posee un centro de datos dedicado.
- El 2% cuenta con solo una laptop para procesamiento de aplicaciones, información y datos personales de la organización, o bien, desconoce el lugar donde se encuentra la infraestructura para llevar a cabo dicho procesamiento.

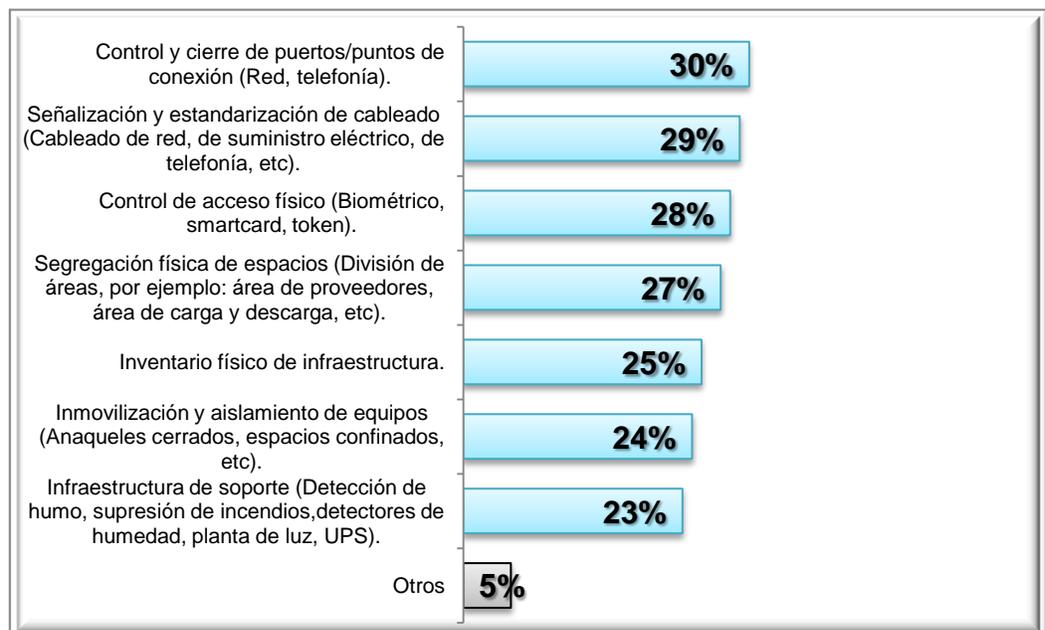


En el caso de aquellas organizaciones que han contratado instalaciones con proveedores especializados, debe considerarse la incorporación de cláusulas legales de servicios de TI relativas a seguridad de la información y datos personales. De esta forma se especificará las responsabilidades de cada una de las partes ante una brecha o vulneración de la seguridad.

III.2.2 Medidas de seguridad que deben implementarse en las instalaciones donde reside la infraestructura de procesamiento de aplicaciones, información y datos personales

La siguiente gráfica muestra que:

- El 30% de las empresas evaluadas considera el control y cierre de puertos como las principales medidas de seguridad.
- Más del 25% de las empresas cuentan con:
 - Señalización y estandarización de cableado
 - Control de acceso físico
 - Segregación física de espacios
- El 25% lleva un inventario físico de infraestructura.
- El 24% lleva a cabo la inmovilización y aislamiento de equipos.
- El 23% cuenta con infraestructura de soporte: detección de humo, supresión de incendios, detectores de humedad, planta de luz, UPS, etc.).
- Solo el 5% no cuenta con medidas de seguridad en sus instalaciones. En algunos casos son implantadas por su proveedor.



El enfoque de aseguramiento de la infraestructura tecnológica es una práctica aceptada por la industria de servicios de TI, que se ha ido fortaleciendo con mecanismos de control. Esta perspectiva podría evolucionar hacia una gestión de seguridad y privacidad.

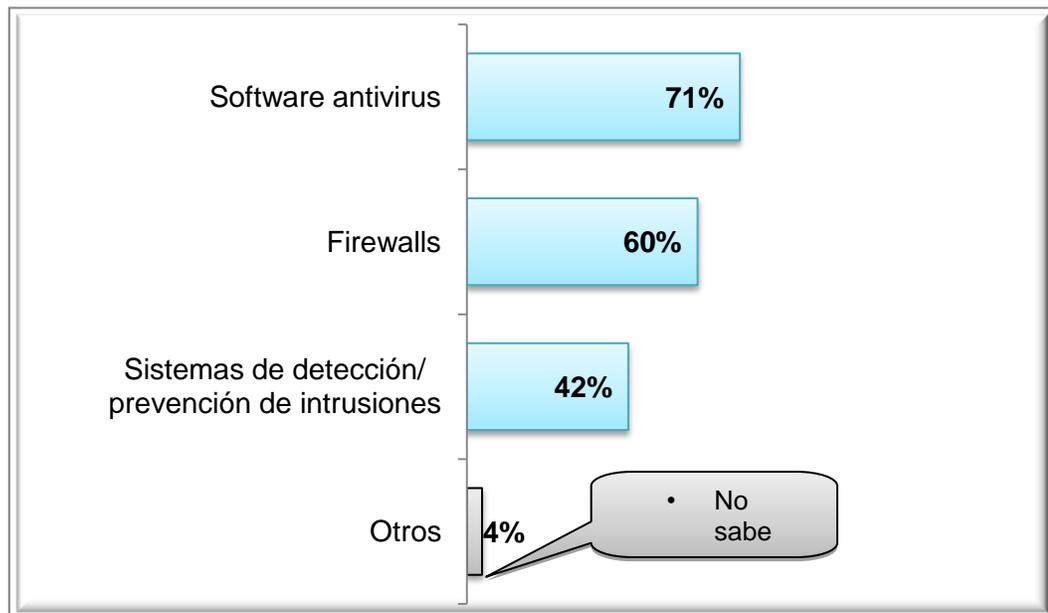
III.2.3 Mecanismos de seguridad implementados para la protección de información y datos personales

En esta sección se dividieron los mecanismos de seguridad en tres sub-secciones: redes y comunicaciones, controles de acceso y procesamiento en las aplicaciones.

III.2.3.1 Redes y Comunicaciones

Las empresas respondieron que lo que más utilizan en sistemas de redes y comunicaciones son software antivirus (71%), uso de firewalls (60%) y sistemas de detección/prevenición de intrusiones (42%). Solo el 4% de los encuestados dijo que desconoce el tipo de mecanismo de seguridad que se lleva a cabo dentro de su organización.

REDES Y COMUNICACIONES

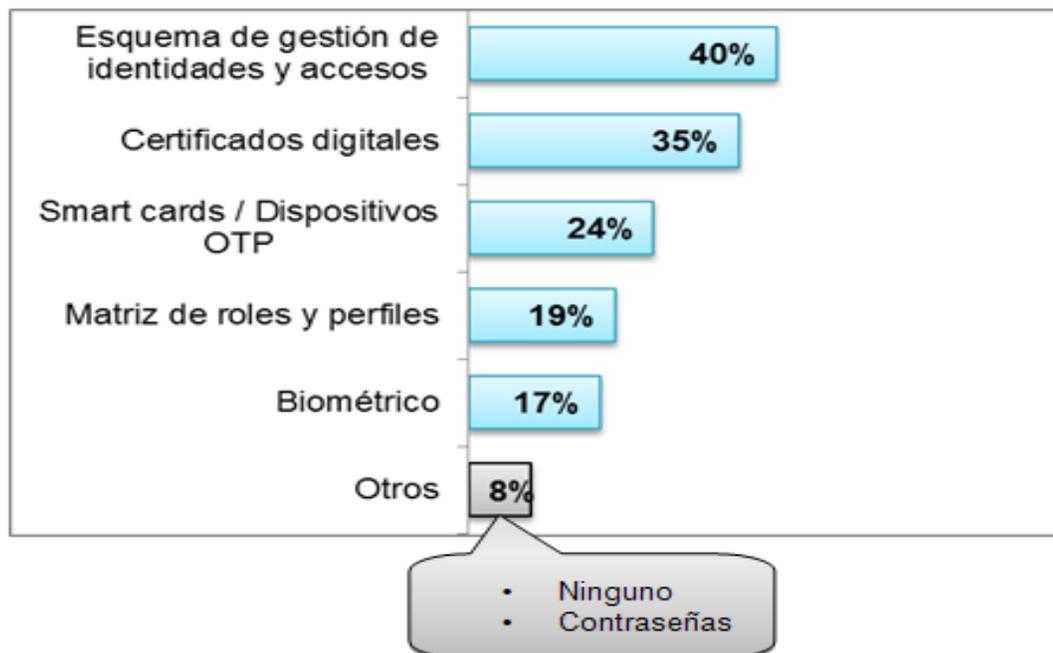


III.2.3.2 Controles de acceso

En lo referente a los controles de acceso implementados por las empresas evaluadas, se detecto lo siguiente:

- El 40% de dichas empresas utilizan esquemas de gestión de identidades y accesos.
- El 35% hace uso de certificados digitales.
- El 24% usa Smart cards y/o dispositivos OTP.
- El 19% cuenta con matrices de roles y perfiles.
- El 17% ha desarrollado un control de acceso biométrico.
- El 8% solo cuenta con contraseñas o no tiene ningún tipo de control de acceso.

CONTROLES DE ACCESO

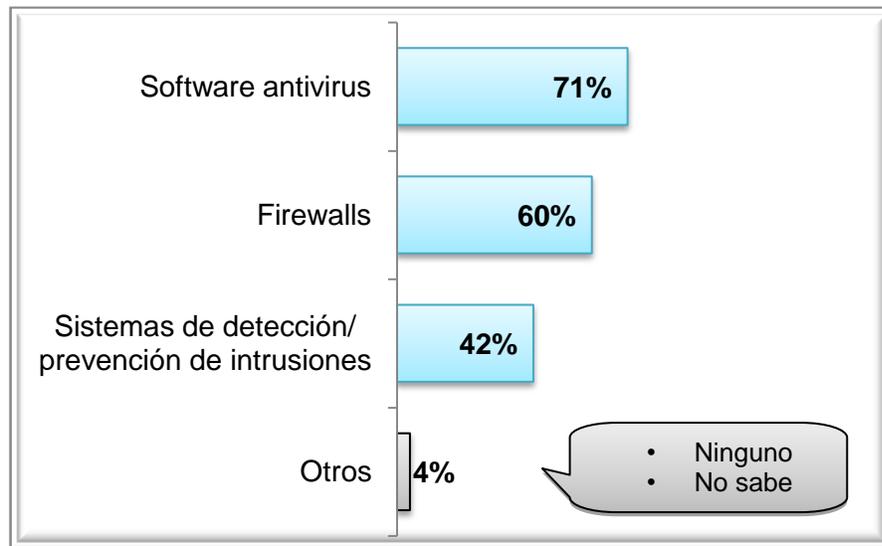


III.2.3.3 Procesamiento en las aplicaciones

Los mecanismos de seguridad implementados en el procesamiento en las aplicaciones, son los siguientes:

- El 71% de las empresas utiliza software antivirus.
- El 60% utiliza firewalls.
- El 42% cuenta con sistemas de detección/prevención de intrusiones.
- Únicamente el 4% no cuenta con ningún mecanismo de seguridad implantado o desconoce si lo tiene.

PROCESAMIENTO EN LAS APLICACIONES



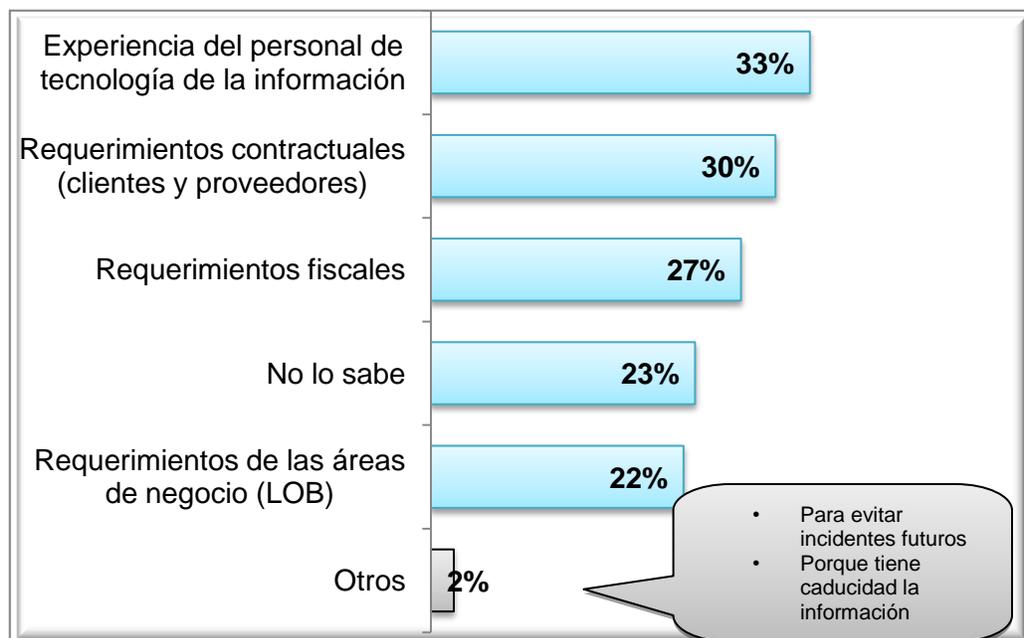
El análisis en conjunto de las tres gráficas anteriores arroja la siguiente información: hay sin duda esfuerzos puntuales en asegurar la infraestructura tecnológica a partir de mecanismos de control generalmente aceptados por la industria, con capacidades de restricción y detección de amenazas conocidas.

El esfuerzo de las organizaciones sobre el tema de seguridad de la información no implica el cumplimiento de la LFPDPPP. Por consiguiente, debe ser imperativo capitalizar el esfuerzo para definir iniciativas que complementen la base de controles con una alineación gradual a los requerimientos de privacidad.

III.2.4 Motivos por los que la organización llega a realizar prácticas de respaldo, retención y destrucción de información y datos personales

Al respecto, se puede observar lo siguiente:

- El 33% lleva a cabo estas prácticas tomando como base la experiencia del personal de tecnología de la información.
- El 30% lo hace derivado de requerimientos contractuales de clientes y proveedores.
- El 27% obedece a requerimientos fiscales.
- El 23% desconoce los motivos.
- El 22% las lleva a cabo debido a requerimientos de las áreas de negocio (LOB).
- El 2% las realiza ya sea para evitar incidentes futuros o porque la información tiene caducidad.



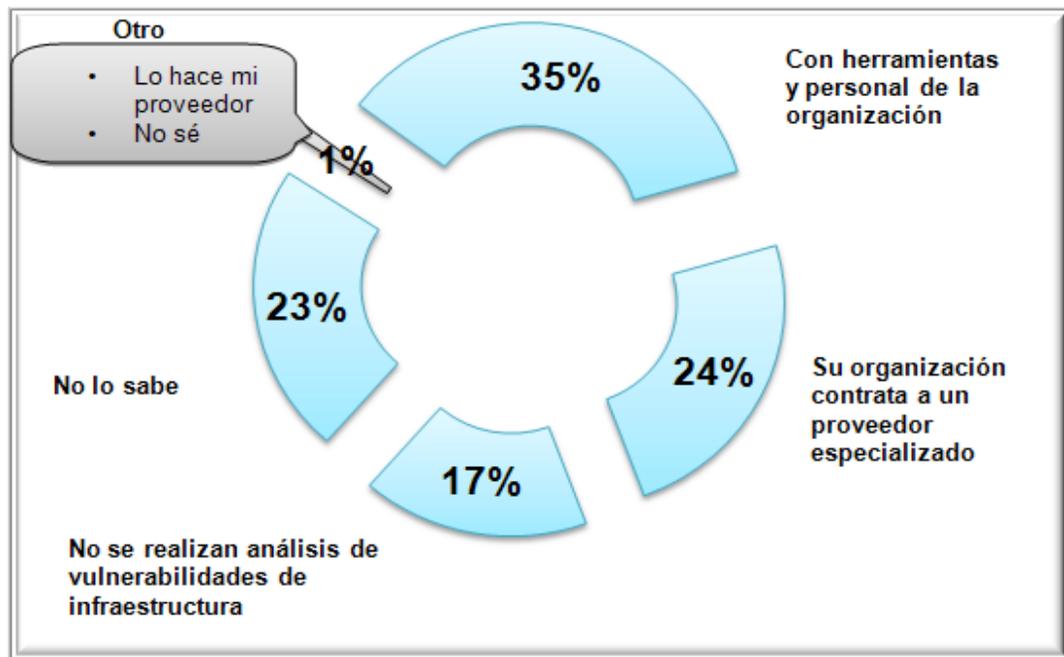
Las prácticas relativas al respaldo, restauración y eventual supresión de la información basadas en la experiencia del personal de tecnologías de la información, denotan una falta de alineación de la función de TI y seguridad de la información con los requerimientos del negocio, clientes y partes interesadas. También denota una carencia de los mecanismos de colaboración entre las diferentes áreas de responsabilidad del negocio.

Esta situación podría generar conflictos respecto a la disponibilidad y resguardo de la información y los datos personales dentro de la organización, así como incumplimiento con lo establecido en la Ley y su Reglamento sobre disponibilidad de los mismos.

III.2.5 Forma en la que las organizaciones ejecutan los análisis de vulnerabilidades de la infraestructura

Las empresas evaluadas ejecutan sus análisis de vulnerabilidades de la infraestructura de la siguiente forma:

- 35% lo hace mediante herramientas y personal de su propia organización.
- 24% contrata a un proveedor especializado.
- 23% no tiene conocimiento al respecto.
- 17% no realiza análisis de vulnerabilidades de infraestructura.
- 1% contestó que no sabe o lo hace su proveedor.

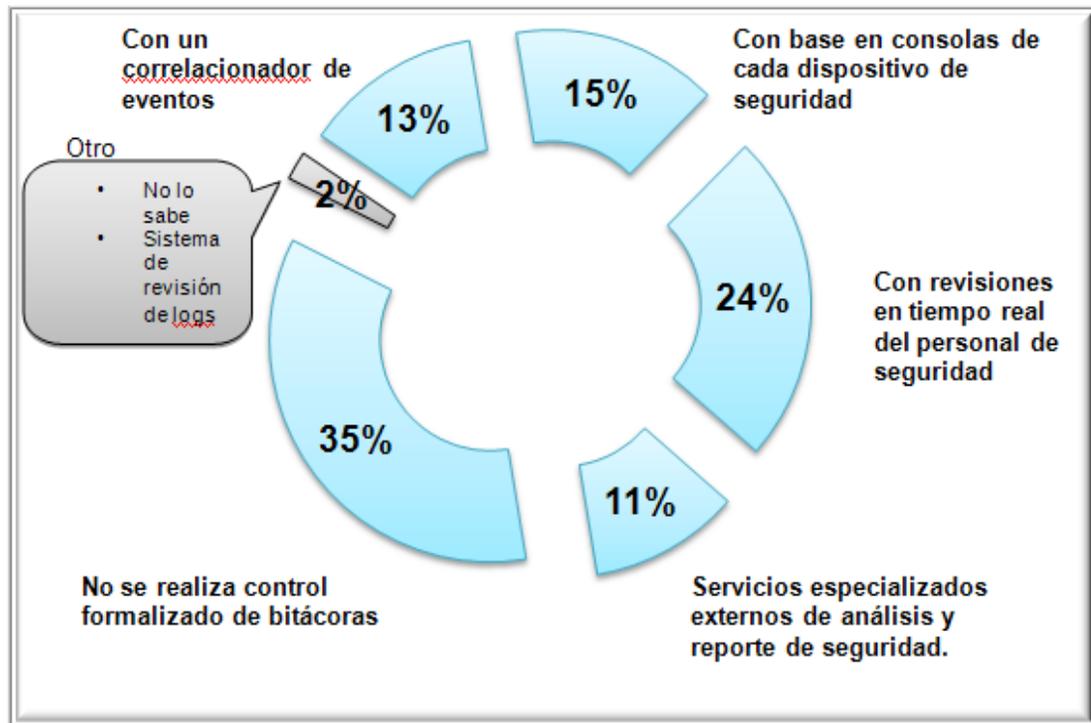


El análisis de vulnerabilidades técnicas es una práctica adoptada por las empresas del sector de servicios de TI, para ayudar en la determinación del nivel de seguridad y principio de remediación de fallas en la infraestructura.

III.2.6 Forma en que realizan la revisión y control de bitácoras de actividades (logs) de la infraestructura de procesamiento de aplicaciones, información y datos personales

En este tema se obtuvieron los siguientes resultados:

- 35% no realiza un control formalizado de bitácoras.
- 24% de las empresas encuestadas realizan revisiones en tiempo real del personal de seguridad.
- 15% lleva a cabo la revisión y control de bitácoras de actividades de la infraestructura a través de consolas de cada dispositivo de seguridad.
- 13% cuenta con un correlacionador de eventos.
- 11% lo hace a través de servicios especializados externos de análisis y reporte de seguridad.
- 2% tiene un sistema de revisión de logs o desconoce lo referente a este tema.

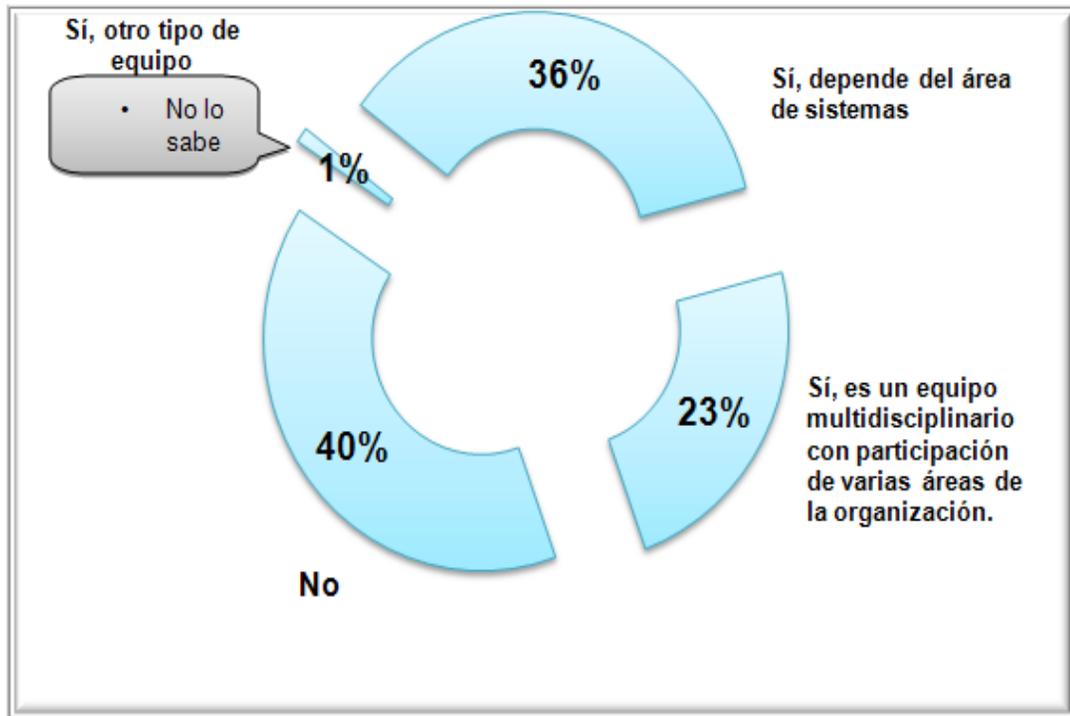


En términos del cumplimiento de la LFPDPPP, se puede inferir que el estado actual de la gestión de bitácoras de la infraestructura tecnológica y de seguridad, imposibilitaría a una organización soportar un proceso legal para proporcionar evidencias jurídicas.

III.2.7 Equipo de respuesta a incidentes de seguridad

En este tópico se puede observar que:

- El 40% no cuenta con un equipo de respuesta a incidentes de seguridad.
- El 36% contestó que sí cuenta con un equipo de esta naturaleza y que éste depende del área de sistemas.
- El 23% respondió que sí tiene un equipo de respuesta a incidentes de seguridad dentro de su empresa y que es un equipo multidisciplinario con participación de varias áreas de la organización.
- El 1% respondió que cuenta con otro tipo de equipo, sin embargo, no fue específico o no tenía conocimiento al respecto.



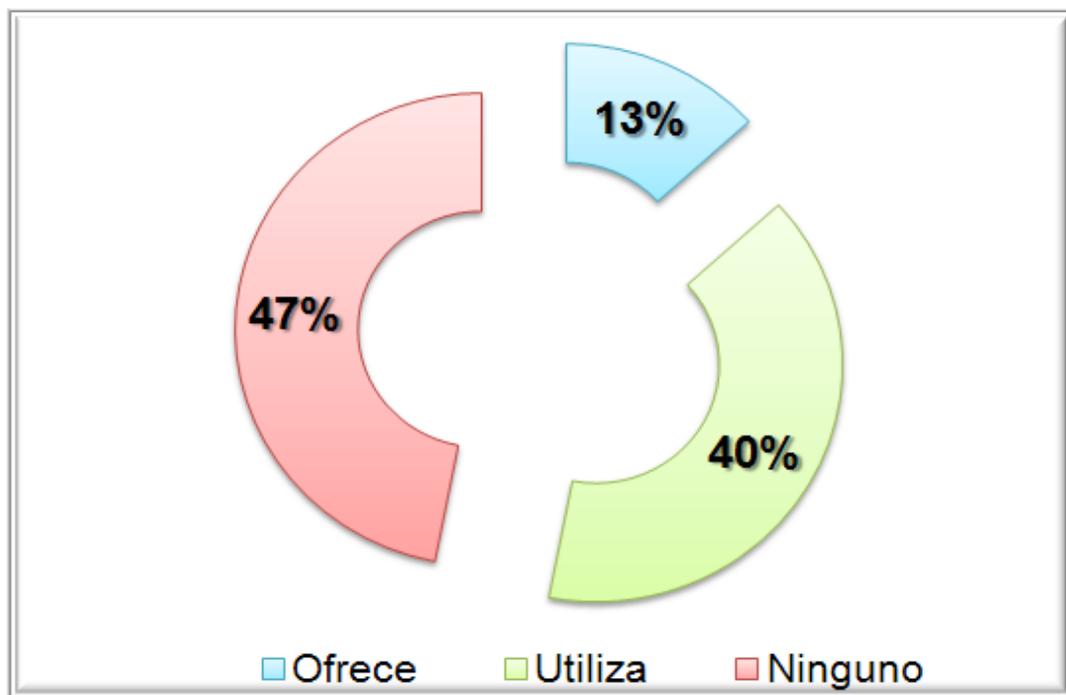
La evaluación de este rubro de control, permite observar que más del 50% de las organizaciones cuenta con un equipo de respuesta a incidentes de seguridad. Es necesario no obstante que se involucren las áreas legales y la Alta Dirección.

III.3 Tratamiento de datos en el denominado Cómputo en la Nube

III.3.1 Servicio de Cómputo en la Nube

Esta gráfica muestra lo siguiente:

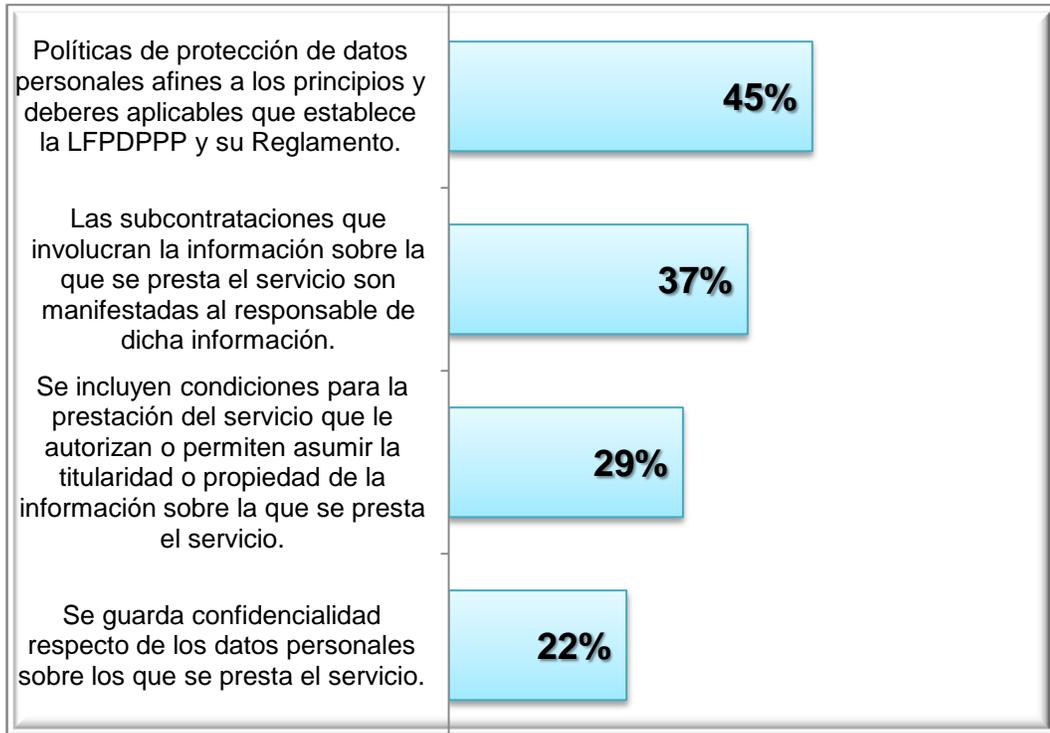
- 53 de cada 100 empresas ofrecen o utilizan servicios de cómputo en la nube.
- El 47% de las empresas no ofrecen ni utilizan este tipo de servicios.



III.3.2 Aspectos contemplados en las empresas que ofrecen servicios de Cómputo en la Nube

Aquí observamos que:

- El 45% de las empresas que ofrecen este tipo de servicios, sí contemplan las políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LFPDPPP y su Reglamento.
- El 37% de las empresas respondió que las subcontrataciones que involucran la información sobre la que se presta el servicio, son dadas a conocer al responsable de dicha información.
- El 29% de las empresas contestó que sí incluyen condiciones para la prestación del servicio, que le autorizan o permiten asumir la titularidad o propiedad de la información sobre la que se presta el servicio, cuando esto no debería presentarse.
- El 22% de las empresas guarda confidencialidad respecto a los datos personales sobre los que se presta el servicio.

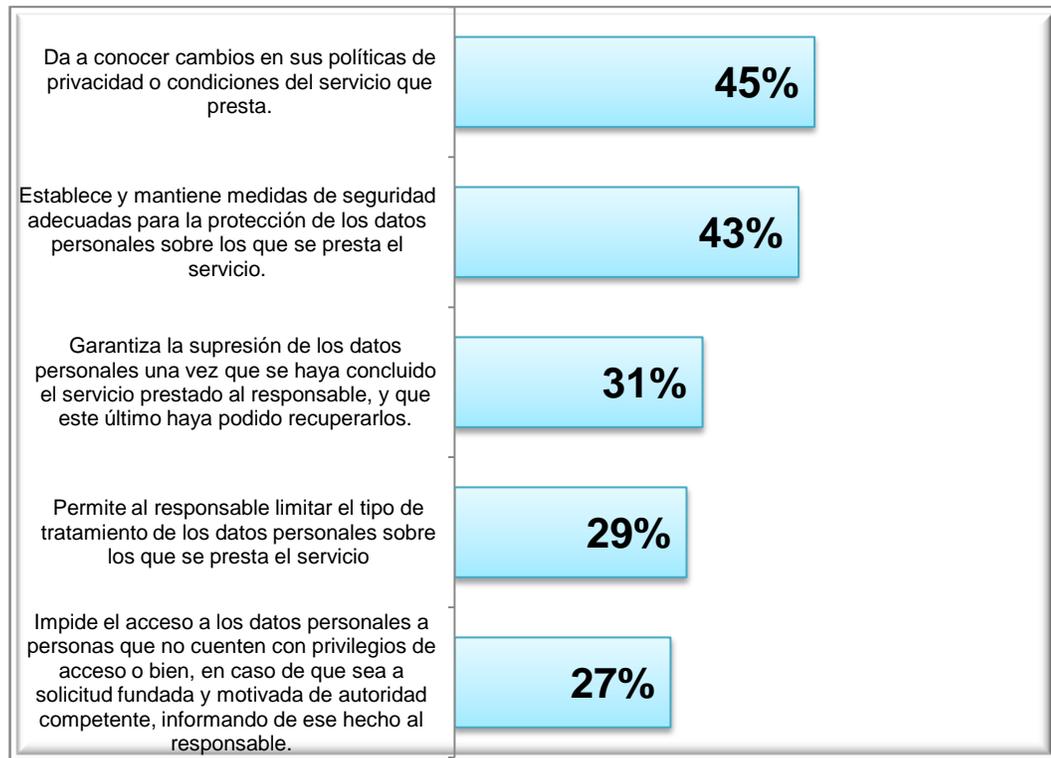


Base: 265 empresas que ofrecen servicios de cómputo en la nube.

III.3.3 Mecanismos implantados en las empresas cuando ofrecen servicios de Cómputo en la Nube

Esta gráfica muestra que:

- El 45% de las empresas da a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.
- El 43% de las organizaciones establece y mantiene medidas de seguridad adecuadas para la protección de los datos personales sobre los que se presta el servicio.
- El 31% de ellas garantiza la supresión de los datos personales una vez que se haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos.
- El 29% de las empresas evaluadas permite al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.
- El 27% de las empresas impide el acceso de datos personales a personas que no cuenten con privilegios de acceso. Solamente se podría obtener la información con base en una solicitud fundada y motivada de autoridad competente, informando de ese hecho al responsable.

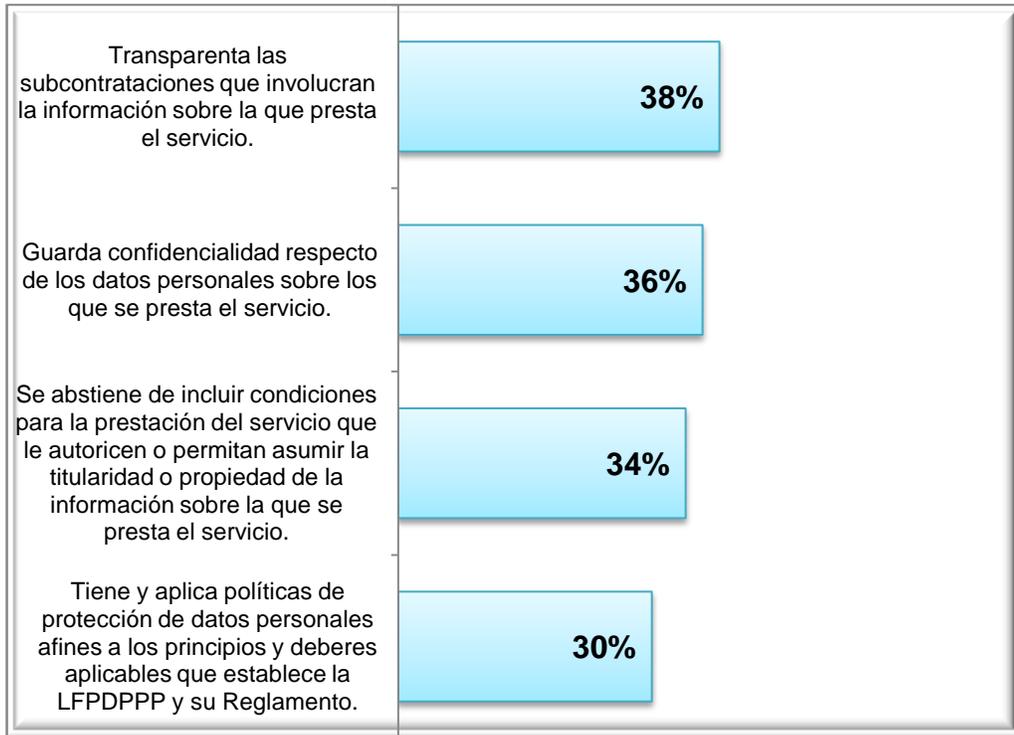


Base: 265 empresas que ofrecen servicios de cómputo en la nube.

III.3.4 Aspectos que contempla el proveedor o proveedores de las empresas encuestadas que utilizan servicios de cómputo en la nube

Con base en las 226 empresas que respondieron que utilizan servicios de cómputo en la nube, se obtuvieron los siguientes resultados:

- El 38% de las empresas que utilizan servicios de cómputo en la nube, contemplan que su proveedor transparente las subcontrataciones que involucra la información sobre el servicio prestado.
- El 36% busca que el proveedor guarde confidencialidad respecto de los datos personales sobre los que se presta el servicio.
- El 34% está consciente del hecho de que el proveedor debe abstenerse de incluir condiciones para la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que se presta el servicio.
- El 30% revisa de forma efectiva que el proveedor tenga y aplique políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LFPDPPP y su Reglamento.

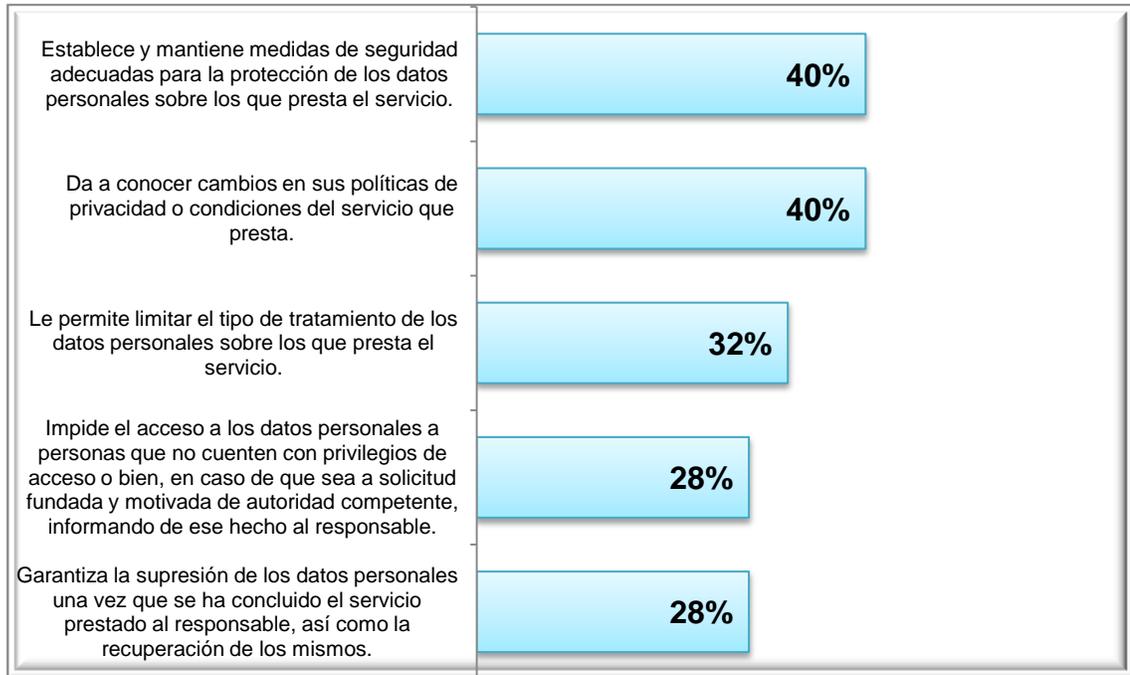


Base: 226 empresas que utilizan servicios de cómputo en la nube.

III.3.5 Mecanismos que implementa el proveedor o los proveedores de Cómputo en la Nube de las empresas encuestadas

Con base en las 226 empresas que respondieron que utilizan los servicios de algún proveedor de cómputo en la nube, se obtuvieron los siguientes resultados:

- El 40% de las empresas mencionaron que su proveedor establece y mantiene medidas de seguridad adecuadas para la protección de datos personales y les da a conocer los cambios en sus políticas de privacidad o condiciones del servicio.
- El 32% afirma que su proveedor le permite limitar el tipo de tratamiento de los datos personales sobre el que presta el servicio.
- El 28% respondió que su proveedor impide el acceso a los datos personales que no cuenten con privilegios de acceso. A no ser que sea a solicitud fundada y motivada de autoridad competente, informando del hecho al responsable.
- El 28% contestó que –una vez que ha concluido el servicio prestado– su proveedor garantiza la supresión de los datos personales y le permite la recuperación de los mismos.





Análisis de empresas de TI en materia de seguridad de datos personales para fomentar la figura de encargado de acuerdo a la LFPDPPP

RESUMEN EJECUTIVO

Julio, 2012

INTRODUCCIÓN

Después de varios años de análisis por el Congreso mexicano, fue publicada la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares** (LFPDPPP) el 5 de julio de 2010 en el Diario Oficial de la Federación y posteriormente, fue emitido por el Presidente de la República su Reglamento el 21 de diciembre de 2011; lo cual representa un importante avance en la tutela de los derechos constitucionales de privacidad y autodeterminación informativa, al tiempo que propicia un marco que da certeza jurídica a los consumidores y otras economías en el uso de las Tecnologías de la Información (TI).

Para la Secretaría de Economía no ha pasado por alto el hecho de que con ese nuevo marco legal se presentan grandes retos para difundir los derechos, obligaciones y deberes que ahora deben asumir los particulares y las empresas del sector de las TI que posean datos personales de personas físicas, con la finalidad de garantizar su tratamiento legítimo, controlado e informado.

En efecto, la LFPDPPP identifica como responsables del tratamiento de datos a las personas físicas o morales de carácter privado que deciden sobre el tratamiento de datos personales, es decir, cualquier información concerniente a una persona física identificada o identificable, y establece diversos principios fundamentales, entre ellos: el principio de responsabilidad, conforme al cual el responsable velará por el cumplimiento de los principios de protección de datos personales establecidos en la Ley, debiendo adoptar las medidas necesarias para su aplicación.

Lo anterior, aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable, para lo cual deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a

conocer al titular de los datos personales, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica. De la misma manera, la LFPDPPP también define la figura de **encargado** como la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

En este contexto se debe destacar que un importante número de empresas relacionadas con las TI actúan como encargados, por lo que es importante desarrollar programas que impulsen la implementación de normas o prácticas reconocidas internacionalmente en materia de seguridad, con la idea de que se promueva la confianza en su contratación y fomente la protección de los datos personales en la práctica organizacional.

Es por ello que con base en lo establecido en el PROSOFT 2.0 y el Componente F del Proyecto de Banco Mundial (Préstamo 7571-MX), se ha encomendado a la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) el desarrollo del proyecto "**ANÁLISIS DE EMPRESAS DE TI EN MATERIA DE SEGURIDAD DE DATOS PERSONALES PARA FOMENTAR LA FIGURA DEL ENCARGADO DE ACUERDO A LA LFPDPPP**", el cual busca –precisamente– fomentar entre el sector de TI la importancia en la implementación de las medidas de seguridad para la protección de datos personales.

En ese orden de ideas, el **objetivo general** del proyecto es: "Desarrollar las habilidades y fomentar el uso de buenas prácticas en materia de seguridad de datos personales en el sector de tecnologías de información para poder brindar certeza a las empresas que las subcontraten bajo la figura de encargado prevista en la LFPDPPP", y como **objetivos particulares** tiene los siguientes:

- a) Identificar habilidades y prácticas nacionales e internacionales en materia de seguridad de datos para empresas de TI.
- b) Valorar el grado de uso de prácticas de seguridad de datos personales actual en empresas de TI en México.
- c) Emitir recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en las empresas de TI.

Una vez concluidas las 5 fases (entregables) del Estudio, se expone ahora un **RESUMEN EJECUTIVO** que condensa los primeros hallazgos, así como las recomendaciones para una efectiva práctica de medidas de seguridad en protección de datos personales en el sector de las TI.

Entrega	Contenido	Actividades
1ª Entrega: Primer Avance	Reporte de las actividades a y b	<ol style="list-style-type: none"> a) Definir la muestra de empresas del Sector de TI (del conjunto de 2,700 unidades económicas) considerando sus características específicas y el número de empresas en diferentes estados. b) Determinar el tipo de información a requerirse a las empresas del sector de TI para el desarrollo de la herramienta de sondeo/encuesta en línea. Se recomienda al menos la siguiente información: <ol style="list-style-type: none"> a. Actividad principal de la empresa (desarrollo de Software, servicios de TI, BPO, call center, etc...) b. ¿En el ámbito de sus

Entrega	Contenido	Actividades
		<p>actividades procesa, almacena o resguarda algún tipo de datos personales?</p> <p>c. ¿Ofrece servicios de <i>outsourcing</i> para dar tratamiento de datos personales?</p> <p>d. ¿Actualmente cuenta con medidas de seguridad?</p> <p>e. ¿Cuáles son los estándares y/o normas utilizados en la implementación de medidas de seguridad internas?</p> <p>f. ¿Cuenta con algún procedimiento establecido en caso de presentarse una vulneración de seguridad?</p>
<p>2ª Entrega: Segundo Avance</p>	<p>Reporte de la actividad c</p>	<p>c) Identificar mejores prácticas en materia de seguridad de datos personales así como los requerimientos del marco normativo previsto en la LFPDPPP.</p>
<p>3ª Entrega: Tercer Avance</p>	<p>Resultados y documentación vinculada a la actividad d</p>	<p>d) Ejecutar la encuesta a la muestra definida de empresas del sector de TI.</p>
<p>4ª Entrega: Cuarto Avance</p>	<p>Reporte sobre actividad e</p>	<p>e) Realizar un análisis de la información obtenida, de la cual se proyecte un esquema estadístico descriptivo sobre la</p>

Entrega	Contenido	Actividades
		existencia, tipo, práctica, efectividad y problemas en la implementación de las medidas de seguridad para la protección de datos personales.
5ª Entrega: Quinto Avance	Reporte de actividad f y documento final	f) Elaborar recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en el sector de tecnologías de información para dar cumplimiento a la LFPDPPP.

I. ÁMBITO DEL ESTUDIO (Universo de Empresas del Sector TI y Encuesta-Sondeo).

En este apartado se resume el resultado de los entregables (avances) 1º, 3º y 4º, toda vez que están estrechamente vinculados entre sí para determinar el universo de empresas que debían ser analizadas a fin de determinar su tipo de actividad, qué tipo de datos procesan, cuáles medidas de seguridad aplican, etc., todo ello mediante una encuesta-sondeo en línea.

I.1 Muestra de empresas del sector TI. Con base en la metodología establecida, la primera parte del estudio comprendió actividades tendientes a definir la muestra de empresas del Sector de TI (del conjunto de 2,700 unidades económicas) considerando sus características específicas y el número de empresas en diferentes estados de la República; así como determinar el tipo de información a requerirse a las empresas del sector de TI para el desarrollo de la herramienta de sondeo-encuesta en línea.

En primer lugar se consideraron como empresas del sector de TI a todas aquellas que realizan alguna de las siguientes actividades económicas:

- a) Desarrollo de software empaquetado
- b) Desarrollo de software de sistema y herramientas para desarrollo de software aplicativo
- c) Desarrollo de software aplicativo
- d) Servicios de consultoría de software
- e) Servicios de análisis de sistemas computacionales
- f) Servicios de diseño de sistemas computacionales
- g) Servicios de programación de sistemas computacionales
- h) Servicios de procesamiento de datos
- i) Servicios de diseño, desarrollo y administración de bases de datos
- j) Servicios de implantación y pruebas de sistemas computacionales
- k) Servicios de integración de sistemas computacionales
- l) Servicios de procesamiento de datos
- m) Servicios de seguridad de sistemas computacionales y procesamiento de datos
- n) Servicios de análisis y gestión de riesgos de sistemas computacionales y procesamiento de datos
- o) Procesos de negocio basados en el uso de sistemas computacionales y comunicaciones
- p) Servicios de valor agregado de análisis, diseño, desarrollo, administración, mantenimiento, pruebas, seguridad, implantación, mantenimiento y soporte de sistemas computacionales, procesamiento de datos y procesos de negocio
- q) Servicios de capacitación, consultoría y evaluación para el mejoramiento de la capacidad humana, aseguramiento de la calidad y de procesos de las empresas del Sector de TI
- r) Servicios de administración de procesos de negocio basados en tecnologías de información que incluyen entre otros centros de

llamado, centros de contacto, administración de nóminas, carteras, cobranza, líneas de producción, entre otros.

- s) Desarrollo de software embebido (embedded software)
- t) Medios interactivos basados en tecnologías de información:
 - I. Desarrollo o creación de entretenimiento interactivo
 - II. Servicios especializados de diseño
 - III. Animación
 - IV. Tecnologías de compresión digital
 - V. Efectos visuales
 - VI. Televisión interactiva, y
- u) Cualquiera otra tecnología que el Consejo Directivo determine.

Tomando como base las actividades económicas mencionadas en las Reglas de Operación del PROSOFT 2.0 para el año 2011, se consideró un universo de 12,200 empresas para determinar la muestra que representara a dicho sector a fin de llevar a cabo una encuesta/sondeo en línea.

El diseño muestral aleatorio probabilístico consideró una muestra base de 530 empresas encuestadas a nivel nacional que, gracias a la participación interesada, permitió que ese número se incrementara a 564 empresas. El nivel de confianza de esta encuesta-sondeo en línea fue del 95%.

I.2 Cuestionario para la Encuesta-Sondeo. Para la encuesta-sondeo se elaboró un cuestionario integrado por 22 preguntas, que a su vez se dividieron en cinco secciones principales:

Introducción. En esta sección se da a conocer de manera breve el programa que el Gobierno Federal a través de la Secretaría de Economía impulsa para promover el crecimiento del sector de servicios de TI, teniendo como uno de sus objetivos particulares el fortalecimiento institucional y mejora del marco legal regulatorio y de políticas

sectoriales. Asimismo, se utilizó este apartado para dar a conocer y/o reforzar entre las empresas participantes el contenido de la LFPDPPP con relación al tratamiento de datos personales así como la figura de encargado.

Clasificación. En esta sección se buscó agrupar a las diferentes empresas que ofrecen servicios de TI en la industria, para las cuales la aplicación de la LFPDPPP es relevante, de acuerdo a la naturaleza de operación, misión, visión y valores. Por un lado, se realizó una estratificación del personal participante, para garantizar que la apreciación de la problemática considere las implicaciones de negocio y del ambiente tecnológico. Asimismo, se llevó a cabo la identificación del número de empleados de las empresas y el monto de sus ventas anuales. Por otro lado, se buscó detectar la existencia de empresas en el país que ofrezcan servicios de outsourcing en el tratamiento de datos personales. Una empresa con este perfil podría cubrir las características y requerimientos de la figura de encargado.

Prácticas Organizacionales de Seguridad y Privacidad de la Información. Con este grupo de preguntas se buscó determinar el tipo de prácticas de gestión y operación relativas a la seguridad y privacidad de la información de las empresas, que en conjunto con su naturaleza operativa, puedan ayudar a determinar las áreas de oportunidad en las mismas de cara al cumplimiento de la LFPDPPP.

Gestión de la Seguridad y Privacidad de la Información, el cual abarcó como temas principales los procesos, roles y responsabilidades, así como la seguridad de los activos informáticos. El objetivo principal de esta sección es determinar la forma en cómo las organizaciones han asignado las responsabilidades de seguridad de la información, así como los mecanismos de control

técnicos, operativos y de proceso encaminados a lograr el nivel de seguridad y privacidad que la operación requiere. A través de estos controles será posible identificar las medidas de seguridad administrativas, técnicas y físicas con las que las organizaciones cuentan.

Tratamiento de Datos en el denominado Cómputo en la Nube. En esta sección se ha buscado identificar los mecanismos de control que las organizaciones han implementado actualmente para la entrega y uso de servicios en un sistema computacional de esta naturaleza. De esta manera se podrá determinar si la industria está preparada para el cumplimiento de la LFPDPPP, manteniendo los niveles de privacidad de las personas sobre su información.

I.3 Ejecución de la Encuesta-Sondeo en línea. A partir de la aprobación del cuestionario, el día 9 de abril de 2012 se lanzó la invitación electrónica a las 12,200 empresas que se encontraban en la base de datos de la AMITI, la CANIETI, la AMIPCI y de la empresa encuestadora.

El periodo original considerado era de cuatro semanas, es decir, del 9 de abril al 4 de mayo de 2012, sin embargo, con el fin de alcanzar la muestra que representaría a las empresas objetivo de dicha encuesta-sondeo, se amplió dicho periodo, por lo que la encuesta en línea permaneció del 9 de abril al 31 de mayo, es decir, aproximadamente ocho semanas.

La invitación electrónica fue abierta por 4,373 empresas, de las cuales participaron 1,385 y completaron el cuestionario únicamente 564.

I.4 Análisis de la Información Obtenida en la Encuesta-Sondeo.

Sobre las actividades económicas que forman el sector de las TI, se detectó que menos del 5% de las empresas encuestadas proporcionan algún tipo de outsourcing.

Si se considera el tamaño de la empresa se observa que alrededor del 80% de las empresas encuestadas se encuentran en la clasificación de micro y pequeña empresa.

Ahora bien, respecto al procesamiento, almacenamiento o resguardo de datos personales –ya sean internos o de clientes– se presentaron los siguientes rangos:

- Del 41% al 45% de las empresas evaluadas procesan datos personales.
- Del 30% al 31% almacenan datos personales.
- Solo el 25% resguarda este tipo de datos.

Prácticas organizacionales de privacidad y seguridad de la información. Es importante señalar que el 26% de las empresas evaluadas desconocen qué regulaciones y/o marcos referenciales se utilizan para implementar la seguridad de la información. Únicamente el 39% señaló a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares como mecanismo de regulación.

Tipo, Existencia y Práctica de Medidas de seguridad. El 27% de las empresas cuenta con una política central y estándares auxiliares de seguridad de información; el 22% considera como lo más relevante la seguridad de recursos humanos; el 15% se basa en los objetivos de control de cumplimiento; y el 11% considera la gestión de incidentes de seguridad de la información como lo más importante.

El 55% de las empresas encuestadas no cuenta con un Comité de Seguridad que vigile el cumplimiento, monitoreo y mejoramiento de las políticas establecidas.

El 36% de las empresas no ha definido ni acuerdos contractuales ni cláusulas con sus clientes o proveedores sobre la responsabilidad del procesamiento e intercambio de información y datos personales.

El 35% de las empresas no poseen indicadores formales de evaluación de la efectividad de la seguridad de la información. Ahora bien, aquellas empresas que sí cuentan con dichos mecanismos realizan reportes de incidentes, evaluaciones de controles generales de TI, reportes de soluciones de vulnerabilidades técnicas realizadas y/o categorización de eventos identificados por la infraestructura.

Identificación y clasificación de la información. En este rubro solo el 29% de las empresas encuestadas lleva a cabo una identificación y clasificación de la información como componente de su marco normativo de seguridad. Además, el 29% señaló que el área responsable de definir y administrar los criterios de clasificación de la información es la Dirección General; el 26% dijo que la responsable de dicha clasificación es el área de seguridad; y sólo el 8% de las empresas asigna dicha actividad al área de datos personales.

Cabe mencionar que en el 27% de los casos no existen criterios formales de clasificación.

Concienciación, formación y capacitación del personal en materia de protección de datos personales. El resultado arrojado en esta encuesta muestra que el 33% lleva a cabo la concienciación de su personal a través de correo electrónico, folletos, medios impresos, etc.

El 53% manifestó que la formación y capacitación se realiza por lo menos una vez al año en su organización. Sin embargo, es importante señalar

que el 35% de las empresas no recuerda cuándo recibió la última capacitación sobre seguridad y privacidad de la información.

Medidas de seguridad físicas. Las medidas de seguridad físicas han sido definidas por las empresas de acuerdo a los siguientes objetivos de control:

- Seguridad física y de instalaciones (25%)
- Inventario de activos de la información (17%) o gestión de activos

Medidas de Seguridad Técnicas. Las empresas encuestadas han definido las medidas de seguridad técnicas dentro de los siguientes objetivos de control:

- Operaciones de cómputo (22%)
- Control de acceso lógico (20%)
- Seguridad de desarrollo de aplicaciones (16%)
- Operación de telecomunicaciones (13%)

Problemas en la implantación de las medidas de seguridad para la protección de datos personales. Para que las empresas del sector de servicios de TI logren adoptar mecanismos de privacidad de datos personales en sus esquemas de seguridad de la información –que cumplan con la LFPDPPP, agregando valor a sus procesos de negocio— deberán atenderse las siguientes causas raíz de las brechas y carencias observadas en los resultados de la encuesta-sondeo:

- El 80% de las empresas del sector de TI se encuentran clasificadas como micro y pequeña empresa, en consecuencia, éstas no han conseguido la capacidad para implementar las medidas de seguridad para protección de datos personales. La carencia se debe principalmente a la falta de recursos económicos y humanos.

- La función de seguridad de la información ha sido concebida y asignada de forma permanente a un contexto tecnológico, que se desenvuelve a través de esfuerzos aislados o puntuales de aseguramiento, basados en herramientas específicas de seguridad. En muchos de estos casos, la premisa principal es satisfacer algún requerimiento de auditoría o evaluación, o bien, resolver problemas acotados.
- Se reconoce una falta de experiencia de la industria de servicios de TI para la asimilación de las regulaciones de privacidad sobre el esquema de seguridad de la información, así como para reconocer las responsabilidades de cada actor especificado en la LFPDPPP y su Reglamento.
- El enfoque de protección que se ha desarrollado a lo largo del tiempo se basa en la infraestructura tecnológica, y no en la sensibilidad, criticidad e importancia de la información para el negocio, y mucho menos con un enfoque de protección de datos personales.
- Se asignan presupuestos y recursos limitados para implantar las iniciativas de seguridad de la información y privacidad de datos personales. Esta carencia se debe a una competencia con otras prioridades de la organización; prioridades que se desprenden recurrentemente del presupuesto asignado a la función de TI. De ahí, pues, que no se logre desarrollar alternativas de seguridad y privacidad en función de los requerimientos organizacionales.
- Las restricciones de recursos han dado como resultado que la mayoría de las organizaciones encuestadas no ejecuten controles fundamentales en la esfera de seguridad, por ejemplo, análisis de riesgos

y estrategia de seguridad, estrategia de capacitación y concientización en seguridad y privacidad, gestión de incidentes de seguridad o mejora continua de la seguridad de la información.

- La remediación de estas causas raíz no se encuentra en una solución única o finita, sino en un proceso permanente de la organización por incorporar los aspectos de seguridad, privacidad y cumplimiento de la LFPDPPP y su Reglamento como parte de una cultura organizacional.

Tratamiento de Datos Personales en el denominado Cómputo en la Nube. La encuesta-sondeo detectó que el 53% de las empresas ofrecen o utilizan servicios de cómputo en la nube.

Se revisaron los aspectos que el Reglamento estipula en relación a las empresas que ofrecen servicios de cómputo en la nube. Y se descubrió lo siguiente: la mayoría de los proveedores desconocen o no cubren los aspectos y mecanismos que dicho Reglamento determina para garantizar la debida protección de los datos personales.

Conclusiones Generales Derivadas de la Encuesta-Sondeo. Con base en las respuestas de las empresas encuestadas sobre el tema de seguridad de información y datos personales, es posible plantear las siguientes conclusiones:

- El porcentaje de participación de empresas micro y pequeña, puede indicar que existe una preocupación genuina por los alcances y requerimientos de seguridad y privacidad para la industria por los esfuerzos a desarrollar en su cumplimiento.
- En el caso de la participación de empresas micro por su nivel de ingreso, es importante no restringir el presupuesto para la implantación de mecanismos de control que ayuden a cumplir con las disposiciones de la Ley. El compromiso de privacidad y seguridad de la información de los datos personales no atiende al

tamaño del negocio, sino al tipo y sensibilidad de dichos datos que se manejan en sus procesos.

- Se identifican a los servicios de outsourcing de tratamiento de datos personales como un área de oportunidad de negocios para las empresas del sector de TI en México, ya que actualmente solo el 31% lo ofrece.
- Si bien en las empresas existe cierto entendimiento sobre algunos componentes clave para el cumplimiento de la LFPDPPP, estos aún no se están ejecutando.
- Existe una percepción en las empresas evaluadas de que el tema de seguridad de datos personales debe ser resuelto por una función de tecnología de la información (TI).
- Las organizaciones han trabajado en la implementación de controles técnicos preventivos y de detección de brechas de seguridad, pero no en un contexto de privacidad de datos personales.
- La implementación de los controles actuales está basada en gran parte en la experiencia de los responsables de la función de TI.
- La mayoría del presupuesto para esfuerzos de iniciativas de seguridad y privacidad están derivados de los presupuestos de TI.
- La efectividad de las funciones de seguridad y privacidad no están siendo monitoreadas, evaluadas y supervisadas en ningún sentido.
- A partir de algunas de las opiniones de los participantes que respondieron la encuesta-sondeo, es posible identificar que las empresas consideran que este tipo de regulaciones aplica únicamente para empresas grandes.
- Actualmente las empresas no cuentan con un equipo de respuesta de incidentes ni con una bitácora de control de actividades de la infraestructura de procesamiento, aplicaciones, información y datos personales, que permitan tener un control formalizado de estas actividades. Por lo tanto, sería complicado proporcionar evidencia

en un proceso legal relativo a brechas de seguridad y afectación de datos personales.

- Considerando la naturaleza de sus servicios y su inercia operativa, el sector de cómputo en la nube debe realizar esfuerzos en la revisión de sus contratos de adhesión, en las características de entrega de servicios y en su esquema operativo, de tal forma que se adapten a los requerimientos que el Reglamento de la LFPDPPP establece en el artículo 52.
- Es importante señalar que las empresas que no reconocen la utilidad del Análisis de Riesgos, basan sus políticas de seguridad de la información en esfuerzos puntuales de remediación de desviaciones o decisiones subjetivas de los responsables de estas funciones.
- El Artículo 20 de la LFPDPPP y los Artículos 63 al 66 de su propio Reglamento, reconocen como prioritario la gestión de incidentes de seguridad de la información. En consecuencia, otra área de oportunidad de cara al cumplimiento de la LFPDPPP, se encuentra en el bajo porcentaje de organizaciones que han trabajado en la gestión de incidentes de seguridad de la información.
- La capacitación sobre seguridad y privacidad de la información representa uno de los esfuerzos más relevantes que la industria de servicios de TI debe ejecutar. Por ello, el carácter organizacional de la privacidad de datos personales en el Reglamento de la Ley implica capacitación activa para el personal de la organización que trate datos personales.

II. IDENTIFICACIÓN DE MEJORES PRÁCTICAS

El segundo reporte de este Estudio, tuvo por objeto "Identificar mejores prácticas en materia de seguridad de datos personales así como los requerimientos del marco normativo previsto en la LFPDPPP".

Las mejores prácticas y estándares que se analizaron fueron los siguientes:

CMMI (Capability Maturity Model Integration)

- Conjunto de mejores prácticas que proporciona los elementos para tener procesos efectivos que ayudan a mejorar la eficiencia, eficacia y calidad dentro de los grupos de trabajo, proyectos y divisiones. En otras palabras, contribuye al mejoramiento de todas las áreas de una organización.
- La seguridad de la información puede ser concebida, dentro del modelo CMMI de desarrollo y de servicios, como un tipo de requerimiento. Sin embargo, el SSE-CMM (System Security Engineering Capability Maturity Model) lo establece de forma específica en sus 11 áreas de procesos de ingeniería de seguridad.

CobIT (Control Objectives for Information and Related Technology)

- Conjunto de prácticas para mejorar el manejo de la información tanto en el área financiera como en la tecnológica. Es un marco de referencia para establecer un rumbo seguro y confiable de las tecnologías de información así como una herramienta que da soporte a la alta dirección para reducir la brecha existente entre las necesidades de control, las cuestiones técnicas y los riesgos propios de un negocio.
- Dentro de los beneficios de CobIT se encuentra que los requerimientos de seguridad y privacidad serán más fácilmente identificados, y su implementación podrá ser monitoreada a través de los dominios establecidos en CobIT: Planear y Organizar (PO),

Adquirir e Implementar (AI), Entregar y Soportar (DS) y Monitorear y Evaluar (ME).

ISO 27001

- Es el estándar internacional de gestión de seguridad de la información que permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad de la información a un nivel adecuado.
- En su anexo A enumera en forma de resumen los objetivos de control y controles que desarrolló la ISO 27002:2005, con la finalidad de que sean seleccionados por las organizaciones para el desarrollo de sus Sistemas de Gestión de la Seguridad de la Información (SGSI).
- En la serie ISO 27000 están en fase de desarrollo la ISO/IEC 27017 –que consistirá en una guía de seguridad para Cloud Computing– y la ISO/IEC 27032 –que consistirá en una guía relativa a la Ciberseguridad–.
- Considerando que la ISO/IEC 27001 es el estándar internacional de seguridad de la información, encontraremos en todos los dominios el criterio de aplicabilidad en la protección de datos personales. Cabe señalar que en el dominio A.15 Cumplimiento, Objetivo de Control “cumplimiento de los requisitos legales” se encuentra –de forma específica– el control 15.1.4 relativo a la protección de datos y privacidad de la información de carácter personal.
- El ISO/IEC 27001 es el estándar en seguridad de información certificable, por lo que las empresas de TI que deseen ser

consideradas como un proveedor confiable deberán tomarlo en cuenta para su estrategia de seguridad de información.

- La ISO/IEC 27005:2011 es una norma esencial para aquellos que requieran gestionar sus riesgos de manera efectiva y, en particular, para cumplir con la gestión de la información de seguridad mediante el estándar ISO/IEC 27001.

ITIL (Information Technology Infrastructure Library)

- Conjunto de directrices (mejores prácticas) y de módulos mediante los cuales podemos establecer un mejor aprovechamiento de los recursos informáticos de una entidad u organización, desde una perspectiva de servicios. ITIL ha trazado el camino del “cómo” obtener mayor beneficio de las tecnologías de información.
- Considerando que ITIL cubre los servicios de TI en todas sus fases, los 5 libros que lo conforman contienen procedimientos útiles, que aplican para la protección de la información.

NIST (National Institute of Standards and Technology)

- Su misión consiste en promover la innovación y la competencia industrial en Estados Unidos.
- Los laboratorios NIST se centran en tres áreas focalizadas: ciencia de medición, tecnología (tecnologías de la información, ingeniería) e instalaciones de usuarios nacionales.
- Las publicaciones para la seguridad informática y la tecnología de la información son los especiales de la serie 800.

- Dentro de la serie 800, los más relevantes en el tema de seguridad y de datos personales se encuentran los siguientes:

Número de Publicación (Fecha)	Título	Contenido
NIST SP 800-12 (Octubre de 1995)	Introducción a la Seguridad Informática: El Manual NIST	Se enfoca a los controles de seguridad de acuerdo a su naturaleza, es decir, se hace una clasificación de los mismos (controles administrativos, operativos y técnicos).
NIST SP 800-14 (Septiembre de 1996)	Principios y Prácticas Generalmente Aceptadas para la Seguridad de los Sistemas Tecnológicos de la Información	Se describen los 8 principios y 14 prácticas de seguridad.
NIST SP 800-39 (Marzo de 2011)	Administración del Riesgo en la Seguridad de la Información	Proporciona a las organizaciones una guía para la administración del riesgo de la seguridad de la información estableciendo los componentes del mismo (establecer, valorar, responder y monitorear el riesgo).
NIST SP 800-122 (Abril de 2010)	Guía para la Protección de la Confidencialidad de la Información	Sugiere categorizar el nivel de impacto de la confidencialidad de la PII (Información de Identificación Personal) en bajo,

Número de Publicación (Fecha)	Título	Contenido
	de Identificación Personal	moderado y alto, y con base en el daño potencial que pudiera resultar a los titulares de la información y/o la organización si esta fuera vulnerada, utilizada o divulgada de forma inapropiada. Adicionalmente, establece que la PII debe ser protegida a través de una combinación de medidas, incluyendo salvaguardias operativas, salvaguardias específicas de privacidad y controles de seguridad.
NIST SP 800-144 (Diciembre de 2011)	Directrices en Seguridad y Privacidad en Cómputo en la Nube de tipo Público	Provee una perspectiva general de los servicios de cómputo en la nube de tipo público y los retos en seguridad y privacidad que conllevan. Asimismo, describe los modelos de uso (nube pública, nube privada, nube comunidad y nubes híbridas) y emite recomendaciones tanto en temas de seguridad y privacidad como de actividades a realizarse para la contratación de un servicio de outsourcing de cómputo en la nube.

PCI/DSS (Payment Card Industry Data Security Standard)

- Estándar internacional que establece un conjunto de requerimientos de seguridad de la información para proteger los datos de los tarjetahabientes.
- Las compañías que procesan, guardan o transmiten datos de los tarjetahabientes deben cumplir con el estándar, de no hacerlo se arriesgan a la pérdida de sus permisos para operar (pérdida de franquicias).
- La información proporcionada por los tarjetahabientes para el manejo de las tarjetas de crédito y débito es de carácter personal (datos de identificación, financieros y patrimoniales), por esta razón, cada uno de los objetivos de control y requerimientos previstos en este estándar aplican para la protección de datos personales.

España

- La Agencia Española de Protección de Datos (AEPD) es la institución encargada de cuidar y fomentar la privacidad y la protección de datos personales en España. A su vez la Península Ibérica pertenece a la Unión Europea, por lo tanto, debe ceñirse a los criterios de ésta.
- La AEPD es un ente de Derecho público con personalidad jurídica propia y plena capacidad pública y privada conforme al Real Decreto 428/1993 del 26 de marzo de 1993.
- El artículo 9 de la Ley Orgánica 15/1999 (LOPD) del 13 de diciembre de 1999 establece que tanto el responsable como el encargado del tratamiento deberán adoptar medidas de índoles

técnica y organizativas, que garanticen la seguridad de los datos de carácter personal para evitar su alteración, pérdida, tratamiento o acceso no autorizado.

- El Reglamento de desarrollo de la LOPD establece que las medidas de seguridad exigibles a las bases de datos (ficheros) y sus tratamientos se deben clasificar en tres niveles: básico, medio y alto.
- La AEPD ha emitido un documento denominado Guía de Seguridad de Datos y la cual recoge una serie de mejores prácticas en materia de protección de datos personales.
- La clasificación de los niveles de seguridad se realiza conforme a la naturaleza de la información tratada y a la necesidad de garantizar la confidencialidad y la integridad de la información.
- Las medidas de seguridad son acumulativas.
- La Guía establece un documento de seguridad, cuyo contenido está estructurado de la siguiente forma:
 - Ámbito de aplicación del documento.
 - Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos.
 - Información y obligaciones del personal.
 - Procedimientos de notificación, gestión y respuestas ante las incidencias.
 - Procedimientos de revisión.
- El Reglamento de la LOPD establece en sus artículos 96 y 110 que a partir del nivel medio de seguridad requerido, las bases de datos

deberán someterse, al menos cada dos años, a una auditoría interna o externa, de la cual se generará un informe que se entregará al responsable de la base de datos y a disposición de la AEPD o a las autoridades de control de las entidades autónomas.

- La Asociación Española de Normalización y Certificación (AENOR) ha publicado entre otras normas relacionadas a la seguridad de la información, las siguientes:
 - Desde el 28 de noviembre de 2007: ISO/IEC 27001 como UNE-ISO/IEC 27001: 2007
 - Desde el 9 de diciembre de 2009: ISO/IEC 27002 como UNE-ISO/IEC 27002: 2009

Reino Unido

- El Reino Unido a través del Data Protection Act 1998 establece que –cuando se tenga un encargado para el tratamiento de datos personales— se deberá seleccionar un encargado que provea suficientes garantías sobre sus medidas de seguridad para proteger el procesamiento que hará en nombre del responsable; se debe revisar que esas medidas de seguridad están llevándose a la práctica y deberá existir un contrato por escrito donde se establezcan las obligaciones del encargado. Existe un modelo de contrato publicado por el Comité Europeo para la Estandarización.
- La Oficina del Comisionado de Información (ICO) es una autoridad independiente en el Reino Unido, que se creó para defender los derechos de información de interés público, y para promover la apertura de los organismos públicos y la privacidad de los datos de los individuos.

- En relación a las medidas de seguridad, el DPA ha establecido lo siguiente: “Principio 7: Se deben tomar medidas técnicas y organizacionales apropiadas en contra del procesamiento sin autorización o ilegal de los datos personales así como en contra de pérdida accidental, destrucción o daño a los datos personales
- Se sugiere diseñar un modelo organizacional de seguridad, acorde con el tipo de datos personales que se poseen y acorde también con las contingencias de vulneración a la seguridad de la información.
- La ICO ha diseñado notas y códigos de buenas prácticas, que a continuación se muestran:
 - Nota de buenas prácticas de datos personales. Seguridad de Información Personal (Data Protection Good Practice Note Security of Personal Information)
 - Nota de buenas prácticas para protección de datos personales (Lista de entrenamiento para pequeñas y medianas empresas) (Data Protection Good Practice Note)
 - Código de Práctica de compartición de Datos (Data Sharing Code of Practice)
 - Código de práctica de información personal en línea (Personal information online code of practice)
 - Cómputo en la nube (Cloud computing)
- El ISF –por sus siglas en inglés, Information Security Forum— se dedica a la investigación, aclaración y solución de temas clave sobre seguridad de la información y administración de riesgo a través del desarrollo de mejores prácticas

- El Estándar de buenas prácticas 2011 contempla la perspectiva empresarial para la seguridad de la información y se divide en cuatro categorías principales:
 - Gobernanza de la seguridad
 - Requerimientos de seguridad
 - Marco de control
 - Monitoreo y mejora de la seguridad

Estados Unidos

- En el ámbito de la protección de datos personales en posesión de los particulares, Estados Unidos de Norteamérica cuenta con regulaciones en materia de privacidad y medidas de seguridad exigibles a los responsables y encargados de datos personales, tanto sectoriales como estatales.
- En el ámbito federal:
 - El Privacy Act de 1974 establece un código de prácticas justas que regulan la recolección, mantenimiento, uso y divulgación de la información de los individuos que se encuentra en los sistemas de registro de las agencias federales de los Estados Unidos.
 - El United States Code (USC) es la codificación por temas de las leyes generales y permanentes de los Estados Unidos de Norteamérica y se divide en amplios temas divididos en 50 títulos. Es publicado por la Oficina de Revisión Legislativa de la Cámara de Representantes de Estados Unidos.

- Dentro del título 15 “Comercio y Negocios” capítulo 94 del USC, se considera el tema de la privacidad de la información personal. Hace un análisis en torno a la divulgación de la información personal privada y al acceso fraudulento de la información financiera.
- En la sección 1173(d) del Health Insurance Portability and Accountability Act of 1996, “Estándares de seguridad para información de salud” se establece que la Secretaría de Servicios de Salud y Humanos, deberá adoptar estándares de seguridad que tomen en cuenta las capacidades técnicas de los sistemas de registro utilizados para mantener la información de salud; los costos de las medidas de seguridad; la necesidad de capacitación de las personas que tengan acceso a la información de salud; el valor de rastros de auditoría en sistemas computarizados de registro; y las necesidades y capacidades de pequeños proveedores del cuidado de la salud y proveedores rurales del cuidado de la salud.
- En el ámbito estatal:
 - El estado de Massachusetts cuenta con un reglamento denominado 201 CMR 17.00: Estándares para la Protección de Información Personal de los residentes de Commonwealth.
 - Los objetivos del instrumento mencionado son los siguientes: garantizar la seguridad y confidencialidad de la información de clientes de acuerdo a los estándares de la industria correspondiente; proteger la información contra amenazas o

riesgos previstos; y proteger contra el acceso no autorizado o uso de la información que pueda dar como resultado un daño o incomodidad a cualquier consumidor.

- Dentro de los Estatutos Revisados de Nevada (NRS) el capítulo 603A trata específicamente sobre la seguridad de la información personal. Aquí se establece, bajo el título de “Regulación de Prácticas de Negocio” en sus artículos NRS 603A.200 y NRS 603A.210, lo referente a destrucción de ciertos registros y medidas de seguridad, respectivamente.
- El artículo NRS 603A.215 estipula que aquellos responsables que acepten tarjetas de pago deberán cumplir con la versión actual del estándar PCI/DSS. En caso de que el responsable no realice esta práctica, tiene la obligación de no transferir información personal a través de una transmisión electrónica o sin voz diferente al fax, a menos que se cifre⁹¹ la información con el fin de garantizar la seguridad de la transmisión electrónica.
- Cabe señalar que otros estados como California, Hawái, Illinois y Vermont, por mencionar algunos, cuentan con legislación en materia de privacidad.
- Existen varias organizaciones gubernamentales y privadas que emiten modelos, mejores prácticas y estándares sobre seguridad de la información en Estados Unidos, por ejemplo, la Universidad de Carnegie Mellon (Software Engineering Institute)- CMMI, ISACA-CobiT o NIST.

⁹¹ Cifrado quiere decir: “La protección de los datos que se encuentren en forma electrónica u óptica, en almacenamiento o en tránsito, utilizando: una tecnología de cifrado que haya sido adoptada por un cuerpo establecido de estándares, incluido, pero no limitado a, los Estándares de Procesamiento de Información Federal publicado por el NIST, la cual procese tales datos de forma indescifrable en ausencia de las llaves criptográficas necesarias para permitir la decodificación de dichos datos.” NRS 603A.215, <http://www.leg.state.nv.us/nrs/nrs-603a.html>, revisado el 21 de febrero de 2012, 20:00 hrs.

III. RECOMENDACIONES Y MEDIDAS CORRECTIVAS

El quinto y último Entregable comprendió como actividad principal la elaboración de "...recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en el sector de tecnologías de información para dar cumplimiento a la LFPDPPP".

III.1 Recomendaciones. Para facilitar la adopción de los mecanismos de control que cada organización requerirá a partir de su análisis particular, así como sus características de operación para el cumplimiento de los requerimientos de la LFPDPPP, que se propusieron dentro del apartado "Marco práctico referencial de mecanismos de control de gestión de seguridad y privacidad de la información", es importante tener en cuenta las siguientes recomendaciones complementarias:

- El esfuerzo para estimar el nivel aceptable de riesgos, y la combinación de controles de seguridad y privacidad en la organización, puede basarse en las referencias documentales de las experiencias en otros países con regulaciones similares, y que han sido incluidos como parte de esta investigación. El uso de estas referencias no implica copiar o adaptar los elementos que se han desarrollado, sino que deben favorecer la generación de alternativas adecuadas a la realidad operativa de la organización.
- Las empresas del sector de TI deben trabajar en la redefinición de sus servicios para clientes finales, considerando los mecanismos de operación y habilitación tecnológica en que se genera el servicio de TI, y los elementos legales y de calidad del servicio que se acuerdan con los proveedores y clientes. De tal suerte que el modelo de operación atienda estos requerimientos de forma natural, y la seguridad de la información y privacidad de datos se

conviertan en atributos naturales de cada servicio ofrecido. Esta recomendación implica que se cambie el enfoque de gestión actual de la infraestructura a un enfoque integral de gestión de servicios informáticos.

Asimismo, se recomienda que dentro de las áreas comerciales de las empresas se defina todo lo relacionado al encargado de acuerdo a la LFPDPPP, considerando entre otros aspectos lo siguiente:

- Objetivo
 - Actividades técnicas a cubrir
 - Beneficios
 - Requerimientos
-
- Una forma positiva de potenciar los esfuerzos para incrementar la seguridad y privacidad de la información, se encuentra en que la organización ejecute sus iniciativas de controles, dentro de un marco referencial de industria que pueda ser evaluado de manera independiente (certificación), y se obtenga garantía razonable de la efectividad de la gestión de seguridad considerando los requerimientos de privacidad de las partes interesadas.
 - Para apoyar las actividades de monitoreo y evaluación de la efectividad de la función de seguridad dentro de los parámetros de riesgo y privacidad, es recomendable que las organizaciones puedan instaurar un mecanismo de autorregulación desde una perspectiva de cumplimiento independiente a la operación de la infraestructura y seguridad, que favorezca la supervisión y mejora continua en el corto plazo, y a su vez, permita preparar el marco de seguridad y privacidad para una revisión externa que determine el cumplimiento de la LFPDPPP en la madurez natural de la regulación.

III.2 Medidas Correctivas. Como recomendaciones en materia de medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en el sector de las TI para dar cumplimiento a la LFPDPPP, se resumen a continuación las más importantes:

Prácticas organizacionales de seguridad y privacidad de la información

Estado general	Medidas correctivas
<ul style="list-style-type: none"> • Las empresas del sector de TI reconocen ciertos mecanismos como el fundamento para la toma de decisiones sobre el nivel de seguridad de la información y privacidad de datos, tales como: análisis de riesgos, cumplimiento con ejercicios de auditoría, recomendaciones de proveedores, análisis técnicos de vulnerabilidades, entre otros. Sin embargo, su ejecución no se encuentra formalizada ni se reconoce como un componente organizacional con una participación multidisciplinaria. • En este sentido, las organizaciones han comenzado a 	<ul style="list-style-type: none"> • El Análisis y Evaluación de Riesgos de Seguridad y Privacidad se debe establecer como un proceso formalmente definido dentro de las prácticas organizacionales para ajustar la operación del negocio y la calidad de los servicios a los clientes, a partir de identificar las prioridades de protección con un estricto sentido de negocio. • A partir de la identificación de las prioridades de protección y privacidad, las organizaciones deben asignar partidas presupuestales específicas para desarrollar los proyectos de seguridad y privacidad, como

Estado general	Medidas correctivas
<p>implantar mecanismos de seguridad de la información a partir de regulaciones y requerimientos puntuales.</p> <ul style="list-style-type: none"> • Por lo que las asignaciones de presupuesto son limitadas y solamente se realizan, en mayor medida, asignaciones para proyectos aislados específicos. • La ejecución de estos proyectos de controles para seguridad y privacidad son ejecutados como parte de las responsabilidades de la función de Sistemas/Informática/TI del negocio, sin incluir un enfoque y ejecución integrales. • Las organizaciones identifican aquellos rubros generales de control que deben considerarse para desarrollar mecanismos específicos de protección y privacidad, sin embargo, no todos han sido implantados. 	<p>parte de un ejercicio estratégico de planeación de presupuesto, que corresponda al nivel de participación de todas las áreas de la organización en el uso de estos controles en sus procesos.</p> <ul style="list-style-type: none"> • Las organizaciones deben ampliar los roles y responsabilidades sobre seguridad y privacidad para todas las áreas y funciones de su estructura, para que se asienten y ejecuten formalmente. • Se debe definir un procedimiento de estrategia de seguridad y privacidad, que aproveche los resultados del análisis y evaluación de riesgos, para la toma de decisiones sobre los rubros de control que se van a desarrollar en la organización a partir de la prioridad, factibilidad y beneficio de estos controles.

Estado general	Medidas correctivas
<p>Gestión de la seguridad y privacidad de la información</p> <p>“Procesos, roles y responsabilidades”</p>	
<ul style="list-style-type: none"> • Se identifica la existencia de un Comité de Seguridad de la Información que vigila las actividades de aseguramiento y cumplimiento de la privacidad de datos dentro de la organización. • Asimismo, se ha incrementado la participación de roles estratégicos en la clasificación de la información (tipo y prioridad de protección) • Las organizaciones no han ejecutado esfuerzos continuos sobre la capacitación del personal en temas de seguridad y privacidad de la información. • De igual forma, no se han desarrollado esquemas de medición de la efectividad de la función de seguridad y privacidad, por lo que solamente se cuenta con métricas operativas o evaluaciones técnicas esporádicas. 	<ul style="list-style-type: none"> • Las organizaciones deben establecer formalmente (como parte del esfuerzo de asignar roles y responsabilidades), un grupo multidisciplinario que tenga responsabilidades sobre la determinación del nivel de riesgo aceptable, la definición de la estrategia de seguridad, medición de la efectividad de la función de seguridad y operación directa de controles. • Las organizaciones deben incluir a las áreas comerciales, de operación y jurídicas en la definición de los roles y responsabilidades de seguridad y privacidad, con una asignación puntual de la determinación de acuerdos y términos legales, niveles de servicio y desviaciones relativas a brechas de seguridad e incidentes para con proveedores, socios de negocio

Estado general	Medidas correctivas
<ul style="list-style-type: none"> Las implicaciones de los requerimientos de privacidad, no se han considerado en los acuerdos contractuales con proveedores, socios de negocio ni clientes. 	<p>y clientes.</p> <ul style="list-style-type: none"> En el primer esfuerzo de mecanismos de control, las organizaciones deben definir y ejecutar una estrategia integral de concientización sobre seguridad y privacidad de la información, dentro de los parámetros corporativos de comunicación institucional. Como parte de los controles relativos a la gestión de incidentes y brechas, deben derivarse componentes de medición de la efectividad de la función de seguridad, considerando activamente el nivel aceptable de riesgo, y el nivel de seguridad que prevalece en la organización, a partir de medir los componentes del riesgo y el manejo de las brechas de seguridad.

Estado general	Medidas correctivas
<p>Gestión de la seguridad y privacidad de la información</p> <p>“Seguridad de los activos informáticos”</p>	
<ul style="list-style-type: none"> • En mayor medida, las empresas del sector de TI son responsables de sus propias instalaciones donde se encuentra la infraestructura tecnológica para el procesamiento de información. • El enfoque de protección se ha centrado sobre aseguramiento de la infraestructura y no sobre el tipo de información que procesa la organización. • Se identifica un avance considerable en mecanismos de protección relativos a redes de telecomunicaciones, plataformas y equipos de usuario final. • Los esfuerzos actuales de controles de seguridad, no se han desarrollado con requerimientos de privacidad. • La premisa de la selección y características de los mecanismos de control de 	<ul style="list-style-type: none"> • Realizar una revisión detallada sobre las características de sus instalaciones de cómputo para asegurarse que cumplen con los requerimientos de la industria (según estándares aplicables) • En su defecto, solicitar al proveedor de las instalaciones de cómputo, que entregue periódicamente resultados de revisiones o evaluaciones de sus instalaciones. • Desarrollar una estrategia de aseguramiento y privacidad de la información basada en controles preventivos, de detección y correctivos, cuya implementación considere políticas, procedimientos y mecanismos técnicos, que ayuden al cumplimiento de la LFPDPPP y ayuden a alcanzar el nivel de operación requerido

Estado general	Medidas correctivas
<p>seguridad, es la subjetividad/experiencia del personal responsable de la función de seguridad en la organización.</p> <ul style="list-style-type: none"> Existen esfuerzos incipientes sobre el monitoreo preventivo de seguridad a partir de la generación, preservación y explotación, por lo que no se contribuyen a generar métricas de la efectividad de la función de seguridad. 	<p>por la organización (las especificaciones recomendadas para estos controles se pueden encontrar en el "Marco práctico referencial de mecanismos de control de gestión de seguridad y privacidad de la información"</p> <ul style="list-style-type: none"> Desarrollar un componente de medición de la efectividad de la función de seguridad de la información. En primera instancia puede considerar capacidades de autorregulación y gradualmente revisiones por terceros.
<p>Tratamiento de datos en el denominado cómputo en la nube</p>	
<ul style="list-style-type: none"> Las organizaciones que ofrecen o consumen servicios de cómputo en la nube, consideran sus implicaciones dentro de su marco normativo de seguridad y privacidad. Sin embargo, los proveedores de estos servicios de cómputo en la nube no tienen un conocimiento 	<ul style="list-style-type: none"> Desarrollar una estrategia de aseguramiento y privacidad de la información basada en controles preventivos, de detección y correctivos, cuya implementación considere políticas, procedimientos y mecanismos técnicos, que ayuden al cumplimiento de la LFPDPPP y ayuden a alcanzar el

Estado general	Medidas correctivas
<p>pleno sobre las implicaciones de la regulación de privacidad sobre la gestión de sus servicios desde el punto de vista de operación, nivel de servicio y legal ante una brecha o desviación de los acuerdos contractuales.</p>	<p>nivel de operación requerido por la organización (las especificaciones recomendadas para estos controles se pueden encontrar en "Marco práctico referencial de mecanismos de control de gestión de seguridad y privacidad de la información".</p> <ul style="list-style-type: none"> Las organizaciones deben incluir a las áreas comerciales, de operación y jurídicas en la definición de los roles y responsabilidades de seguridad y privacidad, con una asignación puntual de la determinación de acuerdos y términos legales, niveles de servicio y desviaciones relativas a brechas de seguridad e incidentes con proveedores, socios de negocio y clientes.

III.3 Políticas Públicas. A la actividad f) en el rubro de Metodología de Trabajo del apartado 5 (Especificaciones Técnicas) de los Términos de Referencia, se añadió lo establecido en el inciso c) del apartado 4 (Alcance del estudio, asesoría o investigación): "c).- Las recomendaciones

y medidas correctivas deberán considerar acciones de política pública así como a nivel empresa”.

Al respecto, dicho reporte 5º pone en contexto el marco jurídico y programático que se requiere para establecer una política pública especial para el tema de la seguridad en el ámbito de las empresas de TI, que traten datos personales con el carácter de “encargados” conforme a la LFPDPPP. En este rubro se señaló que si bien es cierto que el Programa Sectorial de Economía 2007-2012 no es específico en este aspecto, sus objetivos sirven de marco para proveer mecanismos o medidas para elevar la competitividad de las empresas mediante el fomento del uso de las TI en la materia. Se comprende que este Programa no haya determinado líneas de acción exhaustivas para la economía en general, ni para la digital en lo particular, pues cuando fue emitido en mayo del 2008, México no contaba con lo que ahora es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, emitida en el 2010.

Como **políticas públicas** o esquema programático específico, que debe orientarse desde el poder público, se propusieron en este proyecto los siguientes objetivos con sus respectivas líneas de acción:

Objetivo General. Impulsar el conocimiento de buenas prácticas nacionales e internacionales en materia de seguridad de datos para el sector de las TI.

Objetivo 1. Generalizar el uso de buenas prácticas en materia de seguridad de datos personales en el sector de TI, para poder brindar certeza a las empresas y particulares que las subcontraten bajo la figura de encargado prevista en la LFPDPPP.

Objetivo 2. Desarrollar habilidades sobre prácticas nacionales e internacionales en materia de seguridad de datos para personas físicas o morales relacionadas con el sector de las TI, que operen como

encargados en el tratamiento de datos personales en posesión de los particulares.

Objetivo 3. Promover recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en las empresas de TI por parte de las personas físicas o morales, que operen como encargados en el tratamiento de datos personales en posesión de los particulares.

Se requiere señalar que el éxito de las Políticas Públicas que se promuevan para impulsar el conocimiento de buenas prácticas nacionales e internacionales en materia de seguridad de datos personales para el sector de las TI, con los objetivos descritos con antelación y sus líneas de acción correspondientes, radica en que exista infraestructura humana, organizativa y material; que se cuente con recursos financieros; y sobre todo, que los destinatarios de las mismas, en este caso los particulares que fungen como encargados en el tratamiento de datos personales, sean adecuadamente incentivados a alinearse a estándares, buenas prácticas y, principalmente, a las expectativas institucionales de la industria y de los titulares de los datos.

Al efecto, las dependencias deberán considerar en su respectivo Presupuesto de Egresos anual, partidas para Promover dentro de su sector de influencia conforme a la Ley Orgánica de la Administración Pública Federal, el uso de buenas prácticas en materia de seguridad de datos personales en el sector de TI, para poder brindar certeza a las empresas y particulares que las subcontraten bajo la figura de encargado prevista en la LFPDPPP, en coadyuvancia con el IFAIPD; así como para establecer una unidad administrativa que atienda los asuntos de protección de datos personales en posesión de los particulares desde un punto de vista sectorial.

Como **instrumentos de política**, se han recomendado –entre otras- los siguientes: un Sistema Nacional de Información de normas, estándares y buenas prácticas en materia de seguridad de datos personales en el sector de TI, cuyo objetivo será orientar e informar a las empresas y particulares que subcontraten servicios de tratamiento bajo la figura de encargado prevista en la LFPDPPP y un Inventario Nacional de empresas de TI dentro del Sistema de Información Empresarial Mexicano (SIEM).

Y finalmente, sobre el tema de los **responsables institucionales de ejecutar estas políticas públicas**, se destacó que conforme las leyes mexicanas sobre administración pública federal, son 19 instituciones públicas (Secretarías de Estado, Procuraduría General de la República y Consejería Jurídica), más la coadyuvancia del IFAIPD, las que tienen injerencia en el terreno de las regulaciones sobre privacidad. De aquí que estos 20 organismos en total, deban ser considerados como sujetos responsables de encauzar armónicamente las Políticas Públicas correspondientes.

**PROYECTO ELABORADO PARA LA CÁMARA
NACIONAL DE LA INDUSTRIA ELECTRÓNICA, DE
TELECOMUNICACIONES Y TECNOLOGÍAS DE LA
INFORMACIÓN (CANIETI)**



**REALIZADO POR PIVOTAL SERVICIOS, S. DE R.L. DE
C.V.**



www.pivotalmexico.com

flor.hernandez@pivotalmexico.com

2011-2012