Ciber-segurízate

Guía para crear un entorno digital más seguro para tu empresa y para ti

Amiti
Mejores empresas de TI para México

Konesh Soluciones

NYCE Seguridad y Confianza

SIGE

S21 SEC Your Cybersecurity Company

SAP

Cuando las personas y las organizaciones conocemos los riesgos presentes en el mundo digital, podemos prevenir ataques informáticos y tomar las acciones de contención y corrección pertinentes.

Ciber-segurízate

Guía para crear un entorno digital más seguro para tu empresa y para ti

Mejores empresas de TI para México

S21 SEC - Líder Comité de Ciberseguridad

Con el apoyo de: Aurorian, S.A. de C.V. (Konesh), Compusoluciones y Asociados, S.A. de C. V. (CompuSoluciones), Compañía Mexicana de Procesamiento, S.A. de C.V. (CMP) y Normalización y Certificación NYCE, S.C. (NYCE)

Contenido

Introducción

El trabajo cotidiano de las personas y las organizaciones se encuentra cada día más vinculado con el uso de las tecnologías digitales. Se trata de poderosas herramientas en constante evolución, que nos permiten contar con una cantidad inimaginable de datos, relativos a la identidad, los hábitos y las transacciones de los individuos, las empresas y todo tipo de entidades.

Su adecuada gestión resulta complicada y los riesgos inherentes normalmente pasan desapercibidos para la mayor parte de la gente. De hecho, no es extraño que el eslabón más débil sea justamente un directivo confiado, quien se jacta: “a nosotros no nos va a pasar nada, nunca nos ha pasado antes”; un dueño de empresa que se oculta detrás del pretexto: “yo a esas cosas no les entiendo”; o la ingenua presunción de quienes se preguntan: “¿qué les va a importar a los maleantes una empresa tan chica como la mía?”.

Debido a este tipo de actitudes, la situación de riesgo de las micro, pequeñas y medianas empresas es tan alta, que muchas de las medidas de prevención de riesgos que las grandes multinacionales están desarrollando, tienen que ver con el modo como ellas se blindan para evitar los ciberataques que pasan a través de las organizaciones más pequeñas, normalmente desprevenidas, que forman parte de su cadena de valor. En algunos países las leyes han empezado a transformarse a fin de obligar a las empresas a manifestar sus vulnerabilidades ante sus socios de negocio.

Constantemente nos enteramos por las noticias, de fraudes que involucran a grandes empresas, organizaciones gubernamentales o millones de usuarios. Por ello, no dudemos de que en más de una ocasión hayamos sido objeto de alguna agresión, ya sea que ésta haya tenido consecuencias obvias a nuestros ojos o no.

El problema se hace manifiesto cuando este tipo de ofensivas se convierten en pérdidas directas de dinero, nos involucran en responsabilidades jurídicas, afectan nuestra reputación, generan conflictos, violan nuestra privacidad, disminuyen nuestra eficiencia o, incluso, provocan el paro de nuestra operación. Estas implicaciones indeseables son precisamente las que deseamos evitar para ti y para tu organización. La presente guía es un esfuerzo realizado por el Comité de Ciberseguridad de AMITI para ayudar a las pymes a incorporar la ciberseguridad dentro de su gestión, de modo que seamos cada día más capaces de identificar riesgos, favorecer defensas y evitar impactos, mediante el desarrollo de estrategias preventivas y acciones personales e institucionales que nos permitan afrontar los riesgos y amenazas más habituales que, en materia de ciberseguridad, tienen que enfrentar las pymes.

Capítulo 1.
Riesgos y amenazas cibernéticas para las pymes

1.1. Identificación de riesgos y amenazas

En materia tecnológica, existen distintos tipos de riesgos para la información de las empresas. Algunos son provocados por criminales que buscan obtener un beneficio económico basado en el valor de nuestros datos y su uso potencial; otros están vinculados con el deseo de los atacantes de demostrar sus capacidades técnicas para la consecución de infiltraciones de gran calibre, las cuales suelen derivar en actos de extorsión; otros más constituyen acciones de espionaje a nivel personal, corporativo o incluso nacional. Asimismo, existen amenazas que tienen su origen en situaciones no intencionales y difíciles de prevenir, como desastres naturales, accidentes y otros casos fortuitos, cuyas consecuencias pueden dañar la información o infraestructura computacional de las organizaciones.

Todo esto se encuentra en nuestro entorno sin que nosotros podamos evitarlo. Sin embargo, es importante entender que algunos factores, que sí dependen de nuestras decisiones, aumentan los niveles de riesgo de nuestras organizaciones:

- Pocos controles: significa que la exposición de nuestros activos, información e infraestructura relacionada son de fácil acceso para terceros (por ejemplo, miles de personas pueden acceder a la vez a una base de datos a través de un sitio web, pero sólo unas cuantas lo podrían hacer si se trata de una red privada)
- Alta motivación: un potencial atacante estará más interesado en nosotros en la medida en que el beneficio percibido de hacerlo sea mayor, esto es, en la medida en que afectar nuestra reputación, sustraer nuestra información estratégica o robar nuestros recursos

Existen múltiples amenazas cibernéticas que tienen su origen en terceros, así como riesgos para nuestros equipos e información derivados de situaciones difíciles de prevenir, como los desastres naturales, pero la mayor parte de las medidas de prevención están en nuestras manos.

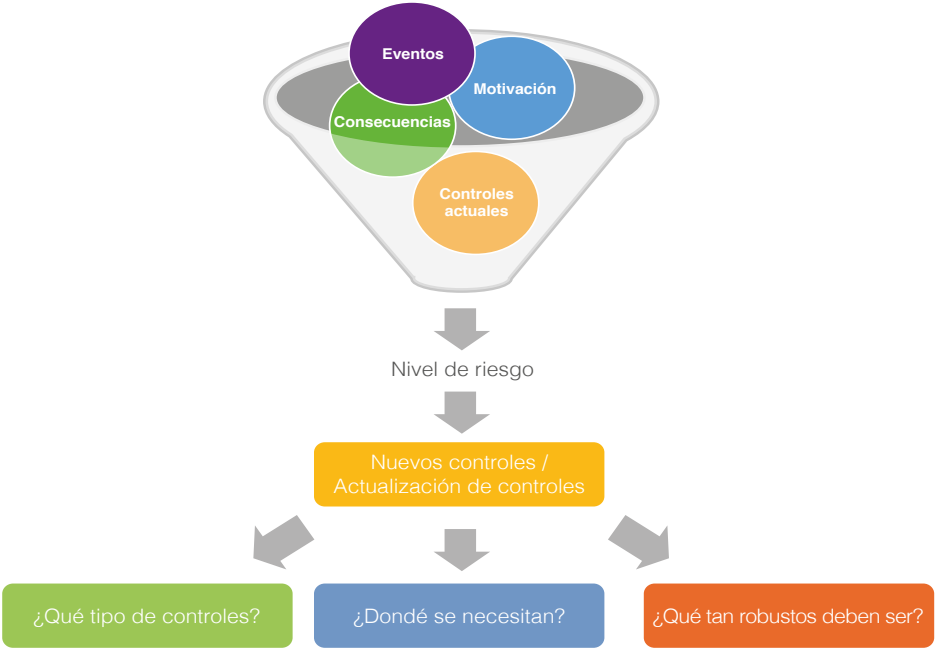
sea más redituable, por lo tanto debemos tener cuidado de la información que hacemos pública de nuestras actividades

- Impunidad: si los potenciales atacantes tienen un amplio rango de anonimato, se dificultará la trazabilidad de sus acciones y, por lo tanto, les será más fácil y conveniente el atacarnos
- Multiplicación de eventos: si ante los ataques y accidentes que nos afectan no existe nunca una respuesta adecuada, los delincuentes o las amenazas se multiplicarán y podrán provocar daños más constantes y severos.

Por lo tanto, si trabajamos para identificar y analizar nuestros riesgos cibernéticos, será más sencillo determinar las medidas necesarias para atender cada uno de ellos, indicando dónde deben ser implementados los controles y qué tan robustos deben ser estos. Por ejemplo, si se identifica que un riesgo está relacionado con la pérdida de confidencialidad de la información, se requerirán implementar controles que refuercen ese aspecto. Si se trata de información confidencial, conviene implementar un nombre de usuario y una contraseña para acceder a ella. Si la información es altamente sensible, será conveniente utilizar una autenticación de dos factores, como el empleo de un "token" o un código de un solo uso, enviado a un dispositivo móvil por mensaje de texto, tal como suelen hacerlo los bancos. Por lo tanto, es fundamental que las empresas evalúen qué tanto cuidado requiere cada tipo de dato que conserva.

Otro tipo de riesgos, como los que se descubren cuando el fallo de un disco duro nos hace conscientes de que no contábamos con un respaldo de la información, tienen, por supuesto, otro tipo de tratamientos preventivos y correctivos.

Toma de decisiones para establecer e innovar controles



1.2. Principales ciberataques

A continuación se describen las amenazas que se presentan de manera más frecuente contra compañías de todo el mundo.

Estas acciones se dirigen hacia todo tipo de industrias. No obstante, de manera histórica, el ámbito financiero siempre ha sido el principal objetivo de los ciberatacantes, debido al tipo de activos que manejan y, por ello, se prevé que esta siga siendo la tendencia predominante.

Sin embargo, hay que considerar que el número de organizaciones que manejan activos digitales es cada vez mayor, por lo que también otras industrias podrían ser objeto de ciberataques con mayor frecuencia en el futuro.

a) *Phising*

Este término hace referencia a la creación de un correo electrónico, un sitio web u otros formatos de comunicación electrónica ilegítimos con apariencia legítima. Son generados con el objetivo de obtener información de la víctima. Los comunicados se hacen pasar por una organización o personas afines a los intereses de las víctimas, con lo cual despiertan su confianza y de ese modo se disfrazan para robar sus credenciales de usuario u otro tipo de información de carácter confidencial.

El método habitual de este engaño es remitir a través de un correo electrónico o un SMS hacia un enlace a un sitio web que suplanta a otro sitio legítimo, su contenido ha sido preparado de tal forma que incite a la persona a introducir la información que el atacante busca obtener de forma ilícita o inadvertida.

En la siguiente imagen, difundida en redes sociales, se observa un ejemplo de *phishing*.

Imagen: identificación de los riesgos y controles requeridos.

No es que esta empresa tenga algún problema particular de seguridad, sino que los maleantes han considerado que, vulnerando información de las personas ligadas a esta compañía aseguradora, podrían obtener beneficios. Lo mismo sucede con miles de organizaciones empresariales de todos los países del mundo.

En dicha foto de pantalla se observa que el contenido presenta problemas de redacción y faltas ortográficas. Éstas suelen provenir de errores de traducción automatizados. Asimismo, incluye enlaces a sitios y correos electrónicos que no corresponden al dominio de la compañía real.

Recomendaciones:

- Presta atención al contenido recibido; léelo con atención y considera que prácticamente ninguna organización seria solicita información sensible a través de medios digitales de este tipo
- No pulses enlaces ni remitas información en correos electrónicos o mensajes de naturaleza sospechosa, es decir, que no corresponden perfectamente con las direcciones oficiales del emisor
- Antes de brindar información a terceros o acceder a algún sitio o enlace, contacta con la empresa que supuestamente ha generado el contenido para verificar la validez del mismo
- Verifica la autenticidad de los sitios que visitas mediante la validación de los certificados de seguridad del sitio; estos comúnmente aparecen junto a la dirección del sitio visitado, indicando con un candado y una barra de color verde que el sitio cuenta con un certificado de seguridad emitido y validado por una entidad certificadora
- No respondas el mensaje o proporciones información personal a una fuente no verificada
- No abras archivos adjuntos que acompañen correos electrónicos sospechosos.

b) *Ransomware*

El término *ransomware* hace referencia a un tipo de *malware* (código malicioso que se instala en una computadora con la intención de generar daños u

obtener información de la misma), cuyo objetivo es la infección de los equipos de las empresas, con el fin de solicitar posteriormente un rescate para recuperar tu información. Este rescate normalmente es conocido como "ransom".

El código malicioso toma el control de los equipos, cifrando su contenido, de forma que la información es "secuestrada" al quedar inaccesible para su dueño legítimo.

Con posterioridad, los delincuentes solicitan un rescate, habitualmente en Bitcoins u otras cripto-monedas, o por medio de algún otro tipo de pago que permita el anonimato del atacante. Una vez que este pago se realiza, los delincuentes envían las claves que permiten nuevamente a la víctima tener acceso a su información.

Este tipo de *malware* puede ser instalado a través de "agujeros" de seguridad en el software o mediante mensajes engañosos, que buscan que el usuario abra archivos adjuntos o acceda a enlaces que descargan los programas que infectan el equipo y terminan cifrando y secuestrando la información.

En la página siguiente mostramos una pantalla típica con la cual los atacantes dan aviso de sus actos e intenciones.

Recomendaciones:

- Actualiza tus sistemas operativos, navegadores, antivirus y aplicacines periódicamente
- Realiza al menos dos copias de seguridad de la información que tienes almacenada en tus discos duros y guárdalas en lugares diferentes, por ejemplo en discos duros externos o memorias USB y, simultáneamente, en la nube u otros servicios de respaldo en línea
- Evita abrir correos electrónicos de procedencia sospechosa
- Evita los sitios web de contenido dudoso
- Utiliza contraseñas robustas e implementa políticas de seguridad de bloqueo de cuentas ante un número determinado de intentos fallidos de acceso, de modo que quienes intenten entrar a tus equipos encuentren resistencia

Pantalla típica con la cual se exige un *ransom* para liberar la información de una víctima.

- Evita el uso de cuentas con permisos de administrador
- Utiliza herramientas de detección de ransomware y de vulnerabilidades en los sistemas
- Realiza simulacros con el personal para ayudarlo a identificar correos y mensajes engañosos, señalando sus características, como direcciones de correo que provienen de un sitio o dominio distinto al del que dicen venir, enlaces a páginas web que no utilizan certificados de seguridad válidos, redacción cuestionable o con faltas de ortografía
- Reporta todo incidente de seguridad al responsable de seguridad de la información de tu organización y contacta a las autoridades correspondientes (ver sección contacto con autoridades en esta misma guía).

c) *Defacement* o suplantación de sitios

Este ataque consiste en la modificación de la información de un sitio web o la sustitución de su contenido por algún otro, ya sea para brindar información falsa, para transmitir algún mensaje político o social, o para instalar algún tipo de *malware* que afecte a terceros. Estos ciberataques afectan sobre todo a la reputación de la organización que se ve implicada, mermando la confianza de sus clientes o usuarios y dificultan por cierto tiempo su capacidad de realizar operaciones sobre su plataforma.

En las imágenes de la página siguiente se observa un ejemplo de *defacement* realizado contra la página web de una gran empresa ubicada en México[1]. Como se puede observar, en la primera imagen se muestra el sitio correcto, mientras que en la segunda de ellas el contenido ha sido modificado por un grupo de hackers argentino, autodenominado "Alfabeto Virtual", quienes en su mensaje presumen de su capacidad para vulnerar los sistemas de empresas de gran capacidad y sólidos sistemas de seguridad.

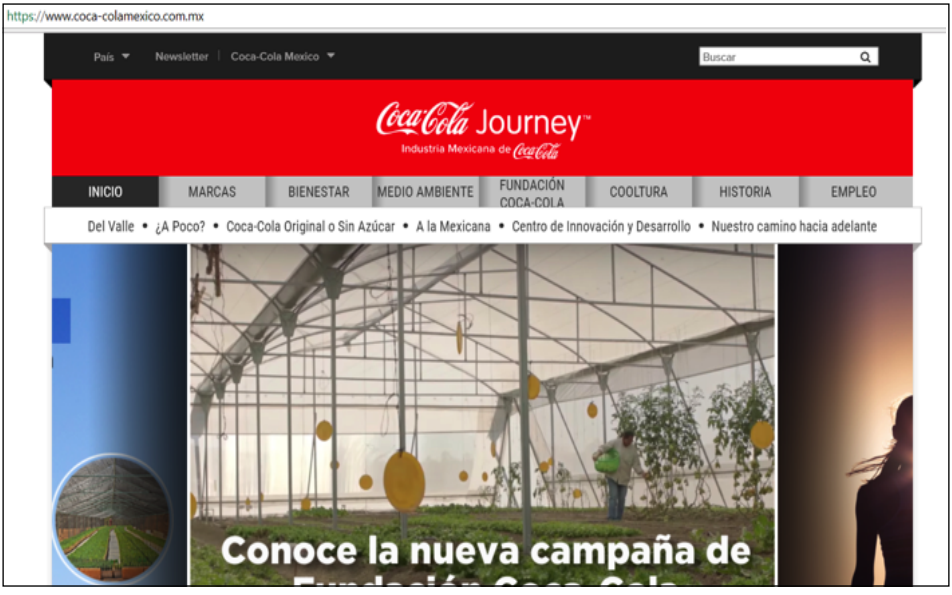
Esta recomendación se dirige principalmente a los administradores de la seguridad de los sistemas informáticos de las organizaciones, con el objetivo de que incrementen las medidas para dificultar el acceso a los intrusos, de modo que eviten que estos lleguen a modificar el contenido de sus sitios web.

Recomendaciones:

- Mantén actualizados los motores de los sitios web, bases de datos y sistemas operativos
- Descarga, instala e implementa sólo software obtenido de forma legal, de orígenes legítimos y sitios oficiales, debidamente licenciado
- Cambia las contraseñas predeterminadas de los sistemas, utiliza contraseñas robustas e implementa políticas de seguridad de bloqueo de cuentas ante un número determinado de intentos fallidos de acceso
- Realiza respaldos periódicos de la información de tu empresa.

---

1 Caso extraído del portal Zone-H.org, donde se reportan ataques a sitios web.


https://www.coca-colamexico.com.mx
País
Newsletter
Coca-Cola Mexico
Buscar
Coca-Cola Journey
Industria Mexicana de Coca-Cola
INICIO
MARCAS
BIENESTAR
MEDIO AMBIENTE
FUNDACIÓN COCA-COLA
COOLTURA
HISTORIA
EMPLEO
Del Valle • ¿A Poco? • Coca-Cola Original o Sin Azúcar • A la Mexicana • Centro de Innovación y Desarrollo • Nuestro camino hacia adelante
Conoce la nueva campaña de


Mirror saved on: 2015-12-13 12:40:55
Notified by: AlfabetoVirtual
System: Linux
Domain: http://www.coca-colamexico.com.mx/a.htm
Web server: Unknown
IP address: 205.218.56.85
Notifier stats
THIS MIRROR IS ONHOLD AND HAS NOT BEEN VERIFIED YET. FAKE DEFACEMENTS WILL BE DELETED WHEN REVIEWED BY OUR STAFF.
This is a CACHE (mirror) page of the site when it was saved by our robot on 2015-12-13 12:40:55
Hacked by AlfabetoVirtual
I'M NOT GONNA CHANGE FOR ANYONE.
I DON'T CARE WHAT PEOPLE THINK ABOUT ME, THAT'S I AM, AND PROUD OF IT.
LOVE: ChinaFans - Kuroi'SH - w4l3XzY3 - Jok3r - IMAM - Tobitow - Libero - iFactoreX
GHoST61 - TiGER-M@TE - NeO-h4ck3r - FORTYS3V3N

1.3. Seguridad física

Todos los sistemas e información que radican en las computadoras, internet, almacenamiento en la nube y otros recursos informáticos, se encuentran ubicados en un espacio físico, aunque ignoremos dónde está. Por lo tanto, una parte importante de la ciberseguridad consiste en proteger los equipos físicos. Para ello, debemos asegurarnos de que sólo tengan acceso a ellos las personas autorizadas para manipular cada uno de los dispositivos propiedad de la organización y su documentación.

Recomendaciones:

- Identifica al personal autorizado a través de mecanismos que permitan validar de forma sencilla su identidad, ya sea de forma visual, por parte de los supervisores relativos, o de forma automatizada, por parte de los sistemas informáticos de seguridad
- Implementa el uso de gafetes con nombre, puesto, fotografía y privilegios de acceso, credenciales de acceso magnético o de radiofrecuencia, identificadores biométricos y privilegios de acceso diferenciados por puesto y persona, acordes con el nivel de confidencialidad de tu información
- Mantén un control adecuado del acceso a instalaciones físicas y sistemas informáticos mediante el uso de bitácoras, asegurando que la información que se registra en ellas sea legítima y válida; para ello es importante que no sean los visitantes o colaboradores quienes registren la información en la bitácora, sino que lo haga el personal encargado de la seguridad, a fin de que valide la identidad de las personas y la registre en la bitácora, evitando así también revelar información de forma inadvertida para potenciales atacantes
- Restringe el uso a los equipos con información sensible o confidencial y, de ser posible, limita su uso para que sólo puedan ser utilizados dentro de las instalaciones
- Si requieres sacar equipos de las instalaciones, usa un cifrado completo de disco

- Emplea cerraduras y candados para las gavetas y archiveros físicos, con un nivel de seguridad correspondiente a nivel de confidencialidad de la información que contienen
- Envía mensajes protegidos, por ejemplo con cifrado de extremo a extremo, según lo requiera el tipo de información a enviar
- Utiliza equipos de video-vigilancia para registrar el acceso y las actividades dentro de las instalaciones, en particular donde exista tratamiento de información sensible o confidencial
- Instala elementos disuasivos, como alarmas, cámaras, guardias de seguridad, rejas y maletines con aditamentos de seguridad, entre otros.

Capítulo 2.
Riesgos y amenazas cibernéticas a nivel personal

En materia de seguridad personal se identifican otro conjunto de riesgos que, en algunos casos, se asemejan a los ya comentados con anterioridad, pero que, en otros, se circunscriben al ámbito de los sujetos físicos y su información.

La finalidad de la información que se detalla enseguida tiene como objetivo ayudar a la identificación de estos potenciales problemas y, por tanto, establecer las medidas preventivas necesarias para evitarlos o al menos mitigar sus efectos.

2.1. Ingeniería social

La metodología de ataque definida como "ingeniería social" hace referencia a aquellos métodos con los cuales los atacantes se benefician del hecho de que el eslabón más débil de la seguridad es el individuo. Mediante el empleo de técnicas de manipulación psicológica se acercan a las rutinas de sus víctimas a fin de obtener el beneficio que desean, buscando chantajearlo o amenazarlo, y en el ámbito cibernético, obtener sus credenciales o información confidencial.

El *modus operandi* más habitual en este entorno se refiere al empleo de correos electrónicos alterados, con características muy similares a las que corresponderían con las reales. Prácticamente a todos nos han llegado a nuestras bandejas de entrada mensajes que se hacen pasar por alguna entidad bancaria que tenemos contratada, algún compañero de trabajo o incluso los comercios en los que habitualmente realizamos nuestras compras.

En estos mensajes se suelen incluir archivos adjuntos con contenido supuestamente fundamental para continuar con la actividad rutinaria del re-

Los individuos somos el eslabón más frágil de la cadena de seguridad, con riesgos que implican nuestra integridad física y la de nuestros seres queridos, por eso es fundamental poner en práctica conductas de "higiene digital" para protegernos.

ceptor o enlaces que redirigen a sitios web que requieren confirmar información, supuestamente por medidas de seguridad.

Obviamente, todos ellos son fraudulentos y en algunos casos incluso incluyen código malicioso que infecta nuestras computadoras, afectando al destinatario y, en ocasiones, a todos aquellos que se encuentran en su red de contactos.

Teniendo todo ello en consideración, la principal medida de seguridad radica en sospechar de todos los correos electrónicos que no esperamos procedan de la persona que asegura ser el emisor, que su contenido está escrito de manera incorrecta o extraña, que solicitan credenciales o en los que existe alguna otra alteración en el encabezado o redacción del correo electrónico. Ante la duda, la mejor prevención es contactar por otro medio con quien supuestamente ha generado el correo para verificar si ha sido su verdadero emisor.

2.2. Conexión a Wi-Fi pública

La necesidad de conexión permanente a la red se ha extendido entre la ciudadanía, de tal forma que se busca la reducción en el consumo de datos en los terminales móviles o el acceso a la misma desde una computadora cuando se está fuera del lugar de trabajo.

Por ello, es preciso tener presente que cuando uno se conecta a internet en algún lugar público existe el riesgo de que los datos o información manejados sean interceptados por otros usuarios.

Dentro de las principales recomendaciones para salvaguardar la información cuando se emplea una red de este tipo, se encuentra la conexión VPN

(Virtual Private Network) [2] . Esta acción permite asegurar un nivel elevado de privacidad entre el dispositivo conectado y el servidor o la red a los que se está conectando. Para asegurar que la VPN está cumpliendo su objetivo, lo mejor es acudir al servicio de tecnologías de información (TI) de tu compañía con el objetivo de verificar que ésta se encuentre correctamente configurada.

No obstante, cuando la mencionada solución no sea posible y se requiera acceder a una red Wi-Fi pública, es preciso guardar cautela y no realizar transacciones bancarias ni transferir o manipular información de carácter sensible o confidencial. Asimismo, es recomendable borrar la caché de los movimientos realizados antes de cerrar la sesión en la que se ha estado trabajando.

En la siguiente tabla se muestran las recomendaciones de uso de una red pública según el grado de seguridad de la misma:

2 Es una tecnología de red de computadoras que permite conectar de forma segura una red local a una red pública o no controlada, como internet.

Tipo de Wi-Fi	A dondé te conectas	Qué puedes hacer
Pública y no segura	Sitio web no seguro	Sólo actividades de bajo riesgo: navegar, leer noticias
	Sitio cifrado (https://) y con candado	Actividades de riesgo moderado: *log in* de inicio en sitios a los que estás suscrito
Pública y segura (WPA)	Sitio cifrado (https://)	Actividades de riesgo medio y alto: e-mail, trabajo con documentos en línea, redes sociales
	Sitio cifrado (https://) y con candado	Actividades de muy alto riesgo: banca en línea, PayPal o tarjetas

Fuente: Incibe, 2016, con ajustes.[3]

2.3. Descarga de aplicaciones móviles fraudulentas

De la misma forma que en el caso precedente, en la actualidad se ha generado una expansión en el uso de aplicaciones móviles, las cuales existen para facilitar multitud de servicios y entretenimiento. La afición a ellas es tan habitual, que los terminales suelen rebasar su capacidad de información debido a la cantidad de aplicaciones que se están requiriendo para el día a día.

Es preciso subrayar que el uso de éstas no supone un riesgo en sí mismo, siempre y cuando se tengan en cuenta dos medidas sencillas a la hora

3 https://www.incibe.es/protege-tu-empresa/blog/7-cuestiones-usar-movil-foma-segura-2

de llevar a cabo su descarga: acudir a los sitios oficiales (principalmente, Apple Store o Google Play) y obtener la última versión cargada por el fabricante, la cual normalmente posee actualizaciones en sus mecanismos de seguridad. Ante la duda de la legitimidad de la aplicación es recomendable contactar con el proveedor para verificar la misma

¿Por qué son necesarias tales medidas? Al igual que en las computadoras, el malware para móviles ha experimentado un crecimiento exponencial en los últimos años y los delincuentes lo usan para obtener datos personales, sobre todo aquellos de carácter bancario, los cuales a menudo están contenidos en tales dispositivos. De esta manera, los cibercriminales alojan el código malicioso en aplicaciones que generan una alteración del comportamiento de los mismos, llegando a acceder al contenido personal para proceder posteriormente a acciones fraudulentas.

A pesar de que este tipo de actividad se ha asociado sobre todo con aplicaciones de gaming o juegos, hoy en día se han detectado en todo tipo de servicios, incluyendo, por supuesto, aquellas de naturaleza bancaria, aseguradoras y compra online.

2.4. Publicación de datos personales y uso de correos electrónicos corporativos

Actualmente, la publicación de información en la red se ha convertido en una constante entre los ciudadanos. La subida de imágenes en redes sociales es considerada por gran cantidad de personas casi como una necesidad, ya que consideran que aquello que no se encuentra difundido parece que no ha existido, además de ese modo se pretende cubrir una exigencia psicológica de reconocimiento social.

Esta situación provoca que, en muchos casos, se publiquen datos que pueden abrir brechas de seguridad, tanto personales como institucionales.

En materia de redes sociales se comprueba que, detrás de cada seudónimo, los individuos generan un anonimato que posibilita un amplio abanico de mensajes que pueden producir graves perjuicios para la reputación

de otras personas o compañías, con independencia de que la misma sea cierta o falsa.

Bajo el mismo método, hay quienes incluso difunden datos sensibles que comprometen la seguridad de las empresas, como por ejemplo, listas de correos electrónicos y datos de las tecnologías corporativas.

En este sentido, las medidas preventivas radican nuevamente en mantener una serie de conductas de "higiene digital" que permitan proteger tanto la propia imagen como la de las empresas. Es por ello que se recomienda que desde estas últimas se establezcan comunicados oficiales y vinculantes, firmados por los departamentos de recursos humanos, mediante los cuales se prohíba el uso del correo corporativo para aquellos casos que se encuentren fuera del ámbito laboral. De la misma manera, deben ampliarse las restricciones a la generación de contenidos en redes sociales u otro tipo de foros públicos a fin de evitar que se vinculen ciertas noticias y comportamientos a la corporación. Las organizaciones deben evitar que sus colaboradores den detalles, por ejemplo, de las tecnologías que se están empleando, sus localizaciones sensibles, el tipo de documentación delicada que manejan, etc. Este tipo de políticas, deben extenderse a un período de entre dos a cinco años para los empleados que dejan de trabajar en las empresas.

Adicionalmente, se recomienda que cada uno de los usuarios de la tecnología digital seamos conscientes de la magnitud de la internet a la hora de propagar contenidos de cualquier naturaleza, con independencia del número de seguidores o de la privacidad de las cuentas. Hay que recordar que, en cuanto se publica algún contenido, éste deja de estar bajo nuestro control. Por ello, aquella información que pueda aportar datos sensibles, como la geolocalización, las rutinas o las características familiares, es aconsejable que se mantenga en el ámbito privado. La recomendación general es clara: todo aquello que no te sentirías confiado de gritar en el vagón del metro o en un café, de modo que todos se enteren, no lo pongas en internet.

Capítulo 3.
Impactos derivados

El resultado de cualquier vulnerabilidad que sea aprovechada por una amenaza y que ocasione una pérdida, se llama “impacto”.

El concepto de impacto es el elemento fundamental para la administración de riesgos. En última instancia, todas las actividades de la administración de riesgos están diseñadas para reducir el impacto a niveles aceptables. Por ello, las amenazas y las vulnerabilidades que no tienen un impacto son irrelevantes.

Por lo general, en organizaciones comerciales el impacto se cuantifica como una pérdida financiera directa o indirecta. Ejemplos de dichas pérdidas incluyen:

- Pérdida directa de dinero (efectivo o crédito)
- Responsabilidad penal o civil
- Pérdida de reputación, buen nombre o imagen
- Reducción en el valor de las acciones
- Conflicto de intereses para el personal, clientes o accionistas
- Violaciones a la confidencialidad/privacidad
- Pérdida de oportunidades de negocio/competencia
- Pérdida de participación en el mercado
- Reducción en el desempeño/eficiencia operativos
- Interrupción en las actividades de negocio
- Contravenciones a la legislación que resulten en la imposición de sanciones.

El proceso de ciberseguridad tiene por objeto evitar los impactos derivados de un ataque o amenaza; afectaciones que pueden ser monetarias, legales, de reputación, de cese de operaciones o personales.

El impacto se determina mediante una evaluación y posterior análisis de repercusiones para el negocio. Este análisis determinará la criticidad de los activos de información involucrados y brindará las bases necesarias para establecer: facultades de control de acceso por persona, planes de continuidad de negocio y tiempos objetivos de recuperación en caso de problemas. Contar con este tipo de información permite priorizar la administración de riesgos y, junto con las valuaciones de activos, establecer los niveles y tipos de protección que se requieran en cada área y para cada clase de información.

Lo fundamental consiste en definir el impacto de los diversos tipos de amenaza con respecto a la misión y objetivos de una organización. Considerándolo así, a continuación clasificamos los principales tipos de impacto que pueden sufrir las empresas y las áreas donde los ataques cibernéticos buscan tener repercusiones.

3.1. Impacto financiero

Un impacto financiero es un gasto con efecto monetario que no puede ser controlado. Los tipos de eventos que crean este tipo de impacto son los desastres económicos, cambios inesperados en las condiciones del mercado, fallos catastróficos de productos y cualquier cosa que interrumpa un negocio y sobre la cual la gestión empresarial no tiene control.

En general, este tipo de eventos cambian la situación financiera de la empresa y de su entorno. Por ejemplo, una compañía que cierra operaciones y proporciona patrocinios, normalmente tiene un impacto financiero en las asociaciones que apoyaba.

Los tipos de situaciones que generan gastos y que producen impactos financieros son los desastres naturales, los cambios en las condiciones del mercado y otros eventos que están fuera del control de la gestión. Los gastos que no pueden ser cubiertos por los ingresos después de este tipo de sucesos son impactos de elevada incidencia, ya que tienen la capacidad de hundir a la empresa.

Estos impactos pueden encontrarse presentes como resultado de ciberataques o de una inadecuada protección de los equipos informáticos y de la información que custodian, tanto en caso de desastres como de accidentes.

3.2. Impacto regulatorio

Debido al incremento de la complejidad de los ataques cibernéticos, la regulación debe adaptarse continuamente, lo que en ocasiones requiere inversiones adicionales por parte de las empresas. En todo caso, los beneficios de una buena regulación incrementarán la capacidad de las organizaciones para defender su reputación y recursos.

Es por ello que la Organización para la Cooperación y el Desarrollo Económicos, OCDE, propuso hace cinco años evaluar el impacto en etapas tempranas de la formulación de nuevas propuestas regulatorias. Eso significa que cuando se innova en términos regulatorios, siempre es necesario tener en cuenta el objetivo a alcanzar, las distintas alternativas para lograrlo y los costos y beneficios de la medida propuesta.

Cada empresa debe verificar cuáles son las normas aplicables y reflexionar sobre los beneficios que le trae su acatamiento.

3.3. Impacto reputacional

Es el impedimento o la disminución de la capacidad de mantener las relaciones comerciales existentes o establecer nuevas por parte de una entidad u organización debido a una opinión o percepción pública negativa. La mala reputación suele ser originada por la materialización de un evento negativo, ya sea interno o externo, ocasionando la disminución

en la compra o utilización de productos o servicios de una entidad u organización.

Como ya se ha explicado antes, este tipo de riesgos se encuentran vinculados a menudo con ataques cibernéticos, pero también con comportamientos inadecuados de las personas que forman parte de las organizaciones.

Es fundamental tener esto en cuenta, pues el impacto reputacional puede ser tan grande, que la entera supervivencia de una empresa dependa de cómo haya gestionado la crisis derivada de dichos comportamientos.

3.4. Impacto operativo

Es la generación de pérdidas inesperadas y la afectación del logro de metas y objetivos de negocio, proveniente de fallas de información en los sistemas o en los controles internos de una organización.

Cuando se presenta alguna de las siguientes situaciones, se generará un impacto operativo que se reflejará en pérdidas a la entidad, así como un aumento de costos y gastos:

- Incumplimiento de normas y procedimientos para la ejecución de un proceso
- Falta de documentación de procesos
- Falta de confidencialidad de la información
- Fallas en los procedimientos por errores humanos.

Este tipo de impacto está directamente asociado con errores humanos, fallas en los procesos e inadecuados sistemas y controles, entre los cuales está el mal uso de la información digital.

3.5. Impacto en seguridad y salud

Es el incremento en costos de atención médica y pérdida de productividad debido a ausencias de los empleados por condiciones de trabajo inseguras.

La medición de esta clase de impactos se realiza en términos de productividad y sueldos perdidos, gastos médicos y compensación por incapacidad. Aunque aparentemente este tipo de riesgos está más lejano del comportamiento digital de los miembros de las organizaciones, no es descabellado considerar que la seguridad física de las personas está vinculada con el comportamiento que tiene en línea, particularmente en sus redes sociales. Por ejemplo, si una persona revela constantemente información sobre sus hábitos y familia, puede ser presa de extorsionadores, ladrones o secuestradores, con los consecuentes impactos en seguridad y salud que estos hechos podrían conllevar.

Capítulo 4.
Iniciativas y estrategias de gestión de la seguridad

Sabiendo que en cualquier momento se puede ver afectado tu negocio por algún ataque cibernético, es necesario estructurar un plan que te garantice seguir operando en caso de que se presente un problema de este tipo.

La forma más sencilla de ejemplificar la importancia de lo anterior se asemeja al aprendizaje que la sociedad mexicana ha desarrollado ante desastres por eventos naturales, como los sismos y huracanes. Dicha respuesta se ha estructurado en tres pasos muy sencillos:

1) acciones preventivas

2) acciones de contención (reactivas) y

3) acciones de regreso a la normalidad (resiliencia).

Para minimizar el efecto de los ciberataques en el entorno empresarial (y personal), es conveniente desarrollar un plan de continuidad de negocio que considere, al menos, los siguientes aspectos:

a) Resguardar los datos vitales en otro equipo o en otras instalaciones de tu empresa

b) Evitar la concentración de datos sensibles en un solo colaborador

c) Incrementar la facilidad para restablecer tu operación en un sitio diferente al cotidiano.

Una vez que el plan ha sido determinado, cada una de las acciones preventivas contenidas en él deben ser probadas, revisando que sean funcionales y eficientes. Si al efectuar pruebas se detectan oportunidades para lograr la mejora continua de tu organización, deberán realizarse los ajustes pertinentes.

Para minimizar el efecto de los ciberataques es conveniente desarrollar un plan de continuidad de negocio que identifique los procesos más sensibles y los proteja considerando los diversos escenarios en que podrían verse afectados.

Una vez que contemos con un plan de continuidad del negocio (COB, por sus siglas en inglés), deberemos estar atentos al momento en que los escenarios de interrupción de servicios se presenten, a fin de reaccionar ágilmente y contener sus efectos. Así mismo, una vez concluida una contingencia, es importante regresar a la normalidad (resiliencia).

Es por eso que nuestro COB debe contemplar diversos pasos, tal como se describe en el siguiente esquema:

Por lo antes descrito, debemos destacar la importancia de determinar tres acciones clave:

a) el análisis del impacto al negocio por alguna interrupción
b) la determinación de los escenarios que produciría la interrupción y

c) la definición de las acciones (preventivas, de contención y de recuperación) a implementar para estar protegidos.

Definición de funciones críticas del proceso:
- Diagrama del proceso
- Variables críticas
- Máximo período de interrupción
- RTO / RPO [4]
- Picos de operación
- Impacto financiero / Operacional
- Dependencias y recursos afectados
- Riesgos

Identificación de escenarios de acuerdo a los siguientes criterios:
- Desastre / Destrucción
- Sin acceso a instalaciones
- Ausencia del personal
- Fallas tecnológicas
- Fallas en servicios

Definición de acciones para enfrentar una contingencia
- Acciones preventivas
- Acciones de contención
- Acciones de recuperación

En la actualidad existen diferentes metodologías y técnicas desarrolladas para lograr la eficiente implementación de lo aquí descrito. Te sugerimos recurrir a los organismos públicos que puedan brindarte apoyo en caso de problemas, así como a los expertos que pueden aportar su experiencia y conocimientos para prevenirlos y, en caso necesario, recuperarte del problema del modo más rápido y eficiente posible.

---

4 RTO *(Recovery Time Objective)* es el tiempo máximo que una organización puede operar sin acceso a sus aplicaciones; RPO *(Recovery Point Objective)* es el máximo volumen de datos que una organización puede perder para poder seguir operando.

Capítulo 5.
Aspectos legales

5.1. Obligaciones legales y contractuales para las empresas en materia de ciberseguridad

México cuenta con un marco normativo que abarca diversos niveles de disposiciones, que ya ofrecen un referente en términos de apoyo a las empresas en el ámbito de la seguridad cibernética.

El artículo 38 del Código de Comercio establece que "el comerciante deberá conservar, debidamente archivados, los comprobantes originales de sus operaciones, en formato impreso, o en medios electrónicos, ópticos o de cualquier otra tecnología, siempre y cuando, en estos últimos medios, se observe lo establecido en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos..., de tal manera que puedan relacionarse con dichas operaciones y con el registro que de ellas se haga, y deberá conservarlos por un plazo mínimo de diez años."

En un tenor similar, el artículo 49 del mismo ordenamiento dispone que "los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones", y que "para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta."[5]

5 http://www.diputados.gob.mx/LeyesBiblio/pdf/3_280318.pdf

México cuenta con un marco normativo que abarca diversos niveles de disposiciones, que ya ofrecen un referente en términos de apoyo a las empresas en el ámbito de la seguridad cibernética.

La norma oficial mexicana a la que se refiere el Código de Comercio es la "NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos" (la "NOM-151")[6]. Cabe mencionar que dicha norma es de observancia general para los comerciantes que conserven mensajes de datos, así como los requisitos a cumplir en la digitalización de toda o parte de la documentación relacionada con sus negocios en soporte papel a medios digitales, conforme a lo establecido en el relativamente reciente Capítulo I Bis del Código de Comercio, "De la Digitalización".

Los mecanismos de seguridad informática previstos en la NOM-151 incluyen la participación de terceros en el proceso de certificación o digitalización, así como la disposición expresa en el sentido de que toda infraestructura con que se realice la migración a soportes digitales, deberá contar con esquemas tecnológicos mínimos para realizar las acciones de digitalización, considerando tamaño, conectividad y seguridad conforme a las normas que rigen a los prestadores de servicios de certificación.

Por cuanto refiere a disposiciones contractuales, es común que los contratos incluyan cláusulas de confidencialidad de información intercambiada entre las partes. En la medida en que la información propia y de terceros sea tratada a través de sistemas de tecnologías de la información y comunicaciones (TIC), la ciberseguridad será indispensable para asegurar la confidencialidad comprometida.

6 dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017

5.2. Seguridad de los datos personales y su utilidad para crear una estrategia mínima de ciberseguridad

La obligación en materia de seguridad más notable es la que procede de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). En esencia, la LFPDPPP y su Reglamento ordenan a las empresas proteger todos los datos personales que traten con motivo de sus actividades, bajo ciertos estándares de seguridad.

Conviene hacer notar que el segmento de datos personales es sólo una porción del universo de información que tratan las empresas; sin embargo, es útil emplear los parámetros legales de seguridad impuestos al tratamiento de datos personales, para extenderlos hacia otros segmentos de información (por ejemplo, información confidencial).

La LFPDPPP impone esencialmente dos tipos de obligaciones: preventivas y correctivas. Por ello, toda empresa que actúe como responsable del tratamiento de datos personales, debe establecer medidas de seguridad administrativas, técnicas y físicas para proteger los datos personales contra daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado.

El parámetro de cuidado es el que jurídicamente se conoce como de “buen padre de familia” (paterfamilias), expresado bajo la expectativa de que la empresa responsable adopte medidas de seguridad no menores a aquellas que utilice para su propio manejo de su información. Es por ello que esta legislación puede usarse como un parámetro de lo que se recomienda para establecer medidas generales de gestión segura de toda información digital; medidas de seguridad que deben tener en cuenta el riesgo existente, las posibles consecuencias para los titulares de los datos, la sensibilidad de la información y el nivel de desarrollo tecnológico involucrado.

Existen además diversos recursos documentales publicados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos, INAI –relacionados con la protección de datos personales, aunque de nuevo son útiles para ser extendidos a otros tipos de información–, tales como:

- Recomendaciones en materia de seguridad de datos personales[7], y Guía para implementar un sistema de gestión de seguridad de datos personales[8]
- Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas[9]
- Guía para el borrado seguro de datos personales[10]
- Guía para el tratamiento de datos biométricos[11]
- Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de seguridad de datos personales[12]
- Metodología de Análisis de Riesgo BAA.[13]

7 http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013
8 http://inicio.inai.org.mx/DocumentosdeInteres/Guía_Implementación_SGSDP(-Junio2015).pdf
9 http://inicio.ifai.org.mx/nuevo/Manual%20seguridad%20MIPYMES.pdf
10 http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf
11 http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf
12 http://inicio.inai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2015).pdf
13 http://inicio.inai.org.mx/DocumentosdeInteres/Metodología_de_Análisis_de_Riesgo_BAA(Junio2015).pdf

5.3. Medidas de seguridad físicas, administrativas y tecnológicas

En términos de la LFPDPPP, para determinar las medidas de seguridad aplicables, deben considerarse al menos los siguientes factores:

- El riesgo inherente por tipo de dato personal
- La sensibilidad de los datos personales tratados
- El desarrollo tecnológico, y
- Las posibles consecuencias de una vulneración para los titulares.

Asimismo, debe tenerse en cuenta:

- El número de titulares
- Las vulnerabilidades previas ocurridas en los sistemas de tratamiento
- El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y
- Otros factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulaciones aplicables al responsable.

Aunque ciertamente el sistema de seguridad establecido en cada empresa establezca un periodo distinto para su actualización, existen casos en que dicha actualización es forzosa, por ejemplo cuando ocurran los siguientes eventos:

- Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivados de las revisiones a la política de seguridad de la empresa
- Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo
- Se vulneren los sistemas de tratamiento, o
- Exista una afectación a los datos personales distinta a las anteriores.

- En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.

5.4. Vulneraciones de seguridad

La vulneración implica cualquiera de los siguientes eventos:

- La pérdida o destrucción no autorizada de datos;
- El robo, extravío o copia no autorizada de datos;
- El uso, acceso o tratamiento no autorizado de datos;
- El daño, la alteración o modificación no autorizada de datos.

Por extensión, es posible decir que existe una vulneración de seguridad cuando cualquiera de estos eventos ocurre en relación con información protegida.

Es por ello que en materia de protección de datos personales existe la obligación de notificar las vulneraciones.

En efecto, la LFPDPPP prevé que la empresa responsable debe informar al titular de los datos personales, las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que: (i) ocurrió la vulneración y (ii) haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y (iii) sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

Este estándar de protección es relevante, pues la obligación de notificar al titular no surge de cualquier evento, sino únicamente de aquel que afecte "de forma significativa" los derechos patrimoniales o morales del titular. Aunque ciertamente se trata de un estándar subjetivo, es clara la intención de la ley en el sentido de que, en cuanto a su obligatoriedad, las vulneraciones de seguridad graves están sujetas al requisito forzoso de notificación, lo cual no quiere decir que conforme a una buena práctica, una empresa notifique a los titulares cualquiera otro tipo de vulneración, aun si ésta no

hubiera sido grave, ni hubiera puesto en peligro de forma significativa los derechos patrimoniales o morales del titular.

Cabe destacar que la ley mexicana no requiere la notificación al INAI –que es el órgano regulador en materia de protección de datos personales–, sino directamente a los titulares de los datos personales involucrados.

La notificación que la empresa responsable dirija al titular de los datos personales, debe incluir lo siguiente:

- La naturaleza del incidente;
- Los datos personales comprometidos;
- Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
- Las acciones correctivas realizadas de forma inmediata, y
- Los medios donde el titular puede obtener más información al respecto.

5.5. Datos en la nube

El artículo 52 del Reglamento de la LFPDPPP dispone que para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación. Por ello, una empresa sólo podrá utilizar aquellos servicios en los que el proveedor de servicios en la nube cumpla con los siguientes requisitos mínimos:

- Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LFPDPPP y su Reglamento;
- Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
- Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y

- Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

Asimismo, el proveedor de servicios en la nube debe contar con mecanismos, al menos, para:

- Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
- Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
- Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;
- Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, e
- Impedir 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, informar de ese hecho al responsable.

Conclusiones

De acuerdo a la encuesta global de software publicada por la Business Software Alliance (BSA) en 2017, en el curso de un año se descubrieron 430 millones de unidades de software malicioso y las organizaciones sufrieron algún tipo de ataque cibernético cada siete minutos. La tendencia va en aumento y las alertas podrían encenderse por muchos motivos.

No obstante, también es verdad que los usuarios –sea a nivel organizacional que personal– han incrementado su conciencia sobre los riesgos y han comenzado a tomar medidas preventivas cada vez más inteligentes, tendentes a resguardar la seguridad de su información, bienes, reputación, productividad y continuidad de sus operaciones.

La atención a los riesgos más comunes no requiere siquiera de fuertes inversiones, sino de una capacitación simple y de tomar decisiones correctas en cuanto al cuidado de nuestros equipos de cómputo, el licenciamiento legal del software que utilizamos, el modo en que operamos en internet y la interrelación que establecemos entre información digital y vida cotidiana.

Debemos distinguir las medidas físicas y las medidas administrativas de ciberseguridad, con independencia de que en ellas se opere o no con el concurso de la tecnología informática, además de las medidas propiamente técnicas o tecnológicas.

Las medidas físicas de seguridad son las acciones y mecanismos destinados a:

- Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;
- Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;

- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y
- Garantizar la eliminación de datos de forma segura.

Las medidas administrativas son acciones y mecanismos cuyo fin es:

- Establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional;
- La identificación y clasificación de la información, así como
- La concienciación, formación y capacitación del personal en materia de protección de datos personales.

Usualmente, este tipo de medidas se reflejan en políticas y procesos de cumplimiento obligatorio dentro de una organización. A este rubro pertenecen, por ejemplo, las políticas de fotocopiado, de "escritorios limpios", de conservación y destrucción de documentos, de manejo y protección de información confidencial, de secretos comerciales, etc.

Finalmente, las medidas técnicas o tecnológicas son esencialmente medidas de ciberseguridad en toda la extensión de la palabra. Se trata de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar:

- Que el acceso a las bases de datos lógicas y a la información en formato lógico sea por usuarios identificados y autorizados;
- Que dicho acceso sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- Que se indiquen las acciones apropiadas para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y
- Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

En este contexto, un *checklist* básico de seguridad de información y datos personales, podría verse de la siguiente manera:

1. Elaborar un inventario de la información que deba estar sujeta a un estándar de confidencialidad y datos personales, así como de los sistemas de tratamiento;
2. Determinar las funciones y obligaciones de las personas que traten información confidencial y datos personales, y asignar responsables dentro de la organización, tanto para la protección de datos personales, como para la seguridad de la información;
3. Identificar y establecer medidas de seguridad físicas, administrativas y técnicas, idóneas para proteger la información confidencial y datos personales de posibles vulneraciones;
4. Contar con análisis de riesgos de información confidencial y datos personales, que identifiquen los peligros y estimen los riesgos a los que están sujetos;
5. Realizar un "análisis de brecha", que consiste en ubicar la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la correcta protección de la información confidencial y los datos personales;
6. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;
7. Llevar a cabo revisiones o auditorías periódicas, tanto internas como externas;
8. Capacitar al personal en materia de preservación de información confidencial, y protección de datos personales;
9. Contar con procedimientos de atención inmediata, y en su caso notificación, de vulneraciones de seguridad, y
10. Asegurarse de que los proveedores de servicios en la nube efectivamente cumplen con los principios afines a la Ley y el Reglamento.

Si la naturaleza de tu organización así lo requiere, te sugerimos contactar a un experto para que las brechas de ciberseguridad de tu compañía no se amplíen y los posibles ataques o amenazas por riesgos naturales que ya percibes, no afecten la continuidad y éxito de tu operación.

Referencias útiles

Contacto con organismos públicos

Para reportar oportunamente incidentes de seguridad de la información ante las autoridades (incluyendo policía, bomberos o protección civil).

CERT-MX	· Policía Cibernética de la Comisión Nacional de Seguridad · Centro Nacional de Respuesta a Incidentes Cibernéticos de México · Policía Federal / División Científica Twitter: @CEAC_CNS Correo electrónico: ceac@cns.gob.mx Teléfono: 088 (55) 1103 6000 ext. 29247
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales Twitter: @INAImexico Correo electrónico: atencion@inai.org.mx Teléfono: (55) 5004 2400 ext. 2480
SANS	Entrenamiento en seguridad de la información y certificaciones en seguridad Twitter: @SANSInstitute Correo electrónico: info@sans.org Teléfono: (301) 654 7267

CFE	· Interrupción y fallas del servicio de energía eléctrica Teléfono: 071
Emergencias	· Emergencias médicas · Emergencias de protección civil · Emergencias de servicios públicos · Emergencias de seguridad Teléfono: 911

Contacto con empresas

AMITI integra a una gran cantidad de empresas especializadas en temas de seguridad cibernética y protección digital. Si así lo requieres, no dudes en consultarlas.

Capa 8 ®	Es una empresa mexicana de jóvenes apasionados por la seguridad de la información. Nos enfocamos en la "capa" más importante de su organización y el eslabón más débil: la gente. Nuestra propuesta de valor es asegurar la plataforma digital de su compañía, así como generar usuarios más conscientes de los riesgos y amenazas en el ciberespacio. Página de internet: www.capa8.com Correo electrónico: contacto@capa8.com Teléfono: (55) 9183 9446
CMP	Compañía Mexicana de Procesamiento, CMP, ofrece *outsourcing* de procesos operativos para el sector financiero, con cobertura nacional. Operamos los 365 días del año bajo el modelo de BPO *(Business Process Outsourcing)*. Contamos con certificaciones ISO 9001:2015 e ISO 27001:2013, aportando soluciones seguras, con economías de escala y proba-

dos modelos de continuidad operativa.
Página de internet: www.cmpnet.mx
Correo electrónico: contacto@cmpnet.com.mx
Teléfono: (55) 5132 5048

Konesh Soluciones

Konesh Soluciones (Aurorian, S.A. de C.V.) es una empresa 100% mexicana formada por expertos en integración y desarrollo de soluciones tecnológicas, servicios de consultoría y seguridad de la información, especializados en facturación electrónica como Proveedor Autorizado de Certificación, colaboración, *big data*, gestión documental, B2B, *e-commerce*, gestión del cambio, inteligencia de negocios e implementación ISO/IEC 27001.
Página de internet: www.konesh.com.mx
Correo electrónico: acastro@konesh.com.mx
Teléfono: (55) 5264 9000

NYCE

Normalización y Certificación NYCE, S.C. es un organismo líder en evaluación de la conformidad –certificación, verificación y dictamen– en materia de electrónica, eléctrica, telecomunicaciones, tecnologías de la información, seguridad de la información, protección de datos, calidad, medio ambiente, antisoborno y continuidad de negocios, así como en normalización para estos y otros sectores. A través de diversas herramientas, NYCE logra respaldar y fortalecer a las empresas brindando seguridad y confianza, tanto a la industria como a los consumidores lo que consolida la armonía de estos dentro de los mercados en que participa.
Página de internet: www.nyce.org.mx
Correo electrónico: nyce@nyce.org.mx
Teléfono: (55) 5395 0777

S21sec

Es una multinacional especializada al 100% en ciberseguridad. S21sec ofrece soluciones integrales de protección, prevención y ciber-inteligencia ante incidentes a nivel mundial las 24 horas del día, 365 días del año.
Página de internet: http//:www.s21sec.com
Correo electrónico: info@s21sec.com
Teléfono: (55) 7822 0127, 7822 0129

SAP

Es líder en el mercado mundial de aplicaciones de software corporativo (aplicaciones y soluciones de movilidad), que ayuda al sector privado y público a que el mundo funcione mejor y mejorar la vida de las personas, solucionando los problemas más complejos que presenta el mundo actual. El portafolio de SAP está enfocado en el mercado de software y servicios de tecnologías de la información, brindando aplicaciones empresariales, aplicaciones analíticas y bases de datos, así como servicios relacionados y soporte.
Página de internet: www.sap.com
Correo electrónico: adriana.servin@sap.com
Teléfono: (55) 1250 7500

Asociación Mexicana de la Industria de
Tecnologías de Información, A.C.

Laguna de Términos 221, Torre B, int. 806
Col. Granada, 11520, Miguel Hidalgo, Ciudad de México

La Asociación Mexicana de la Industria de Tecnologías de Información ofrece a sus socios un foro en donde crear sinergias y elaborar propuestas y proyectos en beneficio de la industria y del país. AMITI cuenta con la representatividad necesaria para interactuar con el resto de la industria, la administración pública, la academia y organismos empresariales nacionales y extranjeros afines.

Con el objetivo de acelerar la transformación digital de México, AMITI ha establecido convenios de colaboración y relaciones con universidades, embajadas, dependencias de gobierno, asociaciones y cámaras, así como con otras instituciones y organismos.

El Comité de Ciberseguridad de AMITI, liderado por S21 SEC, tiene por objetivo que las organizaciones desarrollen un nivel de inteligencia corporativa capaz de identificar riesgos y debilidades en su infraestructura y sistemas informáticos, de tal modo que sean capaces de cerrar las brechas que representen mayores amenazas y así puedan aprovechar toda su información con seguridad.

AMITI