ENJOY SAFER TECHNOLOGY™

GUÍA DEL

Empleado Seguro

Introducción

Año a año, la Seguridad de la Información en una organización adquiere cada vez más relevancia y, en condiciones ideales, es responsabilidad propiamente del área de Seguridad- en empresas grandes-, aunque en función de las características de cada organización, puede depender de otras áreas, como TI u Operaciones.

En un ambiente donde diariamente se identifican nuevas amenazas informáticas y vulnerabilidades los riesgos de seguridad son cada vez más dinámicos.

Por ello, independientemente del área de la que dependa, proteger la información es una tarea que involucra a toda la empresa, puesto que todos los empleados interactúan con ella.

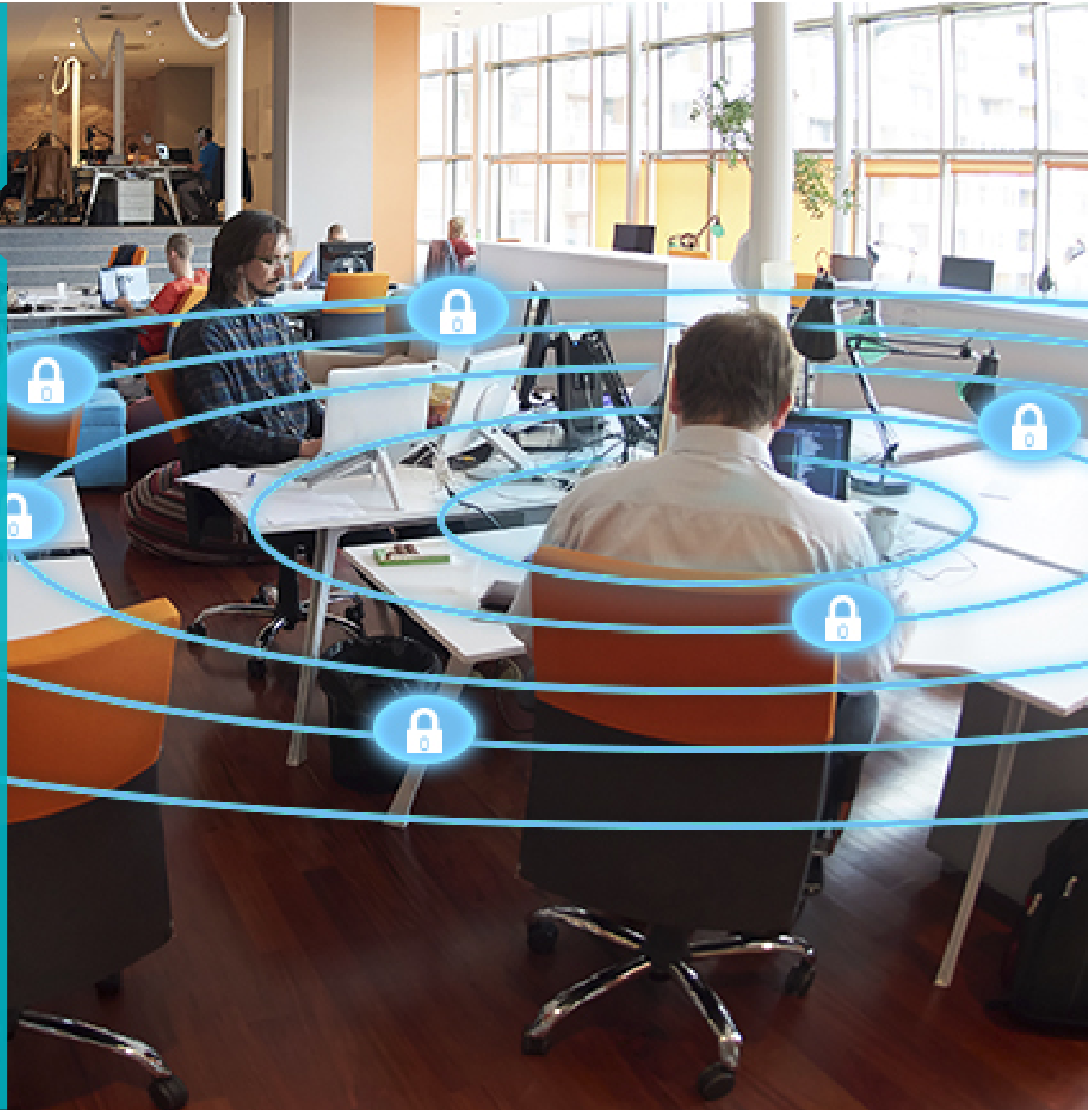
Índice

Empleado Seguro

Un empleado seguro es aquel que sabe administrar y utilizar los recursos de la empresa de manera consciente y responsable.

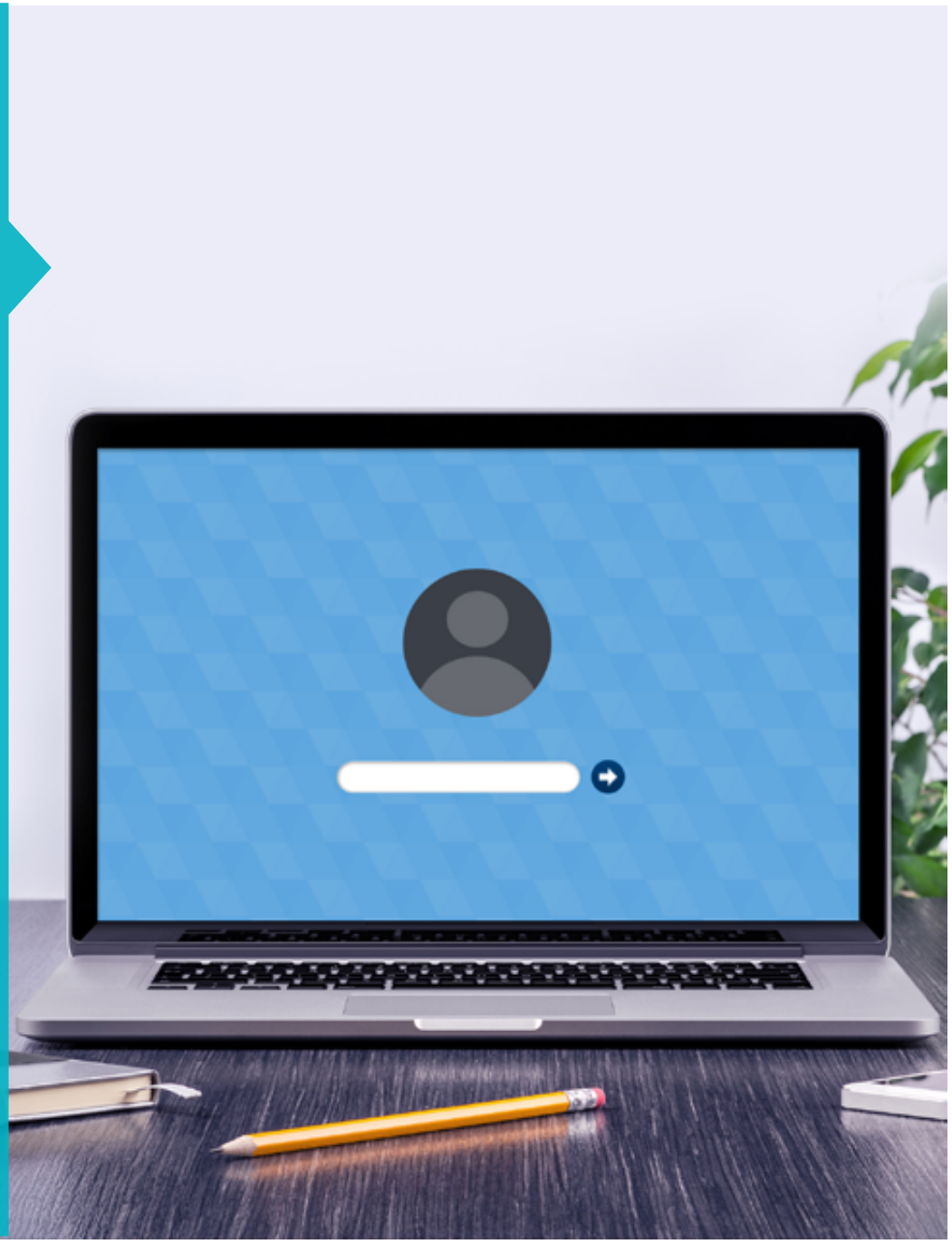
Por ello, esta guía tiene como propósito proporcionar la información necesaria para que cada integrante de una organización pueda convertirse en un empleado seguro y atento a las amenazas informáticas para no poner en riesgo el negocio.

En este contexto, se abordarán las problemáticas más comunes, las principales amenazas y las mejores prácticas para el manejo de información sensible en las empresas.



Seguridad de la Información: definiciones y problemáticas

- Seguridad
- Información
- Seguridad de la Información
- Las propiedades de la información
- Vulnerabilidad, amenaza y ataque
- Riesgo, probabilidad e impacto



Seguridad de la Información: definiciones y problemáticas

Seguridad

De acuerdo con la Real Academia Española, "seguridad" se define como "libre o exento de todo peligro, daño o riesgo", sin embargo, se trata de una condición ideal, ya que en la realidad no es posible tener la certeza de que se pueden evitar todos los peligros.

Por esta razón, el propósito de la seguridad en todos sus ámbitos de aplicación es **reducir riesgos** hasta un nivel que sea aceptable. En un sentido más amplio, la seguridad también comprende todas las actividades que tiene como fin proteger una cosa o una persona de algún de tipo de peligro.

Información

La información es un **activo** que, al igual que otros activos importantes, debe ser protegida. En las empresas es esencial para la toma de decisiones, el logro de los objetivos y el cumplimiento de su misión.

La información puede encontrarse de diferentes maneras y formatos: digital, escrita, impresa y/o no representada, como pueden ser ideas o el conocimiento de las personas. Más allá del formato en el que se encuentra la información, es necesario implementar medidas de seguridad para protegerla en función a su criticidad, sensibilidad e importancia.

Seguridad de la Información

A través de la combinación de los conceptos anteriores, surge la Seguridad de la Información, una disciplina que se sustenta con metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, con la idea de proteger a la información en todos sus formatos.

La seguridad busca preservar la integridad, disponibilidad y confidencialidad de la información de la empresa, con un propósito de mayor alcance aún: proteger el negocio.

Las propiedades de la información

- **Confidencialidad:** que la información sea accesible únicamente por los individuos, entidades o procesos que poseen los privilegios y la autorización para hacerlo.
  Por ejemplo, que un usuario no pueda acceder a la base de datos de un servidor web.

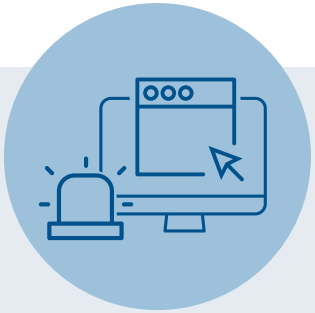
- **Integridad:** que la información mantenga su exactitud y completitud.
  Por ejemplo, que un atacante no pueda modificar los precios de venta de un sitio web.

- **Disponibilidad:** que la información sea accesible y utilizable cuando una entidad lo requiera.
  Por ejemplo, evitar problemas en un servidor que hicieran que se apague.

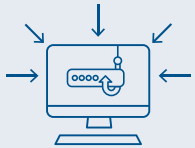
Vulnerabilidad, amenaza y ataque

La Seguridad de la Información también implica la consideración de una amplia gama de riesgos, ya que continuamente son los obstáculos que frenan a las organizaciones en la búsqueda y alcance de sus objetivos de negocio.

Por lo tanto, se intenta minimizar el impacto que pudieran generar los incidentes de seguridad relacionados con las vulnerabilidades (agentes internos) y amenazas (agentes externos). Estos riesgos también pueden materializarse debido a situaciones intencionales o accidentales.



INTERNO



EXTERNO

INTENCIONAL

Un empleado disgustado destruye un documento e información importante.

Un atacante accede a una base de datos del sitio web de la empresas de manera externa.

ACCIDENTAL

Un empleado pierde un dispositivo USB donde transporta información confidencial de la empresa.

El aumento en las visitas a un sitio web excede la capacidad de procesamiento del servidor y se bloquea.

Como se vio anteriormente, los problemas de seguridad se relacionan con los conceptos de vulnerabilidad, amenaza y ataque:

- **Vulnerabilidad:** debilidad en un activo o control que puede ser aprovechada por uno o más agentes externos.
- **Amenaza:** causa potencial de un incidente no deseado que puede resultar en daños a un sistema u organización.
- **Ataque:** intento de destruir, exponer, alterar, inutilizar, robar, obtener acceso no autorizado o hacer uso indebido de los activos.

Los ataques que buscan comprometer un sistema de información y los activos se clasifican en cuatro categorías según su manifestación: intercepción, modificación, interrupción y fabricación.

La intercepción atenta contra la confidencialidad; la modificación lo hace contra la integridad; mientras que la interrupción hace lo propio con la disponibilidad.

Los ataques de fabricación buscan atentar contra la autenticidad de quienes interactúan con la información.

Riesgo, probabilidad e impacto

A través de la aplicación de medidas de seguridad se intenta mitigar riesgos, de manera que la realización de un ataque sea impráctica, no viable o con las consecuencias mínimas aceptables.

Por lo tanto, la idea inicial de seguridad vuelve a tomar relevancia dado que, aunque no se pueda garantizar por completo, los riesgos deben ser tratados y reducidos hasta un nivel que no representen consecuencias considerables.

Para la Seguridad de la Información, los riesgos están asociados a la causa potencial de que una amenaza pueda explotar una o más vulnerabilidades de un activo o grupo de ellos, teniendo como consecuencia un daño a la organización.

Los riesgos generalmente se expresan mediante la combinación de la **probabilidad** de que un evento no deseado suceda y sus consecuencias o **impacto.** Por este motivo, las medidas de seguridad están orientadas a reducir alguna de estas dos variables o, en el mejor de los casos, ambas.

Amenazas que atentan contra la información

- Ingeniería Social
- Malware
- Phishing
- Robo y exposición de información

Amenazas que atentan contra la información

Ingeniería Social

Es la utilización de habilidades sociales para manipular el accionar de una persona. A partir de estas técnicas, los cibercriminales engañan a los usuarios para comprometer la seguridad de una empresa.

Algunos ejemplos son: correos fraudulentos que solicitan información confidencial, falsos llamados telefónicos o propagación de códigos maliciosos en las redes sociales simulando ser aplicaciones benévolas. También suelen utilizarse temas de actualidad o noticias falsas para aumentar la probabilidad de éxito de estos ataques.

Recientemente, se ha visto un incremento de ataques dirigidos a las organizaciones para infiltrarse en la infraestructura tecnológica y acceder a información sensible que, en algunos casos, es expuesta públicamente.

Un empleado seguro identifica los principales ataques relacionados con Técnicas de Ingeniería Social.

Un empleado seguro conoce los diferentes tipos de códigos maliciosos y aplica buenas prácticas para evitar infecciones.

Malware

El malware (acrónimo de malicious software) es uno de los ataques más comunes de la actualidad. Básicamente, se trata de archivos con fines dañinos que, al infectar una computadora, pueden realizar diversas acciones como robar información, controlar el sistema y/o secuestrar datos o, incluso, los sistemas enteros.

Estos códigos maliciosos hacen que los equipos de seguridad se pregunten cosas como: ¿qué sucedería si toda la información que se almacena en un equipo es secuestrada?, ¿cómo afectaría a la productividad?, ¿cuánto tiempo se debería dedicar a solucionar el inconveniente?, entre otras.

Sin duda, estas situaciones afectan directamente el rendimiento de la empresa, por ende, cuestan dinero.

Phishing

Se trata de un ataque que involucra técnicas de Ingeniería Social para adquirir fraudulentamente información personal y/o confidencial, como contraseñas o detalles de tarjetas de crédito, de las víctimas.

Dentro de la organizaciones, suelen realizarse ataques dirigidos a través del denominado spear phishing, es decir, ataques diseñados específicamente para aumentar la probabilidad de infección en una empresa.

Para efectuar el engaño, el estafador (phisher) simula ser una persona o empresa de confianza (generalmente entidades bancarias) a través de una aparente comunicación legítima (como correos electrónicos, sistemas de mensajería instantánea o incluso llamadas telefónicas) y le solicita a la víctima información sensible.

Un empleado seguro reconoce los correos y mensajes fraudulentos que buscan robar información sensible.

Un empleado seguro protege la información almacenada, procesada y transmitida para evitar la fuga de información.

Robo y exposición de información

Uno de los peores escenarios para una empresa es el robo de información sensible cuya exposición puede afectar al negocio. Cabe destacar que el incidente puede ser tanto deliberado como accidental. Asimismo, el robo de información no aplica solo a medios digitales, sino también a los físicos (archiveros, legajos, etc.).

El impacto del robo de información aumenta si los datos son expuestos, ya que no solo se afecta a la organización, sino también a los usuarios de los cuales se conocen públicamente sus datos. Por ello, todos los integrantes de la empresa deben cuidar la información y aplicar las medidas de protección pertinentes.

Prácticas de gestión y controles tecnológicos

- Políticas de seguridad
- Clasificación de la información
- Herramientas de seguridad

Prácticas de gestión y controles tecnológicos

Políticas de seguridad

Las políticas de seguridad son los documentos que respaldan los compromisos adquiridos por los miembros de la organización, o bien las normas que determinan su conducta en relación a la protección de la información y otros activos.

Es ideal que toda empresa cuente con una política de seguridad, que sea conocida por todos los empleados.

Cuando este documento es firmado, la persona certifica que entiende y acata los lineamientos; además se compromete a cumplir todas las normativas de seguridad definidas por la organización.

Un empleado seguro lee, entiende y acata las políticas de seguridad de la organización.

Clasificación de la información

Un aspecto relevante dentro de las organizaciones se relaciona con la clasificación de la información, para definir cuál resulta más relevante para los fines que persigue el negocio.

En este sentido, las medidas de protección se aplican en función de la importancia y criticidad de los datos.

Cuando el costo de los controles de seguridad sobrepasa el valor que se le asigna a la información y otros recursos críticos, resulta más conveniente repensar si estos controles son los adecuados.

Un empleado seguro identifica la información sensible y en consecuencia la protege de acuerdo con los criterios definidos.

Herramientas de seguridad

Los controles tecnológicos son un elemento básico de la Seguridad Informática en las empresas. Los más comunes son:

- **Antivirus:** protege proactivamente los equipos y su información contra distintos ataques de códigos maliciosos nuevos o desconocidos, desde virus, gusanos y troyanos hasta spyware, ransomware y botnets.
- **Firewall:** puede estar integrado con la solución antivirus y protege al equipo de las conexiones entrantes y salientes a Internet que se pueden utilizar en ataques externos, como también las conexiones que un equipo infectado quiera realizar hacia el exterior.
- **Antispam:** software que también puede integrarse con un antivirus o con el cliente de correo y que permite filtrar correos masivo e indeseados en su bandeja de entrada corporativa.

No obstante, hay otras herramientas que se suelen implementar en el perímetro de la red o directamente en los servidores, como soluciones de respaldo, IDS, IPS, DLP, firewall perimetral, gestión de parches, entre otras.

Un empleado seguro conoce y utiliza de manera adecuada las soluciones tecnológicas de seguridad de la empresa.

Buenas prácticas aplicadas al uso de la tecnología

- Contraseñas
- Correo electrónico
- Dispositivos móviles
- Redes Sociales
- Redes inalámbricas

Buenas prácticas aplicadas al uso de la tecnología

Contraseñas

En la actualidad, las contraseñas continúan siendo el principal método para la autenticación de los usuarios en los sistemas y plataformas, por lo que los integrantes de una compañía suelen tener varias contraseñas para los sistemas internos que se utilicen.

Por ello, una contraseña fuerte puede evitar el acceso a información confidencial o a un sistema por parte de un atacante o un código malicioso. Con esto en mente, es importante que las contraseñas sean fáciles de recordar y difíciles de adivinar.

En este sentido, es recomendable la utilización de un software para la gestión de contraseñas, así como el uso de diferentes claves para servicios corporativos distintos. Del mismo modo, soluciones de doble autenticación reducen de manera considerable los riesgos de seguridad asociados a la forma de verificar la identidad de los usuarios.

Un empleado seguro utiliza contraseñas distintas y fuertes para servicios diferentes, y utiliza 2FA.

Un empleado seguro evita acceder a enlaces sospechosos o descargar archivos adjuntos de remitentes desconocidos.

Correo electrónico

El uso masivo del correo electrónico lo convirtió en un elemento utilizado por los cibercriminales con fines maliciosos, como hoax (noticias falsas), scams (estafas), spam (correos masivos e indeseados), phishing o la propagación de malware.

Existen situaciones en donde, para registrarse en algún servicio, o incluso en Redes Sociales, se requiere el ingreso de una dirección de correo. Las direcciones corporativas se utilizan como fuente de comunicación de la empresa y en la medida de lo posible se debe evitar su exposición en Internet.

En el caso de que se utilice para registrarse en un servicio, puede existir cierta exposición de esa dirección y, de esa manera, aumentan las posibilidades de sufrir algún ataque.

Dispositivos móviles

La incorporación de los smartphones a las empresas permiten el acceso a la información en todo momento y desde cualquier lugar. No obstante, transportar información sensible en dispositivos móviles implica un riesgo, ya que puede convertirse en una vía para la fuga o robo de información, así como también sufrir infecciones con malware para móviles.

Para minimizar estos riesgos, es posible utilizar herramientas de control de dispositivos MDM (Mobile Device Management) que eviten la instalación de aplicaciones no permitidas, aplicar políticas de seguridad o realizar el borrado seguro de información de manera remota.

Asimismo, las buenas prácticas incluyen acciones como el uso de un código de seguridad para el bloqueo, el cifrado de la información y la utilización de soluciones antimalware.

Un empleado seguro utiliza su dispositivo móvil de manera responsable y segura para los fines de la empresa.

Un empleado seguro utiliza las Redes Sociales y herramientas de comunicación de manera responsable y con filtros de privacidad.

Redes Sociales

Las Redes Sociales son utilizadas por los cibercriminales como un vector de propagación de amenazas informáticas, especialmente a través de enlaces que dirigen a sitios desconocidos, envío de archivos maliciosos o mensajes falsos.

En este sentido, es recomendable que las organizaciones supervisen el uso de estos servicios en sus oficinas. En ocasiones no pueden ser bloqueados, ya que se utilizan para labores específicas (como el Community Management), por lo que es necesario tener las medidas preventivas necesarias para evitar que amenazas informáticas se distribuyan por estas vías.

Las configuraciones adecuadas de seguridad y privacidad de los perfiles también son prácticas que evitan la divulgación o exposición de información.

Redes inalámbricas

Es común utilizar equipos portátiles de trabajo para conectarse a redes WiFi públicas, como por ejemplo, redes en cafés o aeropuertos. En estos casos debe considerarse que la seguridad está ligada a los controles existentes en dicha red y que, en muchos casos, son inexistentes, tales como la ausencia de una contraseña para realizar la conexión o el uso de protocolos seguros. Es por esto que no es recomendable realizar conexiones sensibles, como acceder al correo corporativo, ya que la red puede estar expuesta y la información sin ningún tipo de cifrado, por lo que muchos de los datos pueden ser visibles por terceros no autorizados conectados a la misma red.

En el caso de que se utilice un equipo público para conectarse, no se debe acceder a archivos con información confidencial de forma local, ya que pueden quedar accesibles en ese dispositivo y ser vistos por cualquier persona que lo utilice en el futuro.

Un empleado seguro emplea conexiones WiFi seguras. Cuando no es posible, utiliza prácticas como el cifrado de comunicaciones o conexiones VPN.

Prácticas del empleado seguro en su lugar de trabajo

Prácticas del empleado seguro en su lugar de trabajo

Seguridad en su lugar de trabajo

Además de las políticas de seguridad que los miembros de la organización deben cumplir, existen otras prácticas que contribuyen a aumentar la seguridad.

Entre ellas se incluyen:

- El empleado tiene la responsabilidad de utilizar adecuadamente todos los activos de la organización, como también de proteger aquellos que estén bajo su resguardo.
- Se deben bloquear los equipos cuando se los desatiende, incluso cuando se deja por pocos minutos el puesto de trabajo, para evitar la extracción o lectura de información por parte de terceros no autorizados.
- Se debe mantener el escritorio limpio, tanto en la vida física como en los sistemas operativos, para no divulgar información sensible accidentalmente.
- Cuando se sospecha que un sistema, o incluso la red completa de la empresa, ha sido comprometido, se debe dar aviso al departamento de seguridad o de TI de manera inmediata.
- Más aun, cuando un incidente efectivamente sucede es indispensable avisar rápidamente al departamento pertinente.

Un empleado seguro aplica buenas prácticas en su lugar de trabajo y notifica inmediatamente ante cualquier sospecha de un incidente de seguridad.

11 Prácticas del empleado seguro en su lugar de trabajo

- **Políticas de seguridad:** leer, entender y acatar las políticas de seguridad de la organización.
- **Clasificación de información:** identificar la información sensible y aplicar la medidas de protección designadas por la organización.
- **Herramientas de seguridad:** utilizar los controles de seguridad tecnológicos, como antivirus, firewall o antispam, de manera adecuada para mitigar los riesgos de incidentes.
- **Contraseñas:** utilizar contraseñas complejas y de más de diez caracteres que sean diferentes para distintos servicios o sistemas de la organización. En caso de ser necesario, emplear un gestor de contraseñas y mecanismos de doble autenticación.
- **Información personal:** evitar compartir información con entidades que no están autorizadas para acceder a la misma.
- **Actualizaciones de seguridad:** actualizar el software y aplicar parches de seguridad para la evitar la explotación de vulnerabilidades.
- **Eliminación segura de información:** destruir documentos impresos con información sensible antes de desecharlos y eliminar información digital sensible con las herramientas adecuadas.
- **Bloqueo de sesión y escritorio limpio:** bloquear el sistema cuando se encuentre desatendido y mantener limpio el escritorio físico y del sistema operativo para no exponer información privada a terceros no autorizados.
- **Correo electrónico:** revisar el correo recibido y evitar acceder a enlaces sospechosos o descargar archivos adjuntos de remitentes desconocidos.
- **Dispositivos móviles:** utilizar el dispositivo móvil corporativo solo con fines laborales y aplicando tecnologías MDM.
- **Incidentes de seguridad:** reportar inmediatamente eventos sospechosos o incidentes de seguridad que puedan comprometer la información sensible y otros activos críticos de la organización.

Prácticas del empleado seguro en su hogar

Prácticas del empleado seguro en su hogar

Del trabajo al hogar y viceversa

Desde hace años, la portabilidad y los beneficios como el Home Office le permiten a los empleados trabajar desde sus casas. Si bien esto es muy cómodo y puede aumentar la productividad, es necesario tomar recaudos dado que una red hogareña puede no estar correctamente configurada y/o controlada, como sucede en la oficina, lo que podría derivar en infecciones y/o fugas de información. Por ello, es necesario aplicar medidas adicionales:

- Contar con un software antivirus en la computadora personal para estar protegidos contra potenciales amenazas.
- Tener el sistema operativo actualizado para contar con todos los parches de seguridad. De igual manera, se debe actualizar el resto del software y las aplicaciones.
- Acatar las políticas de seguridad de la organización, aun cuando el empleado se encuentre fuera del ámbito laboral.

Además, cuando se lleva información y documentación de importancia para trabajar fuera de la organización, se debe tener especial cuidado en lo que respecta al robo, pérdida o exposición de los datos en lugares públicos o en el mismo hogar. Tales documentos deben ser manipulados teniendo en cuenta el nivel de confidencialidad que requieren.

En caso de que se utilicen dispositivos de almacenamiento USB, siempre es necesario realizar un análisis contra malware al momento de insertarlos en el equipo (tanto en el corporativo como en el personal), así como utilizar medidas de seguridad adicionales, como el cifrado de datos.

Un empleado seguro protege la información de la empresa incluso fuera del ámbito organizacional.

Prácticas del empleado seguro en su hogar

- **Políticas de seguridad:** acatar las políticas de seguridad de la organización aun estando fuera de la oficina.
- **Dispositivos móviles:** proteger los dispositivos móviles utilizados en el hogar para acceder a la red o información corporativa.
- **Soluciones contra malware:** si se emplea una computadora personal se deben utilizar, en la medida de los posible, los mismos controles de seguridad descritos en las políticas de seguridad de la organización.
- **Actualizaciones de seguridad:** las actualizaciones no solo incluyen mejoras en las funcionalidades, sino también parches de seguridad que corrigen fallas en los programas.

Conclusiones

Independientemente de las labores de los integrantes de la organización o el nivel jerárquico que posean, proteger la información sensible de la empresa es una tarea fundamental que contribuye a mantener la continuidad de las operaciones y lograr los objetivos de negocio.

Cualquier divulgación, modificación o interrupción de información crítica debido a una infección con malware u otras amenazas informáticas, impacta directamente en la imagen de la empresa y en la confianza de los clientes con la misma.

Entender la seguridad corporativa, aplicar controles tecnológicos y de gestión, seguir las buenas prácticas, mantener a los usuarios educados y conscientes en temas de Seguridad de la Información, otorga un valor agregado a la organización.

Todos estos elementos en conjunto contribuyen a mantener la confidencialidad, integridad y disponibilidad de la información, además de perseguir un propósito de mayor alcance e importancia: proteger el negocio.


ENJOY SAFER
TECHNOLOGY™