Guía del empleado seguro

INTRODUCCIÓN

La seguridad de la información en una empresa es responsabilidad del departamento de IT (tecnologías de la información) o del propio área de Seguridad de la Información (por lo general, en empresas más grandes). Sin embargo, es una tarea de toda la compañía cuidar la información, ya que en las empresas actuales, todos los integrantes trabajan de una u otra forma con datos e información; y por lo tanto todos ellos podrían generar que ocurra un incidente sobre estos que altere la seguridad.

En ese contexto, esta guía pretende ayudar a los empleados de las organizaciones a cuidar y bregar por la seguridad de la información en la organización, a partir de una comprensión de la problemática, una descripción de las principales amenazas y, finalmente, una enumeración de las buenas prácticas para tal fin.

Un empleado seguro es aquel que cuenta con la educación para administrar y utilizar los recursos de la empresa de manera segura y eficiente. La presente guía lo ayudará a convertirse en un empleado seguro, ayudando y colaborando con su organización y el bienestar en su puesto de trabajo.

La Seguridad de la Información se encarga de garantizar la integridad, disponibilidad y confidencialidad de la información de la empresa en búsqueda de cuidar el negocio.

CONFIDENCIALIDAD

La confidencialidad de la información es la necesidad de que esta solo sea conocida por personas autorizadas.

Por ejemplo, si un usuario cualquier pudiera acceder a la base de datos de un servidor web, o cualquier empleado pudiera conocer la información contable de la empresa, se estaría vulnerando la confidencialidad de la información.

INTEGRIDAD

La integridad de la información es la característica que hace que su contenido permanezca inalterado, a menos que sea modificado por personal autorizado.

Por ejemplo, si un atacante pudiera modificar los precios de venta de un sitio web, o un empleado ajeno al área de ventas pudiera hacerlo, se estaría vulnerando la integridad de la información.

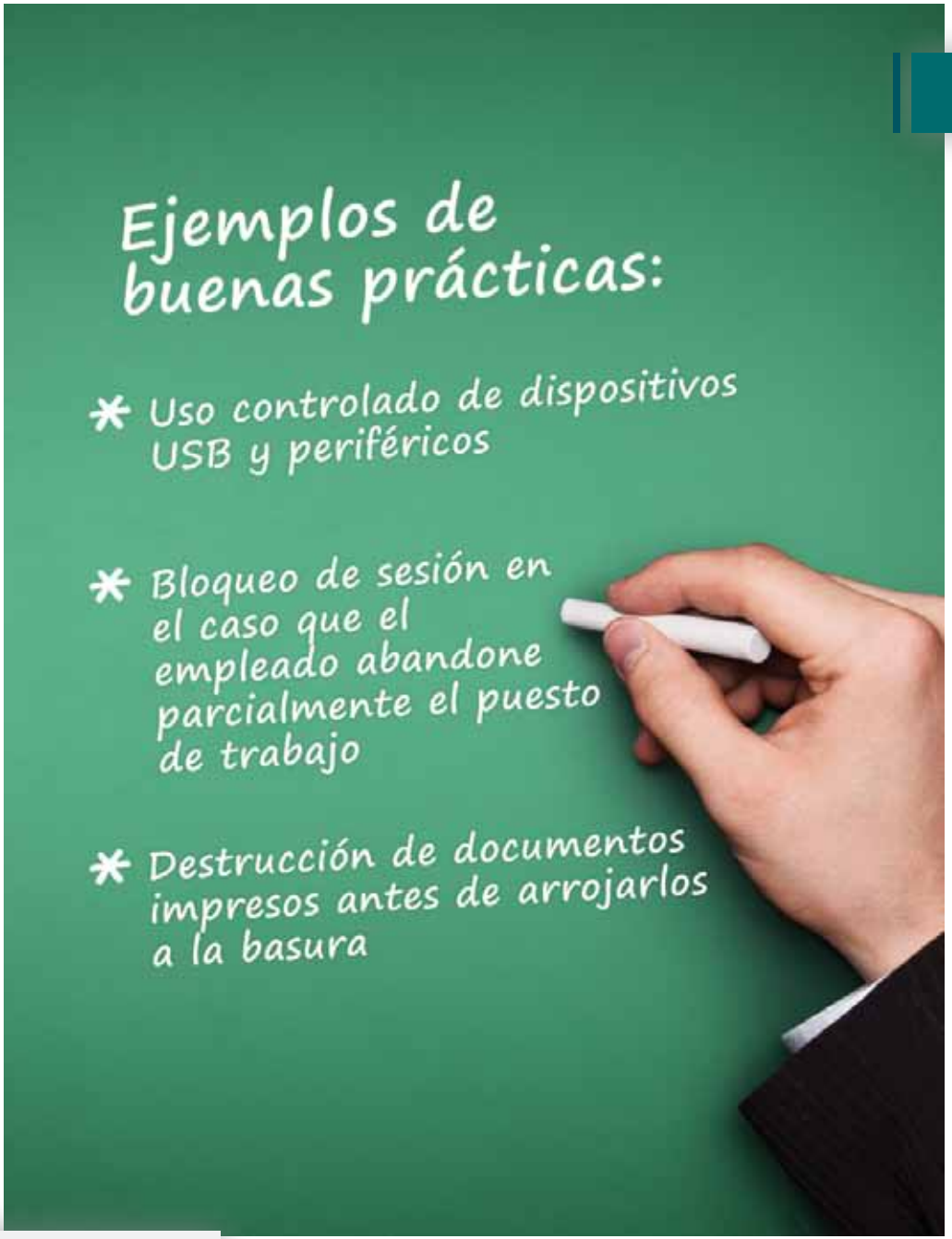
DISPONIBILIDAD

La disponibilidad de la información es su capacidad de estar siempre disponible en el momento que la necesiten, para ser procesada por las personas autorizadas.

Por ejemplo, un ataque contra un sistema de venta en línea, o un problema en un servidor que hiciera que este se apague estarían vulnerando la disponibilidad de la información.

Los incidentes de seguridad de la información pueden ser internos o externos; y a la vez maliciosos o involuntarios, como indican los siguientes ejemplos:

	INTERNO	*EXTERNO*
Malicioso	*Un empleado enojado destruye un documento importante.*	*Un atacante realiza un ataque de denegación de servicio contra el sitio web de la organización.*
Involuntario	*Un empleado pierde un dispositivo USB donde había copiado información confidencial de la empresa.*	*Un exceso de visitas a un sitio web hace que este deje de funcionar y se pierda la disponibilidad.*



LAS POLÍTICAS DE SEGURIDAD

Es ideal que toda empresa cuente con una política de seguridad con el objetivo de que todos los empleados conozcan cuán importante es la protección de la información para la empresa. Cuando un empleado ingresa debe conocer cuáles son los mecanismos básicos para el manejo seguro de la información y los datos de la empresa. En algunas compañías se hace entrega de un documento conocido como políticas de seguridad. Cuando este documento es firmado, la persona confirma que entiende y va a acatar las políticas definidas en este. De esta manera, se compromete a cumplir las normativas de seguridad definidas por la organización. Es necesario comprender que la existencia de este documento es con el fin de proteger los activos de la compañía.

> 1 | *Un **empleado seguro**, lee, conoce, entiende y respeta lo indicado en las políticas de seguridad de la compañía.*

En caso que la empresa no cuente con un documento de Políticas de seguridad es necesario consultar con el departamento correspondiente para saber los procedimientos a seguir y las buenas prácticas recomendadas por la compañía.

HERRAMIENTAS DE SEGURIDAD

Las tecnologías son la base de la seguridad informática en las empresas. Las tecnologías más comunes en la computadora son las siguientes:

Antivirus

Protege los equipos y su información de distintos ataques de códigos maliciosos. Los antivirus más efectivos incluso protegen proactivamente ante malware nuevo o desconocido.

Firewall

Puede estar integrado con el antivirus y protege al equipo informático de las conexiones de Internet entrantes y salientes que se quieren realizar en diversos tipos de ataque o también las automáticas que se intentan realizar desde el equipo.

Antispam

Es un software que muchas veces está integrado con la solución antivirus o con el cliente de correo y permite a la persona no recibir spam o correos no deseados en su bandeja de entrada corporativa.

> 2 | *Un **empleado seguro** debe conocer y respetar las herramientas instaladas en su computadora, y estar atento a las alertas de estas.*

Además, hay muchas otras herramientas que suelen ser implementadas por las empresas en el perímetro de la red o directamente en los servidores para proteger al negocio y que no son visibles para los integrantes de la compañía, como por ejemplo: proxy, IDPS, IPS, firewall perimetral, actualización de parches; entre otras.

MALWARE

El malware (acrónimo de malicious software) es uno de los ataques más comunes de la actualidad. El malware, también conocido como códigos maliciosos, son archivos con fines dañinos que, al infectar una computadora, poseen diversas acciones dañinas como el robo de información, el control del sistema o la captura de contraseñas. Entre muchas de las categorías existentes se destacan los gusanos, troyanos, virus; entre otros.

La infección de un código malicioso pareciera no impactar en su trabajo diario, sin embargo, ¿qué sucede si toda la información que almacena en su equipo se perdiera? ¿Cuánto vale el tiempo que estaría sin poder trabajar? ¿Y cuánto la dedicación del departamento de IT para solucionar el inconveniente? Ambas situaciones afectan directamente el rendimiento de la empresa, por ende, cuestan dinero.

Además, existen códigos maliciosos que son utilizados para el robo de información por lo que, incluso, podrían afectar directamente al negocio de la compañía o cuestiones personales de los empleados que tuvieran o utilizaran en la computadora laboral.

> 3 | *Un **empleado seguro** conoce los códigos maliciosos más comunes y posee buenas prácticas para evitar la infección de su equipo.*

INGENIERÍA SOCIAL

La Ingeniería Social es la utilización de habilidades sociales para manipular el accionar de una persona. A partir de estas estrategias, los desarrolladores de códigos maliciosos y atacantes informáticos suelen utilizar distintos medios para engañar y así comprometer la seguridad de la empresa.

Por ejemplo, a través de correos falsos que indiquen la necesidad de brindar información confidencial, falsos llamados telefónicos o propagación de códigos maliciosos en las redes sociales simulando ser aplicaciones integradas. Este tipo de técnicas buscan lograr que se realice una acción que podría comprometer la seguridad de la compañía, afectando así también al negocio. Por ejemplo, un correo falso que solicita un listado de clientes. Si la víctima no se da cuenta de la veracidad del correo, podría entregar información sensible de los clientes, y así afectar la confidencialidad de la información.

Además, hay ataques de Internet que utilizan mensajes de Ingeniería Social no directamente relacionado con la compañía como puede ser la muerte de un famoso o una catástrofe natural y que, al ser víctima del ataque, se puede perder información sensible para la compañía.

> 4 | *Un **empleado seguro** está atento a este tipo de mensajes y puede identificar posible ataques de Ingeniería Social.*

ROBO DE INFORMACIÓN

Uno de los mayores problemas posibles en una organización es el robo de información sensible; cuya publicación pueda afectar al negocio. El incidente puede ser generado por un mal accionar de las personas y no solo por una acción maliciosa. Es necesario entender que el robo de información no solo se puede dar a través de medios digitales, sino que también involucra al material físico. Si alguien ajeno a la compañía accede a datos confidenciales, el negocio se podría ver afectado de diversas formas. Estadísticas de ESET indican que, ante un caso de robo de información, el **62,9%** de las personas dejarían de utilizar el servicio, es decir, que la empresa podría perder a 6 de cada 10 clientes por no proteger bien sus datos. El impacto que puede significar ser víctima de la fuga de información remarca que todos los integrantes de la empresa deben cuidar la información. Por ejemplo, si alguien se olvida un documento confidencial en un lugar público, como el plan de marketing o la lista de clientes, esto podría caer en manos de la competencia y revelar la estrategia de la compañía.

> 5 | *Un **empleado seguro** está atento a la información que se está transportando tanto a nivel digital como físico para evitar la fuga de información.*

Además, a la hora de desechar material impreso con información confidencial es necesario destruirlo de forma adecuada antes de arrojarlo a la basura.

DISPOSITIVOS MÓVILES

La tecnología y la incorporación de los smartphones a las empresas permiten el acceso a la información en todo momento, aunque transportar información sensible en dispositivos móviles podría ser un gran riesgo, ya que puede abrir las puertas a la fuga o al robo de información. Entonces, ¿qué pasa si se pierde o es robado el teléfono de la empresa?

Para no ser reactivos y salir a buscar una solución una vez que surge el inconveniente, es mejor ser proactivo y evitar la amenaza.

Muchas veces las personas que tienen un teléfono corporativo no tienen en cuenta el cuidado que hay que tener debido a la cantidad de información confidencial que se encuentra disponible en el mismo.

6 | *Un **empleado seguro** utiliza el dispositivo con fines laborales, no comparte el dispositivo con personas ajenas a la organización y mantiene el mismo con las mejores prácticas de seguridad para evitar incidentes sobre la información almacenada.*

CONTRASEÑAS

Dada la cantidad de sistemas, plataformas, correos electrónicos y otros servicios de la empresa existentes, cada integrante de la compañía suele tener varias contraseñas. Es por eso que una contraseña débil puede significar el acceso a información confidencial o a un sistema por parte de un atacante o un código malicioso. Teniendo en cuenta esto, es importante que las contraseñas que se utilizan dentro de la empresa (y también a nivel personal) sean fuertes: es decir, fáciles de recordar y difíciles de descifrar.

Muchas veces la motivación de crear contraseñas fuertes contrae el riesgo de que sean olvidadas. Debido a esto, la utilización de un software para la gestión de contraseñas es la alternativa más adecuada, no siendo así la utilización de cuadernos o papeles pegados en el escritorio para anotar las mismas. Además, la utilización de contraseñas diferentes para los distintos servicios corporativos claves es también muy importante.

7 *Un **empleado seguro** considera la seguridad de las credenciales fundamental para su trabajo, y es por ello que no las comparte con nadie, utiliza claves fuertes, no las anota en ningún lugar visible ni utiliza las mismas contraseñas para servicios laborales y personales.*

CORREO ELECTRÓNICO

Existen situaciones en donde para registrarse en algún servicio, o incluso en las redes sociales, se requiere el ingreso de un correo electrónico para contacto. El correo corporativo se utiliza como fuente de comunicación de la empresa y en la medida de lo posible se debe evitar su exposición en Internet.

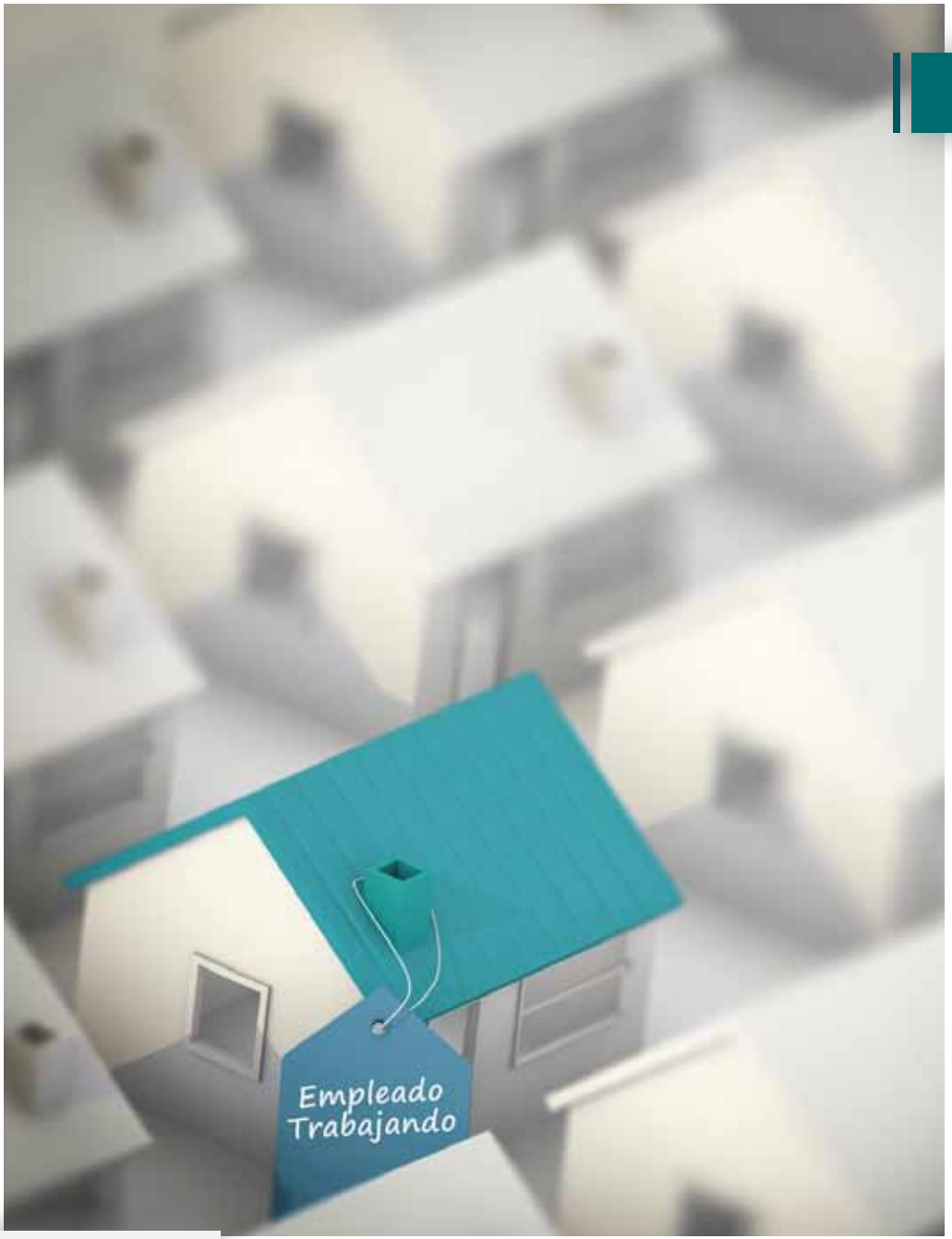
En el caso que se utilice el correo de la empresa para registrar un servicio, puede existir cierta exposición de esa dirección de mail y de esa manera aumentar la posibilidad de sufrir algún ataque de phishing, así como también el aumento de correo no deseado (spam).

Phishing

El phishing consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante.

Otro aspecto a tener en cuenta es el comportamiento frente a correos de origen dudoso.

8 | *Un **empleado seguro** no accede a enlaces que no provengan de un remitente de confianza ya que podría tratarse de un ataque de phishing o malware.*



DEL HOGAR AL TRABAJO Y DEL TRABAJO AL HOGAR

En la actualidad con la existencia de las computadoras portátiles, muchos empleados se llevan el trabajo al hogar, por lo que ciertas veces utilizan herramientas que no existen en el ámbito corporativo y el equipo puede encontrarse expuesto en una red que no está debidamente controlada como la de la organización. Ligado a este concepto, es de vital importancia tomar ciertas medidas.

- ***Contar con un software antivirus en la computadora personal para estar protegidos contra amenazas potenciales.***
- ***Tener el sistema operativo actualizado al día de la fecha para contar con todos los parches de seguridad y todas las aplicaciones también actualizadas.***
- ***Respetar las políticas de seguridad de la organización, aún cuando se encuentre fuera del ámbito laboral.***

Además se debe considerar que existe la posibilidad de fuga de información cuando se encuentra fuera de la red interna de la empresa. De esta manera, las medidas antes expuestas pueden ayudar a evitarla.

Como concepto final, cuando se lleva documentación y papeles de importancia para trabajar fuera de la organización, se debe tener especial cuidado en lo que respecta al robo de los mismos en lugares públicos, o incluso en el mismo hogar. Además tales documentos deben ser manipulados teniendo en cuenta el nivel de confidencialidad que requieren.

En caso de que se utilicen dispositivos de almacenamiento USB o memorias, siempre es necesario realizar un análisis con un antivirus al momento de insertarlos en el equipo (ya sea del ámbito corporativo como en el personal) Para evitar infecciones de los dispositivos de almacenamiento a partir del uso de los mismos en el equipo hogareño, siempre es recomendable contar con una solución antivirus en ese ámbito.

9 | *Un **empleado seguro** cuida la información de la empresa, incluso fuera del ámbito corporativo.*

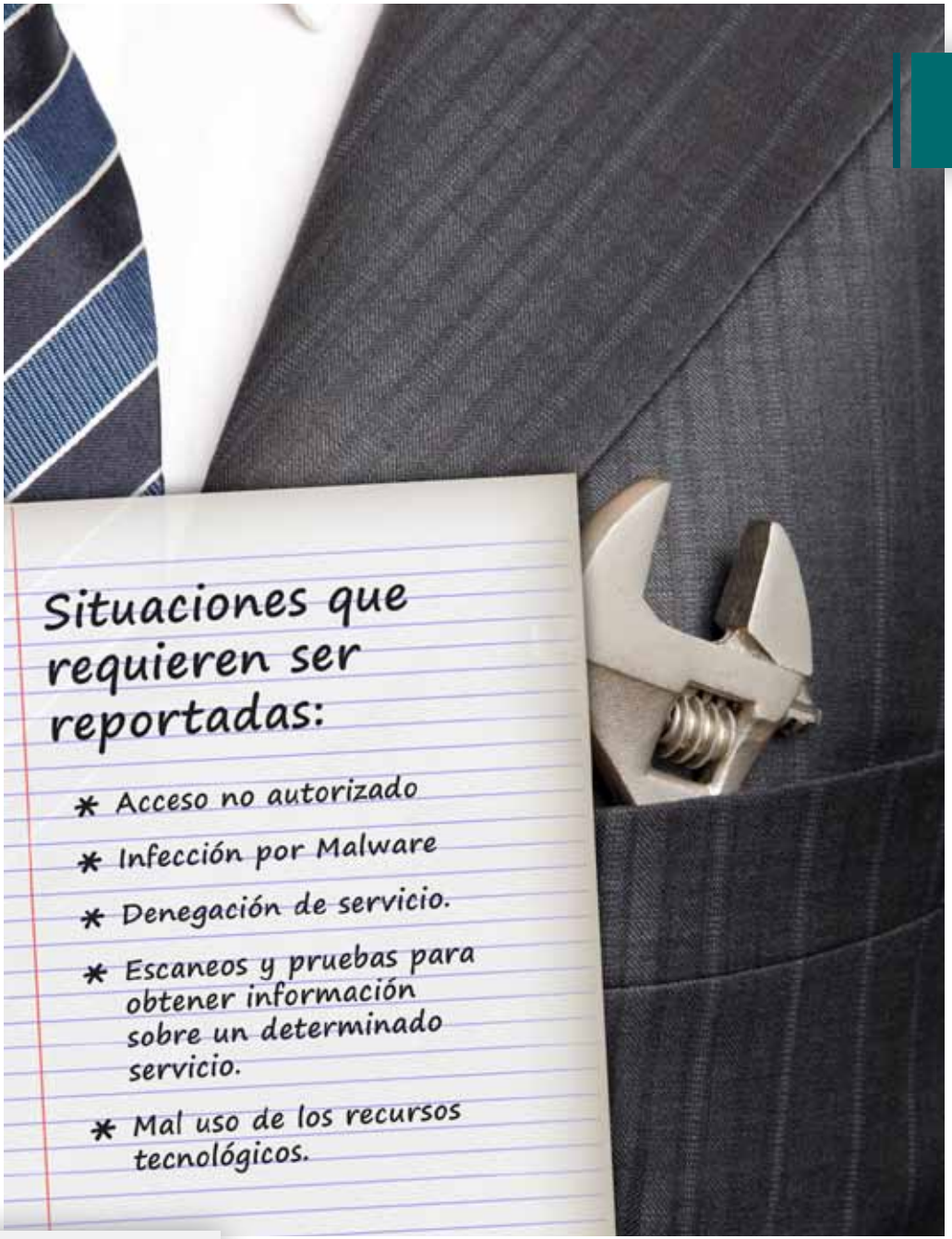
EQUIPOS DEL TRABAJO EN REDES WIFI PÚBLICAS

Es común utilizar el equipo portátil de trabajo para conectarse a redes WiFi públicas, como por ejemplo, redes de bares, cafés, aeropuertos, etc. En estos casos debe considerarse que la seguridad estará ligada a los controles existentes en dicha red. En muchos casos, estos controles son inexistentes, tales como la ausencia de contraseña para realizar la conexión WiFi.

Es por esto que se recomienda al usuario no realizar conexiones sensibles, como por ejemplo 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 otra persona que esté conectada a la misma red.

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

10 | *Un **empleado seguro** utiliza una conexión privada virtual (VPN) cuando se conecta a redes inalámbricas públicas.*



¿CUÁNDO LLAMAR AL DEPARTAMENTO DE SEGURIDAD POR UN INCIDENTE?

Existen casos en lo que se puede sospechar que el sistema o incluso la organización completa hayan sido comprometidos. En caso de sospechar que realmente ha ocurrido un incidente, se le debe dar aviso al departamento de IT o seguridad **de forma inmediata** ya que estos son los encargados de controlar este tipo de situaciones.

En caso de que se dé la existencia de algún incidente de seguridad de cualquier tipo, se debe comunicar el mismo de forma inmediata al departamento correspondiente.

En caso de que se dé la existencia de algún incidente de seguridad de cualquier tipo, se debe comunicar el mismo de forma inmediata al departamento correspondiente.

11 | *Un **empleado seguro** informa inmediatamente ante cualquier sospecha de un incidente de seguridad. Es preferible un reporte erróneo que no sea una amenaza, a la existencia de una amenaza que nunca haya sido reportada.*

BUENAS PRÁCTICAS DE UN EMPLEADO SEGURO - EN EL PUESTO DE TRABAJO

1. **POLITICAS DE SEGURIDAD**
   Leer y respetar las políticas de seguridad de la empresa.

2. **BLOQUEO DE SESIÓN**
   Bloquear la sesión cuando se abandona el puesto de trabajo.

3. **DESTRUIR DOCUMENTOS**
   Destruir documentos impresos sensibles antes de arrojarlos a la basura.

4. **ACCESO A SITIOS DE DUDOSA REPUTACIÓN**
   Evitar el acceso a sitios de dudosa reputación.

5. **DESCARGA DE APLICACIONES NO CONOCIDAS**
   Evitar la descarga de aplicaciones no conocidas que podrían ser malware.

6. **ACCESO A SITIOS DUDOSOS**
   Evitar el ingreso de información en sitios dudosos que podrían ser phishing.

7. **INFORMACIÓN PERSONAL**
   Evitar compartir información con personas no autorizadas a acceder a la misma.

8. **DISPOSITIVOS CORPORATIVOS**
   Utilizar el dispositivo móvil corporativo solo con fines laborales y no compartirlo con personas ajenas a la organización.

9. **CONTRASEÑAS FUERTES**
   Utilizar contraseñas fuertes.

10. **CONTRASEÑAS PERSONALES**
    No compartir contraseñas personales y laborales.

11. **TECNOLOGÍAS DE SEGURIDAD**
    Conectarse solo a redes WiFi conocidas o utilizar tecnologías de seguridad como VPN en caso de acceder a redes inalámbricas públicas.

12. **REPORTAR INCIDENTE DE SEGURIDAD**
    Reportar cualquier sospecha de un incidente de seguridad para la organización.

BUENAS PRÁCTICAS DE UN EMPLEADO SEGURO - EN EL HOGAR

En tu hogar, también debes tener cuidado con tu sistema, cuidar tu información personal es una buena forma de cuidar también la información de tu empresa. Por lo tanto, se recomiendan las siguientes prácticas de seguridad:

1. ***ENLACES SOSPECHOSOS***
   Evitar los enlaces sospechosos.

2. ***ACCESO A SITIOS DE DUDOSA REPUTACIÓN***
   No acceder a sitios web de dudosa reputación.

3. ***ACTUALIZACION DEL SISTEMA OPERATIVO***
   Actualizar el sistema operativo y las aplicaciones.

4. ***APLICACIONES OFICIALES***
   Descargar aplicaciones desde sitios web oficiales.

5. ***TECNOLOGIAS DE SEGURIDAD***
   Utilizar tecnologías de seguridad.

6. ***INFORMACIÓN EN FORMULARIOS DUDOSOS***
   Evitar el ingreso de información personal en formularios dudosos.

7. ***RESULTADOS DE BUSCADORES***
   Tener precaución con los resultados arrojados por buscadores web.

8. ***CONTACTOS CONOCIDOS***
   Aceptar solo contactos conocidos.

9. ***ARCHIVOS SOSPECHOSOS***
   Evitar la ejecución de archivos sospechosos.

10. ***CONTRASEÑAS FUERTES***
    Utilizar contraseñas fuertes.

CONCLUSIÓN

Como parte de una compañía sin importar la tarea que desarrolle o el área a la que se dedique, proteger la información confidencial de la organización es también proteger el negocio. Debido a ello, tanto la utilización de las tecnologías para la seguridad, como la educación a sus usuarios acerca de las amenazas y técnicas de protección, ayudan a asegurar la continuidad del negocio.

Cualquier interrupción o complicación que se afronte por la infección de un código malicioso o ataque a su organización impacta directamente en su imagen, en la empresa y en la confianza que los clientes pueden tener de la compañía. Entender la seguridad corporativa y mantenerse educado, otorga un valor agregado a su organización.