Seguridad Informatica

Todo lo que la **Gerencia de TI** debe conocer para evitarse problemas.

¿Estoy en el E-BOOK correcto?

Lo **estás** si cumples con alguno de los siguientes roles:

Director General

¿Por qué?

Aunque cotidianamente no estás involucrado con tu área de TI es importante que conozcas por cuenta propia los **tipos y niveles de riesgo que toda tu empresa puede estar corriendo** por falta de información.

Gerente de TI

¿Por qué?

Estás a cargo de una de las áreas más importantes y valiosas para tu organización. **Considerar los riesgos que tú y tu área están corriendo es fundamental para prevenirlos con tiempo.** Recuerda que cualquier falla importante es tu responsabilidad.

Apasionado de la Tecnología

¿Por qué?

Disfrutas de leer sobre estos temas y la **seguridad Informática**, es un aspecto básico e importante si de tecnología se trata.

Para una buena lectura de este E-book te recomendamos:

Si tu lectura será desde un dispositivo móvil, girar tu dispositivo de manera horizontal

Tiempo y tu bebida favorita de acompañante

¿Requieres información adicional? ¡Pregúntanos!

contacto@arrobasystem.com

E-book cortesía de:

arroba system

Rubén González Salas

CRO - Co Founder

Karín González Salas

Head of Marketing

Mitchell Alvarez

Marketing Team

Sergio Moctezuma

Marketing Team

Temário

Temário

arroba system

Seguridad informática: Todo lo que la Gerencia de TI debe conocer para evitarse problemas.

Introducción

En la actualidad todas las empresas utilizan Internet de alguna manera dentro de sus actividades diarias en algún proceso interno. Debido al extendido uso de esta herramienta, los **fallos en los sistemas de seguridad informática** representan un riesgo latente y pueden implicar **costos millonarios.**

Desafortunadamente, se ha extendido la falsa idea de pensar que a los ciberdelincuentes no les interesa la información de cualquier empresa, que basta con no abrir archivos desconocidos o contar con un antivirus para estar protegido.

Introducción

La **seguridad informática o ciberseguridad** se encarga de proteger las redes, equipos e información sensible de una empresa al identificar y eliminar amenazas que pueden difundirse en la red de dispositivos. Con la seguridad para las tecnologías de la información se busca a su vez **minimizar el mantenimiento de la infraestructura** y **mejorar su seguridad en todos los niveles.**

La infraestructura de seguridad Informática de las empresas y su información puede verse vulnerada de múltiples maneras aprovechando cualquier oportunidad; por pequeña que sea.

Tipos de seguridad informática

Los **protocolos de seguridad** informática enfocados en la protección de la red protegen la información a la que se accede a través de Internet y evita que personas malintencionadas puedan acceder.

Se usan para combatir amenazas como virus, software espía, phishing, suplantación de identidad, entre otros, la seguridad informática utiliza mecanismos que actúan en **software y hardware.**

Tipos de seguridad informática

Seguridad informática de hardware

La seguridad Informática aplicada al uso del hardware **protege el equipo** de intrusiones no deseadas a través de firewalls y servidores proxy que controlan el tráfico de red, así como HSM (módulos de seguridad de hardware) que utilizan claves criptográficas para la autentificación en los sistemas.

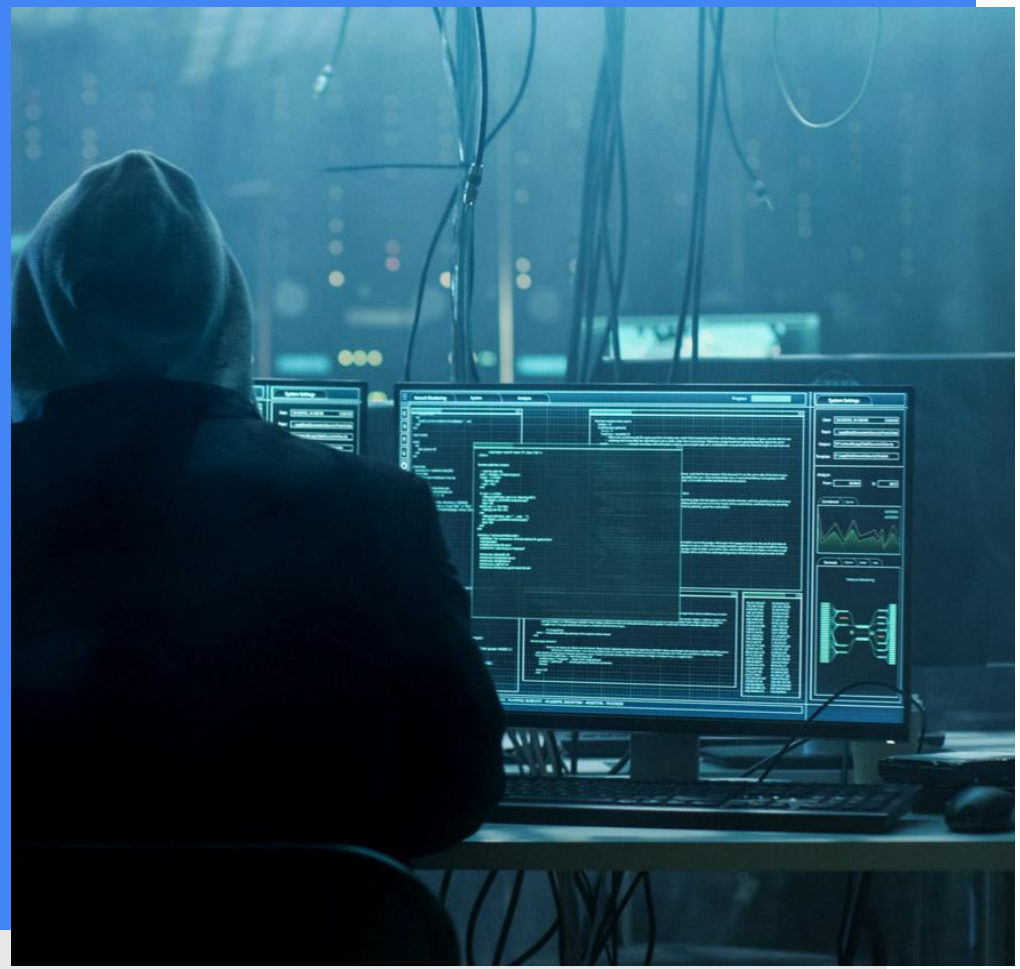
Identifica errores de seguridad en los equipos desde la configuración o código de ejecución, así como los dispositivos de entrada y salida de datos.

Tipos de seguridad informática

Seguridad informática de software

Los ataques a software aprovechan cualquier agujero de seguridad informática, por lo que los fabricantes deben **evitar errores** desde el proceso de desarrollo, como **defectos de diseño**, **desbordamiento de buffer** o **fallos de implementación** que pudieran abrir la puerta a virus o hackers.

La seguridad de software **protege las aplicaciones** y **programas de amenazas exteriores** a través de programas antivirus, cortafuegos, software para filtrar contenido, filtros antispam, entre otros.



Riesgos y amenazas de seguridad Informática que enfrentan las empresas

En la seguridad Informática siempre existe un riesgo de ataques y **robo de información** dentro de las empresas por **amenazas del exterior**, sin embargo, a nivel interno, también se corren riesgos y no sólo se trata exclusivamente de empleados malintencionados que roban información, sino de **usuarios que inadvertidamente causan fugas de datos**.

Las amenazas internas causan las mayores brechas de seguridad y son muy costosas de remediar.

¿Por qué llevar la seguridad de la información a la nube?

Además de amenazas por el uso de Internet existen **riesgos de origen no informático** que no son previsibles con una estrategia de seguridad Informática enfocada sólo en las redes, como **robo del equipo**, **daños por incendio**, **inundaciones** y **otras catástrofes naturales**, un mal manejo del equipo, fallos electrónicos, entre otros.

En estos casos la única solución es contar con un **respaldo de datos externo**. Por este motivo y por las avanzadas herramientas que utiliza para proteger el flujo de datos, un servicio en la nube es la mejor opción como parte del protocolo de seguridad Informática que deben adoptar las empresas.

La seguridad en la nube es similar a la seguridad TI tradicional sin necesidad de mantener instalaciones ni hardware como servidores físicos o dispositivos de almacenamiento.

Es escalable y brinda normas, procedimientos, controles y tecnologías que protegen datos y aplicaciones de forma eficiente.

La seguridad informática empieza en la infraestructura y después en los usuarios

La seguridad informática en Internet requiere de **herramientas que protejan la infraestructura** de los centros de datos pero a su vez exige la implementación de buenas prácticas por parte de los usuarios, quienes suelen ser un factor de riesgo.

Los métodos de acceso seguros que van más allá de *nombre y contraseña* previenen riesgos de forma considerable.

¿Cómo se conforma una infraestructura de seguridad Informática segura?

En los centros de datos es fundamental un **hardware personalizado** que garantice seguridad, rendimiento y una respuesta inmediata ante amenazas.

La **arquitectura de redes** hace que los datos se **distribuyan en diferentes servidores**, por lo que seguirán accesibles en todo momento a pesar de que falle alguno. Por otra parte la seguridad física también es un factor clave para evitar el acceso a cualquier persona ajena.

En una **infraestructura segura** los datos se encriptan en todo momento y limitan su exposición al Internet público, donde pueden ser interceptados. Las claves para las conexiones entre servidores son efímeras, lo que hace imposible la desencriptación.

Para evitar el acceso no autorizado, se utiliza una **verificación en dos pasos**, es decir que además de la contraseña se solicita algún dato extra. También se pueden implementar llaves físicas.

Los administradores tienen el control de datos confidenciales y dentro de la interfaz de uso compartido avanzado pueden inhabilitar la descarga, impresión y copia de archivos si lo consideran necesario, así como definir fechas de vencimiento de los mismos.

Una infraestructura segura utiliza el **aprendizaje automático** para identificar el phishing o suplantación de identidad, analizando patrones y similitudes con sitios donde se ha detectado antes este fraude.

¿Cómo obtener métodos de acceso seguros?

Como ya lo mencionamos, la principal vulnerabilidad de los sistemas suelen ser los usuarios, no necesariamente con malas intenciones, sino por desconocimiento de buenas prácticas de seguridad.

Controlar accesos a los sistemas y aplicaciones se ha convertido en una práctica generalizada y nadie pone en duda la necesidad de hacerlo. Sin embargo, autenticar a través de un nombre de usuario y password o contraseña puede ser insuficiente, sobre todo cuando el usuario utiliza passwords demasiado débiles, predecibles (como fecha de nacimiento o nombres de los hijos) o decide apuntarlo en algún cuaderno para recurrir a él en caso de olvidarlo.

La seguridad informática empieza en la infraestructura y después en los usuarios

Autenticación de doble factor

Para que el acceso a un sistema sea menos vulnerable, además de solicitar algo que el usuario sabe, como el nombre y contraseña, en los **sistemas de doble factor** el ingreso se complementa con algo que el usuario posee, como un **dispositivo físico externo** conocido como **token o una app para celular**, los cuales generan un código aleatorio que se utiliza en una sola ocasión.

Incluso existen sistemas de **autentificación de doble factor**, en los que se solicita algo que es parte del usuario, como la **huella digital**, la **imagen del iris** o **su rostro o el reconocimiento de su voz**. La autenticación de doble factor se recomienda, sobre todo en servicios críticos como cuentas de banco, gestión de tiendas online o administración de sistemas.

Prevenir el robo de datos debe ser una prioridad en todas las empresas. La seguridad informática protege efectivamente la confidencialidad de datos y recursos, limita el acceso a usuarios autorizados a través de sistemas de autentificación efectivos.

Los **servicios en la nube** mantienen la información disponible en todo momento y la protegen de incidentes propios de la red, así como por situaciones externas.

arroba system

Tema II: Importancia de la seguridad en las herramientas de comunicación empresarial

Un nuevo tipo de Seguridad

En muchas ocasiones se considera que la única seguridad con la que deben contar las empresas es la seguridad física. No obstante, se debe tener en cuenta que esta percepción errónea del concepto puede favorecer que, al pasar desapercibidos otros aspectos importantes de la seguridad, las empresas sean el blanco de sofisticados ataques.

Entre los diferentes campos de la seguridad, la gran olvidada es la conocida como **seguridad informática**. Esta rama, abarca todas las medidas destinadas a **prevenir, detectar, identificar y resolver** cualquier uso de los sistemas que no ha sido autorizado.

Amenazas y vulnerabilidades

Son muchas las amenazas para las que la seguridad informática de una empresa debe estar preparada. Algunos de los frentes que se deben tomar en cuenta son:

Correo electrónico empresarial

- Phishing
- Malware
- Spam

Chats y videoconferencias

- Shadow IT

Intranets corporativas y sitios para proyectos

- Intranet

Redes sociales corporativas

- Contraseñas comunes
- Aplicaciones de terceros
- Suplantación de identidad

Correo electrónico empresarial

Puede considerarse como el medio en donde toda empresa es más vulnerable, ya que una persona que consiga acceder a algún correo electrónico corporativo, podrá enviar cualquier tipo de mensaje y, por lo tanto, será necesario contar con una estrategia de seguridad informática.

Atendiendo a esta información debemos considerar las siguientes amenazas:

-Phishing

Es el método utilizado por delincuentes del ciberespacio para robar datos de los usuarios en empresas que no cuentan con suficiente seguridad informática. Buscan acceder a información sobre cuentas bancarias, contraseñas del equipo de finanzas o suplantar a la compañía en su comunicación dentro de las redes sociales.

La detección de este tipo de mensaje puede ser muy difícil si el usuario no está familiarizado con el tema o si no comprobamos la veracidad de su emisor, ya que se pueden suplantar identidades de personas, empresas e incluso compañías con las que se tiene contacto.

Por ello, los protocolos de seguridad informática deben también enfocarse en su prevención, iniciando con la capacitación de los usuarios de los correos electrónicos.

-Malware:

Otro punto débil de los correos electrónicos son los **mensajes con archivos adjuntos**, mediante los cuales los delincuentes de la red pueden esconder virus cuando no existen políticas de seguridad informática. El más temido por toda empresa es el Spyware, que se dedica a vigilar y grabar cada acción que se lleva a acabo en las computadoras infectadas. De esta forma, se pueden llegar a robar nombres de usuarios y contraseñas.

-Spam:

Es la conocida técnica de la publicidad masiva. Esos correos que llegan diariamente a nuestro e-mail ofreciendo productos, promocionando eventos o invitaciones a inscribirnos en alguna red social.

En este caso, las personas encargadas de llevar a cabo este tipo de envíos masivos obtienen los datos del correo electrónico de diferentes páginas web en donde un usuario se haya registrado. Una vez conseguidos los datos de millones de personas, empiezan con el envío intrusivo y masivo de publicidad. Es posible que detrás de un mensaje con Spam se esconda un Malware, aprovechando la publicidad de un producto para instalar un virus en cualquier computadora.

Una campaña de seguridad informática es fundamental para evitar este tipo de prácticas, creando filtros automáticos que eviten que mensajes de este tipo sean recibidos por los usuarios.

Chats y Videoconferencias

Shadow IT:

Este fenómeno se genera cuando el departamento de tecnología de una empresa no ha aprobado o desarrollado un sistema de comunicación corporativa (como salas de chat o un software de videollamadas), colocando en riesgo su seguridad informática.

En estos casos, la ausencia de estos medios de comunicación puede llevar a que los empleados **utilicen soluciones ajenas a la empresa**. Esta falla de seguridad informática es de alto riesgo ya que la compañía no puede controlar lo que sus trabajadores comunican y comparten a través de medios externos a ella, por lo que se arriesgan a que la información pueda ser robada.

Intranets corporativas y sitios para proyectos

Intranet:

Se trata de una red interna a la que podrán acceder los usuarios de una misma institución. Su objetivo es centralizar la información y los datos de los clientes, los proyectos que van a desarrollar y los mensajes entre departamentos, por lo que es una fuente de información codiciada por la mayoría de los delincuentes informáticos.

Aunque por lo dicho anteriormente, pareciese que este tipo de red es segura y se encuentra exenta de cualquier ataque, no es así.

La mayoría de las amenazas a los que se enfrenta una Intranet se deben -en mayor grado- a sus propios usuarios, ya que pueden provocar que esta red sea **infectada al ingresar en páginas web poco fiables**, recibir un correo con *malware*o por un *spyware* contenido en el *spam*.

Intranets corporativas y sitios para proyectos

De esta forma, **usuarios no autorizados podrían acceder a los datos confidenciales de la empresa**, conocer sus clientes, robar información de nuevos proyectos e incluso, acceder a datos bancarios para realizar movimientos de dinero. Una correcta gestión de los protocolos de seguridad informática, pueden prevenir este tipo de amenazas latentes.

Redes sociales corporativas

Si bien las redes sociales potencian la comunicación en las empresas, también pueden ser perjudiciales en términos de seguridad.

Si no se implementa una red social empresarial, entonces lo más probable es que los usuarios utilicen alguna de las **plataformas públicas para comunicarse**, lo que podría originar diversas situaciones:

-Contraseñas comunes:

Un problema común es que los usuarios muchas veces utilizan las mismas contraseñas en todas las plataformas, por lo que un acceso no autorizado a una red social, podría conllevar a que se descubran las credenciales para acceder a información restringida de la empresa.

Redes sociales corporativas

-Aplicaciones de terceros:

Si bien las redes sociales se esfuerzan al máximo por construir entornos seguros, muchas de ellas permiten instalar aplicaciones o módulos desarrollados por terceros, los que no tienen el mismo nivel de control de seguridad y que en muchas ocasiones terminan siendo los puntos de acceso para acceder a la información confidencial de los usuarios.

-Suplantación de identidad:

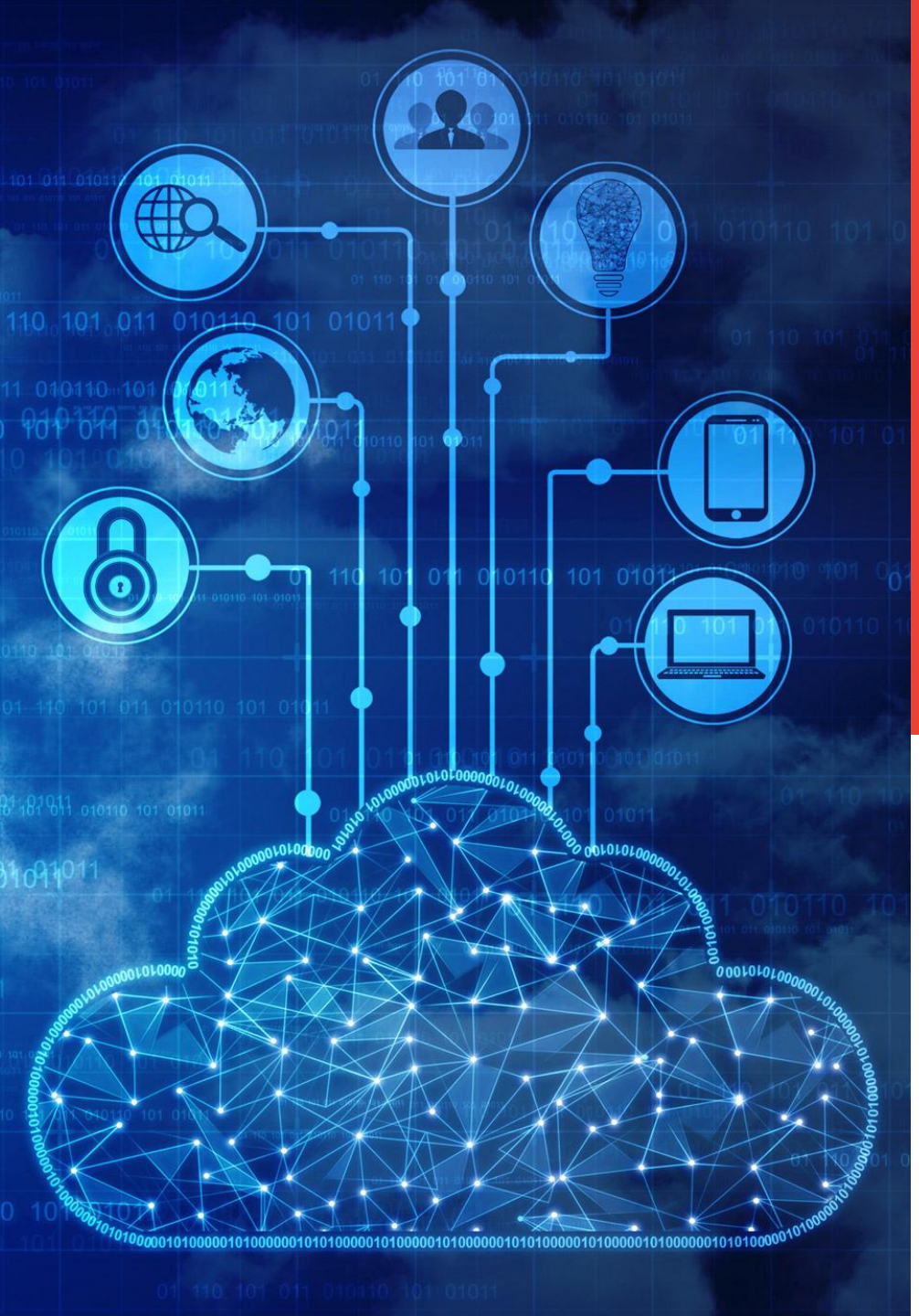
Como sólo basta un correo electrónico para registrarse, es común encontrarse con casos en que u**suarios suplantan la identidad de otros**, dando la posibilidad para que soliciten información privilegiada o que simplemente engañen a otros.

Por estas razones, es conveniente que usar medios de marketing o redes sociales diseñadas especialmente para un uso empresarial, que cuenten con protocolos adecuados de seguridad informática.

Internet es la mayor fuente de información a la cual podemos acceder, pero también el medio en el que más delitos se pueden llegar a cometer. Las que revisamos, son sólo algunas de las múltiples amenazas informáticas que las empresas enfrentan cada día.

Es importante que los usuarios cuenten con una adecuada capacitación en términos de seguridad informática, y que a la vez, sean cautos con la información que publican, los sitios dónde lo hacen y las personas con las que la comparten. Por último, es necesario mantener siempre la seguridad y los terminales informáticos actualizados.

La información es poder. Si no quieres ser víctima de ataques cibernéticos, invierte tiempo y dinero en la seguridad informática de tu empresa.



arroba system

Tema III: Seguridad para archivos, aplicaciones y backups.

Vivimos en una época en la que la información es poder, lo que ha traído una gran revolución en términos de Transformación Digital dentro y fuera de las organizaciones. En la era digital que vivimos, **la pérdida de información es una amenaza constante** que tiene implicaciones fatales y que puede afectar seriamente tu empresa y poner en vilo hasta su misma existencia. La ventaja es que es evitable con seguridad informática.

Los datos informáticos, además de gestionarse en ingentes cantidades y hacer presencia en todas las interacciones de un negocio con clientes y socios, son uno de los **activos más valiosos** porque te permiten tomar decisiones con mayor seguridad y optimizar los flujos de trabajo.

Cuando no se respalda la información o se tiene un plan de seguridad informática débil, los archivos generales, la información privada de la empresa, las bases de datos y los backups pueden desaparecer en cualquier momento, por diferentes razones:

Daño del Hardware:

Nada es eterno. Ni siquiera una supercomputadora o un disco duro externo de vanguardia. Estos equipos tienen una vida útil, el uso los va desgastando y hasta una mala manipulación o un golpe pueden derivar en un daño severo.

En un centro de reparación pueden recuperar tu información. O pueden no hacerlo, si la avería es muy grave.

Vírus:

Internet está lleno de amenazas a la integridad de tus datos. Un virus puede eliminar tu información en segundos o dañar el software que la ejecuta dejándote sin acceso a la información.

Códigos maliciosos (ransomware):

Están diseñados por cibercriminales para obtener ganancias económicas chantajeando a las empresas con su propia información.

Por lo general, roban datos sensibles de la empresa, los dañan o los cifran con contraseñas, todo para pedirte a cambio de la solución al problema cifras millonarias. Recientemente, los ataques más importantes a escala mundial, han recaudado más de 325 millones de dólares de las compañías no protegidas.

Desastres físicos:

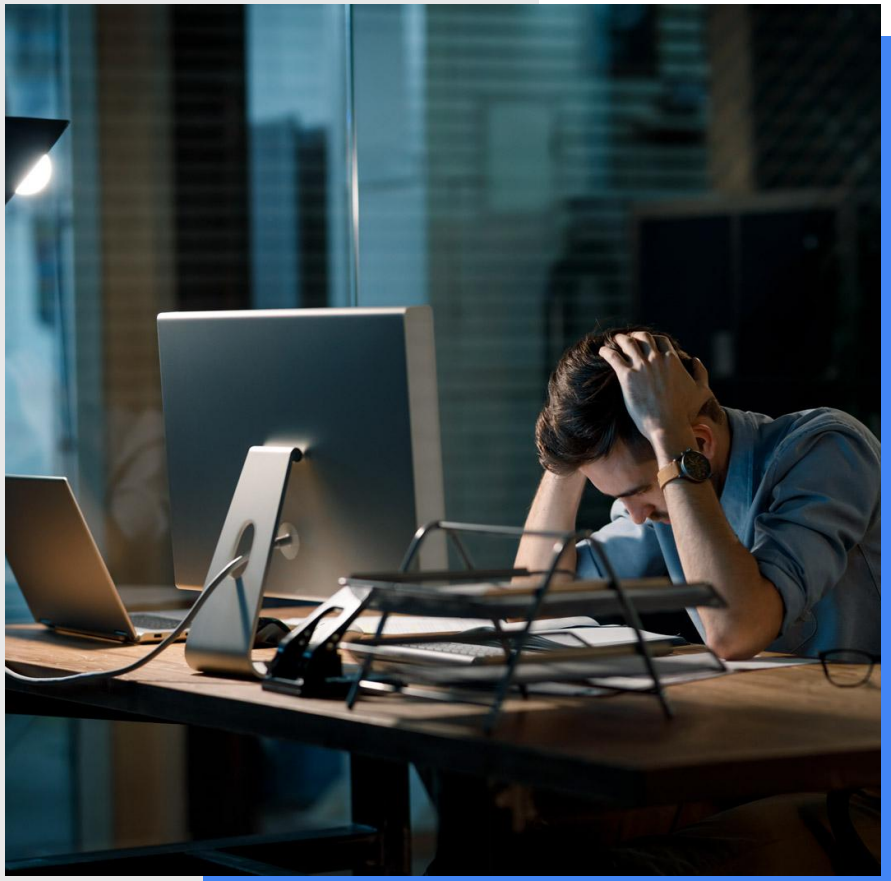
Un incendio, una inundación o cualquier incidente por el estilo también puede destrozar tu computador, USB, o disco duro externo, eliminando así la información que guardan y haciendo que su recuperación sea prácticamente imposible.

Robo de la información:

La delincuencia puede estar en cualquier parte. Por lo tanto, no estás exento de que te hurten el disco duro, memoria USB o PC. Peor aún, tampoco estás libre de que te roben intencionalmente la información; es decir, de que alguna persona inescrupulosa con acceso a tus dispositivos se la lleve para fines malignos. Por ejemplo, los datos de los clientes de la empresa para negociar a su nombre o realizar estafas.

Envío de información confidencial a terceros mediante email o dispositivos físicos:

Una vez sale de tus manos pierdes el control sobre esa data y no sabes que puedan hacer con ella. Si cae en las manos equivocadas, también puede derivar en suplantaciones, estafas y robos.



¿Cuáles son las consecuencias de esa pérdida de información?

Si la **seguridad informática** de tu empresa no es la mejor y no cuentas con copias de seguridad de la data que procesas, al padecer alguno de los eventos anteriormente mencionados entras en graves problemas y puedes sufrir graves consecuencias nefastas para la continuidad de las operaciones del negocio.

Imagina una empresa sin la correcta gestión en seguridad informática y que pierde toda la contabilidad del periodo en marcha. Si bien guarda copias de seguridad para respaldar esta información, resulta que están desactualizadas y toda la data de los últimos meses no aparece.

Como bien lo sabes, eso puede derivar en problemas de alto impacto porque los registros contables y los estados financieros son fundamentales para la toma de decisiones estratégicas. Por no hablar de las consecuencias negativas de índole fiscal.

En esta época de transformación digital toda la administración de **las empresas está mediada por datos**, información valiosa que no puede perderse por ningún motivo.

El Informe Anual de *Ciberseguridad 2017, de Cisco*, reveló que más de la mitad de todas las organizaciones víctimas de un **ataque cibernético o de una violación de datos**, sin protocolos de seguridad informática, sufren posteriormente el escrutinio público y pérdidas en la reputación de la marca, la lealtad del cliente y la confianza del mismo.

Además, el mismo estudio señaló que: Alrededor de 29% de estas empresas pierden ingresos, y casi el 40% de ellas pierden más del 20% de los ingresos totales.

Casi una cuarta parte de las empresas víctimas de ataques o violaciones pierden importantes oportunidades de negocios.

Más del 20% de ellas pierden clientes.

Definitivamente, los resultados son devastadores para una empresa.

Por no hablar de las **pérdidas de dinero** asociadas a los días de trabajo que también se van con la información. Piensa, por ejemplo, en un proyecto adelantado para determinado cliente, que estaba almacenado en una computadora portátil que te acaban de robar y no cuentas con una correcta gestión de seguridad informática **¿Qué harías?**

Las consecuencias negativas de la pérdida de la información pueden **derivar en la quiebra del negocio**. De hecho, 93% de las organizaciones que no contaban con protocolos de seguridad informática y perdieron la totalidad de sus datos de 10 días o más se declararon en bancarrota al año siguiente.

Es necesario fortalecer la seguridad informática de la empresa

Teniendo en cuenta los riesgos y consecuencias de la pérdida de datos y los ataques cibernéticos, queda claro que es **importante que hagas de la seguridad informática una prioridad en tu empresa**. No basta con que almacenes periódicamente datos importantes en discos duros externos o dispositivos USB.

Considera un **plan estratégico de respaldo de la información y seguridad informática** que contemple el uso de diferentes formatos y herramientas sincronizadas con los equipos, que actualicen las copias en tiempo real o, por lo menos, en lapsos de tiempo cortos que garanticen pérdidas mínimas en caso de que se presente un incidente.

Al respecto, es importante que una de **tus copias de seguridad** se albergue en la nube donde estarán **protegidas del robo, accidentes físicos, daño del hardware y ataques cibernéticos.**

Por supuesto, debes hacerlo con un proveedor del servicio de reconocida trayectoria en el mercado, que te brinde todas las garantías y la mejor seguridad informática.

Piensa que las copias de respaldo son solo un elemento del sistema de seguridad informática, pues este incluye antivirus y herramientas para asegurar el envío de información a terceros y proteger el desarrollo y ejecución de aplicaciones externas.

Solo así podrás estar seguro de que la gestión de datos en tu empresa es segura y de alta calidad.

arroba system

Tema IV: Seguridad informática

para equipos de cómputo, dispositivos móviles, auditoría y DLP

Seguridad Informática

Algunas empresas han, de una u otra manera, iniciado cambios en sus procesos de cara a iniciar una verdadera transformación digital, y han implementado diferentes tecnologías, convirtiendo así la información en uno de sus activos más importantes.

En ese sentido, la seguridad informática es una de sus principales prioridades.

Seguridad para Dispositivos

Al respecto, en los protocolos de **seguridad informática** de una empresa existen tres rubros de suma importancia por el rol que desempeñan en el ecosistema tecnológico de las mismas:

- Seguridad para dispositivos móviles MDM o EMM
- Seguridad para equipos de computo
- Auditoría y retención de datos
- Data loss Prevention (DLP)

Seguridad para dispositivos móviles MDM o EMM

Los dispositivos móviles personales en las empresas son una realidad porque pueden ser bastante útiles para el desarrollo de diferentes flujos de trabajo y a la organización le resulta difícil dotar a cada empleado con un smartphone o Tablet. Sin embargo, son claras amenazas a la seguridad informática de la empresa.

Los protocolos de seguridad informática de las empresas con respecto a estos dispositivos se hace importante, pues si los empleados acceden a los sistemas corporativos desde sus móviles la integridad de los datos es más vulnerable.

Mobile Device Management (MDM, en "español gestión de dispositivos móviles"), es un software que te permite controlar este riesgo.

El software permite:

- Instalar aplicaciones de **forma masiva y ejecutar actualizaciones** de forma remota.
- Aplicar **políticas de control** sobre las aplicaciones que los dispositivos móviles pueden ejecutar.
- **Rastrear** los dispositivos.
- **Sincronizar con el servidor** los archivos almacenados en los dispositivos móviles.
- **Bloquear funcionalidades en el dispositivo**, como cámara, micrófono, USB, entre otros.
- Restringir la cantidad de datos transmitidos.
- **Borrar datos de forma remota**, indispensable cuando el dispositivo se extravía.
- **Controlar la información** que se almacena en estos.
- **Crear copias de respaldo** y gestionar el cifrado.
- **Contenedores de información**, que se encargan de separar en el equipo los datos corporativos de la información personal del usuario, con el fin de evitar que información sensible termine siendo filtrada a terceros.

Seguridad para dispositivos móviles MDM o EMM

En términos generales, **MDM te permite asegurar, monitorear y administrar los dispositivos móviles** que se usan dentro de tu empresa, especialmente cuando están vinculados a los sistemas de la misma de forma que se mejoras sustancialmente la seguridad informática.

Todo esto es posible mediante una API exclusiva para tal fin y proveída por los sistemas operativos móviles. Sin duda una excelente solución para optimizar los planes de seguridad informática de la empresa.

Cabe señalar que MDM hace parte de una estrategia de seguridad informática mucho más amplia, denominada **Enterprise Mobility Management** (EMM, en español "gestión de movilidad empresarial").

Se trata de una colección de servicios enfocados a la seguridad informática, que administran todo el entorno corporativo móvil, incluidas las aplicaciones vinculadas al Internet de las Cosas y la administración de identidades y los puntos finales (UEM), incluidos los equipos de escritorio, computadoras portátiles y servidores.

Seguridad para equipos de computo

Los equipos de cómputo de tu empresa albergan información valiosa para su gestión comercial. Si la pierdes, el negocio puede tener serios problemas, que van desde inconvenientes para garantizar la continuidad de los flujos de trabajo hasta la quiebra total. El nivel de la amenaza a la seguridad informática de la empresa depende de la calidad y cantidad de datos perdidos.

Por eso, tanto los ordenadores de escritorio como los portátiles, e incluso los discos duros externos y los dispositivos USB, deben hacer parte del **plan integral de seguridad informática de la empresa**.

¿Qué pasaría, por ejemplo, si te robaran una computadora en el que tienes toda la información de prospectos y clientes?

Seguramente, tendrías serios problemas para ejecutar los planes de marketing y ventas ya planificados y tendrías que empezar de nuevo con la construcción de dicha base de datos. Sin mencionar los graves riesgos a la seguridad informática de la empresa.

La información de tus equipos de cómputo se halla expuesta a múltiples amenazas, como la pérdida por robo o daño del equipo y la infección y secuestro por virus o software malicioso. El protocolo de seguridad informática para ellos debe incluir desde copias de respaldo en diferentes formatos y localizaciones, hasta restricciones de acceso a terceros y protección contra ataques cibernéticos.

Auditoría y retención de datos

La política de retención de datos es clave en la seguridad informática de una empresa. Se trata de un **protocolo establecido** en una empresa para retener la información requerida para las necesidades operativas del negocio y/o para el cumplimiento de las regulaciones en lo que respecta a la conservación de la información, especialmente en **materia fiscal y financiera.**

Contar con este protocolo de seguridad informática es fundamental para **eliminar progresivamente los registros** o datos que dejan de ser relevantes para la empresa. Además, te permite conservar información importante para auditar usuarios en caso de que sea necesario.

Si no lo implementas no tienes ningún control sobre la información que se almacena ni la que se borra, haciendo compleja la búsqueda de datos claves cuando los necesitas.

Data loss Prevention (DLP)

Las soluciones Data Loss Prevention (prevención de pérdida de datos), se emplean para **prevenir y corregir las vulnerabilidades de un sistema** cuando son diagnosticadas y reducir las amenazas vinculadas a la falta de seguridad informática. También te permiten **definir políticas** para que la data de carácter confidencial no salga de la compañía.

Al respecto, existen tres tipos de soluciones DLP que debes conocer:

Network DLP:

Monitorea, rastrea y genera informes de todos los datos de tráfico en la red de la empresa. En términos generales, te permite saber qué información está siendo utilizados, por quién está siendo accedida y hacia dónde se dirige o de dónde proviene.

Storage DLP:

Te permite visualizar archivos confidenciales almacenados y compartidos por los colaboradores que tienen acceso a la red de la empresa. Así, puedes identificar puntos sensibles y prevenir las filtraciones de información.

Data loss Prevention (DLP)

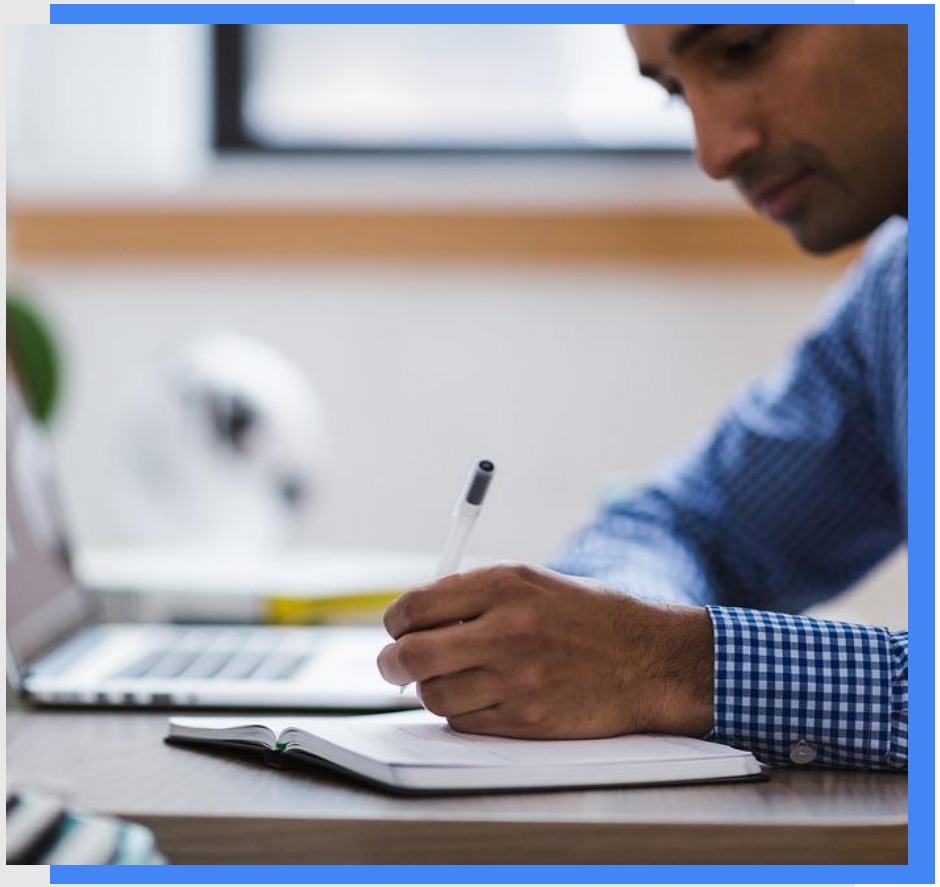
Endpoint DLP:

Se instala en todas las estaciones de trabajo y dispositivos empleados por los colaboradores para supervisar e impedir la salida de datos sensibles en dispositivos de almacenamiento extraíbles, aplicaciones para compartir o áreas de transferencia.

Data loss Prevention (DLP)

La **implementación de soluciones DLP** debe ser posterior a una consultoría que te indique cuáles son las vulnerabilidades del sistema corporativo en materia de seguridad informática. No usarlas puede derivar en que tus datos relevantes se pierdan fácilmente o terminen en manos equivocadas, aun cuando implementes otras soluciones de seguridad como las anteriormente señaladas.

De hecho, las soluciones DLP deben ser el punto de partida de cualquier acción o implementación de soluciones de seguridad informática. Si no sabes qué riesgos corres no puedes saber qué contratar.



No lo olvides...

La seguridad informática de tu empresa no es un juego. Debes prestarle la atención que merece. Una pérdida de información puede ser más perjudicial que la pérdida de dinero o maquinaria en un robo. Por lo tanto, es importante que investigues más sobre las soluciones aquí reseñadas y su implementación.

Acerca de Arroba System

Con más de 20 años de experiencia en transformación digital, Arroba System es uno de los primeros partners de **Google en México** y el primero a nivel Global en haber realizado un cambio de miles de usuarios de la plataforma de Office hacia Google Drive, Docs & Sheets en una empresa financiera, trabajando en conjunto con Google para el diseño de esta metodología, somos el único partner en México integrando la oferta "One Google" - G Suite, Chrome, Adwords, Analytics, Street View, Cloud y cumplimiento de políticas de calidad de Google para posicionamiento SEO.

Estamos entrenados por Google para ofrecer Talleres de **Transformación Digital** para las empresas basados en Design Thinking y servicios adicionales sobre la plataforma de G Suite.

¿Requieres información adicional?
¡Contáctanos!

contacto@arrobasystem.com

México +52 55 55439482

https://arrobasystem.com