20-5-2022

Políticas de seguridad

Administración de Redes

Miguel Lopez Ortega

Introducción:

La **ciberseguridad** es una preocupación creciente entre las empresas españolas. En los últimos tiempos los casos de ataques de *hackers* a diferentes empresas y organismos no han dejado de crecer.

Ser víctima de un ataque que atente contra la seguridad de la información de una empresa puede suponer consecuencias importantes para la organización.

Los **daños y la pérdida de datos** asociados a cualquier ataque son graves no solo por la información que se puede dañar sino, sobre todo, por el coste económico que puede suponer para la empresa paralizar su actividad hasta resolver la incidencia.

Índice:

políticas de seguridad de red

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema. Proporciona una base para la planificación de la seguridad al diseñar nuevas aplicaciones o ampliar la red actual. Describe responsabilidades del usuario como las de proteger información confidencial y crear contraseñas no triviales. La política de seguridad también debe describir cómo se va a supervisar la efectividad de las medidas de seguridad. Esta supervisión le ayudará a determinar si alguna persona podría intentar burlar sus defensas.

1. Test de seguridad.

El punto de partida para que puedas diseñar tu política de seguridad es analizar la situación de tu empresa. De esta forma, podrás saber cuál es la situación y en qué áreas hay vulnerabilidades o pueden surgir problemas. Con la información que te aportará el test puedes diseñar una estrategia de seguridad personalizada.

2. Análisis de riesgos

Con un análisis de riesgos podrás saber cuál es el nivel de seguridad de tu red. Debe analizar cuáles son los puntos de entrada en tu red y los diferentes puntos en los que puede haber riesgos.

Debes ser capaz de definir tres niveles de riesgo en la información y en la red de tu organización:

– Riesgo bajo. Se consideran así los datos que en caso de pérdida no suponen un problema para el desarrollo del negocio en la empresa. Son, por tanto, datos que no suponen una pérdida económica importante ni acarrean repercusiones legales graves.

– Riesgo medio. En este caso se trata de información y datos que, en caso de perderse no supondrán un coste económico muy elevado y, aunque puedan suponer la interrupción del servicio o de la actividad de la empresa, no lo será en gran medida ni por mucho tiempo.

– Riesgo alto. Son datos que, en caso de pérdida, podrían suponer la interrupción de la actividad de la empresa, pondrían en peligro la integridad de una persona y supondrían un nivel alto de gasto o repercusiones legales importantes.

3. Revisión de contraseñas

En caso de que se haya llevado a cabo alguna actualización de *software* o algún cambio en los sistemas de seguridad implementados en la empresa, habrá que modificar las contraseñas.

Las contraseñas usadas por los trabajadores deben ser revisadas y cambiadas con regularidad y evitar en todo momento emplear contraseñas que coincidan con el nombre de la empresa, con números te teléfono o con direcciones.

Es preferible usar contraseñas de alta complejidad que combinen diferentes caracteres con letras y números.

4. Establecer protocolos de seguridad

Algo que siempre debes contemplar en tu organización es hacer copias de seguridad de la documentación que usas en red y de cuanta información sea de vital importancia para la empresa.

Esta información se maneja habitualmente y, en caso de pérdida, puede suponer un problema grave para la organización.

Con el desarrollo de protocolos seguros se minimizarán las consecuencias y los riesgos serán menores.

5. Formar e informar

Un aspecto fundamental para que todo funcione correctamente es que tu personal esté formado e informado sobre las medidas de seguridad que se están implementando en la organización.

Para ello, es importante implicar al trabajador en las decisiones que se adoptan en relación con la seguridad y los protocolos establecidos.

6. Crear un equipo de seguridad y una estructura

Es importante que haya una buena organización de la seguridad y que haya determinadas personas en la organización que estén velando por el cumplimiento de los protocolos y las medidas adoptadas.

En este sentido, debes contar con un equipo fiable que sea estricto en el cumplimiento de las normas establecidas.

Tanto la política de seguridad como los protocolos se deben de revisar con regularidad.

7. Protección antivirus

Debes estar muy pendiente de que en tu organización se mantengan protegidos los equipos y ordenadores. La única forma de conseguirlo es, precisamente,

implantando un sistema de actualización y revisión constante de los ordenadores para que tengan las últimas versiones de antivirus instaladas.

protocolos de seguridad de una red

Los protocolos de seguridad informática son las reglas o normas diseñadas para garantizar la confidencialidad, la integridad y la disponibilidad de la información. Es decir, son las medidas de seguridad implementadas para evitar que personas no autorizadas puedan acceder a la información, manipularla o destruirla. O evitar que eventos o incidentes técnicos tengan ese mismo resultado.

Son ejemplos los protocolos de red, los protocolos de autenticación o las medidas de ciberseguridad implementadas por la empresa.

Por lo tanto, podemos decir que existen diferentes tipos de protocolos de seguridad informática en empresas y de seguridad en Internet.

Protocolos de seguridad básicos para mejorar la seguridad en Internet

Protocolo TCP/IP

El protocolo TCP/IP es el protocolo básico de comunicación en Internet. Se trata de dos protocolos, el TCP (protocolo de control de transmisión) y el IP (protocolo de Internet). A través de ellos, los dispositivos conectados a la Red pueden comunicarse entre sí y transmitir información a través de ella.

Protocolo HTTP

El protocolo HTTP es el protocolo de transferencia de hipertexto empleado para transmitir mensajes por la Red. Basado en la World Wide Web (www), transmite los mensajes entre el navegador y el servidor web.

Para garantizar la seguridad de la información, es necesario usar los certificados HTTPS o SSL, que cifran la información y evitan que esta pueda ser interceptada en un sitio web.

Protocolo FTP

El protocolo FTP o protocolo de transferencias de archivos, se usa para transferir archivos de un equipo a otro a través de la Red. Este

protocolo permite subir y descargar archivos desde o hacia un ordenador en un esquema servidor-cliente, con independencia del sistema operativo que use cada equipo. Emplea un modelo de capas de red TCP/IP y una contraseña para establecer la conexión remota.

Para reforzar la seguridad, se recurre al protocolo SFTP, para proceder al cifrado de datos y evitar el acceso de terceros no autorizados a los archivos.

Protocolo SSH

SSH o Secure Shell es tanto un protocolo como el nombre del programa que lo implementa y permite el acceso remoto a un servidor a través de un canal seguro en el que toda la información viaja cifrada. Este protocolo permite conectar de forma segura dispositivos remotos y autenticar a sus usuarios.

Protocolo DNS

El protocolo DNS traduce los nombres de dominio (direcciones URL) a direcciones IP (conjunto de números), para que podamos acceder a sitios web.

Existen servidores DNS privados y libres, siendo los primeros los más seguros, puesto que garantizan una mayor privacidad cuando navegamos, cifrando toda la información.

Cifrar las bases de datos

Al desarrollar procesos de seguridad informática para la empresa, el cifrado de sus bases de datos es una de las primeras medidas de seguridad a las que debemos recurrir. El cifrado consiste en aplicar un algoritmo asociado a una o varias claves para poder descifrarlo. Existen diferentes formatos, pero el resultado es el mismo, impedir que terceros no autorizados puedan acceder a la información.

Aumentar la seguridad en las contraseñas

Es uno de los consejos de seguridad básicos, aumentar la seguridad de las contraseñas, creando claves complejas, que combinen varias letras (mayúsculas y minúsculas), números y símbolos. O recurrir a un gestor de contraseñas.

Software actualizado

Siempre debe actualizarse cualquier software a su última versión, para evitar vulnerabilidades conocidas que permitan que usuarios no autorizados puedan acceder a nuestros equipos o red interna.

Captchas

El empleo de captchas evitará el acceso de bots en nuestra red y equipos. En este artículo explicamos qué es el captcha y cómo funciona en detalle.

Cumplir con la legalidad

Conocer las normativas te ayudará a cumplir con la legalidad, además de saber qué medidas de seguridad estás obligado a implementar y qué hacer en caso de incidentes de seguridad.

Seguridad en las comunicaciones

Finalmente, mejora la seguridad en las comunicaciones aplicando en tu servidor de correo electrónico reglas de spam y bloqueo de cuentas sospechosas, además, conciencia a tus empleados para que no abran archivos adjuntos o pulsen en enlaces de correos sospechosos.

Conclusión:

En conclusión, la implementación de políticas y protocolos de seguridad informática en una organización es una solución integral que no sólo busca proteger, preservar y administrar de una manera eficiente todo tipo de recursos con los que cuenta una organización, sino que también busca dar solución, prevenir, evitar, controlar y minimizar los daños de incidentes que afectan a la organización.