Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos

La seguridad de los equipos informáticos se basa en una serie de principios que son aceptados a nivel global. Estos principios ayudan a garantizar la protección de los sistemas ante las amenazas más comunes, a través de la gestión adecuada de riesgos y la implementación de salvaguardas tecnológicas y organizativas.

1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información.

En el contexto actual de la seguridad informática, donde las amenazas evolucionan constantemente, es esencial que las organizaciones no solo se limiten a instalar herramientas de seguridad, como antivirus o cortafuegos, sino que adopten un enfoque más integral: la gestión del riesgo. Pero ¿qué significa realmente gestionar el riesgo en un sistema de información? En pocas palabras, se trata de un proceso continuo que busca identificar posibles vulnerabilidades y amenazas que puedan afectar a los sistemas y, con base en ello, aplicar medidas preventivas o correctivas para mitigar sus efectos.

La gestión del riesgo, además de enfocarse en los aspectos técnicos, también incluye decisiones organizativas y estratégicas. Por ejemplo, no todas las empresas tienen los mismos recursos, y no es lo mismo proteger la información de una gran empresa que la de una pequeña tienda local que maneja sus operaciones en un servidor básico. Por eso, un modelo de seguridad orientado a la gestión del riesgo debe adaptarse a las características específicas de cada organización, analizando sus necesidades y limitaciones.

Fases del modelo de seguridad orientado a la gestión del riesgo:

Este modelo se basa en tres fases principales: identificación de riesgos, evaluación de su impacto y probabilidad, y control de esos riesgos mediante la implementación de medidas concretas. A continuación, exploramos cada una de ellas en detalle:

Fase 1: Identificación de riesgos.

El primer paso en la gestión del riesgo es identificar qué amenazas pueden afectar a los sistemas de información. Esto incluye tanto amenazas externas (ataques cibernéticos, malware, etc.) como internas (errores humanos, accesos no autorizados de empleados, etc.). Imaginemos una empresa que gestiona datos sensibles de clientes, como números de cuentas bancarias o direcciones postales. En este caso, uno de los riesgos más evidentes sería una fuga de información o un ciberataque que exponga esos datos a terceros.

La identificación de riesgos debe hacerse de forma sistemática, abarcando los componentes tecnológicos y los procesos de negocio. Por ejemplo, ¿qué sucede si un empleado no sigue

correctamente las políticas de seguridad? ¿O si un dispositivo móvil con información crítica se pierde o es robado? Todos estos escenarios representan riesgos que deben ser tenidos en cuenta.

Además, la identificación no debe limitarse a un momento puntual, sino que debe ser un proceso continuo. Las tecnologías cambian, las amenazas evolucionan, y lo que hoy parece seguro, mañana puede no serlo. Por ejemplo, el uso de la nube se ha extendido en los últimos años, y con ello han surgido nuevos riesgos relacionados con la gestión de la información en servidores remotos.

Fase 2: Evaluación del riesgo.

Una vez identificados los riesgos, el siguiente paso es evaluarlos. Esto se hace en función de dos criterios principales: la probabilidad de que ocurra un incidente y el impacto que tendría en la organización si sucediera. Este análisis es fundamental, ya que permite priorizar qué riesgos deben ser tratados de inmediato y cuáles pueden gestionarse a largo plazo.

Para ilustrarlo, volvamos al ejemplo de la empresa que maneja datos bancarios. Si la probabilidad de que alguien intente acceder sin autorización a esos datos es alta y el impacto de un posible ataque sería catastrófico (multas por incumplir la normativa de protección de datos, pérdida de reputación, etc.), este riesgo debe gestionarse con urgencia. Sin embargo, otros riesgos, como la pérdida de dispositivos móviles de empleados que no contienen información sensible, podrían considerarse menos prioritarios.

La evaluación del riesgo se lleva a cabo utilizando diferentes metodologías, entre las que destacan el análisis cualitativo y el cuantitativo. El análisis cualitativo clasifica los riesgos de manera general (alto, medio o bajo), mientras que el cuantitativo asigna valores numéricos basados en estimaciones de pérdidas económicas o de impacto. Ambos enfoques tienen sus ventajas y desventajas, y muchas organizaciones utilizan una combinación de ambos. A continuación, vamos a desarrollar un ejemplo específico de evaluación del riesgo utilizando ambas metodologías: cualitativa y cuantitativa, en una empresa de servicios financieros que maneja datos sensibles, como información bancaria de sus clientes:

Ejemplo

Imaginemos una empresa de servicios financieros con sede en España que gestiona datos sensibles de 10.000 clientes, incluyendo información bancaria, datos personales y registros de transacciones. Esta empresa está obligada a cumplir con el Reglamento General de Protección de Datos (RGPD), lo que implica que una fuga de información o un ciberataque que comprometa los datos podría resultar en sanciones graves, así como una pérdida significativa de confianza por parte de los clientes.

La empresa ha identificado una vulnerabilidad no parcheada en su servidor de bases de datos, que podría ser explotada por atacantes externos para acceder a la información bancaria de los clientes. El departamento de seguridad ha decidido evaluar este riesgo utilizando dos metodologías: el análisis cualitativo y el análisis cuantitativo, con el fin de priorizar sus esfuerzos y decidir qué medidas implementar para mitigar esta amenaza.

Análisis cualitativo

El equipo de seguridad realiza una evaluación cualitativa basada en su conocimiento y experiencia con incidentes anteriores y la vulnerabilidad existente:

Probabilidad: Media

- Durante los últimos 6 meses, la empresa ha sido blanco de 12 intentos de ciberataques. Aunque ningún ataque ha sido exitoso hasta ahora, la existencia de una vulnerabilidad no parcheada en el servidor aumenta el riesgo de que un atacante tenga éxito en el futuro.
- El equipo clasifica la probabilidad como "media" porque, aunque la empresa ha implementado medidas de seguridad básicas, la vulnerabilidad sigue siendo una puerta potencial para ataques futuros.

Impacto: Alto

- Si la vulnerabilidad es explotada, los datos bancarios de los 10.000 clientes estarían en riesgo. La fuga de información tendría un impacto severo en la empresa, incluyendo multas por violación del RGPD (que podrían alcanzar los 500.000 €), una posible pérdida de confianza y clientes, y el coste de responder legalmente a la situación.
- El equipo clasifica el impacto como "alto", debido a las graves consecuencias financieras y reputacionales de una fuga de este tipo.

Resultado cualitativo: Riesgo Alto

- Aunque la probabilidad es media, el impacto es crítico. Esto lleva al equipo a concluir que el riesgo general es "alto". Esto significa que la empresa debe priorizar este riesgo y tomar medidas correctivas lo antes posible.

Análisis cuantitativo:

El equipo luego procede a realizar un análisis cuantitativo para obtener una visión más precisa del riesgo financiero asociado a esta vulnerabilidad:

Probabilidad: 15%

- A partir de los datos históricos, la empresa estima que existe una probabilidad del 15% de que la vulnerabilidad sea explotada en los próximos 12 meses. Esta estimación se basa en los intentos anteriores de ciberataques y en la falta de actualización de los sistemas.
- La empresa utiliza datos de los últimos 6 meses, en los cuales ha habido intentos recurrentes de acceso no autorizado, ajustando la probabilidad a un 15% debido a la falta de parcheado en el sistema.

Impacto financiero: 1.000.000 €

- Si el ataque es exitoso, el impacto financiero total se estima en 1.000.000 €. Esta cifra incluye:
  - Multas del RGPD: La empresa enfrenta una posible multa de 500.000 € por incumplimiento del RGPD en caso de una fuga de datos.
  - Costes legales: Los costos de defensa y las posibles demandas de clientes se estiman en unos 200.000 €.
  - Pérdida de clientes: La empresa calcula que podría perder hasta un 10% de sus clientes, lo que equivaldría a una pérdida de ingresos de 300.000 € anuales.

Resultado cuantitativo: 150.000 €

- Utilizando la fórmula de evaluación del riesgo cuantitativo, el equipo calcula que:

```
Riesgo = Probabilidad x Impacto financiero = 0.15 x 1.000.000 = 150.000€
```

  - Este cálculo significa que la empresa puede esperar, en promedio, una pérdida de 150.000 € asociada a este riesgo en los próximos 12 meses si no se toman medidas correctivas. Este valor representa una estimación del "costo esperado" del riesgo, y puede ayudar a justificar la inversión necesaria para mitigar este problema.

<u>Aplicación del análisis:</u>

- Con ambos análisis en la mano, la empresa puede justificar la inversión en mitigar la vulnerabilidad, dado que el riesgo es alto tanto cualitativamente como cuantitativamente.
- Con la estimación de un impacto potencial de 150.000 €, la empresa puede decidir invertir en medidas de seguridad que reduzcan significativamente este riesgo, como implementar sistemas de monitoreo, mejorar la protección de sus servidores, o contratar personal especializado en seguridad informática.

Fase 3: Control del riesgo.

El último paso en este modelo es aplicar medidas de control que permitan reducir o eliminar los riesgos identificados. Existen varias formas de hacerlo, que van desde soluciones tecnológicas (como la instalación de un firewall avanzado) hasta medidas organizativas (como la formación de los empleados en prácticas seguras). El objetivo es disminuir tanto la probabilidad de que ocurra el incidente como el impacto que tendría.

Es importante destacar que no siempre es posible eliminar todos los riesgos. Por ejemplo, ninguna medida de seguridad garantiza un 100% de protección contra ciberataques, pero se pueden implementar mecanismos que minimicen las posibilidades de que sucedan. En este sentido, el modelo de gestión del riesgo busca encontrar un equilibrio entre seguridad y funcionalidad. No tiene sentido implementar medidas extremadamente estrictas que entorpezcan el trabajo diario de los empleados o que supongan un coste inasumible para la organización. Supongamos que una pequeña empresa en Sevilla gestiona la contabilidad de sus clientes a través de una aplicación en la nube. Para reducir el riesgo de accesos no autorizados, decide implementar varias medidas: primero, obliga a sus empleados a usar contraseñas complejas y a cambiarlas cada tres meses. Además, activa la autenticación de dos factores (2FA) en todos sus sistemas y configura un sistema de alertas que le notifica si se intenta acceder desde ubicaciones no habituales. Con estas medidas, la empresa no elimina el riesgo de accesos no autorizados, pero sí lo reduce significativamente.

El modelo de gestión del riesgo no es un proceso que se realice una vez y se olvide. Al contrario, debe revisarse y actualizarse de manera constante, ya que tanto el entorno tecnológico como las amenazas evolucionan rápidamente. ¿Recuerdas la última vez que tu sistema operativo te pidió instalar una actualización? Ese es un ejemplo sencillo de cómo las amenazas cambian y los sistemas deben adaptarse. La mejora continua implica actualizar las herramientas de seguridad, revisar los procesos y formar regularmente a los empleados para que estén al tanto de las últimas amenazas. Por ejemplo, hace unos años, las técnicas de phishing eran bastante rudimentarias, pero hoy en día son mucho más sofisticadas, utilizando técnicas de ingeniería social para engañar incluso a usuarios avanzados. Mantenerse al día con estos cambios es fundamental para que la gestión del riesgo sea efectiva.

2. Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes.

En el ámbito de la seguridad informática, existen ciertas amenazas que son más comunes y que afectan a todo tipo de organizaciones, desde grandes corporaciones hasta pequeñas empresas. Conocer estas amenazas es fundamental para poder gestionarlas de manera eficaz. A continuación, analizaremos algunas de las más frecuentes, los riesgos que conllevan y las medidas que pueden adoptarse para protegerse.

Amenazas frecuentes:

Malware

El malware es uno de los términos más conocidos en el mundo de la informática y engloba una amplia variedad de programas maliciosos, como virus, troyanos, ransomware, entre otros. Cada uno de ellos tiene un comportamiento específico, pero todos comparten el mismo objetivo: comprometer la seguridad del sistema o robar información. Un ejemplo muy conocido es el ransomware "WannaCry", que en 2017 afectó a empresas e instituciones en todo el mundo, incluyendo España.

- Riesgo: El malware puede paralizar los sistemas, robar datos confidenciales o incluso destruir información crítica.
- Salvaguardas: Para protegerse contra el malware, es esencial contar con un antivirus actualizado, realizar copias de seguridad periódicas y mantener los sistemas operativos y aplicaciones al día con las últimas actualizaciones de seguridad. En la siguiente imagen se muestran algunos de los antivirus con más popularidad del mercado y sus principales características:

Actividad 1

Lee el artículo y reflexiona sobre lo siguiente:

¿Qué debilidades encontraron los cibercriminales en los sistemas operativos afectados por WannaCry? ¿Por qué muchas organizaciones no estaban preparadas para este tipo de ataque?

¿Por qué crees que afectó a tantos países y organizaciones en todo el mundo, incluyendo hospitales y empresas grandes como Telefónica?

A la luz de lo que has leído, ¿qué medidas crees que son esenciales para prevenir futuros ataques de ransomware? ¿Qué acciones concretas podrías tomar en tu propia vida digital para protegerte de este tipo de amenazas?

Enlace al artículo: https://www.kaspersky.es/resource-center/threats/ransomware-wannacry

Phishing

El phishing es una técnica de ingeniería social utilizada para engañar a los usuarios y hacerles revelar información confidencial, como contraseñas o números de tarjetas de crédito. Normalmente, los atacantes envían correos electrónicos que aparentan ser de fuentes confiables, como bancos o empresas, para inducir a la víctima a que haga clic en un enlace malicioso o proporcione sus datos.

- Riesgo: Los usuarios pueden entregar información sensible a delincuentes sin darse cuenta, lo que puede derivar en el robo de identidad o el acceso no autorizado a cuentas personales o corporativas.
- Salvaguardas: Educar a los empleados sobre cómo identificar correos electrónicos sospechosos y no hacer clic en enlaces o descargar archivos adjuntos de fuentes no verificadas es una de las medidas más efectivas. Además, implementar políticas de autenticación de dos factores (2FA) puede ofrecer una capa adicional de protección.

Ejemplo

Imaginemos una pequeña empresa en España que gestiona cuentas bancarias para sus clientes. Una empleada, Leonor, recibe un correo electrónico aparentemente legítimo de su banco, solicitando que actualice la información de seguridad de la cuenta corporativa. El correo parece provenir de una fuente confiable, pero en realidad es un ataque de phishing.

1. El correo de phishing

Leonor está trabajando en su oficina cuando, de repente, recibe un correo electrónico con el asunto:

"Actualización de seguridad de la cuenta: Acción requerida inmediatamente"

El remitente parece ser “Banco España” (el banco con el que trabaja su empresa), y el correo tiene un logotipo y diseño similar al que habitualmente envía el banco, lo que le da una apariencia legítima.

El cuerpo del mensaje dice:

Estimado cliente,

Estamos actualizando nuestros sistemas de seguridad. Para continuar utilizando su cuenta sin interrupciones, es necesario que verifique sus datos haciendo clic en el enlace a continuación. Esta medida es urgente y debe realizarse dentro de las próximas 24 horas para evitar la suspensión temporal de su cuenta.

Enlace de verificación: Verificar mi cuenta

Agradecemos su atención a este asunto.

Atentamente,

Banco España

2. La toma de decisión de la víctima

Leonor, aunque algo apresurada con su trabajo, ve el correo y piensa: "Es raro que el banco me envíe esto, pero si es urgente, mejor lo hago ahora". El correo parece muy profesional, con el logotipo del banco, una dirección de correo electrónico que contiene el nombre del banco y un enlace que, a simple vista, parece confiable.

Aunque Leonor tiene dudas, decide hacer clic en el enlace antes de que expire el supuesto plazo.

3. La página de phishing

Al hacer clic en el enlace, se abre una página web que parece ser la página de inicio de sesión del Banco España. Todo se ve exactamente igual: el logotipo, el diseño, los colores y los campos de entrada para nombre de usuario y contraseña. Sin embargo, esta página es una falsa réplica creada por el atacante para robar la información de Leonor.

La página solicita su número de cuenta y contraseña. Leonor, confiada de que está en la página oficial del banco, introduce sus datos.

4. La explotación del ataque

Una vez que Leonor introduce su información, esta es enviada inmediatamente a los delincuentes cibernéticos que organizaron el ataque de phishing. En este momento, los atacantes ya tienen acceso directo a la cuenta bancaria corporativa de su empresa.

Los atacantes utilizan las credenciales robadas para acceder a la cuenta, donde empiezan a realizar transferencias fraudulentas o extraen información sensible de la empresa para planificar ataques futuros más dirigidos.

5. Detectando el ataque demasiado tarde

Horas más tarde, Leonor recibe una notificación directamente del banco (esta vez, real) informando de transacciones inusuales en la cuenta. Al revisar el correo electrónico original con más atención, Leonor se da cuenta de algunos detalles sospechosos que no había notado antes:

La dirección de correo electrónico del remitente es similar pero ligeramente diferente a la oficial del banco.

El enlace del correo, al revisarlo con más calma, dirige a una URL extraña que no pertenece al dominio del banco.

El tono del correo suena demasiado alarmista, lo que debería haber sido una señal de advertencia.

Desafortunadamente, en ese momento, ya es demasiado tarde: los atacantes han tenido acceso durante horas y ya han hecho uso de la información robada.

Nota

Para evitar el phishing, alguien debe fijarse en:

- Remitente del correo: Verifica si la dirección de correo es legítima o tiene pequeñas variaciones sospechosas.
- Enlaces: Pasa el ratón sobre los enlaces sin hacer clic para ver la URL real. Si parece extraña o no coincide con el dominio oficial, no sigas el enlace.
- Errores gramaticales: Correos oficiales suelen ser impecables. Los mensajes de phishing a menudo contienen errores.
- Tono urgente: Desconfía de correos que insistan en tomar acción inmediata o amenacen con bloquear tu cuenta.
- Archivos adjuntos: Evita abrir archivos adjuntos de remitentes no verificados.

Ataques de denegación de servicio (DoS)

Los ataques de denegación de servicio buscan sobrecargar un servidor o red con tráfico, de manera que los usuarios legítimos no puedan acceder a los servicios. En el caso de un ataque distribuido (DDoS), el tráfico malicioso proviene de múltiples fuentes, lo que hace que sea más difícil de bloquear. Aunque estos ataques suelen dirigirse a grandes organizaciones, también pueden afectar a pequeñas empresas con infraestructuras menos robustas.

- Riesgo: Los ataques DoS pueden causar una interrupción completa de los servicios en línea, lo que genera pérdidas económicas y afecta la reputación de la empresa.
- Salvaguardas: Utilizar firewalls que puedan filtrar el tráfico no deseado, implementar sistemas de detección de intrusos y contar con proveedores de servicios que ofrezcan protección contra DDoS son medidas clave para mitigar este tipo de amenazas.

Ejemplo

Por ejemplo, un hacker puede utilizar una red de bots para enviar miles de solicitudes simultáneamente a un servidor web de una empresa pequeña. El servidor, incapaz de gestionar tal cantidad de tráfico, colapsa, interrumpiendo los servicios legítimos y generando una denegación de servicio. Esto puede afectar a la reputación de la empresa y causar pérdidas económicas debido a la inactividad.

Se puede implementar un IDS basado en red (NIDS), que monitoree el tráfico en tiempo real buscando patrones anormales. Este IDS puede identificar un aumento inusual en las solicitudes, activar alertas y bloquear automáticamente las direcciones IP maliciosas. Además, es recomendable integrar un firewall que filtre el tráfico y utilice análisis heurísticos para detener ataques DoS/DDoS antes de que afecten al servidor.

Una solución adicional es el uso de servicios de protección anti-DDoS ofrecidos por proveedores especializados, que pueden filtrar y dispersar el tráfico malicioso.

Accesos no autorizados

El acceso no autorizado a los sistemas de información es una amenaza constante. Puede ocurrir por el robo de contraseñas, la explotación de vulnerabilidades en el software o incluso mediante el acceso físico a dispositivos no protegidos. Un ejemplo clásico es el uso de contraseñas débiles o repetidas, que pueden ser adivinadas o robadas por un atacante.

- Riesgo: Si un atacante obtiene acceso a un sistema, puede modificar, robar o eliminar información crítica, lo que puede causar daños irreparables.
- Salvaguardas: Para evitar accesos no autorizados, es fundamental utilizar contraseñas complejas y únicas, activar la autenticación de dos factores y restringir el acceso a los sistemas solo a los usuarios que realmente lo necesiten.

Nota

Al elegir una contraseña utiliza combinaciones de letras mayúsculas, minúsculas, números y símbolos. no reutilices contraseñas entre diferentes cuentas.

Pérdida o robo de dispositivos

En la actualidad, gran parte de la información empresarial se maneja en dispositivos móviles, como portátiles, smartphones o tabletas. Estos dispositivos son especialmente vulnerables a pérdidas o robos, lo que podría poner en peligro la información sensible almacenada en ellos.

- Riesgo: La pérdida o robo de un dispositivo puede derivar en el acceso no autorizado a datos empresariales o incluso a toda la red corporativa.
- Salvaguardas: Implementar el cifrado de discos duros y dispositivos móviles, así como usar herramientas de gestión remota que permitan borrar los datos en caso de pérdida, son medidas esenciales. Además, siempre es recomendable que los dispositivos estén protegidos por contraseñas o sistemas de autenticación biométrica (huellas dactilares, reconocimiento facial).

3. Salvaguardas y tecnologías de seguridad más habituales.

Las salvaguardas son medidas que se implementan para proteger los sistemas de información y minimizar el riesgo de sufrir incidentes como ciberataques, pérdida de datos o accesos no autorizados. Además, a lo largo de los años se han desarrollado diversas tecnologías de seguridad que facilitan la protección de sistemas informáticos, y es fundamental conocer las más utilizadas en la actualidad.

Pie de imagen: Tipos de salvaguardas de seguridad.

Las salvaguardas o medidas de seguridad que se aplican para proteger los sistemas de información pueden clasificarse en tres tipos: preventivas, detectivas y correctivas. Cada una cumple una función específica en la protección contra amenazas:

- Salvaguardas preventivas: Son aquellas que buscan evitar que un incidente ocurra. Por ejemplo, la instalación de un firewall o la formación de empleados para que no caigan en ataques de phishing. Estas medidas se implementan antes de que el riesgo se materialice. Algunas de las salvaguardas preventivas más comunes son:
  - Cifrado de datos: Consiste en convertir la información en un código ilegible para cualquier persona que no tenga la clave de desencriptado. Este mecanismo es especialmente útil cuando los datos se transfieren a través de redes públicas o se almacenan en dispositivos portátiles. Por ejemplo, si pierdes un pendrive con información sensible, el cifrado garantiza que nadie más pueda leer los datos.
  - Cortafuegos (firewalls): Los cortafuegos actúan como una barrera entre la red interna de una organización y el exterior, filtrando el tráfico para evitar que intrusos accedan a los sistemas. Hay varios tipos de cortafuegos, desde los tradicionales hasta los de "próxima generación", que analizan el contenido de los paquetes de datos. Por ejemplo, en una empresa que utiliza internet para la mayoría de sus operaciones, el cortafuegos es la primera línea de defensa frente a intentos de acceso no autorizados.
  - Contraseñas robustas: Aunque puede parecer una medida básica, el uso de contraseñas seguras sigue siendo una de las salvaguardas más eficaces. Una contraseña robusta debe combinar letras, números y símbolos, y no ser fácilmente

adivinable. ¿Cuántos usuarios utilizan "1234" o "password" como contraseña? Es sorprendente, pero sigue siendo una práctica común en muchos lugares. Establecer políticas que obliguen a los empleados a usar contraseñas fuertes y a cambiarlas periódicamente es fundamental.

- Autenticación de dos factores (2FA): Cada vez más servicios están incorporando la autenticación de dos factores como una medida estándar de seguridad. Esta técnica requiere que el usuario proporcione dos formas de verificación (normalmente una contraseña y un código enviado al móvil). Un ejemplo claro es cómo los bancos en España solicitan este tipo de autenticación para acceder a la banca en línea, lo que añade una capa adicional de seguridad.

- Salvaguardas detectivas: Se encargan de detectar la actividad sospechosa o anómala una vez que esta ha ocurrido. Las salvaguardas detectivas no evitan el incidente, pero permiten detectarlo rápidamente para tomar medidas correctivas. Es como si tuvieras una alarma en casa: no impide que entren los ladrones, pero te avisa cuando alguien lo intenta. Un sistema de detección de intrusos (IDS) o la monitorización de logs de seguridad son ejemplos de salvaguardas detectivas:
  - Sistemas de detección de intrusos (IDS): Estos sistemas monitorizan la actividad en la red para detectar comportamientos sospechosos o intentos de intrusión. Por ejemplo, si una red está siendo objeto de un ataque de fuerza bruta (cuando un atacante intenta adivinar las contraseñas mediante múltiples intentos), el IDS puede identificar este patrón y alertar a los administradores de red para que tomen medidas.
  - Monitorización de logs: Los logs o registros son archivos donde se guarda toda la actividad de un sistema. Revisarlos regularmente permite detectar comportamientos anómalos, como accesos no autorizados o cambios en configuraciones importantes. En una empresa que almacena datos sensibles, monitorizar estos logs puede ser la clave para detectar intentos de ataque antes de que causen daño.

- Salvaguardas correctivas: Se aplican después de que ha ocurrido un incidente de seguridad, con el objetivo de minimizar el daño y restaurar la normalidad lo antes posible. Añgunos ejemplos comunes son:
  - Restauración de copias de seguridad (backups): Tener copias de seguridad es esencial para poder recuperar la información perdida o comprometida. En España, donde muchas pymes no tienen grandes recursos tecnológicos, contar con backups periódicos puede ser la diferencia entre perder toda la información y continuar operando sin mayores contratiempos. Por ejemplo, una empresa que sufre un ataque de ransomware (donde los archivos son encriptados por un atacante) puede restaurar su información desde una copia de seguridad sin tener que pagar el rescate.
  - Actualización y parcheo de sistemas: Cuando un sistema o software ha sido atacado porque tenía una vulnerabilidad, es fundamental aplicar parches que solucionen ese fallo para evitar que se repita. ¿Sabías que muchos de los ataques se deben a que las empresas no actualizan sus sistemas a tiempo? Mantener el software al día es una de las formas más efectivas de corregir problemas de seguridad.

4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas.

Aunque las salvaguardas y las tecnologías de seguridad son esenciales para proteger los sistemas informáticos, no son suficientes por sí solas. Aquí es donde entra en juego la gestión de la seguridad informática, que actúa como complemento necesario para garantizar que las medidas técnicas se apliquen de forma coherente y efectiva dentro de la organización.

Pie de imagen: Gestión de la seguridad informática.

La gestión de la seguridad implica la planificación, implementación y supervisión de políticas, procedimientos y buenas prácticas que aseguren la protección de la información. No basta con instalar un antivirus o un firewall; también es necesario gestionar cómo se utilizan estas herramientas, cómo se capacita a los empleados y cómo se reacciona ante posibles incidentes.

Una política de seguridad es un conjunto de reglas y directrices que establece cómo se deben proteger los sistemas y los datos dentro de una organización. Estas políticas no solo cubren los aspectos técnicos, sino también los organizativos. Por ejemplo, en una empresa que maneja datos de clientes, puede ser necesario definir quién tiene acceso a qué tipo de información, cómo se almacenan los datos y cómo se deben gestionar los dispositivos portátiles.

Imagina una empresa en Berriozar que tiene una política estricta sobre el uso de dispositivos personales. Los empleados no pueden llevarse a casa información confidencial en sus móviles o portátiles sin cifrado, y el acceso a la red interna desde casa solo se permite a través de una conexión VPN. Estas políticas protegen la empresa de un posible ataque y crean una cultura de seguridad entre los empleados:

POLÍTICA DE USO DE DISPOSITIVOS Y SEGURIDAD

ACCESO A LA RED INTERNA

El acceso remoto a la red interna de la empresa desde fuera de la oficina solo se permitirá a través de una conexión VPN segura provista por el departamento de TI.

USO DE DISPOSITIVOS PERSONALES

Está estrictamente prohibido almacenar información confidencial en dispositivos móviles personales, como portátiles o smartphones, sin el cifrado de datos autorizado por el departamento de TI.

POLÍTICAS DE SEGURIDAD ADICIONALES

- No se permite la descarga de documentos sensibles en dispositivos no autorizados.
- Los dispositivos personales deben ser revisados periódicamente por el equipo de TI para garantizar que cumplen con los estándares de cifrado.
- El acceso a datos críticos estará protegido mediante autenticación de dos factores (2FA).

PROTECCIÓN DE LA RED DOMÉSTICA

Se recomienda asegurar la red Wi-Fi doméstica con cifrado WPA2 o superior, utilizando contraseñas robustas.

REPORTES DE SEGURIDAD

Cualquier sospecha de violación de seguridad o acceso no autorizado debe ser reportada de inmediato al departamento de TI, siguiendo los protocolos establecidos.

SANCIONES

El incumplimiento de estas políticas podrá resultar en sanciones, incluyendo la suspensión de accesos o medidas disciplinarias, según la gravedad del incumplimiento.

Una parte fundamental de la gestión de la seguridad es la formación continua de los empleados. Las mejores medidas de seguridad pueden fallar si las personas que trabajan con ellas no saben cómo usarlas correctamente o no entienden su importancia. Por ejemplo, ¿de qué sirve tener contraseñas robustas si los empleados las anotan en un post-it pegado al monitor?

Supongamos que una pyme en Logroño decide formar a sus empleados sobre phishing, ya que han detectado varios intentos de este tipo en su sistema de correos electrónicos. Durante la formación, se enseña a los empleados a identificar correos sospechosos, a no hacer clic en enlaces sin verificar y a informar rápidamente si reciben un correo dudoso. Esta formación puede ser decisiva para evitar que la empresa caiga en una trampa de ingeniería social.

Otra parte importante de la gestión de la seguridad es definir cómo se debe reaccionar ante un incidente de seguridad. Es decir, qué hacer cuando algo sale mal. Tener un plan de respuesta bien definido puede marcar la diferencia entre un pequeño susto y un desastre total. Este plan debe incluir procedimientos claros sobre cómo identificar, contener y remediar el incidente. Por ejemplo:

Imagina que una empresa detecta que un empleado ha descargado un archivo infectado con malware. Un buen plan de respuesta a incidentes podría incluir aislar inmediatamente el equipo afectado de la red, realizar una evaluación del daño, restaurar una copia de seguridad si es necesario, y revisar todos los sistemas para asegurarse de que no hay otros equipos comprometidos. Además, este plan debería incluir un análisis posterior para determinar cómo sucedió el incidente y qué medidas deben tomarse para evitarlo en el futuro.

Las auditorías son revisiones periódicas que se realizan para comprobar que las políticas y medidas de seguridad se están aplicando correctamente. Estas auditorías permiten detectar fallos o áreas de mejora que pueden haberse pasado por alto. Por ejemplo, una auditoría interna de seguridad en una empresa de Orio revela que varios empleados no están utilizando la autenticación de dos factores para acceder a los sistemas, a pesar de que es una política obligatoria. La auditoría permite corregir este fallo antes de que se convierta en un problema mayor, recordando a los empleados la importancia de cumplir con las medidas establecidas.

5. Prueba de autoevaluación.

¿Cuál es el primer paso en la gestión del riesgo en un sistema de información?

a) Evaluación del impacto del riesgo

b) Identificación de riesgos

c) Implementación de medidas preventivas

¿Qué tipo de análisis utiliza valores numéricos para evaluar los riesgos? a) Análisis cualitativo

b) Análisis cuantitativo

c) Análisis comparativo

¿Qué es el phishing? a) Un tipo de malware

b) Una técnica de suplantación de identidad

c) Un ataque de denegación de servicio

¿Qué herramienta se utiliza para evitar accesos no autorizados desde la red externa? a) Firewall

b) Antivirus

c) IDS (Sistema de Detección de Intrusos)

¿Cuál de los siguientes NO es un ejemplo de salvaguarda preventiva? a) Cifrado de datos

b) Monitorización de logs

c) Contraseñas robustas

El primer paso en la gestión del riesgo es la _____ de amenazas.

Un análisis _____ asigna valores numéricos para evaluar el impacto del riesgo.

El _____ es una técnica de suplantación de identidad utilizada para robar datos personales.

Las salvaguardas _____ buscan minimizar el daño tras un incidente de seguridad.

El _____ es una herramienta que filtra el tráfico para evitar accesos no autorizados a la red.

Análisis de impacto de negocio