Víctor Daniel Torres Solano

Paso 1

¿Qué son los activos críticos y por qué son importantes?

Los activos críticos son todos aquellos recursos que resultan esenciales para el funcionamiento de una empresa. En una empresa de comercio electrónico, estos activos pueden incluir sistemas, datos y personas que, si se ven comprometidos, pueden afectar gravemente la operación del negocio.
Protegerlos es fundamental para evitar pérdidas de información, fraudes financieros, caída del servicio y daño a la reputación.

Lista de activos más importantes

- La base de datos de clientes, donde se guarda la información personal y de contacto de cada comprador.
- La información de tarjetas de crédito, que es muy sensible y puede ser usada de forma maliciosa si no está protegida.
- El sitio web de ventas, que es el principal canal para realizar pedidos y recibir pagos.
- Los servidores donde se aloja la página y los datos, que deben estar siempre en funcionamiento.
- El sistema de gestión de pedidos, que ayuda a organizar el inventario, los envíos y las facturas.
- Los empleados clave, como los encargados de seguridad o los administradores de sistemas, que tienen acceso a información crítica.

Clasificación por nivel de criticidad

- **Nivel 1(muy crítico):** Información de tarjetas de crédito, Base de datos de clientes, Sitio web de ventas.
- **Nivel 2(crítico):** Servidores, Sistema de gestión de pedidos.
- **Nivel 3(Moderado):** Empleados clave.

Paso 2

¿Qué son las amenazas y los riesgos cibernéticos?

Las amenazas cibernéticas son acciones o eventos que pueden afectar negativamente a los activos críticos de una empresa. Estas amenazas pueden provenir de hackers, errores humanos, fallos técnicos o incluso desastres naturales. Los riesgos se refieren a la probabilidad de que una amenaza ocurra y al daño que podría causar. Algunos ejemplos comunes de amenazas son:

- **Phishing**: correos falsos o mensajes que engañan al usuario para robar contraseñas o datos personales.
- **Malware**: software malicioso que se instala en los sistemas y puede robar o destruir información.
- **Ransomware**: tipo de malware que bloquea los archivos de la empresa y pide un rescate para liberarlos.
- **Ataques DDoS**: saturan el sitio web con tráfico falso hasta que deja de funcionar.

Lista de activos más importantes

- La base de datos de clientes, donde se guarda la información personal y de contacto de cada comprador.
- La información de tarjetas de crédito, que es muy sensible y puede ser usada de forma maliciosa si no está protegida.
- El sitio web de ventas, que es el principal canal para realizar pedidos y recibir pagos.
- Los servidores donde se aloja la página y los datos, que deben estar siempre en funcionamiento.
- El sistema de gestión de pedidos, que ayuda a organizar el inventario, los envíos y las facturas.
- Los empleados clave, como los encargados de seguridad o los administradores de sistemas, que tienen acceso a información crítica.

Priorización de amenazas y evaluación de impacto

Una vez identificadas las amenazas más probables, se priorizan según el daño que causarían y qué tan probable es que ocurran.

Amenazas más críticas:

- **Ransomware**: porque puede dejar toda la empresa sin acceso a sus datos y operaciones.
- **Phishing**: porque es fácil que un empleado caiga en la trampa y entregue acceso sin querer.
- **Malware**: porque puede pasar desapercibido y robar datos durante mucho tiempo sin ser detectado.
- **Ataques DDoS**: aunque no roban información, pueden dañar la reputación y causar pérdidas si el sitio deja de funcionar.

Paso 3

¿Qué es un equipo de respuesta a incidentes y por qué es importante?

Un equipo de respuesta a incidentes es un grupo de personas que se encarga de actuar rápidamente cuando ocurre un problema de ciberseguridad, como un ataque, una filtración de datos o una caída del sistema. Su objetivo es contener el daño, recuperar los sistemas lo antes posible y evitar que el incidente se repita.

Este equipo debe estar bien organizado, tener funciones claras y contar con un plan de acción. Cada miembro del equipo cumple un rol específico para asegurar una respuesta rápida y efectiva.

Ejercicio Grupal: Asignación de roles en un equipo simulado

- Responsable de comunicaciones: se encarga de informar al resto de la empresa, a los clientes o incluso a los medios si es necesario. También mantiene el contacto con proveedores y equipos externos.
- Técnico de sistemas: es quien analiza y contiene el problema en los sistemas. Revisa servidores, redes, aplicaciones y aplica las soluciones necesarias.
- Responsable legal: se encarga de verificar si el incidente requiere una denuncia, si se violaron leyes de protección de datos, y qué acciones legales deben tomarse.
- Coordinador del equipo: lidera al grupo, organiza las tareas, y se asegura de que se siga el protocolo establecido.

Contactos de emergencia y responsabilidades

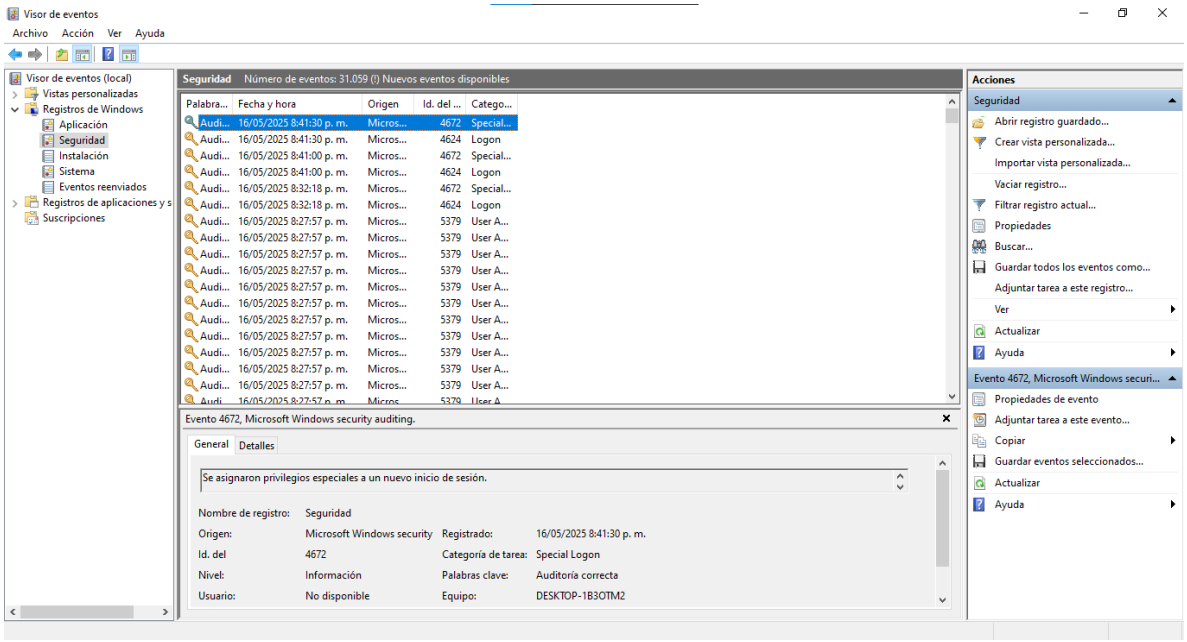
- Número de contacto del proveedor de hosting o soporte técnico externo.
- Correo del encargado de sistemas o administrador del servidor.
- Contacto legal o asesor en protección de datos.
- Teléfono de comunicación interna para alertas urgentes.
- Responsable de comunicación con clientes en caso de afectación.

Paso 4

Herramientas y técnicas para detectar incidentes

- Monitoreo de logs: los registros (logs) guardan todo lo que ocurre en los sistemas, como accesos, errores o cambios. Revisarlos ayuda a detectar comportamientos fuera de lo normal.
- Detección de anomalías: se analizan los patrones habituales del sistema, y si ocurre algo diferente (como un acceso a la madrugada o desde otro país), se genera una alerta.
- Sistemas de alertas: son configuraciones que notifican por correo, mensaje o panel de control cuando ocurre una posible amenaza, como múltiples intentos fallidos de inicio de sesión.

Ejemplo simple de revisión de logs



Diseñar un procedimiento básico de monitoreo

1. Definir qué se va a monitorear: accesos al sistema, cambios en archivos importantes, fallos del sitio web, etc.
2. Establecer una rutina de revisión: por ejemplo, revisar logs una vez al día o configurar alertas automáticas para accesos sospechosos.
3. Asignar responsabilidades: decidir quién será el encargado de revisar los logs o de recibir las alertas.
4. Establecer un canal de notificación: como correo electrónico o mensaje instantáneo para reportar incidentes rápidamente.

Paso 5

¿Qué es la contención y por qué es clave?

La contención es una fase crítica dentro de la respuesta a incidentes de ciberseguridad. Su objetivo es detener el avance del ataque, evitar que se propague a otros sistemas, y minimizar los daños mientras se prepara una solución definitiva.

Por ejemplo, si un equipo detecta un virus o un ataque en un servidor, contener el incidente significa aislar ese servidor del resto de la red antes de que el malware se expanda o robe más información.

Si no se actúa con rapidez, una amenaza pequeña puede afectar a toda la empresa y provocar pérdida de datos, caída del sistema o incluso consecuencias legales.

Crear un plan de contención básico

1. Identificar el sistema afectado
   Por ejemplo, detectar que el ataque está ocurriendo en el servidor web o en el equipo de un empleado.
2. Aislar el sistema del resto de la red
   Desconectar el equipo de internet o de la red interna para evitar que el ataque se propague.
3. Detener los procesos sospechosos
   Finalizar programas desconocidos, cerrar sesiones activas o apagar temporalmente servicios comprometidos.
4. Notificar al equipo de respuesta
   Informar inmediatamente al encargado técnico, al responsable de comunicaciones y al coordinador del equipo de respuesta.
5. Registrar lo ocurrido
   Guardar evidencias del ataque (capturas, logs, mensajes de error) para analizarlas luego.
6. Mantener informadas a las partes necesarias
   Si el incidente afecta a clientes o proveedores, se les debe informar según el protocolo de comunicación establecido.

Paso 5

¿Por qué es importante la recuperación y continuidad?

Después de un incidente de ciberseguridad (como un ataque de ransomware, una caída del servidor o una filtración de datos), lo más importante es recuperarse rápidamente para volver a operar y reducir el impacto en los clientes y en la reputación de la empresa.

La recuperación de datos implica restaurar información crítica desde copias de seguridad, verificar su integridad y volver a poner en marcha los sistemas comprometidos.

La continuidad del negocio se refiere a tener un plan que permita seguir funcionando, al menos parcialmente, mientras se resuelve el problema. Esto evita la pérdida de clientes y mantiene la confianza.

Crear un plan de recuperación

1. Activar el plan de respaldo de datos
   Restaurar archivos, bases de datos y configuraciones desde una copia de seguridad segura, preferiblemente almacenada fuera del sistema comprometido.
2. Verificar que los datos restaurados estén completos y limpios
   Comprobar que la información no esté dañada o infectada antes de volver a ponerla en producción.
3. Reinstalar o reparar sistemas afectados
   Actualizar el software, aplicar parches de seguridad y revisar configuraciones antes de reactivar los servicios.
4. Notificar a los clientes y usuarios afectados
   Informar de forma clara y oportuna si hubo pérdida de información o interrupciones en el servicio.
5. Reforzar la seguridad antes de volver al funcionamiento normal
   Cambiar contraseñas, revisar accesos, implementar mejoras para evitar que el incidente se repita.

Simulación de escenario y evaluación

Escenario de ejemplo:
La tienda en línea sufre un ataque de ransomware que encripta la base de datos de clientes.

Respuesta esperada del equipo:

- Se identifica el ataque y se contiene desconectando el servidor.
- Se activa el plan de recuperación, restaurando una copia de seguridad del día anterior.
- Se revisan las medidas de seguridad, se reinstala el servidor afectado, y se informa a los clientes.
- En menos de 24 horas, el sistema vuelve a estar activo con los datos seguros.

Este plan es un buen punto de partida para garantizar la continuidad en una pequeña empresa de comercio electrónico, siempre que se complemente con copias de seguridad frecuentes, capacitación del personal y revisiones constantes. Así se minimizan riesgos y se mejora la resiliencia frente a incidentes futuros.