Análisis de riesgos

Los pasos para realizar un análisis de riesgos son:

1. Delimitar los activos que pueden ser vulnerables.
2. Seleccionar activos críticos.
3. Identificar las amenazas que pueden afectar a los activos.
4. Determinar el impacto de las amenazas y la probabilidad de que ocurran.
5. Comprobar las medidas ya existentes.
6. Establecer medidas de control para reducir el riesgo.

Escenarios de riesgo relacionados con hardware

- Utilización de dispositivos de almacenamiento externos
- Uso de dispositivos móviles y wearables, que son propensos a robos o pérdidas.
- Conexión de dispositivos no autorizados a la red de la organización.
- Uso de dispositivos obsoletos o sin actualizaciones de seguridad.

Escenarios de riesgo relacionados con software

- Descarga o instalación de software no autorizado.
- Paquetes ofimaticos que puedan usar macros maliciosas.
- Uso de software sin licencia.
- Uso de software obsoleto o sin actualizaciones de seguridad.
- Uso de software con vulnerabilidades conocidas.
- Uso de software con configuraciones inseguras.
- Uso de software con permisos excesivos.
- Uso de software con acceso a internet sin restricciones.

Escenarios de riesgo relacionados con las instalaciones

- No tener control de acceso a dependencias con material sensible (CPD, salas de servidores, etc.).
- Confiar en que los empleados no dejarán la puerta abierta.
- Confiar en que nadie entrará en dependencias sin autorización.
- Puertos Ethernet accesibles en zonas comunes.
- Falta de control de acceso a la red.

Escenarios de riesgo relacionados con las comunicaciones

- Uso de redes Wi-Fi no seguras.
- Uso de redes Wi-Fi públicas.
- Uso de redes Wi-Fi con contraseñas débiles.
- Uso de redes Wi-Fi con dispositivos no seguros.

Escenarios de riesgo relacionados con los datos

- Uso de datos personales sin autorización.
- Uso de datos personales sin cifrar.
- Uso de datos personales sin control de acceso.
- Uso de documentos en papel, mas propensos a perdidas, robos o accesos no autorizados.

Escenarios de riesgo relacionados con las personas

- Falta de concienciación en ciberseguridad.
- Falta de formación en ciberseguridad.
- Falta de políticas de seguridad.
- Falta de medidas de control de acceso.
- Contraseñas débiles o compartidas.
- Ingeniería social.

Medidas de seguridad

Las medidas de seguridad se pueden clasificar en:

- **Preventivas**: evitan que se produzca un incidente.
- **Monitorización**: medidas para supervisar y controlar de forma continua un sistema.
- **Correctivas**: medidas para restaurar un sistema a su estado original tras un incidente.

Medidas relacionadas con hardware

- **Desactivar puertos USB**: evita la conexión de dispositivos no autorizados.
- **Proteger los dispositivos móviles**: con acceso biométrico.
- **BYOD**: establecer políticas de uso.

Medidas relacionadas con las comunicaciones

- **Firewalls**: Bloquear tráfico no autorizado mientras se mantiene a los usuarios legítimos.
- **VPN**: Conexiones seguras y cifradas entre dispositivos, esto protege nuestra red incluso si un trabajador usa una red Wi-Fi pública.

Medidas relacionadas con software

- **Control de software**: permitir solo software autorizado.
- **Actualizaciones**: mantener el software actualizado.
- **Antivirus**: proteger contra malware.
- **Uso de software con configuraciones seguras**: para evitar vulnerabilidades.
- **Uso de software con permisos mínimos**: para evitar accesos no autorizados.
- **Uso de software con acceso a internet restringido**: para evitar accesos no autorizados siempre que sea posible.

Medidas relacionadas con las instalaciones

- **Control de acceso**: solo personal autorizado, en especial a zonas sensibles como salas de servidores.
- **Cámaras de seguridad y alarmas**: para monitorizar el acceso a las instalaciones y detectar intrusiones.
- **Sistemas de detección de incendios y sobretensiones**: para proteger la infraestructura.
- **Sistemas de alimentación ininterrumpida (SAI)**: para evitar la pérdida de datos.
- **Sistemas de refrigeración**: para evitar el sobrecalentamiento de los equipos.
- **Sistemas de extinción de incendios**: para proteger la infraestructura.
- **Sistemas de control de acceso a la red**: para evitar accesos no autorizados.
- **Puertos Ethernet en zonas seguras**: para evitar accesos no autorizados.

Medidas relacionadas con las personas

- **Política de contraseñas**: establecer contraseñas seguras, renovarlas periódicamente, forzar el no compartirlas mediante 2FA.
- **Concientización y formación en ciberseguridad**: para que los empleados sean conscientes de los riesgos y sepan cómo actuar.
- **Formación en ingeniería social**: para que los empleados sean conscientes de las técnicas de engaño.

Es importante diseñar un plan de formación y concienciación que capacite sobre estas medidas, **no basta** con plasmarlas en un documento, enviarlas por email y esperar que los empleados las entiendan y las cumplan.