Basque CyberSecurity Centre

Protección de sistemas informáticos industriales

Checklist

☐ Inventario de sistemas.

Mantener un registro de los dispositivos que deben ser protegidos.

☐ Inventario de software.

Mantener un registro del software utilizado para gestionar cuestiones como las actualizaciones o la gestión de su ciclo de vida.

☐ Configuraciones de seguridad.

Verificar que los dispositivos disponen de una configuración segura.

☐ Arquitectura de red robusta.

Mediante la segmentación de la red y el acceso restringido a sistemas críticos.

☐ Protección antimalware multinivel.

La utilización de distintos sistemas para la protección frente al malware incrementa la capacidad de protección.

☐ Autenticación y autorización.

Verificar que se utilizan formas de autenticación segura en todos los dispositivos que sea posible, que no se utilizan credenciales por defecto y que se emplea un segundo factor de autenticación.

☐ Registro y análisis centralizado de eventos.

Los registros de los sistemas deben ser recogido, almacenados y analizados de forma centralizada.

☐ Protección física.

Los sistemas y sus periféricos deben estar protegidos frente al acceso no autorizado.

☐ Copias de seguridad y recuperación.

Los procesos de copia y recuperación deben estar definidos y ser verificados de forma periódica.

☐ Procedimiento de gestión de incidentes de seguridad.

Definir procesos para la detección, respuesta y prevención de incidentes de seguridad.

☐ Cultura de seguridad.

Mediante la definición de procesos y responsabilidades relacionados con la seguridad de los sistemas industriales.

Para conocer más información sobre cómo protegerte puedes visitar **https://www.basquecybersecurity.eus/es/**

Si necesitas asesoramiento profesional, puedes consultar el catálogo de proveedores de ciberseguridad de Euskadi disponible en la web.