TECNOLOGIAS DE LA INFORMACION Y CUBERSEGURIDAD

nacap

CIS CONTROLS

Fundamentos de Seguridad de la Informacion

nacap

¿Qué son los Controles CIS?

- Los Controles CIS son un conjunto de mejores prácticas para proteger los sistemas y datos de las organizaciones.
- Desarrollados por expertos en seguridad cibernética, estos controles ayudan a prevenir ataques cibernéticos.
- Componen un conjunto de 20 controles clave para mejorar la postura de seguridad.

CIS Center for Internet Security®

nacap

¿Qué son los Controles CIS?

- ✓ Proporcionan un marco claro para fortalecer la seguridad.
- ✓ Permiten a las organizaciones priorizar sus esfuerzos de seguridad.
- ✓ Son aplicables a empresas de diferentes tamaños y sectores.

20 controles CIS

- Controles básicos (1-6)
- Controles fundacionales (7-16)
- Controles organizacionales (17-20)

Controles básicos

Inventario y control de activos de hardware: Mantener un inventario actualizado y preciso de todos los dispositivos de hardware dentro de la red de la organización.

Inventario y control de activos de software: Gestionar y rastrear todas las aplicaciones y programas instalados en los dispositivos de la organización.

Gestión continua de vulnerabilidades: Implementar procesos para identificar, evaluar y remediar vulnerabilidades en sistemas y aplicaciones.

Uso controlado de privilegios administrativos: Asegurar que los privilegios administrativos se gestionen y controlen adecuadamente para minimizar el riesgo de abuso.

Controles fundacionales

Configuración segura de dispositivos de hardware y software: Establecer y mantener configuraciones seguras para todos los dispositivos y software dentro de la organización.

Mantenimiento, monitoreo y análisis de registros de auditoría: Recopilar, gestionar y analizar registros de auditoría para detectar y responder a incidentes de seguridad.

Protección de datos: Implementar medidas para proteger los datos en reposo y en tránsito, incluyendo el cifrado y la gestión de claves.

Defensa contra malware: Utilizar software antivirus y otras herramientas para detectar y prevenir infecciones de malware.

Controles organizacionales

Desarrollo y mantenimiento de políticas de seguridad: Crear y mantener políticas claras y comprensibles que guíen las acciones de seguridad en la organización.

Gestión de la seguridad de proveedores: Evaluar y gestionar los riesgos asociados con los proveedores y socios externos.

Formación y concienciación de los usuarios: Implementar programas de formación y concienciación para educar a los empleados sobre las prácticas de seguridad y las amenazas cibernéticas.

Planificación y ejecución de respuestas a incidentes: Desarrollar y mantener planes de respuesta a incidentes para gestionar y mitigar los impactos de los incidentes de seguridad.

Implementación de los Controles CIS

- Se recomienda comenzar con los primeros controles (los básicos).
- Evaluar los riesgos y priorizar los controles de acuerdo con las necesidades de la organización.
- Monitorear y ajustar la implementación de forma continua.

Beneficios controles CIS

- Mejora la protección contra amenazas cibernéticas.
- Facilita la conformidad con normativas y auditorías.
- Reduce los costos de respuesta ante incidentes.

Conclusiones

Los Controles CIS son fundamentales para establecer una ciberseguridad sólida.

Aplicarlos de manera efectiva ayuda a reducir vulnerabilidades y proteger datos críticos.