NIST SP 800-53

Identificación y Etiquetado de Activos

"• Clasificación de Datos: Determinar el nivel de sensibilidad y confidencialidad de cada tipo de dato (e.g., datos personales, financieros, de salud).

• Etiquetas de Confidencialidad: Asignar etiquetas que clasifiquen los activos de acuerdo a su nivel de confidencialidad (e.g., público, interno, confidencial, restringido).

• Propietarios de los Activos: Identificar a los responsables de cada activo y sus funciones para la supervisión y protección de los mismos."

Control de acceso

"• Listas de Control de Acceso (ACL): Definir y mantener ACLs que especifiquen quién puede acceder, modificar o eliminar cada activo de información.

• Roles y Permisos de Usuarios: Asignar roles y permisos de acceso según el principio de privilegios mínimos y separar las funciones para minimizar riesgos.

• Autenticación y Autorización: Implementar métodos de autenticación y autorización robustos (e.g., autenticación multifactor) para acceder a los activos críticos."

Integridad y disponibilidad de activos

"• Controles de Integridad de Datos: Asegurar la exactitud y consistencia de los datos durante su ciclo de vida mediante el uso de técnicas como el hashing o la firma digital.

• Resiliencia y Recuperación: Implementar medidas de respaldo y recuperación ante desastres para garantizar la disponibilidad de los activos.

• Pruebas de Integridad: Realizar auditorías y pruebas periódicas para verificar la integridad de los datos y detectar cualquier cambio no autorizado."

Protección de la privacidad

"• Minimización de Datos: Mantener solo los datos necesarios para los propósitos específicos y limitar la recolección de información confidencial.

• Anonimización y Pseudonimización: Aplicar técnicas de anonimización o pseudonimización cuando sea posible para proteger la identidad de los individuos.

• Retención de Datos: Establecer políticas de retención de datos que limiten el tiempo en que los datos personales se almacenan y asegurar su eliminación segura cuando ya no sean necesarios."

Control de seguridad y monitoreo

"• Monitoreo Continuo: Implementar sistemas de monitoreo que registren accesos y modificaciones a los activos críticos en tiempo real.

• Detección de Incidentes: Definir procedimientos y herramientas para la detección temprana de incidentes de seguridad relacionados con los activos de información.

• Auditorías de Seguridad: Realizar auditorías periódicas para evaluar la efectividad de las medidas de protección y cumplir con las políticas de privacidad y seguridad."

Gestión de riesgos

"• Evaluación de Riesgos: Identificar y clasificar los riesgos asociados a cada activo crítico, considerando factores como la sensibilidad de los datos y el impacto de una potencial vulneración.

• Evaluación de Impacto en la Privacidad (PIA): Realizar evaluaciones para entender los riesgos de privacidad y el impacto de su manejo inadecuado.

• Planes de Mitigación: Desarrollar e implementar planes para reducir riesgos mediante controles de seguridad y medidas de contingencia."

Evaluación de controles de seguridad

"• Pruebas de Vulnerabilidades: Ejecutar evaluaciones de vulnerabilidad y pruebas de penetración sobre los sistemas que contienen activos críticos para identificar posibles fallos de seguridad.

• Análisis de Incidentes Previos: Analizar incidentes pasados para aprender y reforzar la seguridad de los activos.

• Evaluaciones Independientes: Contar con evaluaciones de terceros para garantizar una visión imparcial sobre la efectividad de las medidas de seguridad y privacidad aplicadas."