NIST SP 800-53 Rev. 5

La norma NIST SP 800-53 Revision 5, desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST), establece un catálogo integral de controles de seguridad y privacidad para sistemas de información. Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información procesada, almacenada o transmitida. Esta norma es ampliamente utilizada en organizaciones públicas y privadas para la implementación de controles técnicos, físicos y administrativos.

# AC – Control de Acceso

🔹 Propósito: Garantizar que solo usuarios autorizados accedan a los sistemas y datos.

🔹 Controles clave:

* • AC-2: Gestión de cuentas de usuario
* • AC-3: Control de acceso
* • AC-6: Separación de funciones

🔹 Ejemplo práctico: Revisar los privilegios de acceso de los empleados cada 90 días para evitar accesos indebidos.

🔹 Relevancia para auditoría: Verificar que existan políticas de acceso basadas en roles (RBAC) y revisiones periódicas de permisos.

# AU – Auditoría y Rendición de Cuentas

🔹 Propósito: Registrar eventos relevantes y asegurar la trazabilidad de acciones en los sistemas.

🔹 Controles clave:

* • AU-2: Eventos de auditoría
* • AU-6: Revisión de registros de auditoría
* • AU-8: Sincronización de tiempo

🔹 Ejemplo práctico: Registrar accesos fallidos y notificar al administrador si se detectan múltiples intentos.

🔹 Relevancia para auditoría: Comprobar que los registros se almacenan de forma segura y se revisan regularmente.

# CM – Gestión de Configuraciones

🔹 Propósito: Establecer y mantener la integridad de las configuraciones del sistema.

🔹 Controles clave:

* • CM-2: Línea base de configuración
* • CM-3: Cambios en la configuración
* • CM-6: Aplicación de configuraciones seguras

🔹 Ejemplo práctico: Usar una herramienta de gestión para monitorear y validar cambios en configuraciones.

🔹 Relevancia para auditoría: Evaluar el control de versiones de software y que se aprueben los cambios antes de aplicarse.

# CP – Planificación de Contingencia

🔹 Propósito: Garantizar la disponibilidad de los servicios ante eventos disruptivos.

🔹 Controles clave:

* • CP-2: Plan de contingencia
* • CP-4: Copias de seguridad
* • CP-9: Restauración de datos

🔹 Ejemplo práctico: Realizar pruebas de restauración de respaldos al menos dos veces por año.

🔹 Relevancia para auditoría: Auditar que existan respaldos regulares y pruebas documentadas de recuperación.

# IR – Respuesta a Incidentes

🔹 Propósito: Detectar, responder y recuperarse de incidentes de seguridad de manera oportuna.

🔹 Controles clave:

* • IR-4: Manejo de incidentes
* • IR-5: Seguimiento posterior a incidentes
* • IR-6: Reporte de incidentes

🔹 Ejemplo práctico: Disponer de un equipo de respuesta que documente y analice cada incidente.

🔹 Relevancia para auditoría: Verificar si se mantiene un historial de incidentes y sus respuestas.