Plan de Respaldo y Custoria de Claves Criptográficas en HSM

Tabla de contenidos

Objetivo

Establecer los controles y procedimientos para garantizar el respaldo seguro y la custodia adecuada de las claves criptográficas generadas y almacenadas en el HSM, de conformidad con los requisitos de la norma ISO/IEC 27001

Alcance

Aplica a todos los sistemas que utilizan el HSM de la organización para el cifrado de información crítica, incluyendo servidores de correo seguro, VPN, firma digital y almacenamiento cifrado.

Generación de claves

Las claves maestras y subordinadas se generan dentro del HSM. El proceso de generación está registrado y requiere la presencia de al menos 2 custodios autorizados (principio de doble control).

Respaldo de claves

El respaldo de las claves maestras se realiza mediante un "key export" seguro hacia un token criptográfico (por ejemplo, smart card o dispositivo USB HSM). El respaldo está cifrado con una clave de envoltura (key wrapping key), almacenada solo en el HSM.

Custodia física

Los tokens de respaldo son almacenados en cajas fuertes con control de acceso biométrico en áreas restringidas. El acceso físico a las cajas fuertes requiere al menos 2 custodios diferentes (acceso dual). Se registra cada evento de acceso a los tokens.

Custodia lógica

Solo los usuarios con rol de "HSM Admin" pueden gestionar claves dentro del sistema. Las claves respaldadas están etiquetadas y versionadas; no se sobrescriben.

Pruebas de recuperación

Se realiza un test de restauración semestral para verificar la validez de los respaldos de claves. Se documenta el resultado de la prueba en el registro de auditoría.

Registro de custodios

Nombre	Rol	Fecha de Asignación	Identificador
Empleado_ID_25096 (Director TI)	Custodio 1	30/06/2025	EMPA00096
Empleado_ID_25050 (Técnico Consultoría)	Custodio 2	30/06/2025	EMPA00050

Revisión y actualización

Este plan se revisa al menos una vez al año o tras cualquier cambio en la infraestructura HSM, en la política criptográfica de la organización o en la disponibilidad de los custodios.