Configuración de Sistemas de Cifrado y Certificados (PKI)

Tabla de contenidos

1 Propósito y Objetivos

Propósito:

Establecer el marco y los criterios que regirán la emisión, gestión y uso de certificados digitales dentro de la organización, garantizando su integridad, autenticidad y confiabilidad para todos los procesos que requieran firma, cifrado o autenticación electrónica.

Objetivos:

- Asegurar que los certificados emitidos cumplan los requisitos de seguridad, normativa y operativos definidos por la organización y la legislación aplicable.
- Definir roles y responsabilidades claras en el ciclo de vida de los certificados, desde la solicitud hasta la revocación.
- Proteger la confidencialidad, integridad y disponibilidad de las claves y certificados mediante controles técnicos y organizativos adecuados.
- Facilitar la interoperabilidad y el reconocimiento de los certificados dentro y fuera de la organización, según estándares internacionales (p. ej., X.509, eIDAS).
- Garantizar la trazabilidad y el registro de todas las operaciones relacionadas con certificados para fines de auditoría y cumplimiento

2 Alcance

Ámbito de Aplicación

Es de obligatorio cumplimiento para:

- Todos los empleados, directivos y contratistas de la organización.
- Colaboradores externos, proveedores y terceros que participen en la emisión, gestión o uso de certificados digitales.
- Sedes físicas, entornos de trabajo remoto y dispositivos corporativos o autorizados bajo BYOD.

Activos y Sistemas Incluidos

- Infraestructura de Autoridad de Certificación (AC) interna y repositorios de certificados públicos y privados.
- Plataformas de solicitud, emisión y revocación de certificados, incluyendo sistemas automatizados y manuales.
- Hardware criptográfico (HSM, tokens USB, smartcards) y software gestor de claves.
- Sistemas de directorio (LDAP, Active Directory) y servicios IAM ligados a la validación de identidad y autorización.

Procesos y Usos

- Solicitud, emisión, distribución, renovación y revocación de certificados digitales.
- Uso de certificados para firma electrónica, cifrado de comunicaciones (TLS, VPN, SMIME) y autenticación fuerte (2FA, MFA).
- Registro y auditoría de todas las operaciones criptográficas relacionadas con los certificados.

Exclusiones

- Dispositivos personales no autorizados o no conformes con los estándares de seguridad corporativos en teletrabajo.
- Certificados gestionados por entidades ajenas sin integración técnica o contractual con la organización.

Duración y Revisión

Este alcance estará vigente hasta su revisión anual o previo cambio significativo en la infraestructura de certificación, en los procesos de negocio o en el marco normativo aplicable.

3 Roles y Responsabilidades

Esta sección define los roles clave implicados en la gestión de certificados digitales y sus correspondientes responsabilidades.

3.1 Autoridad de Certificación (AC)

- Emitir, renovar y revocar certificados conforme a los procedimientos establecidos.
- Mantener la infraestructura criptográfica y los repositorios de certificados disponibles y seguros.
- Registrar y auditar todas las operaciones de emisión, revocación y renovación.

3.2 Autoridad de Registro (AR)

- Verificar la identidad y elegibilidad de los solicitantes según los criterios definidos.
- Gestionar el proceso de solicitud de certificados, incluyendo la recopilación de documentación y firma de acuerdos.
- Remitir solicitudes validadas a la AC para emisión de certificados.

3.3 Solicitantes / Suscriptores

- Presentar la solicitud de certificado con la documentación requerida y seguir los procedimientos de autenticación.
- Custodiar su clave privada y notificar inmediatamente cualquier compromiso o pérdida.
- Utilizar los certificados únicamente para los fines autorizados y según las directrices de la política.

3.4 Responsables de Seguridad de la Información

- Definir los criterios de aprobación y las políticas de uso de certificados digitales.
- Supervisar el cumplimiento de la política y realizar auditorías periódicas.
- Gestionar los roles y autorizaciones de AR y AC, así como la capacitación de personal.

3.5 Equipo de Soporte Técnico / TI

- Instalar y mantener el hardware criptográfico (HSM, tokens, smartcards) y software gestor de claves.
- Configurar y administrar sistemas de directorio y servicios IAM para la validación de identidad.
- Proporcionar asistencia a los suscriptores en la instalación y uso de los certificados.

3.6 Comité de Certificación

- Aprobar cambios y excepciones en la política de certificación.
- Revisar los informes de auditoría y decidir acciones correctivas en caso de incumplimientos.
- Validar las actualizaciones de la política en función de la evolución normativa y tecnológica.

3.7 Auditor Interno / Externo

- Realizar revisiones de cumplimiento y verificar la trazabilidad de las operaciones de certificación.
- Informar sobre desviaciones y proponer mejoras en controles y procedimientos.

- Cerciorar que la gestión de riesgos asociada a la infraestructura de certificación esté actualizada.

4 Requisitos de Emisión de Certificados

4.1 Autoridad de Certificación (AC) designada.

La AC responsable deberá contar con acreditación interna o de un tercero reconocido (p. ej., FNMT, Camerfirma) y cumplir con estándares como X.509 y eIDAS.

4.2 Verificación de identidad del solicitante

La Autoridad de Registro (AR) debe aplicar procedimientos de autenticación según nivel de certificación:

a) Simple (documento válido con fotografía).
b) Avanzada (firma biométrica o DNIe).
c) Cualificada (presencia física y certificados cualificados).

4.3 Documentación y formularios.

Cada solicitud incluirá formulario oficial, copia de identidad, comprobante de rol/función y aceptación de términos de uso.

4.4 Controles de aprobación.

a) Revisión inicial por AR: validación de identidad y datos.
b) Aprobación final por AC: comprobación técnica de par de claves y generación del certificado.

4.5 Generación y entrega de claves.

a) El par de claves se generará en HSM o dispositivo seguro aprobado.
b) La clave privada nunca abandonará el dispositivo seguro.
c) La clave pública se incorporará al certificado y se publicará en el repositorio correspondiente.

4.6 Plazo de emisión.

El certificado se emitirá en un plazo máximo de 2 días hábiles tras aprobación, salvo casos especiales de certificación cualificada (hasta 5 días).

4.7 Registro y auditoría.

Todas las operaciones de solicitud, emisión y entrega quedarán registradas con marca temporal y responsables definidos, para auditoría interna y cumplimiento normativo.

5 Requisitos de Uso de Certificados

- El uso de cada certificado se limitará a los fines especificados en sus extensiones Key Usage y Extended Key Usage, según lo definido en el estándar RFC 5280.
- La clave privada asociada deberá permanecer bajo custodia segura y los certificados deberán instalarse únicamente en dispositivos y aplicaciones aprobadas por la organización.
- Cada certificado estará ligado de forma unívoca a una identidad o sistema; queda prohibida la compartición, transferencia o exportación entre sujetos distintos.
- No se permitirá el uso de certificados caducados o revocados; éstos deberán eliminarse de los almacenes activos y no utilizarse para firma, cifrado o autenticación.

6 Gestión del Ciclo de Vida del Certificado

La gestión del ciclo de vida del certificado comprende las fases necesarias para asegurar la vigencia, validez y seguridad de los certificados digitales de forma automatizada y controlada.

6.1 Descubrimiento y Catalogación.

Identificar y registrar todos los certificados activos en la infraestructura, asegurando visibilidad continua para evitar certificados huérfanos o caducados.

6.2 Solicitud y Emisión.

Generar solicitudes de firma (CSR) con datos validados por la Autoridad de Registro y emitir certificados jugando sobre un HSM o dispositivo seguro, garantizando la integridad de la clave privada.

6.3 Despliegue y Provisionamiento.

Instalar y configurar automáticamente los certificados en los sistemas y aplicaciones autorizadas, ajustando parámetros de Key Usage según RFC 5280.

6.4 Monitoreo y Alertas.

Supervisar las fechas de expiración y el estado de los certificados en tiempo real, generando alertas tempranas para renovación anticipada y evitando interrupciones de servicio.

6.5 Renovación.

Automatizar la renovación antes de la fecha de expiración, estableciendo plazos de vencimiento escalonados (p. ej., 30 días antes) y validación de la identidad con procedimientos adaptados al nivel de certificación.

6.6 Revocación y Sustitución.

Invalidar inmediatamente certificados comprometidos o fuera de uso, publicando las Listas de Revocación (CRL) o respondiendo a OCSP para asegurar que no se utilicen en operaciones criptográficas.

6.7 Retiro y Archivo.

Eliminar certificados caducados de los repositorios activos, almacenando registros de emisión, renovación y revocación con marcas temporales para auditoría y cumplimiento de normativas.

Estas etapas permiten un ciclo de vida de certificados optimizado, reduciendo riesgos operativos y garantizando una postura de seguridad robusta.

7 Controles de Seguridad

Esta sección detalla de manera concisa los controles técnicos y organizativos necesarios para proteger la infraestructura de certificación y asegurar la integridad, confidencialidad y disponibilidad de los certificados digitales.

7.1 Controles de Acceso Lógico

a) Autenticación multifactor (MFA) para todos los sistemas de gestión de certificados, incluyendo HSM y portales de emisión.
b) Gestión de privilegios basada en roles (RBAC) con revisión trimestral de cuentas y permisos.

7.2 Controles de Protección de Claves

c) Generación de claves en módulos de seguridad hardware (HSM) certificados según FIPS 140-2 Nivel 3.
d) Almacenamiento de copias de seguridad de claves privadas cifradas y selladas en entornos aislados físicamente.

7.3 Monitoreo y Registro

e) Registro inmutable de eventos criptográficos (emisión, renovación, revocación) con sellado de tiempo.
f) Monitoreo continuo de integridad de archivos de configuración y binarios de la AC mediante sistemas IDS/IPS.

7.4 Controles de Red y Perímetro

g) Segmentación de red para aislar la infraestructura de AC y AR en zonas de alta seguridad.
h) Firewalls y listas blancas de IP para acceso restringido a servicios de emisión y OCSP.

7.5 Protección Física

i) Ubicación de HSM y servidores de AC en salas seguras con control de acceso biométrico y CCTV.
j) Procedimientos de respuesta ante desastres y recuperación ante incidentes con pruebas semestrales.

7.6 Gestión de Vulnerabilidades

k) Escaneo de vulnerabilidades y pruebas de penetración anuales en la infraestructura de certificación.
l) Aplicación de parches críticos en un plazo máximo de 15 días tras su publicación.

7.7 Plan de Continuidad

m) Respaldo periódico de configuraciones y bases de datos de certificados con recuperación garantizada en 4 horas SLA.
n) Procedimientos documentados de conmutación por error (failover) para AC secundarias.

8 Procedimientos de Revocación

8.1 Causas de Revocación

Los certificados digitales emitidos por la Autoridad de Certificación interna podrán ser revocados por las siguientes causas:

- Compromiso de clave privada: Sospecha o confirmación de acceso no autorizado a la clave privada.
- Cambio de rol o cesión de responsabilidades: El suscriptor cambia de puesto o deja de cubrir funciones que requieren certificado.
- Incumplimiento de políticas internas: Uso indebido del certificado, violación de términos de uso o de controles de seguridad establecidos.
- Datos de identidad incorrectos o caducados: Información personal o de organización desactualizada o inexacta en el certificado.
- Solicitud explícita del suscriptor o dirección: El titular solicita la revocación por cualquier motivo justificado o la alta dirección ordena su revocación.

8.2 Proceso de Revocación

La revocación de certificados se realizará siguiendo estos pasos:

1. **Recepción de solicitud de revocación**: AR o suscriptor presenta el motivo y documentación mínima (ID empleado, identificador de certificado) al sistema de emisión.
2. **Verificación de solicitud**: AR comprueba identidad del solicitante y validez del motivo frente al inventario de procesos certificados en Barcelona.
3. **Emisión de orden de revocación**: La AC firma una orden de revocación utilizando HSM, generando entrada con marca temporal en la lista de revocación (CRL) conforme a RFC 5280.
4. **Publicación de CRL y OCSP**:
    1. CRL: Se actualiza el repositorio interno y se publica cada 24 horas; versión etiquetada y firmada según perfil X.509 v2.
    2. OCSP: Actualización casi en tiempo real con respuesta firmada y campos thisUpdate/nextUpdate claros conforme a RFC 6960.
5. **Notificación a interesados**: Suscriptores, sistemas automatizados (VPN, portales cliente) y equipo de TI reciben alerta de revocación instantánea por SIEM y correo cifrado.
6. **Retirada de certificados de almacene**s: Se purgan certificados revocados de dispositivos, HSM y repositorios de aplicaciones autorizadas (Jira, LDAP) en menos de 2 horas tras publicación.

8.3 Notificación de Revocación

La notificación de revocación asegura que todos los sistemas y usuarios afectados conozcan inmediatamente el estado inválido de un certificado.

8.3.1 Destinatarios

- Suscriptor propietario del certificado revocado.
- Equipos y sistemas que confían en el certificado (VPN, portales internos, clientes TLS).
- Autoridad de Registro y seguridad TI para seguimiento y registro.

8.3.2 Canales de Comunicación

- Correo electrónico cifrado al suscriptor y responsables de proceso.
- Alertas automáticas en el SIEM y dashboard de monitoreo.
- Mensajería interna en plataforma de gestión de incidencias (Jira, ServiceNow).

8.3.3 Formato del Mensaje

- Identificador único del certificado y motivo de revocación.
- Marca temporal de la operación y firma electrónica de la AC.
- Acciones recomendadas: desmontar certificado de dispositivos y repositorios, generar nuevo CSR si procede.

8.3.4 Tiempo de Notificación

- Inmediata tras la publicación en la CRL y actualización OCSP (≤ 2 horas) para sistemas críticos.
- Notificación al suscriptor en un plazo máximo de 4 horas tras revocación.

8.3.5 Registro de Notificaciones

- Entrada en el registro de auditoría con destinatarios, hora de envío y canal usado.
- Conservación de comprobantes de entrega (logs de SIEM, acuses de email) por un mínimo de 2 años.