Procedimiento de Cifrado del Grupo FCC

Julio de 2025

Historial de Versiones				
Versión	**Fecha**	**Autor**	**Detalle**	**Aprobador**
1.0	Mayo 2024	IS	Creación del Documento	Chief Information Security Officer (CISO)
2.0	Junio 2025	IS	Adecuación al ENS nivel Medio e ISO 27001	Chief Information Security Officer (CISO)

ÍNDICE

1. Introducción

El presente documento forma parte del Marco Normativo de Seguridad de la Información del Grupo FCC, que desarrolla los preceptos de obligado cumplimiento en el Grupo en materia de Seguridad de la Información.

El Marco Normativo de Seguridad es revisado y actualizado periódicamente por el departamento de Seguridad de la Información (en adelante departamento de SI), de acuerdo con lo establecido en el Documento de Gestión y Mantenimiento del Marco Normativo. Este documento contiene información sobre el historial de versiones, revisiones y aprobaciones del presente procedimiento, así como su relación y dependencia con el resto de los documentos normativos.

Este procedimiento será revisado, por lo menos, anualmente, salvo que existan circunstancias que recomienden o exijan una revisión antes de dicha fecha.

1.1 Objeto

El objeto del presente procedimiento es proporcionar y dar a conocer las recomendaciones de seguridad en cuanto a métodos de cifrado se refiere. Estas se deben utilizar en los sistemas de información del Grupo FCC.

1.2 Alcance

Este procedimiento se aplica a la información del Grupo FCC, cuyo nivel de confidencialidad aconseje la necesidad de protegerla mediante mecanismos de cifrado.

Toda implementación o uso de criptografía basada en tecnologías de la información debe cumplir y adherirse a este procedimiento. Esto incluye:

- Aplicaciones y servicios desarrollados y utilizados para el consumo y uso interno.
- Aplicaciones y servicios desarrollados y utilizados como productos externos, de cara a los colaboradores.
- Aplicaciones y servicios en la nube (Saas) o en las instalaciones.
- Infraestructura y plataforma en la nube (IaaS y PaaS) o en las instalaciones.
- Documentación Restringida del Grupo FCC.

2. Métodos de Cifrado Aprobados

La Dirección de Seguridad de la Información del Grupo FCC ha definido los requisitos, métodos y tecnologías que se deben utilizar para cifrar la información. Esta información se cifrará en base al estado de los datos a los que se hace referencia:

2.1 Datos en reposo

2.1.1 Sistemas Cloud

En la actualidad existe una gran cantidad de proveedores de Cloud y cada uno de ellos utilizan sus propios métodos de cifrado y gestionan su propio conjunto de claves. Por ello, el Grupo FCC debe seguir los requisitos definidos en la Norma de Criptografía y asegurar que los proveedores contratados cumplan con los siguientes requisitos:

- Se debe utilizar protocolos TLS para proteger la información cuando se desplazan entre los servicios en la nube y los clientes.

Se debe utilizar protocolos similares a Perfect Forward Secrecy (PFS) para proteger las conexiones entre los sistemas cliente de los usuarios y los servicios en la nube del proveedor garantizando que el descubrimiento de las claves utilizadas actualmente no compromete la seguridad de las claves usadas con anterioridad.

- Las conexiones deben usar longitudes de clave de cifrado basadas en RSA de 2.048 bits, como mínimo.
- Se deben proteger los datos en tránsito entre una aplicación y la nube mediante el cifrado del lado cliente HTTPS o SMB 3.0. para servidores Windows.
- Puede habilitar el cifrado para el tráfico entre sus propias máquinas virtuales (VM) mediante el protocolo IPsec estándar del sector para cifrar el tráfico entre la puerta de enlace VPN corporativa y la nube, así como entre las máquinas virtuales ubicadas en la red virtual.
- Para los datos en reposo, se debe utilizar alguna tecnología de cifrado basada en AES-256 o superior.
- Los procesos de cifrado, descifrado y administración de claves deben ser totalmente transparentes para los usuarios.

Las comunicaciones entre centros de datos del proveedor deben tener lugar a través de TLS o IPsec, y todos los servidores orientados al cliente negocian una sesión segura con TLS con máquinas cliente (recomendación mínima TLS 1.2 con una intensidad de cifrado de 256 bits).

Todos los certificados emitidos por proveedor tienen una longitud mínima de 2048 bits y el cumplimiento de la confianza web requiere SSL-Admin para asegurarse de que los certificados se emiten sólo a direcciones IP públicas propiedad de la entidad.

- Es recomendable que utilicen una tecnología similar a BitLocker en centros de datos y máquinas cliente, además de un administrador de claves distribuidas (DKM) en centros de datos del proveedor.
- Para el servicio de correo se debe utilizar cifrado de mensajes S/MIME y TLS para correo electrónico en tránsito.

Para los servicios de mensajería instantánea se deberá usar Protocolos TLS y mTLS para cifrar los mensajes de texto. El tráfico multimedia se cifrará mediante Secure RTP (SRTP) o

similar. Y para intercambios de claves de cifrado se utilizarán algoritmos compatibles con FIPS (Federal Information Processing Standard) para la validación de estas claves.

2.1.2 Servidores Propios

En este apartado se hace referencia a todos los activos o sistemas de información propios como servidores y bases de datos, donde se almacene información del Grupo FCC. Por ello, el Grupo FCC debe seguir los requisitos definidos en la Norma de Criptografía, y deben asegurar que:

- Los datos con nivel de clasificación Restringida se cifran y descifran de forma transparente al usuario.
- Se usará, en la mediad de lo posible, el estándar de cifrado AES 256. Se permite el cifrado de 128 bits en caso de necesidad y únicamente bajo la aprobación del departamento de SI.
- Se deberán asegurar medidas análogas a las descritas en el punto anterior para Sistemas Cloud.

2.2 Datos en tránsito

2.2.1 Redes de Comunicaciones

Las recomendaciones en relación a los protocolos de autenticación y cifrado para redes inalámbricas realizadas por la Industria (*Wifi Alliance)* y, por ende, el departamento de SI, son:

- Conexiones Wireless LAN basadas en IEEE 802.11i / WPA2 Enterprise. Se recomienda WPA2 por ser considerado más avanzado que WPA.
    - WPA2 Se recomienda AES-256 para este cifrado, pero se requiere un cifrado mínimo de AES 128 bits.
    - Si fuera posible, se deberá implementar el protocolo WPA3.
- Implementar autenticación IEEE 802.1X/EAP.
    - Los tipos de EAP soportado por IEEE 802.1X incluyen: EAP-TLS, EAP-TTLS, PEAP v.0, PEAP v.1.
    - Para la selección del tipo de EAP se deberá tener en cuenta el tipo de servicio de autenticación en la organización (DA, LDAP, etc.), así como el requisito de autenticación (password, certificados, etc.).
    - El uso de autenticación PSK (Pre-shared keys) sólo deberá implementarse por motivos de negocio debidamente justificados o en situaciones de no disponibilidad de un servidor de autenticación. En esos casos la contraseña deberá ser lo suficiente robusta (al menos 16 caracteres) y ser cambiada periódicamente (30 días).
- Adquirir productos WPA2 o WPA3 certificados.
- Deshabilitar en los puntos de acceso la posibilidad de uso del protocolo WEP y de autenticación TKIP.

No utilizar modelos de router wifi con vulnerabilidades reconocidas.

- Para la navegación a través de la red de internet se deberá realizar bajo el protocolo HTTPS.

2.2.2 Transmisión de Ficheros

El cifrado de ficheros para su distribución se rige por el nivel de clasificación de la información que guardan. Las recomendaciones de seguridad en cuanto a la transmisión de archivos son:

- Para la trasmisión entre aplicativos y hacia fuera del centro de datos se deberá utilizar el protocolo SFTP o cualquier otro aprobado por el departamento de SI.
- Se deben seguir las recomendaciones y buenas prácticas en el intercambio seguro de la información.

2.2.3 Certificados

Para la navegación y el acceso por determinadas páginas en Internet se deberá realizar mediante certificados digitales. Los certificados digitales son pequeños archivos de datos verificables que contienen credenciales de identidad para ayudar a los sitios web, las personas y los dispositivos a representar su auténtica identidad en línea. Esta autenticación la realiza las Entidades de Certificación, o Autoridades de Certificación, en adelante CA.

El certificado aprobado por el departamento de SI es el denominado SSL. Un certificado SSL es un tipo popular de certificado digital que vincula los datos de propiedad de un servidor web (y de un sitio web) a claves criptográficas. Estas claves se utilizan en el protocolo SSL/TLS para activar una sesión segura entre un navegador y el servidor web que alberga el certificado SSL. Para que un navegador confíe en un certificado SSL y, establezca una sesión SSL/TLS sin advertencias de seguridad, el certificado SSL debe contener el nombre de dominio del sitio web que lo utiliza, estar emitido por una CA de confianza y no haber caducado.

Para una gestión segura de claves se deberá tener en cuenta la autenticidad de las claves públicas. Este proceso de autenticación puede llevarse a cabo utilizando certificados de clave pública. Estos, suelen ser expedidos por la propia organización (si tiene su propia infraestructura de generación de claves denominada PKI – Public Key Infrastructure) o, una autoridad de certificación, que debería ser una organización reconocida y debe contar con unos controles y procedimientos mínimos adecuados para ofrecer el grado de confianza necesario.

El Grupo FCC, para la gestión de claves, deberá utilizar:

- PKI Propia: La infraestructura de clave pública (PKI) es un conjunto de roles, políticas, hardware, software y procedimientos necesarios para crear, administrar, distribuir, usar, almacenar y revocar certificados digitales y administrar el cifrado de clave pública. La PKI del Grupo FCC sólo se usará para los siguientes casos o, cualquier otro aprobado por el departamento de SI:
  - VPN
  - Autenticación de dispositivos
  - TLS para comunicaciones telemáticas
  - Correo electrónico S/MIME
  - Servicios GDI (conectores con dominios): El servicio de Gestión de Identidades actualiza información en diferentes Directorios Activos de FCC utilizando conectores con sus controladores de dominio que requieren el uso de certificados internos de la PKI-CA-FCC.

- Las recomendaciones del departamento de SI sobre infraestructuras de clave pública (PKI) son las siguientes:
    - El usuario no podrá solicitar certificados sin previa autorización de su responsable y del departamento de SI.
    - Si se requiere el uso de la PKI para los procesos de negocio o los controles de acceso, es esencial que las claves privadas estén protegidas con el mayor nivel de seguridad posible a través de un dispositivo de seguridad dedicado: un módulo de seguridad de hardware (HSM).

2.2.3.1 GESTIÓN DE LOS CERTIFICADOS EN EL GRUPO FCC:

De forma periódica, el equipo de la PKI de Infraestructuras generará un informe de certificados que vencerán en los próximos 3 meses. Basado en el Master of Certificates y la información de la PKI, en el informe aparecerá:

- Certificado a expirar en los próximos tres meses.
- Servidores y aplicaciones en donde se tiene constancia que están instalados.
- Fecha de expiración.
- Grupo Responsable o Encargado de la renovación.

Sistema Middelware

- Sistema .NET – SharePoint
- Sistema Windows
- Sistema Exchange

Otros sistemas involucrados (en caso de ser necesario).

- Este informe es enviado a los diferentes grupos de Infraestructuras o encargados de la renovación de los certificados y al Gestor responsable:
    - Para servidores a los diferentes grupos responsables de la infraestructura.
    - Para las aplicaciones a los diferentes grupos responsables de las aplicaciones.

En el caso de hacer certificados fuera del alcance de este equipo, se escalará a los responsables del Delivery del Grupo FCC para su gestión por parte del SPOC.

Este listado se enviará a todos los grupos propietarios de cada certificado, donde cada grupo en primera instancia en el plazo de 5 días confirmará que todos los certificados en los que aparecen como propietario son suyos y, en el caso de existir algún error, lo comunicará para su corrección y posterior envío al grupo correspondiente.

- Si existiera algún certificado próximo a su caducidad en el entorno de producción el SPOC se encargará de gestionar su renovación con el personal L4 con objeto de realizar la actualización en el menor tiempo posible.
- Los certificados serán renovados como máximo 10 días antes de su caducidad.
- Una vez actualizado el certificado, se procederá a actualizar la información del nuevo certificado desplegado en el fichero maestro de control para su seguimiento.

Autoridades de Certificación, CA: Las CA desempeñan un papel fundamental en el funcionamiento de Internet y en la realización de transacciones de información transparentes y fiables en línea. Las CA emiten millones de certificados digitales cada año, y estos certificados se utilizan para proteger la información, cifrar miles de millones de transacciones y permitir una comunicación segura. El uso de los certificados emitidos por CAs se aplicará únicamente para los siguientes casos o cualquier otro que sea aprobado por el departamento de SI:

  - **Proyectos:** Los diferentes proyectos del Grupo FCC pueden tener bajo gestión necesidades de certificados públicos (alta, baja, modificación o renovación).
  - **Servicios ADFS:** Servicio federados de Directorio Activo para permisos y accesos de cuentas de FCC a servicios por ejemplo en Cloud.
  - **Netscaler:** Publicación a Internet de servicios web, agrupación por content switches certificados de HTTPs.

- Las recomendaciones del departamento de SI sobre certificados emitidos por la CA son las siguientes:
  - Se deben usar certificados digitales emitidos únicamente por CAs reconocidas y aprobadas por el departamento de SI.
  - No se recomienda el uso de certificados digitales con claves públicas RSA de 1024 bits. Y, por tanto, se recomiendan claves de RSA de 2048 bits.
  - En las CAs emisoras deben entregar la lista de revocación de certificados (CRL) y de respuestas del Online Certificate Status Protocol (OCSP)

El responsable de la generación de certificados enviará el listado actualizado de certificados públicos al SPOC para incluir dicha información en el fichero Master of Certificate. Esto se realizará la última semana de cada mes.

- Este informe es enviado a los diferentes grupos de Infraestructuras o encargados de la renovación de los certificados y al Gestor responsable:
  - Para servidores a los diferentes grupos responsables de la infraestructura.
  - Para las aplicaciones a los diferentes grupos responsables de las aplicaciones.

En el caso de hacer certificados fuera del alcance de DXC, se escalará a los responsables del Delivery del Grupo FCC para su gestión por parte del SPOC.

Este listado se enviará a todos los grupos propietarios de cada certificado, donde cada grupo en primera instancia en el plazo de 5 días confirmará que todos los certificados en los que aparecen como propietario son suyos y, en el caso de existir algún error, lo comunicará para su corrección y posterior envío al grupo correspondiente.

- Si existiera algún certificado próximo a su revocación en el entorno de producción el SPOC se encargará de gestionar su renovación con el personal L4 con objeto de realizar la actualización en el menor tiempo posible.
- Los grupos responsables abrirán un cambio para su renovación en el caso de los entornos de producción y con peticiones técnicas genéricas para el resto de entorno.
- Los certificados serán renovados a más tardar 10 días antes de su caducidad.
- Una vez actualizado el certificado, se procederá a actualizar la información del nuevo certificado desplegado en el fichero maestro de control para su seguimiento.

3. Referencia normativa

El presente documento ha sido revisado por el departamento de SI y su redacción toma como referencia el estándar internacional ISO27001:2022 y ENS.

3.1 Controles de la normativa ISO27001:2022 y ENS

ID Control ISO	Control ISO/IEC 27001:2022	Correspondencia ENS
7.10	Soportes de almacenamiento	[mp.si.1] Marcado de soportes; [mp.si.2] Criptografía; [mp.si.3] Custodia; [mp.si.4] Transporte; [mp.si.5] Borrado y destrucción
8.1	Dispositivos finales de usuario	[mp.eq.3] Protección de dispositivos portátiles; [mp.eq.4] Otros dispositivos conectados a la red
8.12	Prevención de fugas de datos	[mp.com.1] Perímetro seguro; [mp.com.2] Protección de la confidencialidad; [mp.si.2] Criptografía; [mp.eq.3] Protección de dispositivos portátiles
8.24	Uso de la criptografía	[op.exp.10] Protección de claves criptográficas; [mp.si.2] Criptografía; [mp.info.3] Firma electrónica