Norma de Seguridad en Contraseñas del Grupo FCC

Mayo de 2025

Historial de Versiones				
Versión	**Fecha**	**Autor**	**Detalle**	**Aprobador**
1.0	Abril 2009	IS	Creación del Documento	Chief Information Security Officer (CISO)
2.1	Febrero 2012	IS	Actualización general e integración con el procedimiento de seguridad en contraseñas	Chief Information Security Officer (CISO)
	Octubre 2019	IS	Revisión del Documento	Chief Information Security Officer (CISO)
2.2	Junio 2020	IS	Actualización de la Norma de contraseñas y Revisión General	Chief Information Security Officer (CISO)
2.3	Abril 2021	IS	Actualización Sistema de Gestión de contraseñas y revisión general	Chief Information Security Officer (CISO)
3.0	Julio 2021	IS	Revisión del Documento Unificación del formato con el resto de la Normativa.	Chief Information Security Officer (CISO)
4.0	Mayo 2025	IS	Revisión del documento y adaptación a normativa ISO27001:2022 y ENS	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 de la presente Norma, así como su relación y dependencia con el resto de los documentos normativos.

Esta norma será revisada, por lo menos, anualmente, salvo que existan circunstancias que recomienden o exijan una revisión antes de dicha fecha

1.1 Objeto

El objetivo de la presente Norma es establecer, gestionar y promover las mejores prácticas en la creación y uso de contraseñas en los sistemas del Grupo FCC, con el fin de garantizar un apropiado proceso de autenticación y prevenir fallos durante el proceso.

1.2 Alcance

Esta norma se aplica a todo el personal interno y colaboradores del grupo FCC que utiliza contraseñas como mecanismo de autenticación para acceder a:

- Sistemas de información del grupo FCC.
- Sistemas de almacenamiento datos.
- Dispositivos y medios tecnológicos corporativos.
- Instalaciones de procesamiento de información.

2. Desarrollo

2.1 Principios

- Los sistemas de información que utilizan contraseñas como método de autenticación deben incorporar un sistema de gestión de contraseñas para garantizar la seguridad y la calidad de las mismas.
- Todas las contraseñas son personales e intransferibles. Todo el personal con acceso a los medios tecnológicos del Grupo FCC debe gestionar sus contraseñas de forma estrictamente confidencial y cumplir con las directrices para la selección y uso adecuado de la contraseña descritas en esta norma.
- La provisión de contraseñas se desarrollará de forma que se garantice la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad.

2.2 Sistema de Gestión de Contraseñas

El sistema de gestión de contraseñas debe ajustarse el siguiente conjunto de reglas para garantizar una buena calidad y una gestión correcta.

2.2.1 Reglas generales

- Todas las cuentas de usuario de los datos deben estar protegidas por una contraseña que pueda ser modificada libremente por el usuario y contar con un procedimiento para resolver errores en la introducción de caracteres.
- Se debe forzar al usuario a realizar un cambio de contraseña tras el primer login.
- Prevenir la reutilización de contraseñas anteriores.
- No mostrar por pantalla la contraseña durante su introducción.
- El usuario nunca debe acceder a la contraseña de otro usuario, ni modificar las contraseñas de otros usuarios, sin la autorización expresa y el conocimiento previo del responsable de la información.
- El usuario no debe compartir cuentas y contraseñas con otros usuarios, aunque sean superiores o colaboradores, ni hablar de ellas en público.
- El usuario no debe anotar las contraseñas en medios físicos o digitales visibles o de fácil acceso, ni guardarlas en un medio tecnológico sin protección.
- La longitud mínima de la contraseña debe ser de 12 caracteres.
- Las contraseñas deben combinar diferentes caracteres tipográficos: mayúsculas, minúsculas, números y caracteres especiales.
- Están prohibidas las secuencias de caracteres fácilmente predecibles y/o que contengan información personar del usuario.
- La caducidad de las contraseñas debe ser la siguiente:
    - Las contraseñas de usuarios personales o de usuarios (cuentas de red de FCC, cuentas de correo electrónico y servicios web, etc.) deben caducar en seis meses.
    - Las contraseñas de los administradores personales (sistemas operativos, bases de datos, aplicaciones, comunicaciones, etc.) deben cambiarse al menos una vez cada seis meses o, en caso de que estos se desvinculen o cambien de actividad.
    - Las contraseñas de cuentas de sistemas y/o servicios que no estuvieran asociadas a una persona pueden no tener fecha de caducidad, pero deben cambiarse al menos una vez al año.
- Las últimas 10 contraseñas no deben poder repetirse.
- El primer acceso al sistema debe requerir un cambio de contraseña inicial.
- Se debe cambiar la contraseña en caso de que haya algún indicio de estar comprometida.
- No está permitido cambiar las contraseñas repetidamente para mantener la contraseña inicial.
- Utilizar siempre que sea posible y conveniente, el factor de doble autenticación que el grupo FCC pone a disposición del usuario para acceder a los sistemas de información o medios tecnológicos.

- Utilizar gestores de contraseñas seguros, oficiales y previamente autorizados por el departamento de SI.

2.2.2 Inicio de sesión

- Está estrictamente prohibida la visualización de las contraseñas en el momento de su introducción.
- El inicio de sesión debe bloquearse después de cinco intentos fallidos de acceso durante al menos 15 minutos. Después de ese periodo, se puede volver a intentar el acceso.
- No se debe utilizar la opción "Recordar contraseña" que ofrecen algunas aplicaciones, como los navegadores web o el correo electrónico.

2.2.3 Bloqueo de sesión

- Las estaciones de trabajo bloquearán automáticamente la sesión después de quince (15) minutos de inactividad. Además, el usuario deberá bloquear la sesión manualmente cuando deje el ordenador sin vigilancia.
- En el caso de las aplicaciones empresariales y, en función de los riesgos, se puede añadir un bloqueo de contraseña por inactividad, con un periodo suficiente para que surta efecto pero que no cause interrupciones continuas a los usuarios.

2.2.4 Almacenamiento y trasmisión

Los sistemas de autenticación deben almacenar y transmitir las contraseñas de forma cifrada y alineada con las directrices de la Norma de Criptografía.

2.3 Provisión de Contraseñas

- La entrega de cualquier contraseña después de crear una cuenta de usuario debe hacerse a través de un entorno seguro y privado (ejemplos: correo electrónico, sellado, teléfono personal) al solicitante.
- En caso de restauración de la contraseña, la entrega se hará directamente al usuario. En estos casos, es fundamental identificar y autenticar de forma segura al solicitante, para evitar la suplantación de identidad.
- En todos los casos, la contraseña por defecto será temporal y se cambiará obligatoriamente después del primer acceso.
- La contraseña suministrada será temporal y se deberá modificar durante o, inmediatamente después, de la recepción de la misma por parte del usuario. Esta, tendrá una vigencia de 21 días naturales desde su creación.
- Las contraseñas por defecto, de cualquier sistema suministrado por los fabricantes, se deberán modificar durante o inmediatamente después de la instalación de los productos.

2.4 Selección y Uso de Contraseñas adecuadas

Independientemente de las medidas que se implementen en la gestión de las contraseñas de los sistemas, todos los usuarios deben cumplir con las directrices para la selección y el uso adecuado de la contraseña que se detallan en el Política de uso de los Medios Tecnológicos.

2.5 Contraseñas en Dispositivos Móviles

Las contraseñas utilizadas en los dispositivos móviles, por su naturaleza, deben tener características de seguridad diferentes. Deben cumplirse las siguientes condiciones:

- Las contraseñas deben tener una longitud mínima de 6 caracteres.
- Se recomienda incluir al menos una letra del alfabeto y un número.
- El usuario no debe asociarlas con información personal o fácil de adivinar, como: "0000", "9999", fecha de nacimiento, fecha actual, matrícula del vehículo, etc.
- El dispositivo debe bloquearse después de 10 intentos fallidos. Tras el bloqueo, se prohibirá el reintento de la contraseña durante un tiempo determinado.
- El dispositivo puede requerir la reintroducción de la contraseña después de cinco minutos de inactividad.
- La contraseña debe cambiarse cada 6 meses.
- No se debe utilizar como contraseña patrones de desbloqueo.

Cualquier caso en el que no sea posible cumplir las condiciones anteriores debido a las limitaciones técnicas del dispositivo tecnológico o cuando se utilice un mecanismo diferente a la autenticación por contraseña, deberá ser evaluado y aprobado por el departamento de SI.

3. Responsabilidades

El departamento de SI debe:

- Coordinar las tareas de seguridad relacionadas con la creación, salvaguarda y control de las contraseñas.
- Supervisar los intentos de acceso fallidos asociados a errores en las contraseñas de los usuarios autorizados.
- Informar a los usuarios de los requisitos establecidos en esta Norma.
- Elaborar las directrices operativas para desarrollar el Procedimiento de Seguridad de Contraseñas.

La División de Sistemas y Tecnología de la Información debe garantizar que todos los administradores puedan:

- Generar y gestionar todas las contraseñas de sistemas y aplicaciones bajo su control, de acuerdo con esta Norma.
- Informar al departamento de SI de cualquier sospecha sobre la divulgación de una contraseña.

El personal de la FCC debe:

- Salvaguardar sus contraseñas de cualquier posible pérdida, robo o divulgación.
- Comprender las consecuencias de la violación de esta Norma y asumir las responsabilidades que pudieran derivarse de dicha violación.

4. Informar inmediatamente al departamento de SI de cualquier sospecha sobre la seguridad de las contraseñas. 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.

4.1 Controles de la normativa ISO27001:2022 y ENS

ID Control ISO	Control ISO/IEC 27001:2022	Correspondencia ENS
5.10	Uso aceptable de la información y otros activos asociados	[org.2] Normativa de Seguridad; [org.3] Procedimientos de Seguridad; [mp.si.3] Custodia
5.17	Información de autenticación	[op.acc.6] Mecanismos de autenticación (usuarios de la organización)
5.18	Derechos de acceso	[op.acc.4] Proceso de gestión de derechos de acceso
8.2	Derechos de acceso privilegiado	[op.acc.2] Requisitos de acceso
8.3	Restricción del acceso a la información	[op.acc.3] Segregación de funciones y tareas
8.5	Autenticación segura	[op.acc.6] Mecanismos de autenticación (usuarios de la organización)