Control de versiones

Versión	Motivo	Realizado por	Fecha
0.9	Versión preliminar.	Consultor externo	07-11-2023
1.0	Versión aprobada	Comité de seguridad	15/06/2026

Aprobado por: Comité de seguridad el 15/06/2026

Contenido

Introducción

Este documento expone la Política de Seguridad de la Información de la Cooperativa Farmacéutica de Tenerife (en adelante, "COFARTE"), como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de la norma ISO 27001

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de COFARTE. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La Seguridad de la Información es la protección de este activo, con la finalidad de asegurar la calidad de la información y la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y en el que es fundamental la máxima colaboración e implicación de todo el personal de COFARTE.

La dirección de COFARTE, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento.

Definiciones

- **Sistema de Información:** conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- **Riesgo:** estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- **Gestión de riesgos:** actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

- **Disponibilidad:** Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
- **Integridad:** La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- **Confidencialidad:** La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

Propósito

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información de COFARTE, asegurando para ello la disponibilidad, integridad y confidencialidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente.

Alcance

La presente Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de COFARTE para los procesos descritos.

El personal sujeto a esta política incluye a todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre esta y de si el usuario es empleado o no de COFARTE. Por lo tanto, también se aplica a cualquier otra tercera parte que tenga acceso a la información o los sistemas de COFARTE.

Para garantizar que el proceso de seguridad implantado será actualizado y mejorado de forma continua, se implantará y documentará un Sistema de Gestión de la Seguridad de la Información. De esta forma, el contenido de la Política de Seguridad de la Información, será desarrollado en normas y procedimientos complementarios de seguridad.

Objetivos o Misión de la Organización

Prestar servicios de distribución farmacéutica a través de un modelo de gestión solidario, sostenible y con arraigo a la provincia de Santa Cruz de Tenerife, ofreciendo un servicio excelente y personalizado a las oficinas de farmacia, bajo un fuerte espíritu cooperativista y orgullo de pertenencia, y creando valor para la sociedad en general y el paciente en particular.

Ser reconocida como la empresa líder del sector de la distribución cooperativa farmacéutica canaria en la provincia de Santa Cruz de Tenerife, que fomente

e impulse su esencia cooperativista y su excelencia, su relevancia en el sistema canario de salud y la innovación y mejora continua como herramienta clave para su sostenibilidad (financiera, social y ambiental) en el largo plazo.

Fundamentos de esta Política

El objetivo último de la seguridad de la información es garantizar que una organización pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

Seguridad como proceso integral.

La seguridad debe entenderse como un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

Se promoverá la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Gestión de la seguridad basada en los riesgos.

El análisis de los riesgos es parte esencial y continua del proceso de seguridad. La gestión de esos riesgos permitirá el mantenimiento de un entorno controlado, con dichos riesgos a niveles aceptables, y se realizará mediante la aplicación de medidas de seguridad de manera proporcionada a la naturaleza de la información tratada y de los servicios a prestar.

Prevención, detección, respuesta y conservación.

La seguridad del sistema contempla medidas que implementen los aspectos de prevención, detección y respuesta ante incidentes de seguridad, y de conservación de la información y servicios en caso de que el incidente se produzca.

Existencia de líneas de defensa.

COFARTE implementa una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Vigilancia continua y reevaluación periódica.

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

COFARTE implementa controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Las medidas de seguridad se evaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Diferenciación de responsabilidades.

COFARTE ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge más adelante en este documento.

En los sistemas de información se diferenciará el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina la decisiones para satisfacer los requisitos de seguridad. En los supuestos de tratamiento de datos personales además se identificará el responsable de tratamiento y, en su caso, el encargado de tratamiento.

Requisitos Legales y marco normativo

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 Abril del 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de

26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

- BPD (Buenas Prácticas de la Distribución): son las normas sanitarias obligatorias que garantizan que los medicamentos mantengan su calidad, seguridad y eficacia desde que salen de la fábrica hasta que llegan a la farmacia o al hospital.
- UNE-ISO/IEC 27001:2023 Seguridad de la Información, ciberseguridad y protección de la privacidad. SGSI. Requisitos.
- UNE-ISO/IEC 27002:2023 Seguridad de la Información, ciberseguridad y protección de la privacidad. Control de Seguridad de la Información.
- Reglamento UE 2024/1689: Reglamento Europeo de inteligencia artificial.

Roles, Responsabilidades y Deberes

Usuarios

Toda persona o sistema que acceda a la información tratada, gestionada o propiedad de COFARTE se considerará un usuario. Los usuarios son responsables de su conducta cuando acceden a la información o utilicen los sistemas informáticos de COFARTE. El usuario es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los usuarios tienen la obligación de:

- Cumplir la Política de Seguridad de la Información y las normas, procedimientos e instrucciones complementarias.
- Proteger y custodiar la información de COFARTE, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.
- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y el resto de políticas, normas, procedimientos y medidas de seguridad aplicables.

Los usuarios que incumplan la Política de Seguridad de la Información o las normas y procedimientos complementarios podrán ser sancionados de acuerdo con lo establecido en los contratos que amparen su relación con COFARTE y con la legislación vigente y aplicable.

Dirección

La dirección de COFARTE está profundamente comprometida con la política descrita en este documento y es consciente del valor de la información y del grave impacto económico y de imagen que puede producir un incidente de seguridad.

Todos los socios de la cooperativa son propietarios de los activos de información propios de COFARTE, y la junta rectora es responsable de los riesgos.

La dirección asume las siguientes responsabilidades:

- Demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información
- Asegurar que se establece la política y los objetivos de seguridad de la información y que estos son compatibles con la dirección estratégica de la organización.
- Aprobar y comunicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y la importancia de su cumplimiento a todos los usuarios, internos o externos, a los clientes y a los proveedores.
- Reunirse al menos una vez al año, y cuando cualquier evento o solicitud extraordinaria lo demande, con los Responsables de Seguridad y de Sistemas, para ser informado sobre el SGSI y actualizar la estrategia en materia de Seguridad de la Información.
- Fomentar una cultura corporativa de seguridad de la información.
- Apoyar la mejora continua de los procesos de seguridad de la información.
- Asegurar que estén disponibles los recursos necesarios para el cumplimiento de la política de seguridad de la información, de las normas de uso de los sistemas y para el funcionamiento del sistema de gestión de seguridad de la información.
- Definir el enfoque para el análisis y la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos y asegurar la evaluación de los mismos al menos con una periodicidad anual.
- Asegurar que se realizan auditorías internas de seguridad de la información y que se revisan sus resultados para identificar oportunidades de mejora.

- Definir y controlar el presupuesto para seguridad de la información.
- Aprobar los planes de formación y las mejoras y proyectos relacionados con la Seguridad de la Información.
- Aprobar la documentación hasta su segundo nivel de normas y procedimientos.
- Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad.

Responsable de Seguridad

El responsable de la seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios y supervisa la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones

La persona con el cargo de Responsable de Seguridad de la Información asumirá las siguientes funciones:

- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de la Seguridad de la Información cumple con los requisitos del de la Norma UNE-ISO/IEC 27001.
- Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.
- Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos declarando la aplicabilidad de dichas medidas.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
- Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación a las normas especificadas en colaboración con el Responsable de Sistemas.
- Realizar con la colaboración del Responsable del Sistema, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable

del Sistema, aceptar los riesgos residuales calculados en el análisis de riesgos.

- Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones a presentar al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
- Coordinar el proceso de Gestión de la Seguridad, en colaboración con el Responsable de Sistemas.
- Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
- Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el Responsable de Sistemas.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, en coordinación con el Responsable del Sistema, aportando información puntual para la toma de decisiones.
- Responsable de la ejecución directa o delegada de las decisiones de la Dirección, se reunirá con esta y con el Responsable del Sistema para asegurar la estrategia.

Respecto a la documentación, y apoyándose en el Responsable del Sistema, son funciones del Responsable de Seguridad:

- Proponer a la Dirección y al Responsable de Sistemas para su aprobación la documentación de seguridad de segundo nivel (Normas de Seguridad TIC –STIC– y Procedimientos Generales del Sistema de Gestión de la Seguridad de la Información –SGSI–) y firmar dicha documentación.
- Aprobar la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).
- Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Para el desarrollo de cualquiera de sus funciones el Responsable de Seguridad podrá recabar la colaboración del Responsable del Sistema.

Delegado de Protección de Datos.

Siguiendo lo indicado en el RGPD y en la LOPDGDD, el Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben en relación al RGPD y otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
- Cooperar con la autoridad de control;
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

Responsable del Sistema.

El responsable del sistema, por sí o a través de recursos propios o contratados, se encarga de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Serán funciones del Responsable del Sistema las siguientes:

- Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

- Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
- Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de Seguridad.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de Seguridad y la Dirección.
- Realizar con la colaboración del Responsable de Seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de Seguridad, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Elaborar en colaboración con el Responsable de Seguridad, la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).

El Administrador de la Seguridad del Sistema.

Las funciones que desempeñará son las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los procedimientos operativos de seguridad.

- Aplicar los cambios de configuración del sistema de información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los respectivos Responsables de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Comité de Seguridad de la Información

Compuesto por el responsable de seguridad, el responsable del sistema y la dirección se reúne al menos semestralmente para coordinar la seguridad de la información a nivel de la organización.

Sus funciones son las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las

actuaciones en materia de seguridad cuando los recursos sean limitados.

- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Revisar regularmente la presente Política de Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas de la norma ISO 27001 y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la organización en materia de seguridad de la Información.

El Comité de Seguridad de la Información, finalmente, adoptará además las funciones del Responsable de Seguridad.

Procedimiento de designación y resolución de conflictos

La **dirección** de COFARTE **asigna, renueva y comunica** las responsabilidades, autoridades y roles en lo referente a la seguridad de la información, determinando en cada caso los motivos y el plazo de vigencia. También se asegurará de que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados, **resolviendo los conflictos** que se generen en relación a cada responsabilidad en Seguridad de la Información.

El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos.

Datos de Carácter Personal

La organización sólo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

De este modo, con la LOPDGDD se han adaptado las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

Terceras partes

Cuando la organización preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. COFARTE definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de actuaciones que COFARTE lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando COFARTE utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Desarrollo del SGSI, Revisión y Auditorías

La dirección ha aprobado el desarrollo de un sistema de gestión de seguridad de la información (SGSI) que es establecido, implementado, mantenido y mejorado conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles de la ISO 27001. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados. Existe un procedimiento de gestión documental que establece las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en el Documento de Aplicabilidad, y serán proporcionales a la criticidad de la información a proteger y a su clasificación.

El Comité de Seguridad de la Información revisará esta política anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la dirección. Las revisiones comprobarán la efectividad de la política, valorando los efectos de los cambios tecnológicos y de negocio.

La dirección será responsable de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a las situaciones de riesgo establecidas en el presente documento.

El sistema de gestión de seguridad se auditará anualmente según un plan de auditorías desarrollado por el responsable de seguridad.