	Título	Edición/Fecha Emisión	Preparado por	Aprobado por	Página
ciber	Política de Seguridad de la Información de CIBER	V.1.1 21/05/2026	Unidad Técnica	Gerencia	Página **1** de **22**

Responsable del proceso	Cliente del proceso	Uso
Responsable de Calidad Gerente	Personal CIBER	Interno

Control de modificaciones		
Modif. Nº	**Fecha**	**Descripción**
1	09/02/2026	Política de Seguridad de la Información de CIBER
2	21/05/2026	Política de Seguridad de la Información de CIBER. Aprobada en el CSI

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL CONSORCIO CENTRO PARA LA INVESTIGACIÓN BIOMÉDICA EN RED

ÍNDICE

1. INTRODUCCIÓN

Consorcio Centro De Investigación Biomédica En Red (en adelante CIBER), depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, autenticidad, trazabilidad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la confidencialidad, integridad, autenticidad y trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y la valoración de su coste deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

La Dirección del Consorcio CIBER manifiesta su compromiso con la protección de la información, los sistemas y servicios digitales que soportan la actividad investigadora y administrativa de la organización, promoviendo una cultura de seguridad basada en la mejora continua, la gestión del riesgo y el cumplimiento del marco normativo aplicable.

2. OBJETIVO

El propósito de este documento es definir y plantear la política de seguridad de la información de la entidad, que debe recoger el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

3. ALCANCE

Lo dispuesto por la presente Política se aplica a los sistemas y servicios de CIBER así como a todo su personal.
Esta política será igualmente de aplicación a terceros, proveedores, colaboradores, personal externo y entidades que accedan, procesen o gestionen información, sistemas o servicios de CIBER.

4. MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades y competencias de la organización, y que implica la implantación de medidas de seguridad en los sistemas de información, está constituida por la legislación, normativa técnica y estándares aplicables en materia de seguridad de la información, administración digital, protección de datos y ciberseguridad.
Sin perjuicio del detalle y actualización permanente recogidos en el "Anexo – Análisis de la Legislación Aplicable" mantenido por CIBER, tendrán especial consideración, entre otras, las siguientes disposiciones:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Reglamento (UE) 2016/679 General de Protección de Datos (RGPD).
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 40/2015, de Régimen Jurídico del Sector Público.
- Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real Decreto 4/2010, por el que se regula el Esquema Nacional de Interoperabilidad.
- Directiva (UE) 2022/2555 (NIS2) y normativa nacional de transposición que resulte de aplicación.
- Normas ISO/IEC 27001 y demás estándares y buenas prácticas relacionados con la seguridad de la información y continuidad de negocio.
- Guías CCN-STIC y normativa técnica de desarrollo aplicables.

CIBER mantendrá actualizado el correspondiente Anexo de Legislación Aplicable con objeto de garantizar la adecuación continua al marco normativo vigente.

5. MISIÓN

Realizar la investigación de excelencia en el campo de la Salud a través del desarrollo de proyectos colaborativos y traslacionales en el Sistema Nacional de Salud y en el Sistema de Ciencia y Tecnología.
Con el fin de lograr esta misión, el CIBER concentra esfuerzos y recursos interdisciplinares y multiinstitucionales de investigación con una dedicación preferente

de recursos económicos en torno a redes de conocimiento conformadas por centros y grupos de investigación dependientes de distintas administraciones e instituciones públicas y privadas.

6. VISIÓN

El consorcio CIBER aspira a ser un líder europeo en la investigación biomédica colocando a España en la vanguardia del conocimiento traslacional en biomedicina, capaz de resolver problemas de salud por la multidisciplinariedad de sus investigaciones y un referente en la transferencia de ese conocimiento a la sociedad. Ser un potente dinamizador de la difusión y la comunicación de los resultados de la investigación en salud a la sociedad.

La seguridad de la información deberá garantizar igualmente la protección de los datos científicos, biomédicos y personales tratados por CIBER, preservando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

7. RESPONSABILIDADES Y ESTRUCTURA

Para garantizar el cumplimiento de la normativa y establecer la organización de la seguridad de la información en CIBER, se designarán roles de seguridad y constituirá un Comité de Seguridad.

7.1. ROLES O PERFILES DE SEGURIDAD

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Responsable/s de Información y Servicios
- Responsable de Seguridad
- Responsable del Sistema

7.2. COMITÉ DE SEGURIDAD

Se ha constituido un Comité de Seguridad, como órgano colegiado, y está formado por los siguientes miembros:

- Presidente/a: Responsable de información y servicio
- Secretario/a: Responsable de Seguridad
- Vocales:
    - Responsable del Sistema.
- Asistentes:

- Delegado de Protección de Datos.

Asimismo, y con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

Los miembros del Comité serán renovados cada cuatro años o con ocasión de vacante.

7.3. FUNCIONES Y RESPONSABILIDADES

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad:

7.3.1. Funciones del Responsable de la Información y de los Servicios

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del alcance.
- Efectúa las valoraciones para la categorización de seguridad, así como, en su caso, su posterior modificación.
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.
- Recibe información sobre los incidentes y de las actuaciones realizadas para su resolución.

7.3.2. Funciones del Responsable de Seguridad

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Mantener y verificar el nivel adecuado de la continuidad del servicio.
- Promover la formación y concienciación en materia de seguridad de la información y continuidad del negocio.
- Designar responsables de la ejecución del análisis de riesgos y análisis de impacto en el negocio, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la valoración del sistema, en colaboración con el Responsable del Sistema.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.

- Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.

7.3.3. Funciones del Responsable del Sistema

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la 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.
- Prestar al Responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Monitorizar el estado de la continuidad de los sistemas.

7.3.4. Funciones del Delegado de Protección de Datos

El Delegado de Protección de Datos (DPD) ejercerá las funciones atribuidas por el Reglamento (UE) 2016/679 General de Protección de Datos, la Ley Orgánica 3/2018 y demás normativa aplicable en materia de protección de datos personales.

En particular, corresponderá al Delegado de Protección de Datos:

- Informar y asesorar a CIBER y a su personal sobre las obligaciones en materia de protección de datos personales.
- Supervisar el cumplimiento de la normativa de protección de datos y de las políticas internas relacionadas con dicha materia.
- Asesorar en la realización de evaluaciones de impacto relativas a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control y actuar como punto de contacto en cuestiones relativas al tratamiento de datos personales.
- Coordinarse con el Responsable de Seguridad en la gestión de incidentes de seguridad que afecten a datos personales.

El Delegado de Protección de Datos podrá participar en el Comité de Seguridad con voz, pero sin voto, a efectos de asesoramiento especializado en materia de protección de datos personales.

7.3.5. Funciones del Comité de Seguridad

Las funciones propias de un Comité de Seguridad de la Información son las siguientes:

- Revisión de indicadores de desempeño relacionados con la seguridad de la información.
- Evaluación de los resultados de auditorías internas y externas.
- Análisis de la satisfacción del cliente y retroalimentación recibida.
- Revisión de las acciones correctivas y preventivas implementadas.
- Actualización sobre la capacitación y sensibilización del personal.
- Definición de nuevas oportunidades de mejora y la asignación de recursos.
- Atender las solicitudes en materia de seguridad de la información, así como de las partes interesadas y de los diferentes roles de seguridad y/o áreas informando regularmente del estado.
- Asesorar en materia de seguridad de la información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades.

- 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.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
    - Aprobar y revisar la normativa de seguridad de la información
    - Aprobar y revisar 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 en particular en materia de 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 y de protección de datos que permitan verificar el cumplimiento de las obligaciones en las materias definidas.

7.3.6. Procedimiento de designación

La designación de los Responsables identificados en esta Política ha sido realizada por la Dirección de CIBER y comunicada a las partes afectadas. Los roles de seguridad serán revisados cada cuatro años en el caso de que exista una vacante, la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

Las funciones asociadas a los distintos roles de seguridad podrán ser desempeñadas por personal interno o mediante servicios prestados por entidades externas especializadas, siempre que exista designación formal, definición expresa de responsabilidades y cumplimiento de los requisitos establecidos en el Esquema Nacional de Seguridad y demás normativa aplicable.

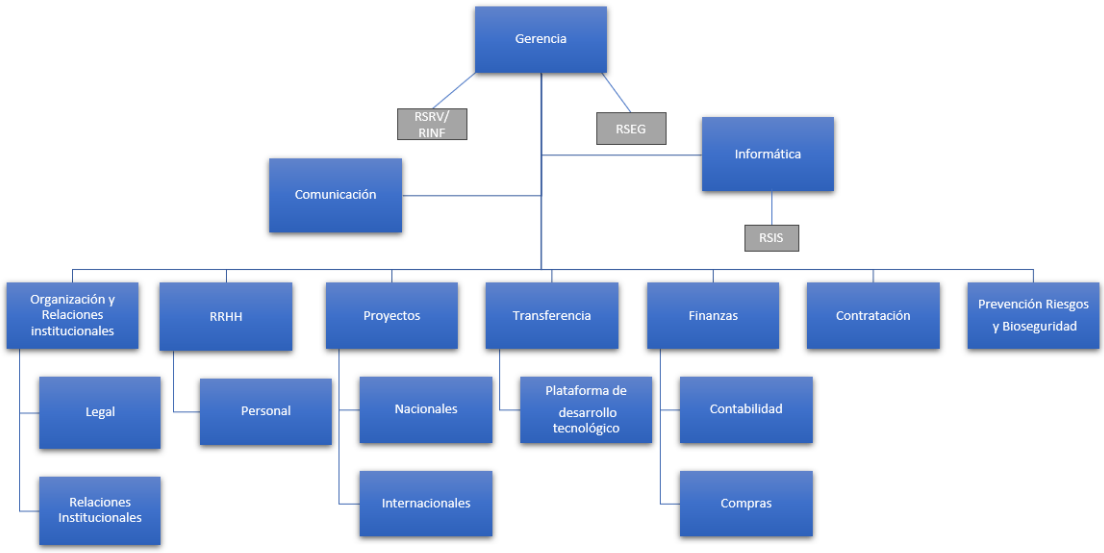
En caso de externalización de funciones de seguridad, CIBER garantizará la adecuada supervisión, coordinación y control de las actividades desempeñadas.

7.3.7. Resolución de conflictos

Si hubiera conflicto entre los Responsables, será resuelto por el Comité de Seguridad y, en última instancia, por la Dirección.

7.3.8. Organigrama de la estructura de CIBER

El organigrama que representa la estructura organizativa de CIBER



8. PRINCIPIOS BÁSICOS Y CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS

8.1. PRINCIPIOS BÁSICOS

La política de seguridad de la información se desarrolla con carácter general de acuerdo con los siguientes principios:

- Principio de confidencialidad: se deberá garantizar que los activos sean accesibles únicamente para aquellas personas expresamente autorizadas para ello.

- Principio de integridad y actualización del sistema: se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.
- Principio de disponibilidad, resiliencia y continuidad: se garantizará la prestación continuada de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada. Se debe procurar que los activos estén disponibles cuando lo requieran las personas autorizadas para acceder a ellos.
- Principio de autenticidad: se deberá garantizar que la información se intercambie con los interlocutores idóneos y que los servicios se acrediten correctamente.
- Principio de trazabilidad: se deberá garantizar el seguimiento de las operaciones efectuadas sobre la información y los servicios que lo requieran, registrándose la actividad de los usuarios.
- Seguridad integral: la seguridad es considerada como parte de la operativa habitual y como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. Además, está presente y aplicándose desde el diseño inicial de los sistemas de información.
- Principio de gestión del riesgo: gestionar la seguridad de la información consiste en analizar los riesgos, establecer medidas de seguridad adecuadas, eficaces y proporcionadas e incluir la corrección y mejora continuas que lleven a que la organización sea cada vez más preventiva que reactiva frente a los incidentes de seguridad. Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.
- Principio de prevención, reacción y recuperación: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir, detección, corrección de fraudes, incumplimientos o incidentes relacionados con la seguridad, así como de protección de las instalaciones de la compañía y a la plataforma tecnológica comprendida en el alcance.
- Principio de mejora y reevaluación continua: se revisará, de manera recurrente, el grado de eficacia de los controles de seguridad implantados en la organización para aumentar la capacidad de adaptación a la constante evolución de los riesgos y del entorno tecnológico.
- Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco

presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.

- Principio de concienciación y formación: se articularán programas de formación, sensibilización y concienciación para las personas usuarias en materia de seguridad de la información, debidamente apoyados en las políticas corporativas y con un acomodado proceso de seguimiento y actualización.
- Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.
- Principio de vigilancia continua y reevaluación periódica: La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

  Las medidas de seguridad se reevaluarán 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.

8.2. REQUISITOS MÍNIMOS

8.2.1. La Seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a. El sistema proporcionará la funcionalidad imprescindible para que CIBER alcance sus objetivos competenciales o contractuales.

b. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

c. En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d. Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

8.2.2. Vigilancia continua, reevaluación periódica e integridad, actualización del sistema y mejora continua del proceso de seguridad

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

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán 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.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información

8.2.3. Gestión de personal y profesionalidad

Todo el personal, propio o ajeno relacionado con los sistemas de información de CIBER, dentro del alcance, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

8.2.4. Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año.
- cuando se produzcan cambios en la información manejada.
- cuando se produzcan cambios en los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.
- cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

8.2.5. Incidentes de seguridad, prevención, detección, reacción y recuperación

CIBER dispone de procedimientos de gestión de incidentes de seguridad acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

8.2.6. Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados

CIBER, ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema de CIBER se conecta a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

8.2.7. Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

CIBER deberá organizar 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 en la presente Política y en la documentación de desarrollo.

8.2.8. Autorización y control de los accesos

CIBER deberá implementar, teniendo en cuenta los riesgos y amenazas identificadas, mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

8.2.9. Protección de las instalaciones

CIBER deberá implementar, teniendo en cuenta los riesgos y amenazas identificadas, mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

8.2.10. Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad, CIBER, tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

8.2.11. Protección de la información almacenada y en tránsito y continuidad de la actividad

CIBER prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

8.2.12. Registro de actividad y detección de código dañino

CIBER con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de CIBER y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, la organización podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

8.2.13. Infraestructuras y servicios comunes

CIBER tendrá en cuenta que la utilización de infraestructuras y servicios comunes, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto.

8.2.14. Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras

CIBER tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para Entidades Locales que sean de aplicación.

8.3. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento de la normativa y estándares de aplicación.

La siguiente figura representa, de forma esquemática, la jerarquía de la documentación en materia de seguridad de la información.

CIBER ha definido una Norma de Gestión de la Documentación, que establece las directrices para la creación, gestión y acceso.

La revisión anual de la presente Política corresponde al Comité de Seguridad proponiendo en caso de que sea necesario mejoras de esta, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

9. DATOS DE CARÁCTER PERSONAL

CIBER en el tratamiento de los datos personales, cumple con los principios y obligaciones de la normativa vigente, entre otra el Reglamento 679/2016, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos-RGPD-) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

En todo caso, cualquier tratamiento de datos de carácter personal deberá tener en cuenta los siguientes principios en la materia:

- Licitud, lealtad y transparencia: Los datos serán tratados de manera lícita, leal y transparente en relación con el interesado.
- Limitación de la finalidad: Los datos serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de

investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales.

- Minimización de datos: Los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- Exactitud: Los datos serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
- Limitación del plazo de conservación: Los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con lo dispuesto en la norma, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado.
- Integridad y confidencialidad: Los datos serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.
- Responsabilidad proactiva: El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en la normativa de protección de datos y deberá ser capaz de demostrarlo.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de CIBER tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad de la a través del Comité de Seguridad de la Información y del área de personal de disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de CIBER atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de CIBER en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una

responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.