**ESQUEMA NACIONAL DE SEGURIDAD**

*Real Decreto 311/2022*

# Política de seguridad de la información

POL-01

| | |
|---|---|
| **Entidad** | Erain Elkarteko Osasun Mentala Sociedad Cooperativa |
| **Referencia ENS** | org.1 Política de Seguridad |
| **Clasificación** | PÚBLICA |
| **Revisión** | 1.0 |
| **Fecha revisión** | 02/11/2026 |

## Control de versiones

| Revisión | Fecha | Autor | Descripción del cambio |
| --- | --- | --- | --- |
| 1.0 | 02/11/2026 | Responsable de seguridad | Versión inicial |

# 1. ÍNDICE

# 2. MEDIDAS ENS CUBIERTAS

Este documento desarrolla la siguiente medida del Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

| Código | Medida | BÁSICA | MEDIA | ALTA |
|---|---|---|---|---|
| **org.1** | Política de seguridad | aplica | aplica | aplica |

# 3. TRAZABILIDAD CON EL ARTÍCULO 12 DEL REAL DECRETO 311/2022

El artículo 12 del Real Decreto 311/2022 enumera los extremos que, como mínimo, debe incluir el instrumento que apruebe la política de seguridad, y los requisitos mínimos con los que ha de desarrollarse. La siguiente tabla localiza cada uno de ellos en este documento.

| Precepto | Exigencia | Apartado de esta Política |
|---|---|---|
| 12.1.a | Objetivos o misión de la organización | *Misión y objetivos de la organización* |
| 12.1.b | Marco regulatorio de las actividades | *Marco normativo y referencias* |
| 12.1.c | Roles de seguridad: deberes, responsabilidades y procedimiento de designación y renovación | *Funciones y responsabilidades* · *Procedimiento de designación, renovación y cese de roles ENS* |
| 12.1.d | Estructura y composición del comité y sus miembros, ámbito de responsabilidad y relación con otros elementos de la organización | *Estructura y composición del Comité de Seguridad de la Información* · Anexos II y III |
| 12.1.e | Directrices para la estructuración de la documentación de seguridad, su gestión y acceso | *Pirámide normativa* |
| 12.1.f | Riesgos derivados del tratamiento de los datos personales | *Datos de carácter personal y protección de la privacidad* |
| 2.3 párr. 2.º (en lugar del 12.2, propio del sector público) | Aprobación formal por el órgano competente, que en las entidades del sector privado es el que ostenta | *Aprobación, vigencia y revisión* |



Con tecnología de Auditat

| Precepto | Exigencia | Apartado de esta Política |
|---|---|---|
| | las máximas competencias ejecutivas | |
| 12.3 a 12.5 | Supuestos que no concurren en Erain Elkarteko Osasun Mentala Sociedad Cooperativa | — |
| 12.6 | Desarrollo mediante los quince requisitos mínimos (a–ñ) | *Requisitos mínimos de seguridad* |
| 12.7 | Exigencia proporcional a los riesgos de cada sistema | *Proporcionalidad en la exigencia de los requisitos mínimos* |

## 4. COMPROMISO

Erain Elkarteko Osasun Mentala Sociedad Cooperativa reconoce la información como un activo estratégico de valor fundamental y se compromete formalmente a garantizar su protección adecuada mediante la implantación y mejora continua de un sistema de Gestión de Seguridad basado en el Esquema Nacional de Seguridad (ENS).

Nuestra política se fundamenta en asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos tratados, garantizando el cumplimiento de la legalidad vigente y la prestación de servicios seguros y resilientes.

Erain Elkarteko Osasun Mentala Sociedad Cooperativa asume la responsabilidad de dotar a la organización de los recursos necesarios, fomentar una cultura de seguridad en todos los niveles y gestionar proactivamente los riesgos, asegurando así la excelencia en la prestación de los servicios y la plena confianza de todas las partes interesadas.

## 5. MISIÓN Y OBJETIVOS DE LA ORGANIZACIÓN

En cumplimiento del artículo 12.1.a del Real Decreto 311/2022, se recogen a continuación los objetivos y la misión de Erain Elkarteko Osasun Mentala Sociedad Cooperativa:

La misión de la entidad es la prestación de servicios y soluciones a sus clientes, entre ellos entidades del sector público, con los niveles de calidad, disponibilidad y seguridad comprometidos contractualmente. Sus objetivos en materia de seguridad de la información son proteger la información propia y la confiada por sus clientes, asegurar la continuidad de los servicios prestados y mantener la conformidad con el Esquema Nacional de Seguridad como requisito para operar con el sector público.

La presente Política de Seguridad se orienta a garantizar que la organización pueda cumplir dicha misión utilizando sistemas de información de forma segura.

## 6. OBJETO



Con tecnología de Auditat

El objeto de esta Política de Seguridad es fijar los principios generales y el marco organizativo y tecnológico necesarios para garantizar la protección adecuada de la información tratada y de los servicios prestados por la entidad.

La seguridad de la información es un pilar fundamental para la organización y, por ello, se pretende cumplir con una serie de propósitos específicos:

- Garantizar el cumplimiento de la legislación vigente, reglamentos y acuerdos con terceros en lo que afecta al tratamiento de la información.
- Asegurar la continuidad en las operaciones de la organización con el fin de permitir el normal funcionamiento de los servicios críticos, aun cuando alguna de sus funciones se viese dañada por un accidente interno o externo.
- Promover la competencia, la toma de conciencia y la formación en materia de seguridad de la información.
- Establecer la responsabilidad del personal empleado en relación con la notificación de las violaciones de seguridad; preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y cumplir las políticas y procedimientos inherentes a la Política de Seguridad de la Información, sin excepciones.

Por tanto, el fin principal de esta Política de Seguridad es asegurar que los activos de información estén protegidos contra amenazas, internas o externas, accidentales o deliberadas, con el fin de garantizar el cumplimiento de los principios básicos de la seguridad:

- Confidencialidad. Asegurar que la información sea accesible solo a quienes estén autorizados.
- Integridad. Garantizar la exactitud de la información y los sistemas contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- Disponibilidad. Asegurar que los usuarios autorizados tengan acceso a la información cuando lo requieran.
- Autenticidad. Garantizar la identidad de quien genera o accede a la información.
- Trazabilidad. Asegurar que las actuaciones de una entidad, persona o proceso puedan ser trazadas de forma indiscutible hasta dicha entidad, persona o proceso.

Por supuesto, el objeto de esta política no es un elemento aislado, sino que está alineado con la misión de la organización. La seguridad se entiende como un proceso integral que no se limita a la tecnología, sino que abarca a las personas, los procesos, la estructura organizativa y las instalaciones físicas.

## 7. ALCANCE

Esta Política de Seguridad es de aplicación, en cuanto a las medidas de seguridad, a todos los activos de información, sistemas, infraestructuras y procesos que soportan los servicios y sistemas de información incluidos dentro del alcance de conformidad con el Esquema Nacional de Seguridad (ENS) definido por la organización.

El alcance detallado, incluyendo la relación de sistemas de información, sedes físicas, servicios afectados y activos críticos, se encuentra documentado y actualizado en la Categorización del sistema y en el Inventario de activos vigentes.

Las directrices y principios de esta Política obligan a toda la organización y a todo su personal, interno y externo, con independencia de su ubicación geográfica o relación contractual. Las medidas de seguridad del Anexo II del Real Decreto 311/2022 se implantan sobre los activos, sistemas y servicios comprendidos en el alcance de conformidad definido por la organización, en los términos de la Declaración de aplicabilidad.



Con tecnología de Auditat

# 8. MARCO NORMATIVO Y REFERENCIAS

En cumplimiento del artículo 12.1.b del Real Decreto 311/2022, se identifica a continuación el marco regulatorio en el que Erain Elkarteko Osasun Mentala Sociedad Cooperativa desarrolla sus actividades: las normas españolas y europeas relativas a la administración electrónica, la ciberseguridad, la seguridad de la información y la protección de datos personales, junto con la normativa sectorial y las obligaciones contractuales que resulten de aplicación.

La relación que sigue tiene carácter enunciativo y no exhaustivo. Erain Elkarteko Osasun Mentala Sociedad Cooperativa dispone de un procedimiento de identificación de la legislación aplicable, que determina las fuentes a consultar, el responsable de hacerlo y la forma de registrarla, y mantiene actualizado el Registro de legislación y guías CCN-STIC, donde consta la situación de cada norma —entrada en vigor, fecha de aplicación y norma que en su caso la derogue—. Dicho registro prevalece sobre la relación siguiente.

## 8.1. Normativa general

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Reglamento (UE) 2016/679 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, que rige la actuación de Erain Elkarteko Osasun Mentala Sociedad Cooperativa en su condición de licitadora y contratista del sector público: capacidad y solvencia, prohibiciones de contratar, deber de confidencialidad, obligaciones en la ejecución del contrato y régimen de la subcontratación.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

Las normas que se relacionan a continuación rigen primordialmente la actuación de las Administraciones públicas a las que Erain Elkarteko Osasun Mentala Sociedad Cooperativa presta servicio, y la alcanzan por dos vías: por su condición de interesada en los procedimientos administrativos —en particular, la obligación de las personas jurídicas de relacionarse por medios electrónicos con las Administraciones públicas— y a través de los pliegos y contratos que suscribe con ellas y de los requisitos de seguridad que en ellos se establezcan.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

## 8.2. Instrucciones Técnicas de Seguridad

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.



Con tecnología de Auditat

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

### 8.3. Normas técnicas y guías

- Guías CCN-STIC (series 800 y 900).
- UNE-EN ISO/IEC 27002:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Control de la seguridad de la información (ISO/IEC 27002:2022).
- UNE-EN ISO/IEC 27001:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos (ISO/IEC 27001:2022).

### 8.4. Normativa sectorial aplicable a Erain Elkarteko Osasun Mentala Sociedad Cooperativa

- Normativa sectorial sanitaria

Ley 12/2008 de Servicios Sociales del País Vasco Ley 1/2023 de Educación de la Comunidad Autónoma del País Vasco Ley 2/2024 de Infancia y Adolescencia del País Vasco Ley 2/2000: Ley de creación del Colegio de Educadores Sociales del País Vasco (CEESPV)

## 9. APROBACIÓN, VIGENCIA Y REVISIÓN

En cumplimiento del artículo 2.3 del Real Decreto 311/2022, que impone a las entidades del sector privado la obligación de contar con la política de seguridad a que se refiere su artículo 12 y cuyo párrafo segundo atribuye su aprobación al órgano que ostente las máximas competencias ejecutivas, esta Política de Seguridad de la Información se aprueba formalmente por el Consejo Rector, a propuesta del Comité de Seguridad de la Información, que es el órgano encargado de su elaboración y revisión periódica.
A los efectos de esta Política, las referencias al órgano de gobierno se entienden hechas al órgano que la aprueba conforme a este apartado.

| | |
|---|---|
| **Órgano competente que aprueba** | El Consejo Rector |
| **Propuesta y elaboración** | Comité de Seguridad de la Información |
| **Fecha de aprobación** | _____ |
| **Firma** | _____ |

Esta Política tiene carácter público. Una vez aprobada, se publica y se difunde a todo el personal y a los colaboradores de Erain Elkarteko Osasun Mentala Sociedad Cooperativa, así como a los terceros que resulten vinculados por ella, a través de los canales habilitados al efecto. La organización conserva evidencia de su publicación y de su difusión, con indicación de la fecha y del medio empleado.
El contenido de esta Política de Seguridad entra en vigor desde la fecha de su aprobación encontrándose vigente hasta que sea reemplazada por una nueva Política aprobada por el mismo órgano. El historial de versiones, con la fecha y la descripción de cada revisión, consta en el control de versiones que encabeza este documento.



Con tecnología de Auditat

Esta Política se revisa con periodicidad **anual**, con el fin de mantener su pertinencia, suficiencia y eficacia. La revisión queda documentada en acta del Comité de Seguridad de la Información aunque concluya que no procede modificar el contenido.
Toda modificación posterior requiere una nueva aprobación por el órgano competente.

### 9.1. Ámbito subjetivo

Erain Elkarteko Osasun Mentala Sociedad Cooperativa queda sujeta al Esquema Nacional de Seguridad en su condición de operador del sector privado que presta servicios o provee soluciones al sector público, conforme al artículo 2.3 del Real Decreto 311/2022. Esta Política de Seguridad es propia de la entidad y ha sido aprobada por su órgano competente. Conforme al párrafo tercero de ese mismo artículo 2.3, los pliegos de las Administraciones contemplan la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el Esquema Nacional de Seguridad; los requisitos de seguridad adicionales que cada Administración cliente imponga en sus pliegos o contratos se identifican en la relación con dicha Administración y se recogen en la Declaración de aplicabilidad.
Si esta circunstancia cambiara —porque Erain Elkarteko Osasun Mentala Sociedad Cooperativa pasara a integrarse en el sector público institucional o a quedar comprendida en la política de seguridad de un grupo u organización del que forme parte, o dejara de estarlo—, se hará constar expresamente y este documento se revisará para mantener la coherencia con aquella.

## 10. PRINCIPIOS BÁSICOS

El objeto último de la seguridad de la información es garantizar que la 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:

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.
c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Vigilancia continua.
f) Reevaluación periódica.
g) Diferenciación de responsabilidades.

Estos principios rigen también la relación de Erain Elkarteko Osasun Mentala Sociedad Cooperativa con los proveedores de servicios y productos de los que depende el sistema, y se extienden a su cadena de suministro en la medida que resulte necesario conforme al análisis de riesgos, tal como prevé el artículo 2.3 del Real Decreto 311/2022.
De este modo se reduce la probabilidad de que las amenazas se materialicen y, si llegan a ocurrir, se limita su efecto sobre la información que se maneja y los servicios que se prestan.

### 10.1. Ámbitos de desarrollo de la política

La aplicación de los principios básicos anteriores se proyecta, al menos, sobre los siguientes ámbitos de la seguridad de la información. La exigencia concreta que corresponde a cada uno de ellos se detalla en el apartado *Requisitos mínimos de seguridad* y en el cuerpo normativo al que dicho apartado remite:

a) Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones.



Con tecnología de Auditat

b) Gestión de activos de información inventariados, categorizados y asociados a un responsable.
c) Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
d) Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
e) Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
f) Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.
g) Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de dichos sistemas.
h) Gestión de los incidentes de seguridad implantando mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
i) Gestión de la continuidad implantando mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

## 11. PREVENCIÓN

Erain Elkarteko Osasun Mentala Sociedad Cooperativa evita que la información y los servicios se vean perjudicados por incidentes de seguridad.
A tal fin implanta las medidas de seguridad exigibles al sistema conforme al Anexo II del Real Decreto 311/2022, así como cualquier control adicional identificado a través de la evaluación de amenazas y riesgos.
Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.
Para garantizar el cumplimiento de la política, las áreas responsables deben:

- Autorizar formalmente, con carácter previo, la puesta en operación de los elementos del sistema y los demás supuestos previstos en el Procedimiento de autorización.
- Evaluar regularmente la seguridad, incluyendo el análisis de los cambios de configuración realizados de forma rutinaria.
- Verificar el cumplimiento del Esquema Nacional de Seguridad al menos cada dos años, conforme a los artículos 31 y 38 y al Anexo III del Real Decreto 311/2022, mediante la auditoría de certificación que corresponde a los sistemas de categoría MEDIA, y documentar su resultado en el Informe de auditoría ENS.

## 12. DETECCIÓN

Erain Elkarteko Osasun Mentala Sociedad Cooperativa establece controles sobre la operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia, conforme al artículo 10 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (vigilancia continua y reevaluación periódica).



Con tecnología de Auditat

Se implantan mecanismos de detección, análisis y reporte cuya información llega a los responsables de forma regular y, de manera inmediata, cuando se produce una desviación significativa de los parámetros preestablecidos como normales. Estos mecanismos forman parte de la estrategia de protección en capas prevista en el artículo 9 del citado real decreto (existencia de líneas de defensa).
El desarrollo de este apartado, incluido el sistema de métricas, consta en el Procedimiento de monitorización del sistema.

## 13. RESPUESTA

Erain Elkarteko Osasun Mentala Sociedad Cooperativa y las áreas responsables deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad, dejando constancia de las actuaciones realizadas.
- Designar un punto de contacto para las comunicaciones relativas a incidentes, tanto internas como con otras entidades u organismos.
- Notificar los incidentes de seguridad al INCIBE-CERT, equipo de respuesta de referencia del sector privado conforme al artículo 33.7 del Real Decreto 311/2022 —que los pondrá inmediatamente en conocimiento del CCN-CERT—, y conforme a la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad en lo que resulte aplicable, sin perjuicio de la notificación de brechas de datos personales prevista en el apartado *Notificación de brechas de datos personales*.
- Establecer protocolos para el intercambio de información relacionada con el incidente, incluidas las comunicaciones en ambos sentidos con los equipos de respuesta a incidentes de seguridad (CSIRT/ CERT) competentes, en particular el INCIBE-CERT y, a través de este, el CCN-CERT.

El desarrollo de este apartado consta en el Procedimiento de gestión de incidentes y registro de actividad.

## 14. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios, Erain Elkarteko Osasun Mentala Sociedad Cooperativa dispone de los medios y las técnicas necesarias que permiten la recuperación de los servicios más críticos.
Erain Elkarteko Osasun Mentala Sociedad Cooperativa realiza copias de respaldo de la información y de los servicios y comprueba su correcta ejecución, así como su capacidad de restauración mediante pruebas periódicas, conforme al Procedimiento de copias de seguridad y restauración.
Asimismo, determina para cada servicio el tiempo máximo de interrupción admisible y mantiene, con el alcance que fija la Declaración de aplicabilidad, el análisis de impacto.

## 15. ESTRUCTURA Y COMPOSICIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

En cumplimiento del artículo 12.1.d del Real Decreto 311/2022, se detalla a continuación la estructura y composición del Comité de Seguridad de la Información de Erain Elkarteko Osasun Mentala Sociedad Cooperativa, su ámbito de responsabilidad y su relación con el resto de la organización.
Erain Elkarteko Osasun Mentala Sociedad Cooperativa adopta el modelo de gobernanza estándar de la seguridad de la información: los cuatro roles que diferencia el artículo 11 del Real Decreto 311/2022 y cuyas funciones detalla su artículo 13 —Responsable de la Información, Responsable del Servicio, Responsable de Seguridad y Responsable del Sistema—, coordinados por un Comité de Seguridad de la Información. No se



Con tecnología de Auditat

acoge, por tanto, al modelo de gobernanza simplificado previsto en el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad (CCN-STIC 890).

## 15.1. Composición

El Comité de Seguridad de la Información está integrado por una Presidencia, una Secretaría y los cuatro roles de seguridad que diferencia el artículo 11 del Real Decreto 311/2022 y cuyas funciones detalla su artículo 13 —Responsable de la Información, Responsable del Servicio, Responsable de Seguridad y Responsable del Sistema—, sin perjuicio de los miembros adicionales que el propio Comité acuerde incorporar.

Podrá designarse más de un Responsable de la Información o más de un Responsable del Servicio —uno por cada tipo de información tratada o por cada servicio prestado—, en cuyo caso el ámbito de cada titular queda delimitado de forma expresa en el acuerdo de nombramiento. Podrán asimismo designarse Responsables de Seguridad Delegados y Responsables del Sistema Delegados por ámbito, a propuesta de su respectivo titular y con dependencia funcional directa de este, que delega funciones pero no responsabilidad. El Comité podrá incorporar miembros adicionales e invitar a sus reuniones, con voz, a otras personas internas o externas cuando el asunto lo requiera, sin que su participación altere el régimen de adopción de acuerdos descrito en el apartado *Régimen de funcionamiento*.

En ningún caso el Responsable de Seguridad y el Responsable del Sistema recaen en la misma persona, ni existe dependencia jerárquica entre ambos, conforme al artículo 13.3 del Real Decreto 311/2022.

La Presidencia del Comité la ejerce quien ostenta el rol de Responsable de la Información, sin que ello afecte al ejercicio de dicho rol. La Secretaría del Comité la ejerce uno de los titulares del rol de Responsable del Servicio y de Responsable de Seguridad, según determine el acuerdo de nombramiento, sin que ello afecte al ejercicio de dicho rol.

La identidad de quienes ocupan cada rol en cada momento, con sus fechas de designación y cese, consta en el Acuerdo de nombramiento de los roles de seguridad adoptado por el órgano de gobierno, en el Acta de constitución del Comité de Seguridad y en el Registro de nombramientos y ceses de roles ENS, que se incorporan a esta Política como anexos. Las variaciones en las personas designadas no requieren la modificación de esta Política, que se mantiene vigente en sus propios términos.

## 15.2. Régimen de funcionamiento

El Comité se reúne con periodicidad semestral, sin perjuicio de las convocatorias extraordinarias que la Presidencia considere necesarias, en particular ante incidentes graves de seguridad o cambios relevantes del alcance.

La Presidencia convoca y dirige las reuniones. Los acuerdos se adoptan por consenso de los miembros del Comité; de no alcanzarse, decide quien preside la sesión, que es responsable último de las decisiones adoptadas. La Secretaría levanta acta de cada sesión, custodia los acuerdos y hace seguimiento de las acciones asignadas. Los acuerdos se documentan en actas conforme a la plantilla de actas de reunión, que constituyen la evidencia del funcionamiento del Comité.

## 15.3. Ámbito de responsabilidad

El ámbito de responsabilidad del Comité abarca todos los sistemas, servicios, activos e instalaciones incluidos en el alcance declarado de esta Política. Dentro de ese ámbito, el Comité es el órgano competente para coordinar la seguridad de la información, resolver los conflictos de responsabilidad entre roles y áreas,



Con tecnología de Auditat

y elevar al órgano de gobierno cuanto exceda de sus atribuciones, en particular la aprobación de esta Política y la dotación presupuestaria de los planes de mejora.

### 15.4. Resolución de conflictos

Los conflictos de responsabilidad o de criterio entre roles de seguridad, o entre áreas de la organización, se elevan al Comité de Seguridad de la Información, que resuelve de forma motivada y deja constancia del acuerdo en el acta de la sesión correspondiente. La Presidencia puede convocar sesión extraordinaria cuando el conflicto afecte a la seguridad de un servicio en operación.
Si el conflicto excede de las atribuciones del Comité, o si su resolución compromete recursos no previstos, se eleva al órgano de gobierno. Hasta que exista resolución, se mantiene la opción más protectora para la información y los servicios afectados.

### 15.5. Relación con otros elementos de la organización

- **Órgano de gobierno**: el Comité le eleva la propuesta de aprobación y revisión de esta Política, los planes de mejora con su dotación presupuestaria y el estado de los riesgos residuales. El órgano de gobierno aprueba y provee los recursos.
- **Roles de seguridad ENS**: los cuatro responsables integran el Comité y le reportan en su respectivo ámbito. El principio de diferenciación de responsabilidades del artículo 11 rige sus relaciones, y el Responsable de Seguridad no puede ostentar simultáneamente el cargo de Responsable del Sistema.
- **Áreas y departamentos**: el Comité coordina sus actuaciones en materia de seguridad para evitar duplicidades y asegurar la coherencia con la estrategia aprobada. Las áreas ejecutan las medidas y reportan las incidencias.
- **Función de auditoría**: el Comité promueve las auditorías periódicas, recibe sus informes y acuerda las medidas correctoras derivadas de los hallazgos.
- **Terceros y proveedores**: el Comité establece los canales de comunicación y coordinación con los comités o responsables de seguridad de las entidades con las que existan servicios o interconexiones, conforme al apartado *Relación con terceras partes*.

## 16. FUNCIONES Y RESPONSABILIDADES

Los diferentes roles de seguridad de la información se limitan a una jerarquía simple: el Comité de Seguridad de la Información y los diferentes responsables, donde rige el principio básico de diferenciación de responsabilidades tal y como se establece en el artículo 11 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que distingue el Responsable de la Información, el Responsable del Servicio, el Responsable de Seguridad y el Responsable del Sistema.
A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

### 16.1. Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la dirección de la entidad y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.



Con tecnología de Auditat

- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes áreas y departamentos.
- 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 por Erain Elkarteko Osasun Mentala Sociedad Cooperativa 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.
- Elaborar y aprobar la normativa de Seguridad de la Información, en coordinación con la Dirección de la entidad.
- Verificar y aprobar los procedimientos de seguridad de la información y demás documentación.
- 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 ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de Erain Elkarteko Osasun Mentala Sociedad Cooperativa en materia de seguridad de la Información.

## 16.2. Funciones del Responsable de la Información y del Responsable del Servicio

Ambos roles son designados de forma diferenciada, conforme al apartado *Composición*, y ejercen las siguientes funciones cada uno sobre su ámbito —la información tratada y los servicios prestados, respectivamente—:

- Determinar los niveles de seguridad de la información y del servicio en cada dimensión de seguridad, dentro del marco establecido en el Anexo I del Real Decreto 311/2022, con el asesoramiento del Responsable de Seguridad.
- Establecer y aprobar los requisitos de seguridad aplicables a la información y al servicio, previa propuesta del Responsable de Seguridad o del Comité de Seguridad de la Información.
- Aceptar los niveles de riesgo residual que afecten a la información y al servicio.
- Mantener y verificar el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.



Con tecnología de Auditat

- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, de los planes de continuidad, procediendo a su validación.
- Aprobar los cambios que afecten a la información o al servicio que les corresponde.

## 16.3. Funciones del Responsable de Seguridad

- Procurar que la documentación de seguridad se mantenga organizada y actualizada, y gestionar los mecanismos de acceso a la misma.
- 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 al Esquema Nacional de Seguridad.
- Realizar los análisis de riesgos, seleccionar las salvaguardas a implantar y revisar el proceso de gestión del riesgo, elevando un informe anual al Comité.
- 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 para que el Comité adopte las medidas correctoras adecuadas.
- Coordinar el proceso de Gestión de la Seguridad.
- Firmar la Declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema (artículo 28.2 y Anexo II, apartado 2, del Real Decreto 311/2022).
- Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
- Comprobar, directamente o a través del Administrador de Seguridad si lo hubiere, que los controles de seguridad establecidos son adecuadamente observados y que se aplican los procedimientos aprobados para manejar el sistema de información.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y los mecanismos de auditoría técnica, así como que la actividad desarrollada en el sistema se ajusta a lo autorizado.

## 16.4. Funciones del Responsable del Sistema de Información

- Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio cuando tenga conocimiento de deficiencias graves de seguridad que lo aconsejen. La decisión se acuerda previamente con el Responsable de la Información afectada, con el Responsable del Servicio afectado y con el Responsable de Seguridad, antes de ser ejecutada (artículo 13 del Real Decreto 311/2022).
- Desarrollar, operar y mantener el sistema de información durante 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.



Con tecnología de Auditat

- Prestar al Responsable de Seguridad y/o al Comité de Seguridad 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, directamente o a través del Administrador del Sistema si lo hubiere, las funciones de administración 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 del sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema.
- La aplicación de los Procedimientos Operativos de Seguridad (POS).

### 16.5. El Administrador de Sistemas / Seguridad

Atendiendo a su estructura organizativa, la organización podrá contar con uno o varios Administradores de Sistemas / Seguridad. Cada Administrador depende funcionalmente del Responsable del Sistema o del Responsable de Seguridad, pero no de ambos, y sus funciones vienen determinadas por dicha dependencia:

- **Administrador dependiente del Responsable del Sistema**: implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información; gestionar, configurar y actualizar el hardware y el software en los que se basan los mecanismos y servicios de seguridad; aplicar los Procedimientos Operativos de Seguridad (POS); informar al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad, y colaborar en la investigación y resolución de incidentes de seguridad.
- **Administrador dependiente del Responsable de Seguridad**: comprobar que los controles de seguridad establecidos son adecuadamente observados y que se aplican los procedimientos aprobados para manejar el sistema de información; gestionar las autorizaciones y privilegios concedidos a los usuarios, monitorizando que la actividad desarrollada en el sistema se ajusta a lo autorizado; monitorizar el estado de seguridad del sistema; informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad, y colaborar en la investigación y resolución de incidentes de seguridad.

El Administrador ejecuta funciones bajo la responsabilidad del titular del que depende: la delegación transfiere funciones, no responsabilidad. Cuando la complejidad, la distribución, la separación física de los elementos del sistema o el número de usuarios lo requieran, podrán designarse administradores delegados, a solicitud del Administrador y con dependencia funcional directa de este. La identidad de los Administradores y de sus delegados, así como el alcance de cada delegación, consta en la documentación de seguridad del sistema y en el Registro de nombramientos y ceses de roles ENS.

La organización no cuenta con Administradores, por lo que las funciones de administración descritas las ejerce directamente el titular correspondiente: las de ejecución, el Responsable del Sistema; las de comprobación y supervisión, el Responsable de Seguridad.

## 17. PROCEDIMIENTO DE DESIGNACIÓN, RENOVACIÓN Y CESE DE ROLES ENS

En cumplimiento del artículo 12.1.c del Real Decreto 311/2022, Erain Elkarteko Osasun Mentala Sociedad Cooperativa establece el siguiente procedimiento formal para la designación, renovación y cese de los roles de seguridad del Esquema Nacional de Seguridad.



Con tecnología de Auditat

## 17.1. Designación

Los roles de Responsable de la Información, Responsable del Servicio, Responsable de Seguridad y Responsable del Sistema son designados formalmente por el órgano de gobierno de la organización. La designación inicial de los roles de seguridad y la constitución del Comité de Seguridad de la Información se realizan directamente por el órgano de gobierno, mediante el correspondiente acuerdo de nombramiento, y se formalizan en el Acta de constitución del Comité de Seguridad y en los documentos individuales de aceptación del cargo. Las designaciones posteriores —renovaciones, sustituciones y nuevos roles— se realizan por el órgano de gobierno a propuesta del Comité de Seguridad de la Información.
Los requisitos mínimos para la designación de cada rol son:

- **Responsable de la Información**: conocimiento de los procesos de negocio y del valor de la información tratada.
- **Responsable del Servicio**: conocimiento de los servicios prestados y de sus requisitos de disponibilidad.
- **Responsable de Seguridad**: formación y experiencia en seguridad de la información. No podrá ostentar simultáneamente el cargo de Responsable del Sistema (art. 13.3 del Real Decreto 311/2022).
- **Responsable del Sistema**: competencia técnica demostrada en la administración de los sistemas del alcance.

Los Administradores son designados por el órgano de gobierno a propuesta del Responsable del Sistema o del Responsable de Seguridad, según la dependencia funcional del puesto. Sus administradores delegados, si los hubiere, son designados por el órgano de gobierno a solicitud del propio Administrador, del que mantienen dependencia funcional directa.
Los Responsables de Seguridad Delegados y los Responsables del Sistema Delegados, si los hubiere, son designados por el órgano de gobierno a propuesta de su respectivo titular, que delega funciones pero no responsabilidad y del que mantienen dependencia funcional directa.
Todas estas designaciones siguen el mismo régimen formal de comunicación y registro que el resto de roles de seguridad.

## 17.2. Duración del mandato y renovación

La designación en un rol de seguridad se realiza por tiempo indefinido y se ratifica anualmente por el Comité de Seguridad de la Información, con ocasión de la revisión de esta Política, dejando constancia en el acta correspondiente.
Si un responsable deja de cumplir los requisitos de su puesto o se produce un cambio organizativo que afecte a sus funciones, el Comité de Seguridad propone sin dilación al órgano de gobierno un sustituto, que lo designa con carácter provisional si fuera necesario, de modo que ningún rol de seguridad quede vacante.

## 17.3. Cese y sustitución

El cese en un rol de seguridad puede producirse por:

- Renuncia voluntaria comunicada por escrito al Comité de Seguridad.
- Revocación por el órgano de gobierno, a propuesta del Comité, por incumplimiento de las funciones asignadas.
- Extinción de la relación laboral o contractual con la organización.
- Reorganización que elimine o transforme el puesto.



Con tecnología de Auditat

En todos los casos, el cese se formaliza mediante el Acta de Cese y Nueva Designación. La persona saliente traspasa al sustituto, sin dilación, el conocimiento del estado de seguridad de su ámbito, la documentación asociada y los asuntos pendientes, dejando constancia en la misma acta.

### 17.4. Comunicación

Toda designación, renovación o cese se comunica a:

- El propio interesado.
- El Comité de Seguridad (si no es el proponente).
- Las entidades externas con las que existan servicios o interconexiones, cuando el cambio afecte al punto de contacto acordado con ellas.

### 17.5. Registro

La organización mantiene el Registro de nombramientos y ceses de roles ENS, accesible para auditorías, con al menos: nombre, cargo, ámbito, fecha de inicio, fecha de fin, motivo del cese, referencia al acta correspondiente y, en el caso de los Administradores, dependencia funcional.

## 18. DATOS DE CARÁCTER PERSONAL Y PROTECCIÓN DE LA PRIVACIDAD

Erain Elkarteko Osasun Mentala Sociedad Cooperativa trata datos de carácter personal a los que tendrán acceso únicamente las personas autorizadas. Todos los sistemas de información se ajustarán a las medidas técnicas y organizativas apropiadas al riesgo, conforme al artículo 32 del Reglamento (UE) 2016/679, atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento.
En aplicación del principio de responsabilidad proactiva establecido en el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD), las actividades de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

### 18.1. Riesgos derivados del tratamiento de datos personales

En cumplimiento del artículo 12.1.f del Real Decreto 311/2022, se identifican a continuación los riesgos que se derivan de los tratamientos de datos personales que realiza Erain Elkarteko Osasun Mentala Sociedad Cooperativa en el ámbito de esta Política. Se trata de riesgos que, además de comprometer la seguridad del sistema, pueden lesionar los derechos y libertades de las personas físicas, por lo que reciben atención específica en el análisis de riesgos:

- **Acceso no autorizado a datos personales**, por personal propio o ajeno, por exceso de privilegios o por fallo de los mecanismos de identificación y autenticación.
- **Divulgación o cesión indebida** de datos personales a terceros no autorizados, incluida la derivada del envío erróneo de comunicaciones o de la publicación accidental de información.
- **Tratamiento incompatible con la finalidad** para la que los datos fueron recogidos, o conservación más allá del plazo necesario.
- **Pérdida de integridad o exactitud** de los datos, que pueda dar lugar a decisiones incorrectas que afecten a las personas interesadas.
- **Pérdida de disponibilidad** de los datos personales, impidiendo atender las obligaciones de la organización o el ejercicio de los derechos de las personas interesadas.



Con tecnología de Auditat

- **Pérdida de trazabilidad** sobre quién ha accedido a los datos y con qué finalidad, que imposibilite acreditar la licitud del tratamiento o investigar un incidente.
- **Riesgos asociados a encargados del tratamiento y a terceros**, incluidos los servicios en la nube y las transferencias internacionales de datos.
- **Riesgos derivados de los soportes y de los equipos**, en particular la pérdida o el robo de dispositivos portátiles y soportes extraíbles, y la destrucción insegura de soportes que contengan datos personales.
- **Riesgo agravado por el tratamiento de categorías especiales de datos** (artículo 9 del RGPD), cuya materialización puede tener consecuencias especialmente graves para las personas afectadas.

Estos riesgos se evalúan y tratan en el marco del proceso único de gestión del riesgo descrito en el apartado *Gestión de riesgos*, cuyo resultado consta en el Análisis de riesgos. Las medidas que de él se deriven se coordinan con las exigidas por la normativa de protección de datos, y su suficiencia se somete al criterio del Responsable de Seguridad.

## 18.2. Registro de Actividades de Tratamiento

La entidad mantiene un Registro de Actividades de Tratamiento (RAT) conforme al art. 30 del RGPD, gestionado por el personal designado de la entidad, que distingue las actividades en las que actúa como Responsable y aquellas en las que actúa como Encargado del tratamiento. Cada actividad recoge finalidad, base jurídica, categorías de interesados y datos, destinatarios, plazos de conservación y medidas de seguridad aplicadas. El RAT se revisa al menos una vez al año y siempre que se incorpora, modifica o cesa un tratamiento.

## 18.3. Tratamiento de categorías especiales de datos

La entidad trata datos de categorías especiales (artículo 9 del RGPD), lo que obliga a aplicar medidas de seguridad reforzadas y a realizar una Evaluación de Impacto en la Protección de Datos (EIPD) conforme al artículo 35 del RGPD para cada tratamiento que suponga un alto riesgo para los derechos y libertades de las personas.

## 18.4. Evaluación de Impacto en la Protección de Datos (EIPD)

Será obligatoria la realización de una EIPD cuando un tratamiento:

- Utilice nuevas tecnologías que por su naturaleza, alcance, contexto o fines supongan un alto riesgo.
- Implique elaboración de perfiles que produzcan efectos jurídicos o afecten significativamente al interesado.
- Trate datos de categorías especiales a gran escala.
- Monitorice de forma sistemática zonas de acceso público.

La EIPD será responsabilidad del Responsable de la Información, sin perjuicio de la responsabilidad que corresponde a la entidad como responsable del tratamiento, y su resultado se comunicará al Comité de Seguridad antes de iniciar el tratamiento.

## 18.5. Derechos de los interesados

La organización garantizará el ejercicio de los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición conforme al RGPD, disponiendo de procedimientos documentados y plazos de respuesta no superiores a un mes desde la recepción de la solicitud.



Con tecnología de Auditat

### 18.6. Notificación de brechas de datos personales

Cuando Erain Elkarteko Osasun Mentala Sociedad Cooperativa actúe como responsable del tratamiento, toda violación de seguridad que afecte a datos personales se notificará a la Agencia Española de Protección de Datos (AEPD) en un plazo máximo de 72 horas desde que se haya tenido constancia de ella, conforme al artículo 33 del RGPD, salvo que sea improbable que constituya un riesgo para los derechos y libertades de las personas. Si la brecha supone un alto riesgo para los interesados, se les comunicará sin dilación indebida conforme al artículo 34.
Cuando Erain Elkarteko Osasun Mentala Sociedad Cooperativa actúe como encargada del tratamiento por cuenta de sus clientes, notificará la violación al responsable del tratamiento sin dilación indebida desde que tenga constancia de ella, en los términos y plazos previstos en el contrato de encargo, facilitándole la información necesaria para que este cumpla sus propias obligaciones de notificación.
En ambos casos, la brecha se registra y gestiona conforme al Procedimiento de gestión de incidentes y registro de actividad, y el Responsable de Seguridad es informado de inmediato.

## 19. ACCESO A LA INFORMACIÓN

Todos aquellos usuarios que traten información responsabilidad de la entidad y que no sea de acceso público, deberán estar debidamente identificados y tener los privilegios de acceso a la información estrictamente necesarios para desempeñar sus funciones, a través de credenciales suministradas por la organización.
En consecuencia, el acceso a los sistemas de información estará controlado y limitado exclusivamente a los usuarios, procesos, dispositivos y sistemas de información que estén autorizados, de forma que el acceso quede restringido exclusivamente a las funciones permitidas.

## 20. GESTIÓN DE INCIDENTES DE SEGURIDAD

Las unidades de la entidad y sus responsables deben dar respuesta a los incidentes de seguridad mediante las medidas organizativas y operativas adecuadas.
Los incidentes de seguridad pueden ser detectados proactivamente, por los responsables o administradores del sistema de información, por inspección o alarmas remitidas automáticamente al correo de la entidad, procediéndose a centralizar la recogida, análisis y gestión de los incidentes identificados.
Asimismo, cualquier usuario debe trasladar incidentes, sugerencias y/o debilidades que puedan tener relación con la seguridad de la información y las directrices contempladas en la presente política comunicándolas de inmediato a la organización.

## 21. GESTIÓN DE RIESGOS

Las decisiones en materia de seguridad deben basarse en el análisis y gestión de riesgos como proceso esencial de seguridad, que deberá mantenerse permanentemente actualizado.
La evaluación de riesgos identifica las amenazas y vulnerabilidades, y debe ser suficientemente amplia como para abarcar los principales factores internos y externos, tales como tecnológicos, físicos y humanos, políticos y servicios de terceros con implicaciones de seguridad.
La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.



Con tecnología de Auditat

La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad. Debido a la creciente interconexión de los sistemas de información, la evaluación de riesgos debe incluir la consideración de los posibles daños que pueden proceder de otros o ser causados por terceras personas.

Todos los sistemas sujetos a esta Política deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos contemplará asimismo los requisitos del artículo 32 del Reglamento (UE) 2016/679, de modo que un único proceso de gestión del riesgo sustente tanto las medidas exigidas por el Esquema Nacional de Seguridad como las medidas técnicas y organizativas apropiadas que impone la normativa de protección de datos personales.

El detalle de la metodología, el alcance, los resultados, la periodicidad de revisión y los supuestos que obligan a repetir el análisis constan en el Análisis de riesgos; el tratamiento acordado para los riesgos que lo requieren consta en el Plan de tratamiento de riesgos.

# 22. REQUISITOS MÍNIMOS DE SEGURIDAD

Conforme al artículo 12.6 del Real Decreto 311/2022, esta Política se establece de acuerdo con los principios básicos del capítulo II —recogidos en el apartado *Principios básicos*— y se desarrolla aplicando los quince requisitos mínimos que se enuncian a continuación, cada uno de ellos regulado con mayor detalle en los artículos 13 a 27 de la citada norma.

Cada requisito se formula aquí como directriz de obligado cumplimiento y se concreta en el cuerpo normativo de segundo y tercer nivel descrito en el apartado *Pirámide normativa*, cuya relación completa consta en el Inventario y mapa de procedimientos de seguridad.

## 22.1. a) Organización e implantación del proceso de seguridad

La seguridad de la información es un proceso permanente y organizado, no un conjunto de actuaciones aisladas. Erain Elkarteko Osasun Mentala Sociedad Cooperativa mantiene una estructura de seguridad con responsabilidades diferenciadas, un Comité de Seguridad de la Información que coordina el proceso y un cuerpo normativo que lo soporta, comprometiendo a todos los miembros de la organización en su cumplimiento. La estructura, la composición y las relaciones de esa organización se detallan en los apartados *Estructura y composición del Comité de Seguridad de la Información* y *Funciones y responsabilidades*, y se desarrollan en la Normativa de seguridad.

## 22.2. b) Análisis y gestión de los riesgos

Toda decisión en materia de seguridad se fundamenta en el análisis y la gestión de los riesgos, como proceso continuo y permanentemente actualizado. El análisis identifica las amenazas y las vulnerabilidades sobre los activos del alcance, evalúa el riesgo inherente y el residual, y determina las medidas de seguridad a implantar, que serán proporcionales al riesgo y estarán justificadas. Este requisito se desarrolla en el apartado *Gestión de riesgos* y se materializa en el Análisis de riesgos, el Plan de tratamiento de riesgos, la Categorización del sistema y la Declaración de aplicabilidad.

## 22.3. c) Gestión de personal



Con tecnología de Auditat

Todo el personal, propio o ajeno, que acceda a la información o a los servicios del alcance conoce sus deberes y obligaciones en materia de seguridad antes de asumirlos, así como las consecuencias previstas para su incumplimiento. La organización formaliza los compromisos de confidencialidad, define las actuaciones aplicables en las incorporaciones, los cambios de puesto y las bajas, y retira los permisos y los activos entregados cuando la relación finaliza. Este requisito se desarrolla en el Procedimiento de gestión del personal, en el compromiso de confidencialidad y en el Manual de seguridad para usuarios.

## 22.4. d) Profesionalidad

La seguridad de los sistemas se atiende, revisa y audita por personal con la cualificación, la dedicación y la formación suficientes. Erain Elkarteko Osasun Mentala Sociedad Cooperativa determina los requisitos de formación y capacitación de las personas con responsabilidad en el uso, la operación o la administración de los sistemas, exige que dicha formación sea previa a la asunción de la responsabilidad y mantiene un programa continuo de formación y concienciación para toda la organización. Este requisito se desarrolla en el apartado *Obligaciones del personal (usuarios)*, en el Plan de formación y concienciación y en la Guía de buenas prácticas de contraseñas y credenciales.

## 22.5. e) Autorización y control de los accesos

El acceso a la información y a los servicios se limita a los usuarios, procesos, dispositivos y sistemas expresamente autorizados, previa identificación y autenticación, y queda restringido a las funciones permitidas. Las autorizaciones se conceden mediante un procedimiento formal, se documentan y se revisan periódicamente para retirar las que hayan dejado de ser necesarias. Este requisito se desarrolla en el apartado *Acceso a la información*, en el Procedimiento de gestión de usuarios y derechos de acceso, en la Normativa de control de acceso y autenticación y en el Procedimiento de autorización.

## 22.6. f) Protección de las instalaciones

Los sistemas y los activos de información se emplazan en áreas seguras, dotadas de control de acceso físico proporcionado a su criticidad y protegidas frente a amenazas físicas y ambientales. Se controla y registra la entrada y la salida de personas y de equipamiento esencial, y se mantienen los elementos auxiliares de los que depende la operación. Este requisito se desarrolla en el Procedimiento de protección de instalaciones e infraestructuras y en la Normativa de protección de instalaciones e infraestructuras.

## 22.7. g) Adquisición de productos de seguridad y contratación de servicios de seguridad

En la adquisición de productos de seguridad y en la contratación de servicios de seguridad se valoran de forma objetiva las funcionalidades de seguridad requeridas, atendiendo con carácter preferente a los productos y servicios que cuenten con certificación reconocida, en los términos del artículo 19 del Real Decreto 311/2022 y de las instrucciones técnicas y guías CCN-STIC aplicables. Los requisitos de seguridad y su financiación se identifican e incorporan a la planificación y a los pliegos o solicitudes de oferta desde el inicio. Este requisito se desarrolla en el Procedimiento de adquisición de componentes y se evidencia en el Inventario de componentes certificados.

## 22.8. h) Mínimo privilegio

Los sistemas se diseñan y operan concediendo únicamente los privilegios estrictamente necesarios para cumplir la finalidad prevista, eliminando o desactivando las funciones, los servicios, los puertos y las cuentas que no resulten precisos, y separando las funciones incompatibles para que ninguna persona concentre por



Con tecnología de Auditat

sí sola la capacidad de comprometer el sistema. Este requisito se desarrolla en el Procedimiento de gestión de usuarios y derechos de acceso, el Procedimiento de segregación de funciones, la matriz de roles y perfiles y la Guía de bastionado de sistemas.

## 22.9. i) Integridad y actualización del sistema

Toda incorporación o modificación de un elemento físico o lógico del sistema requiere autorización formal previa. Se conoce en todo momento el estado de seguridad de los componentes respecto a las especificaciones del fabricante y a las vulnerabilidades y actualizaciones que les afecten, reaccionando con diligencia en función del riesgo. Este requisito se desarrolla en el Procedimiento de configuración y mantenimiento, el Procedimiento de gestión de cambios, la Guía de bastionado de sistemas y el Procedimiento de protección de las aplicaciones informáticas.

## 22.10. j) Protección de la información almacenada y en tránsito

La información recibe una protección equivalente en todos los estados de su ciclo de vida y en todos los entornos por los que transita, con atención específica a los equipos portátiles, los soportes extraíbles, los dispositivos periféricos, los entornos fuera de las instalaciones y las comunicaciones sobre redes no controladas. Se aplican los mecanismos de cifrado, de firma y de sellado de tiempo que correspondan al nivel de la información, y se garantiza su recuperación mediante copias de respaldo verificadas. Este requisito se desarrolla en el Procedimiento de protección de los soportes de información, el Procedimiento de protección de las comunicaciones, el Procedimiento de copias de seguridad y restauración, el Procedimiento de gestión de claves criptográficas y la Tabla de controles criptográficos.

## 22.11. k) Prevención ante otros sistemas de información interconectados

Cuando el sistema se conecta con otros sistemas o redes ajenos al alcance, se analiza previamente el riesgo de la interconexión, se protege el perímetro con los mecanismos adecuados, se limita el flujo de información al estrictamente necesario y se vigila el punto de unión. La conexión se formaliza documentando las condiciones de seguridad exigidas a la otra parte. Este requisito se desarrolla en el Procedimiento de interconexión de sistemas, el Procedimiento de gestión de servicios externos y proveedores, el Procedimiento de protección de servicios en la nube y el Documento de arquitectura de seguridad.

## 22.12. l) Registro de la actividad y detección de código dañino

Se registran las actividades de los usuarios en los términos del artículo 24 del Real Decreto 311/2022, conservando la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, y permitiendo identificar en cada momento a quién se atribuye dicha actividad. Los registros se protegen frente a manipulación y se revisan periódicamente. Asimismo, se implantan y mantienen actualizados mecanismos de prevención y detección de código dañino, con la correspondiente capacidad de reacción. Estos registros se realizan con las garantías que impone la normativa de protección de datos personales y respetando los derechos de las personas trabajadoras. Este requisito se desarrolla en el Procedimiento de gestión de incidentes y registro de actividad, el Procedimiento de monitorización del sistema, el Registro de revisiones de los registros de actividad y el Procedimiento de protección de los servicios.

## 22.13. m) Incidentes de seguridad



Con tecnología de Auditat

Se dispone de mecanismos para detectar, clasificar, registrar, responder y cerrar los incidentes de seguridad, con designación de un punto de contacto para las comunicaciones internas y externas y con los protocolos de intercambio de información con los equipos de respuesta a incidentes competentes. Se registran las actuaciones realizadas y se extraen las lecciones aprendidas para evitar su repetición. Cuando el incidente afecte a datos personales, se activa además el régimen de notificación previsto en el apartado *Notificación de brechas de datos personales*. Este requisito se desarrolla en el apartado *Gestión de incidentes de seguridad*, en el Procedimiento de gestión de incidentes y registro de actividad y en el Registro de incidentes de seguridad.

### 22.14. n) Continuidad de la actividad

Erain Elkarteko Osasun Mentala Sociedad Cooperativa identifica los servicios críticos y los requisitos de disponibilidad que les son exigibles, y dispone de las previsiones necesarias para mantener o restablecer su prestación ante una interrupción, incluidas las copias de respaldo. Este requisito se desarrolla en el apartado *Recuperación* y en el procedimiento de análisis de impacto que corresponda a la disponibilidad exigida a cada servicio.

### 22.15. ñ) Mejora continua del proceso de seguridad

El proceso integral de seguridad se revisa y actualiza de forma continua, aplicando el criterio de mejora continua y los criterios y métodos reconocidos en la práctica nacional e internacional. A tal fin, Erain Elkarteko Osasun Mentala Sociedad Cooperativa evalúa periódicamente el estado de la seguridad mediante auditorías, autoevaluaciones e indicadores, analiza los resultados y las causas de las desviaciones, y traslada las conclusiones a planes de mejora cuyo seguimiento corresponde al Comité de Seguridad de la Información. Este requisito se materializa en el Informe de auditoría ENS, en el sistema de métricas del Procedimiento de monitorización del sistema y en el Plan de tratamiento de riesgos.

## 23. PROPORCIONALIDAD EN LA EXIGENCIA DE LOS REQUISITOS MÍNIMOS

Conforme al artículo 12.7 del Real Decreto 311/2022, los requisitos mínimos enumerados en el apartado anterior se exigen en proporción a los riesgos identificados en cada sistema, de acuerdo con lo dispuesto en el artículo 28, pudiendo obviarse alguno de ellos en sistemas sin riesgos significativos.

La determinación de qué medidas resultan exigibles a este sistema, con qué nivel y con qué refuerzos, se realiza a partir de la categoría del sistema y de la valoración de sus dimensiones de seguridad, y se documenta de forma trazable en la Categorización del sistema, el Análisis de riesgos y la Declaración de aplicabilidad.

Toda medida del Anexo II que se declare no aplicable consta motivada en la Declaración de aplicabilidad, firmada por la persona Responsable de Seguridad. La no aplicabilidad de una medida no exime del cumplimiento de la directriz general recogida en esta Política, cuyo alcance es el conjunto de la organización.

## 24. PIRÁMIDE NORMATIVA

El cuerpo normativo sobre seguridad de la información será de obligado cumplimiento y se desarrollará en tres niveles según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un



Con tecnología de Auditat

determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de documentación de seguridad son los siguientes:

a. **Primer nivel normativo**: el presente documento que da soporte a la política de seguridad de la información.
b. **Segundo nivel normativo**: las políticas específicas de Seguridad de la Información y Normas de Seguridad TIC (Normas STIC).

Las Políticas Específicas desarrollan con un mayor grado de detalle la Política dentro de un ámbito determinado.

Las Normas dan respuesta, sin entrar en detalles de implementación ni tecnológicos, a qué se puede hacer y qué no en relación a un cierto aspecto, desde el punto de vista de la seguridad, tales como: qué se considera un uso apropiado o inapropiado, las consecuencias derivadas del incumplimiento, entre otros aspectos.

Las políticas y normas serán aprobadas por el Comité de Seguridad de la información de la entidad.

c. **Tercer nivel normativo**: los Procedimientos e Instrucciones Técnicas STIC.

Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la organización y los procesos internos y responsabilidades en ella establecidos.

Los Procedimientos e Instrucciones Técnicas STIC serán aprobados por el Comité de Seguridad de la información de la entidad.

Adicionalmente, la documentación de seguridad podrá contar, bajo criterio de la persona Responsable de Seguridad, con documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, entre otros aspectos.

El Responsable de Seguridad se responsabilizará de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos de acceso a la misma.

La documentación de seguridad de segundo y tercer nivel se revisa con ocasión de la revisión de esta Política, con la periodicidad fijada en el apartado *Aprobación, vigencia y revisión*. La revisión comprueba, documento a documento, que su contenido sigue correspondiéndose con el sistema, la organización y el marco normativo vigentes: los documentos que no requieren cambios se ratifican como vigentes y los demás se actualizan y se aprueban de nuevo por el órgano que corresponde a su nivel. El resultado de la revisión, incluida la relación de documentos ratificados sin cambios, consta en el acta de la sesión. Con independencia de ese ciclo, cada documento se actualiza cuando cambian las circunstancias que regula.

El Comité de Seguridad de la información de la organización establece los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo en todo el ámbito de aplicación de la PSI.

La documentación de seguridad se custodia en un repositorio o gestor documental único, regido por una norma interna que regula su elaboración, aprobación, control de versiones, conservación, estructura y acceso, de modo que en todo momento sea identificable la versión vigente de cada documento y quién está autorizado a consultarla.

El Responsable de Seguridad supervisa el proceso de identificación y actualización de la normativa legal, reglamentaria y contractual aplicable descrito en el apartado *Marco normativo y referencias*, y asegura que el cuerpo documental se adapte a los cambios normativos, previa aprobación de los órganos competentes.

## 25. OBLIGACIONES DEL PERSONAL (USUARIOS)



Con tecnología de Auditat

Todo el personal de la entidad tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de seguridad desarrollada a partir de ella, siendo responsabilidad del Comité o del Responsable de Seguridad disponer de los medios necesarios para que la información llegue a los afectados. Su incumplimiento se rige por el régimen disciplinario previsto en la Normativa de seguridad.
Todo el personal de la entidad debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como que ellos mismos son una pieza esencial para el mantenimiento y mejora de la seguridad.
Se establecerá un programa de concienciación continua que alcance a todo el personal de la entidad y, de forma específica, a los nuevos miembros de la organización con ocasión de su incorporación.
Todo el personal recibirá al menos una acción de concienciación en materia de seguridad de la información **con periodicidad anual**. Su programación consta en el Plan de formación y concienciación, y cada acción impartida queda registrada, con indicación de la fecha, el contenido y las personas asistentes, en el Registro de formación y concienciación, que constituye la evidencia de su realización.
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 como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

## 26. RELACIÓN CON TERCERAS PARTES

Cuando Erain Elkarteko Osasun Mentala Sociedad Cooperativa presta servicios a otros organismos o maneja información de éstos, el responsable de esa relación les hace partícipes de esta Política de Seguridad y de las normas e instrucciones derivadas.
Erain Elkarteko Osasun Mentala Sociedad Cooperativa establece canales de comunicación y coordinación entre los respectivos Comités o Responsables de Seguridad de la Información, así como procedimientos de actuación para la reacción ante incidentes de seguridad.
Asimismo, cuando se utilizan servicios de terceros o se cede información a terceros, el responsable de esa relación les hace igualmente partícipes de esta Política y de la normativa e instrucciones de seguridad que atañen a dichos servicios o información. La tercera parte queda sujeta a las obligaciones y medidas de seguridad establecidas en dicha normativa e instrucciones, pudiendo desarrollar sus propios procedimientos operativos para satisfacerlas. Se establecen procedimientos específicos de prevención, detección, reporte y resolución de incidencias, y se exige que el personal de terceros con acceso a la información o a los servicios esté concienciado en materia de seguridad en la medida que corresponda al riesgo de la relación.
Las condiciones de seguridad exigibles a cada tercero —requisitos contractuales y acuerdos de nivel de servicio, supervisión de la prestación, garantías sobre la cadena de suministro y acreditación de la devolución o destrucción de la información a la finalización del contrato— se establecen en proporción al riesgo que cada relación introduce en el sistema y a la criticidad de la información y los servicios afectados.
Cuando algún aspecto de esta Política no puede ser satisfecho por una tercera parte, el Responsable de Seguridad emite un informe que precisa los riesgos en que se incurre y la forma de tratarlos, y su aprobación es requisito previo para continuar.

## 27. ANEXOS



Con tecnología de Auditat

Los siguientes documentos se incorporan a esta Política como anexos, forman parte del instrumento aprobado por el órgano competente y recogen la información nominal y de detalle que, por su naturaleza cambiante, no se reproduce en el cuerpo de la Política:

| Anexo | Documento | Contenido |
|---|---|---|
| **ANEXO I** | Acuerdo de nombramiento de los roles de seguridad | Designación por el órgano de gobierno de los roles de seguridad y, en su caso, de los Administradores, con su ámbito y dependencia |
| **ANEXO II** | Acta de constitución del Comité de Seguridad | Constitución del Comité y aceptación individual de los roles de seguridad |
| **ANEXO III** | Registro de nombramientos y ceses de roles ENS | Registro histórico de los roles de seguridad, de los miembros del Comité y de los Administradores y sus delegados: nombre, cargo, ámbito, fecha de inicio, fecha de fin, motivo del cese, referencia al acta y, para los Administradores, dependencia funcional |
| **ANEXO IV** | Acta de Cese y Nueva Designación | Formalización de los ceses y de las sustituciones en los roles de seguridad |
| **ANEXO V** | Actas de reunión del Comité de Seguridad | Evidencia del funcionamiento del Comité y de los acuerdos adoptados |
| **ANEXO VI** | Plan de formación y concienciación | Programa anual de formación y concienciación; cada acción impartida se documenta en el Registro de formación y concienciación |

La modificación de un anexo no requiere una nueva aprobación de la Política, siempre que no altere las directrices establecidas en ella. Los cambios en los anexos se documentan en el propio anexo y se ponen en conocimiento del Comité de Seguridad de la Información.

## 28. REFERENCIAS CRUZADAS

Esta Política constituye el primer nivel normativo. Se desarrolla y se apoya en los siguientes documentos del sistema, cuya relación completa y actualizada consta en el Inventario y mapa de procedimientos de seguridad:

- **Segundo nivel normativo**: Normativa de seguridad y normativas específicas por ámbito.
- **Categorización y aplicabilidad**: Categorización del sistema y Declaración de aplicabilidad.
- **Gestión del riesgo**: Análisis de riesgos, Plan de tratamiento de riesgos, Acta de aceptación del riesgo residual y Acta de aprobación del análisis de riesgos por el Comité de Seguridad.
- **Alcance y activos**: Inventario de activos y Documento de arquitectura de seguridad.
- **Marco legal**: Registro de legislación y guías CCN-STIC.
- **Verificación**: Informe de auditoría ENS y sistema de métricas del Procedimiento de monitorización del sistema.



Con tecnología de Auditat