Marco Organizativo

# Política de Seguridad

| | |
|---|---|
| Título | Org 1. Marco organizativo **POLÍTICA SEGURIDAD** |
| Clasificación información | Pública |
| Aprobada por | Comité de Seguridad |

**Gestión de versiones**

| Versión | Fecha | Descripción |
|---|---|---|
| 1 | 22/05/2026 | Versión inicial |

**INDICE**

1. INTRODUCCIÓN 3

2. MISIÓN Y OBJETIVOS DE LA POLÍTICA 4

3. MARCO NORMATIVO 5

4. ROLES Y FUNCIONES DE SEGURIDAD 6

5. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN 8

6.DATOS DE CARÁCTER PERSONAL 9

7. GESTIÓN DE RIESGOS 9

8.GESTIÓN DEL PERSONAL 9

9.PROFESIONALIDAD 10

10.AUTORIZACIÓN Y CONTROL DE ACCESOS 10

11.PROTECCIÓN DE LAS INSTALACIONES 10

12.ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD 10

13.MINIMO PRIVILEGIO 11

14.INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA 11

15.PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO 11

16.PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS 11

17.REGISTRO DE ACTIVIDAD 12

18.INCIDENTES DE SEGURIDAD 12

19.CONTINUIDAD DE LA ACTIVIDAD 12

20.MEJORA CONTINUA DEL PROCESO DE SEGURIDAD 12

21.RELACIONES CON TERCEROS 12

# 1. Introducción

La presente Política de Seguridad de la Información, se aplicará a todos los activos de información.

GRUPO EMPRESAS AREA
Dirección C/ Ruiz Zorrilla, 1 Castellón

Se establece las directrices y principios bajo los cuales nuestra empresa se compromete a proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, cumpliendo con los requisitos establecidos en el Esquema Nacional de Seguridad (ENS) para garantizar la seguridad de los servicios y la protección de los datos de nuestros clientes.

La información constituye un activo de primer orden para las organizaciones actuales, ya que resulta imprescindible para la prestación de los servicios que ofrecen a terceras partes. Por su parte, las tecnologías de la información y las comunicaciones (TIC) se han hecho imprescindibles, ya que contribuyen de forma muy eficaz al tratamiento de esa información.

Sin embargo, las mejoras que aportan las TIC al tratamiento de la información vienen acompañadas de nuevos riesgos. Por esa razón es necesario introducir medidas específicas para proteger tanto la información, como los servicios que dependen de ella.

La seguridad de la información tiene como objetivo proteger la información y los servicios, reduciendo los riesgos a los que están sometidos hasta un nivel que resulte aceptable.

## 2. Misión y objetivos de la Política

GRUPO EMPRESAS AREA ha establecido un alineamiento con la gestión de la seguridad de la información, según lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, reconociendo como activos estratégicos la información y los sistemas que la soportan. GRUPO EMPRESAS AREA ha establecido un alineamiento con la gestión de la seguridad de la información, según lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, reconociendo como activos estratégicos la información y los sistemas que la soportan.

Uno de los objetivos fundamentales de la implantación de esta Política de Seguridad de la Información es establecer las bases sobre las que tanto empleados internos, como otras partes interesadas, puedan acceder a los servicios ofrecidos por *la organización*, en un entorno seguro y de confianza.

La Política de Seguridad de la Información define el marco global para la gestión de la seguridad de la información, protegiendo todos los activos de información y garantizando la continuidad en el funcionamiento de los sistemas.

Se pretende de esta forma minimizar los riesgos derivados de un posible fallo en la gestión de la seguridad de la información, y asegurar el cumplimiento de los objetivos ante un hipotético incidente de seguridad de la información.

Para ello, se establecen los siguientes objetivos generales en materia de seguridad de la información:

1) Contribuir desde la gestión de la seguridad, al cumplimiento de la misión y objetivos establecidos.

2) Disponer de las medidas de control necesarias para garantizar el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal.

3) Asegurar la accesibilidad, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información.

4) Asegurar la prestación continuada de los servicios, tanto de forma preventiva, como de forma reactiva ante los incidentes de seguridad.

5) Proteger los activos de información y la tecnología que los soporta frente a cualquier amenaza, intencionada o accidental, interna o externa.

Esta Política de Seguridad de la Información asegura un compromiso continuo y manifiesto de GRUPO EMPRESAS AREA, para la difusión y consolidación de la cultura de la seguridad.

# 3. Marco normativo

Sin carácter exhaustivo, la legislación y normativa en materia de seguridad de la información que debe servir de referencia es la siguiente:

a) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

b) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

c) Ley 9/1968, de 5 de abril, sobre secretos oficiales.

d) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

e) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

f) Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

g) 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.

h) Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

i) 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.

j) 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.

k) Norma UNE-EN ISO/IEC 27001:2022.

l) 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 (en adelante RGPD).

m) Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos de carácter personal y sus normas de desarrollo.

n) Ley 10/2021, de 9 de julio, de trabajo a distancia.

# 4. Roles y funciones de seguridad

Se designa a determinados órganos y cargos, con las funciones que se señalan para cada uno en este apartado:

Comité de Gestión de la Seguridad de la Información, Responsables de la Información, Responsables del Servicio, Responsable del Sistema de Información, Responsables de Seguridad y, en caso de que sea pertinente, Responsables o Administradores de Seguridad Delegados.

- El Comité de Gestión de la Seguridad de la Información es el organismo que centraliza la gestión de la seguridad de la información.

- El Responsable de la Información será la persona con competencia suficiente para decidir sobre la finalidad, contenido y uso de dicha información y determinará, dentro del marco establecido en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, los requisitos de seguridad de la información tratada. A tal efecto:

  i. Determinará los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información.

  ii. Realizará, junto a los Responsables del Servicio y del Responsable de Seguridad, los preceptivos análisis de riesgos, y seleccionarán las salvaguardas que se han de implantar.

  iii. Aceptará los riesgos residuales respecto de la información calculados en el análisis de riesgos.

  iv. Realizará el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad.

d) El Responsable del Servicio será la persona con competencia suficiente para decidir sobre la finalidad y prestación de dicho servicio y determinará dentro del marco establecido en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad los requisitos de seguridad de los servicios prestados. A tal efecto:

  i. Realizará, junto a los Responsables de la Información y de Seguridad, los preceptivos análisis de riesgos, y seleccionarán las salvaguardas que se han de implantar.

  ii. Aceptará los riesgos residuales respecto de la información calculados en el análisis de riesgos.

  iii. Realizará el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad.

  iv. Suspenderá, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

e) El Responsable de Seguridad será la persona determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Tendrá las siguientes funciones:

  i. Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.

  ii. Promover la formación y concienciación en materia de seguridad de la información.

  iii. Proponer a los Responsable del Servicio y de la Información, la determinación de los niveles de seguridad en cada dimensión de seguridad siempre que se le solicite.

iv. Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

v. Realizar el seguimiento y control del estado de seguridad de los sistemas de información.

vi. Proponer al Comité de Gestión de la Seguridad de la Información las normas de seguridad y los procedimientos de seguridad, además de la aprobación de cambios y otros requisitos del sistema.

vii. Gestionar las revisiones externas o internas del sistema.

viii. Gestionar los procesos de certificación

f) El Responsable del Sistema de Información será la persona encargada de desarrollar la forma concreta de implementar la seguridad en el sistema, y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad. Tendrá las siguientes funciones:

i. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

ii. Definir la topología y la gestión del Sistema de Información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

iii. 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.

iv. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.

v. 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.

vi. Aprobar los cambios en la configuración vigente del Sistema de Información.

vii. Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.

Los roles citados, son designados inicialmente, y su renovación deberá contar con la aprobación del Comité de Gestión de la Seguridad de la Información.

# 5. Estructuración de la documentación

Se establece un marco normativo en materia de seguridad de la información estructurado por diferentes niveles de forma que los objetivos marcados por el presente documento tengan un desarrollo específico.

La política de seguridad estructurará su marco normativo en los siguientes niveles:

a. La presente Política de Seguridad de la Información, que establece los requisitos y criterios de protección de carácter global.

b. Las normas de seguridad que definen qué hay que proteger y los requisitos de seguridad deseados.

i. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información.

ii. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política.

iii. Las propone el Responsable de Seguridad y las aprueba el Comité de Gestión de la Seguridad de la Información.

c. Los procedimientos de seguridad en los que describirá de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento.

i. Son documentos que especifican cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

ii. Su aprobación dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado.

Además, se podrán establecer guías con recomendaciones y buenas prácticas.

En la medida de lo posible, toda esta documentación será gestionada según establece el procedimiento vigente de Control de documentos, que tendrá como objetivo establecer los criterios para el control de la documentación utilizada en el Sistema de Gestión de la Seguridad de la Información, y que se extiende a toda la documentación que da soporte al cumplimiento del Esquema Nacional de Seguridad.

## 6.Datos de carácter personal

Cuando se maneje datos de carácter personal, le será de aplicación lo dispuesto en la Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo, sin perjuicio de los requisitos establecidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal.

## 7. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos.

Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

1. al menos una vez al año (mediante revisión y aprobación formal).
2. cuando cambie la información manejada.
3. cuando cambien los servicios prestados.
4. cuando ocurra un incidente crítico de seguridad.

Las contramedidas medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos identificados

## 8.Gestión del personal

Todo el personal con responsabilidad en el uso, operación, o administración de sistemas de tecnologías de la información y las comunicaciones tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad derivada, independientemente del tipo de relación jurídica que les vincule con la empresa.

Las actuaciones del personal serán supervisadas para verificar que se siguen los procedimientos establecidos.

Todas las personas recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

La Política de Seguridad estará accesible para todo el personal que preste sus servicios en los órganos y entidades a que se refiere el punto relativo al 'Alcance'.

Con el objetivo de fomentar la 'Cultura de la seguridad', el Comité de Gestión de la Seguridad de la Información promoverá un programa de concienciación continúa para formar a todo el personal.

Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe 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 determinada actividad.

El incumplimiento de la Política de Seguridad y su normativa de desarrollo dará lugar al establecimiento de medidas preventivas y correctivas encaminadas a salvaguardar y proteger

los sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria.

## 9.Profesionalidad

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidentes y desmantelamiento.

El personal designado recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios.

## 10.Autorización y control de accesos

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

## 11.Protección de las instalaciones

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

## 12.Adquisición de productos de seguridad

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados, se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada.

Para la contratación de servicios de seguridad, si fueran necesarios, se estará a lo dispuesto en los apartados anteriores y en el artículo “Relaciones con terceros” de la presente Política.

## 13.Minimo privilegio

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

a) El sistema proporcionará la mínima funcionalidad requerida para el alcance de los objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, 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 no sean de interés, las que sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) 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.

## 14.Integridad y actualización del sistema

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

## 15.Protección de la información almacenada y en tránsito

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, smartphones, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos.

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

## 16.Prevención ante otros sistemas de información interconectados

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 32 del Anexo II, de la Ley 9/2014 de 9 de mayo, General de Telecomunicaciones.

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

## 17.Registro de actividad

Con la finalidad exclusiva de lograr el cumplimiento del objeto de la presente Política, 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, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

## 18.Incidentes de seguridad

Se establecerá un sistema de detección y reacción frente a código dañino.

Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.

Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

## 19.Continuidad de la actividad

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

## 20.Mejora continua del proceso de seguridad

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 gestión de las tecnologías de la información.

## 21.Relaciones con terceros

Cuando se preste servicios o ceda información a terceras partes, se les hará partícipe de esta Política de Seguridad de la Información y de las normas e instrucciones derivadas.

Asimismo, cuando se utilice servicios de terceros, o ceda información a terceros, se les hará igualmente partícipe de esta Política de Seguridad de la Información y de la normativa e instrucciones de seguridad que ataña a dichos servicios o información.

Si la empresa necesitara servicios de seguridad de terceros, exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados, y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Los terceros quedarán sujetos a las obligaciones y medidas de seguridad establecidas en dicha normativa e instrucciones, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de detección y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad de la información, al menos al mismo nivel que el establecido en esta Política de Seguridad de la Información.

En concreto, los terceros deberán garantizar el cumplimiento de la Política de Seguridad de la Información basadas en estándares auditables que permitan verificar el cumplimiento de estas políticas. Asimismo, se garantizará mediante auditoría o certificado de destrucción/borrado, que el tercero cancela y elimina los daos pertenecientes a la finalización del contrato.

Cuando algún aspecto de la Política de la Seguridad de la Información no pueda ser satisfecho por una tercera parte, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Responsable de la Información y de los Servicios afectados, antes de seguir adelante.