



Política de Seguridad

Política de Seguridad de la información

Clasificación: Documento interno



Índice

Introducción.....	3
Objetivos	3
Alcance	3
Actividad.....	4
Organización y responsabilidades.....	5
Responsable de Seguridad de la Información	5
Responsable de la información y servicios	5
Responsable del sistema de información.....	6
Comité de seguridad corporativo	7
Designación.....	8
Estructura documental de la Seguridad de la Información	8
Clasificación de la información.....	9
Aplicación de la política	9
Formación y concienciación	10
Auditoría	10
Vigencia.....	10
Obligaciones del Personal.....	10
Marco legal.....	11

Historial de versiones

Fecha	Responsable	Cambios
Noviembre 2025 – v0.1	dooingIT	Versión inicial
Enero 2026 – V1.0	RSI	Versión final

Introducción

La presente Política de Seguridad de la Información se desarrolla para dar cumplimiento a los requisitos del Esquema Nacional de Seguridad y la norma ISO/IEC 27001.

La organización está compuesta por tres empresas: **Sinergia**, **Fish & Food Technology**, y **Raxia Formación** (en adelante, **Grupo Sinergia**).

Esta política es **corporativa** y aplica a todas las empresas del Grupo Sinergia, así como a todo el personal interno y externo que acceda a información o activos del grupo.

El **Grupo Sinergia** manifiesta su compromiso con la mejora continua de la seguridad de la información, la protección de los activos críticos y la gestión adecuada de los riesgos, contribuyendo a la continuidad del negocio y a la consolidación de una cultura de seguridad.

Objetivos

Grupo Sinergia depende de los sistemas TIC (Tecnologías de la Información y Comunicaciones) para alcanzar sus objetivos, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados.

Esta Política persigue la implantación y operatividad continuada de normativas y procedimientos destinados a preservar los cinco principios básicos de la seguridad de la información en **Grupo Sinergia** según el Esquema Nacional de Seguridad:

- **Confidencialidad:** garantizar que la misma será accesible sólo por recursos autorizados.
- **Disponibilidad:** garantizar que la misma estará disponible para su uso y acceso por los actores autorizados cuando lo soliciten.
- **Integridad:** garantizar que la misma será modificada o destruida sólo por actores autorizados.
- **Autenticidad:** propiedad que garantiza que el usuario que envía o recibe información es quien dice ser.
- **Trazabilidad:** garantizar que las acciones de los usuarios sobre la información o sistemas de información quedan adecuadamente registradas.

Alcance

Esta Política es de aplicación a todos los activos, procesos, sistemas y personas que traten información del **Grupo Sinergia**, incluyendo a todo el personal propio y externo con acceso a la información corporativa.

La Política de Seguridad se pone a disposición de todo el personal en la Intranet corporativa y se comunica mediante los canales internos establecidos (correo electrónico con enlace a la documentación)

Actividad

Sinerxia es una compañía dedicada al **desarrollo de actividades profesionales, científicas y técnicas, implementación y optimización de soluciones tecnológicas, digitalización, relaciones con instituciones públicas y privadas, toda clase de estudios técnicos y formaciones.**

Los sectores de la economía azul, agroalimentación, y la industria alimentaria en toda su cadena de valor, son potencialmente importantes para la actividad de Sinerxia.

FFTech se especializa en el desarrollo de I+D+i, de tecnologías y servicios para los sectores de la economía azul, toda la cadena de valor de la alimentación, el sector industrial y en el sector de defensa.

Raxia se especializa en formación y proyectos de empleabilidad y relevo generacional.

En concreto, en lo que se refiere al marco de aplicación de la presente política, Grupo Sinerxia se encarga de:

SINERXIA

- Estudios técnicos y científicos en el sector pesquero
- Observación pesquera en diferentes caladeros pesqueros del mundo y diferentes artes de pesca.
- Desarrollo de estrategias pesqueras para las administraciones.
- Desarrollo de estrategias en el ámbito agroalimentario y rural.
- Promoción de productos y servicios de empresas y administraciones públicas.
- Prestación de servicios de comunicación y marketing.
- Formación en materia de pesca y agroalimentación, en toda su cadena de valor.
- Desarrollo de proyectos vinculados con convocatorias de las diferentes administraciones.
- Digitalización del sector pesquero.
- Servicio de búsqueda, tramitación y gestión de subvenciones y financiación para empresas.
- Colaboración y gestión de proyectos europeos e internacionales.

FFTech

- Digitalización del sector pesquero y naval.
- Digitalización del sector Defensa.
- Desarrollo de tecnología(productos) para la pesca.

- Digitalización de la industria.
- Desarrollo de tecnologías para sectores naval, industria y defensa.
- Desarrollo de producto tecnológico para sectores naval y defensa.
- Desarrollo de sistemas de descarbonización para sectores de la economía azul.
- Aplicación de la IA para el desarrollo de nuevas tecnologías.

RAXIA

- Formación en diferentes materias.
- Desarrollo de proyectos en el ámbito del relevo generacional y la empleabilidad.

Organización y responsabilidades

La política es de obligado cumplimiento para toda la organización.

Responsable de Seguridad de la Información

El responsable de velar por el cumplimiento de esta política en toda la organización es el Responsable de Seguridad de la Información. Se ocupa, fundamentalmente, de las siguientes tareas:

- Asesorar a los responsables correspondientes en las tareas de identificación de la información y servicios, así como en la evaluación de los niveles de seguridad requeridos para la información y el servicio.
- Realizar la categorización del sistema de información.
- Elaborar la política de seguridad.
- Realizar el análisis de riesgos sobre los sistemas de información.
- Elaborar el documento de aplicabilidad del Esquema Nacional de Seguridad.
- Promover el establecimiento de las medidas de seguridad necesarias en el sistema de información.
- Mantenimiento de la seguridad de la información que se maneja en la organización y de los servicios prestados por los sistemas de información, de acuerdo con lo establecido con los responsables de información y los distintos servicios.
- Promoción de la formación y concienciación en materia de seguridad de la información a los usuarios.

Responsable de la información y servicios

El responsable de la información tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección, así como de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

Asimismo, determina los requisitos de seguridad de la información tratada, y valora las consecuencias de un impacto negativo sobre la seguridad de la información.

Tiene la potestad de determinar los niveles de seguridad de los servicios de información prestados. Asimismo, valora las consecuencias de un impacto negativo sobre la seguridad de los servicios sobre los que sea responsable.

El resto de sus atribuciones se detalla a continuación:

- Identificar y valorar la información tratada por la organización relativa a las administraciones públicas.
- Identificar y valorar los servicios tecnológicos prestados a las administraciones públicas.

Responsable del sistema de información

Es el encargado de la operación del sistema de información organizativo en su conjunto, atendiendo a las medidas de seguridad determinadas por el Responsable de Seguridad.

Tiene las siguientes funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Implementación de las medidas técnicas de seguridad, indicadas por el Responsable de Seguridad.
- 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 de seguridad se integren adecuadamente en el marco general de seguridad.
- Administrador de Seguridad
- Forma parte del comité de seguridad.
- Reporta al comité los incidentes relativos a la seguridad del sistema y de las acciones de configuración, actualización o corrección.
- 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, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los procedimientos operativos de seguridad.

- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- Recopila información sobre el desempeño del sistema de información en materia de seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Comité de seguridad corporativo

El Gobierno de Seguridad de la Información en la organización recae en el Comité de Seguridad corporativo, que se encarga de formular las directrices y principios básicos de seguridad y de velar por el cumplimiento del presente documento. Está compuesto por:

- El responsable del sistema de información.
- El responsable de la información y servicios.
- El Responsable de Seguridad de la Información (RSI).

Las funciones del Comité de Seguridad son las siguientes:

- Divulgación de la Política y normativa de seguridad de la organización.
- Aprobación de la normativa de seguridad de la organización.
- Revisión anual de la Política de seguridad.
- Coordinar adquisiciones y desarrollos, decidiendo inversiones y controlando el gasto.
- Coordinar servicios para evitar disfunciones y maximizar el uso.
- Definir el riesgo aceptado por Grupo Sinerxia
- Aprobar el riesgo residual en la planificación de acciones de tratamiento del riesgo.
- Revisar la política de Seguridad de la Información y establecer, revisar y aprobar la Política de Seguridad de la Información_ ENS en Grupo Sinerxia
- Coordinar todas las funciones de seguridad de Grupo Sinerxia.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Velar por el alineamiento de las actividades de seguridad y los objetivos de Grupo Sinerxia
- Recaba de los responsables informes regulares del estado de seguridad de Grupo Sinerxia y de los posibles incidentes.
- Definir la asignación de los roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de tareas.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevándolo a la Dirección en aquellos casos en los que no tenga suficiente autoridad para decidir.

Todo usuario de los sistemas de información es responsable del uso adecuado que haga de los mismos y de cumplir con los controles y recomendaciones establecidas.

Designación

El Responsable de Seguridad de la Información es nombrado por la Dirección propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

Estructura documental de la Seguridad de la Información

La estructura documental del sistema de seguridad de la información se compone de los siguientes elementos:

- Declaración de aplicabilidad del Sistema de Información.
- Categorización de los Sistemas de Información.
- Inventario de activos del Sistema de Información.
- Metodología y análisis de Riesgos de Seguridad de la Información.
- Política de Seguridad de la Información.
- Plan de continuidad de negocio y su correspondiente BIA.
- Normativas de seguridad y otros documentos asociados.

El desarrollo de esta política está basado en la aplicación de los siguientes requisitos mínimos, establecidos de acuerdo a los principios básicos señalados por el Esquema Nacional de Seguridad y la norma ISO/IEC 27001:

- Organización e implantación del proceso de seguridad. Se recoge en este propio documento de **Política de Seguridad de la información**.
- Análisis y gestión de los riesgos. Desarrollado en el documento **"Metodología de Análisis de Riesgos"** y su propia herramienta.
- Gestión de personal. Se desarrolla dentro del documento **"Política de gestión de administración y RRHH"**.
- Profesionalidad.
- Autorización y control de los accesos, incluido dentro del documento **"Política de gestión de informática interna"**.
- Protección de las instalaciones, incluido dentro de la **"Normativa de seguridad"**
- Adquisición de productos de seguridad y contratación de servicios de seguridad, incluido dentro de la **"Gestión de proveedores"**
- Mínimo privilegio: Se desarrolla en el documento de política de **"Política de gestión de informática interna"**.

- Integridad y actualización del sistema: Se desarrolla en el documento de **"Política de gestión de informática interna"**.
- Protección de la información almacenada y en tránsito: Se desarrolla en el documento de **"Política de gestión de informática interna"**
- Prevención ante otros sistemas de información interconectados: Se desarrolla en el documento de **"Política de gestión de informática interna"**.
- Registro de la actividad y detección de código dañino: Se desarrolla en el documento de **"Política de gestión de informática interna"**.
- Incidentes de seguridad: El proceso relacionado con los incidentes de seguridad se recogen en el documento de **"Política de gestión de informática interna"**.
- Continuidad de la actividad: Se desarrolla en el documento de "Política de gestión de informática interna"
- Mejora continua del proceso de seguridad: En los varios comités de seguridad se repasan muchos de los puntos mencionados. Se analizan las necesidades del momento actual de la organización y se trabaja en la mejora continua de los procesos de seguridad que lo precisen.

La Política de Seguridad de la Información y Normativa de seguridad se encuentran publicadas en la Intranet de la organización. El resto de los documentos se encuentran almacenados por el Responsable de Seguridad de la Información, de forma que estén solamente accesibles por éste y el personal en quien delegue la gestión de la seguridad en el sistema de información.

Clasificación de la información

Se establecen tres categorías diferenciadas para catalogar la información en la organización, según su nivel de confidencialidad.

- **Confidencial:** Información a la que sólo determinadas personas o departamentos dentro de la organización deben tener acceso. Si se filtrara a terceras partes, podría tener consecuencias negativas para la organización.
- **Interna:** Información a la que sólo debe tener acceso el personal de la organización. Si se filtrara a terceras partes, podría tener consecuencias para la organización.
- **Pública:** Información sin ninguna restricción de acceso. Si se filtrara a terceras partes, no tendría consecuencias para la organización.

Aplicación de la política

Con el objetivo de aplicar los principios expuestos en esta Política, existe un conjunto de Normativas y Procedimientos que sirven de soporte para la implantación de las soluciones y procesos idóneos para satisfacer las necesidades de Negocio en relación con la Seguridad de la Información.

A nivel operativo, la organización dispone de sus propias normativas, procedimientos y guías de seguridad, que garanticen la integridad, confidencialidad y disponibilidad de la información.

Formación y concienciación

Con la finalidad de mejorar el conocimiento de la seguridad por parte de todos los recursos de **Grupo Sinergia**, se realizarán actividades de formación sobre Seguridad de la Información acordes con las respectivas áreas.

Asimismo, se realizarán campañas de concienciación sobre seguridad dirigidas a todo el personal y proveedores a través del medio que se considere más efectivo.

Auditoría

Los sistemas de información, de manera total o parcial se someterán periódicamente a auditorías internas y externas con la finalidad de verificar el correcto funcionamiento de la seguridad, determinando grados de cumplimiento y recomendando medidas correctoras, consiguiendo, así, una mejora continua. Estas auditorías se detallan en el documento **“Procedimiento de auditoría interna y revisión del SGSI”**.

Vigencia

La Política de Seguridad de la Información entra en vigor desde el mismo día de su publicación y se revisa anualmente obteniendo la correspondiente aprobación por la Dirección.

Del mismo modo, cualquier otro documento del cuerpo normativo será revisado también con periodicidad anual para asegurar que estos se adaptan y reflejan el estado actual y las necesidades de la organización.

Obligaciones del Personal

Todos los miembros de Grupo Sinergia tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establece un programa de concienciación continua para atender a todos los miembros de Grupo Sinergia y en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Marco legal

Asimismo, se citan a continuación los decretos a los cuales se adecúa la presente Política.

- **Real Decreto 311/2022**, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- **Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.
- **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