AECOC

SGSI

Política de Seguridad de la Información

-

2025

AECOC

Historial de versiones

Versión	Desarrollado por Fecha	Verificado por Fecha	Aprobado por Fecha	Comentarios
1.0	SEIDOR 05/10/2023	Responsable de SGSI 15/01/2024	Dirección 30/05/2024	Creación del Documento
1.1	Responsable de SGSI 15/07/2025	Responsable de SGSI 15/07/2025	Dirección 08/06/2025	Actualización del Documento
1.2	Responsable de SGSI 05/11/2025	Responsable de SGSI 05/11/2025	Dirección 14/11/2025	Actualización del Documento

Contenido

1. Información General

1.1. Objeto

La presente política tiene como objetivo establecer el compromiso de la Dirección de AECOC, representada por Director del Departamento de GS1 e IT, respecto a la seguridad de la información y la protección de activos de información necesarios para el desempeño de las funciones descritas en el alcance, permitiendo así la consecución de sus objetivos de negocio y estratégicos.

Este compromiso se materializa mediante la implantación y el mantenimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI) en conformidad con el estándar internacional ISO/IEC 27001.

La Política de Seguridad de la Información tiene el objetivo fundamental de garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a las incidencias que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve AECOC para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- **Disponibilidad**: propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- **Integridad**: propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- **Confidencialidad**: propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- **Autenticidad**: propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- **Trazabilidad**: propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en AECOC serán:

- Velar por la seguridad de la información, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de disponibilidad y continuidad de la actividad que se definan para los distintos servicios ofrecidos por la organización.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

1.2. Alcance

La presente Política de Seguridad se aplicará a todo el personal y departamentos que estén relacionados directamente con AECOC

- Departamentos involucrados, tanto sus directivos como empleados.
- A los proveedores, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la organización.
- A bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- A la información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas

1.3. Distribución

Aprobada por la Dirección de AECOC, esta Política debe ser accesible a todas las personas y organismos afectados dentro del alcance del SGSI, mediante los canales adecuados. De igual modo, la Política se encontrará accesible para cualquier parte interesada u órgano competente que lo solicite por vía formal.

2. Marco Normativo del SGSI

El control de la normativa y legislación de aplicación de esta política de seguridad que se incluye dentro del Sistema de Gestión de la Seguridad de la Información de AECOC en el que se referencian entre otras las siguientes normativas y leyes:

- 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 (RGPD).
- Ley Orgánica de Protección de Datos y garantías de los derechos digitales, Ley 03/2018 (LOPDGDD).

3. Compromiso de la dirección en la seguridad de la información

La Dirección de AECOC se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del SGSI de la entidad, así como a demostrar liderazgo y compromiso respecto a éste, a través de las siguientes responsabilidades:

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que éstos sean compatibles con la estrategia de AECOC.
- Asegurar la integración y el cumplimiento de los requisitos aplicables del SGSI en los procesos de la entidad.
- Asegurar que los recursos necesarios para el SGSI estén disponibles.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del SGSI.
- Asegurar que el SGSI consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI.
- Promover la evolución y mejora continua.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.
- Supervisando los Indicadores para evaluar el resultado/cumplimiento.

3.1. Objetivos de la seguridad de la información

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.
- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.
- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
- Factores externos como los avances tecnológicos cuya aplicación mejore la eficacia del tratamiento de los riesgos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará tomando en cuenta los siguientes elementos:

- Lo que se va a hacer.
- Los recursos necesarios.
- El responsable.
- Plazo de consecución.
- Indicadores para evaluar el resultado/cumplimiento.

3.2. Implantación y mejora del SGSI

El despliegue del SGSI de AECOC se iniciará a partir del Análisis de Riesgos, que permitirá determinar el nivel de riesgo de seguridad de la información en que se encuentra la entidad e identificar los controles de seguridad necesarios para el tratamiento del riesgo y llevarlo a un nivel aceptable, así como las oportunidades de mejora, considerando las cuestiones internas y externas y los requisitos de las partes interesadas antes indicados.

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada, mediante procedimientos, normativas, instrucciones técnicas, manuales, etc., revisados y aprobados por el Responsable del SGSI junto con la supervisión del Director de GS1 e IT.

La presente Política de Seguridad se desarrolla aplicando los siguientes requisitos mínimos y que deben incluirse en la documentación del sistema:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos.
- Seguridad por defecto.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (empleados y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del SGSI.

La información documentada será clasificada en: pública, interna y confidencial, dando el uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en el procedimiento de clasificación, etiquetado y protección de la información.

Se realizarán auditorías que revisen y verifiquen el cumplimiento del SGSI basado en la norma ISO/IEC 27001, por lo que, en caso necesario, el personal afectado por el alcance deberá colaborar en éstas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo.

3.3. Roles y Responsabilidades en el SGSI

Se establecen, de manera no extensiva, las siguientes funciones y responsabilidades dentro del SGSI:

- La Dirección de AECOC, representada por el director de GS1 e IT, será el órgano encargado de aprobar la política y será la responsable de la autorización de sus modificaciones, así como de toda la información documentada del SGSI de la entidad.

- El Responsable de SGSI será el encargado de notificar la presente política al personal de la entidad y de los cambios que en ella se produzcan, así como de coordinar las acciones de implantación, mantenimiento y mejora del SGSI de la entidad, y de sus auditorías.
- Todo el personal de la entidad (interno y externo) será responsable de cumplir la presente política dentro de su área de trabajo, así como de aplicar toda la información documentada del SGSI de la entidad en sus actividades laborales que afecta a su desempeño en seguridad de la información.

3.4. Revisión de la Política de Seguridad de la Informacion

La presente Política de Seguridad de la Información será revisada por la dirección siempre que se produzcan cambios significativos y como mínimo, una vez al año.

3.5. Cumplimiento Legal

La dirección de la organización establece como principio fundamental el cumplimiento de todos los requisitos legales, reglamentarios y contractuales que rigen la seguridad de la información, la privacidad de los datos y la ciberseguridad.

Esta observancia es crucial para mantener la confianza de nuestras partes interesadas, proteger la reputación corporativa y evitar sanciones legales o impactos negativos. Nuestro Sistema de Gestión de Seguridad de la Información (SGSI) está diseñado para asegurar esta conformidad de manera sistemática, siendo el detalle y la gestión de estos requisitos explícitamente abordados en el documento **AECOC_SGSI_PR_07_Cumplimiento**

4. Aceptación del documento

La presente Política de Seguridad de la Información será aprobada por la Dirección de AECOC mediante firma y será comunicada a las partes interesadas.

Ronda General Mitre 10 · 08017 Barcelona
T. 93 252 39 00
F. 93 280 21 35 · G-08557985

www.aecoc.es