

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

080 FORMACIÓN	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**	**PÚBLICO**
Revisión 1	Fecha 28/05/2026	Aprobado por Dirección

Contenido

1. APROBACIÓN Y ENTRADA EN VIGOR 3
2. INTRODUCCIÓN 3
3. ALCANCE 4
4. MISIÓN 4
5. PRINCIPIOS RECTORES DE LA POLÍTICA 5
6. MARCO NORMATIVO 6
7. ORGANIZACIÓN DE LA SEGURIDAD 7
8. TRATAMIENTO DE DATOS PERSONALES EN LA ORGANIZACIÓN 7
9. GESTIÓN DE RIESGOS 8
10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 8
11. OBLIGACIONES DEL PERSONAL 8
12. PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES 9
13. GESTIÓN DE INCIDENTES DE SEGURIDAD 10
14. APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR/EFECTIVIDAD 10

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 28 de mayo de 2026 por la Dirección. Esta Política se Seguridad de la Información está vigente desde la fecha de aprobación y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

Área 080 Cualificación Profesional S.L. (en adelante **080 Formación**), depende de los sistemas de información para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que la organización pueda cumplir con sus objetivos, desarrollar sus funciones o competencias y prestar los servicios para la cual se ha sido constituida la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

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

Los diferentes departamentos de **080 Formación** deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en adquisición o prestación de servicios TIC que afecten a los sistemas de información.

3. ALCANCE

La presente Política de Seguridad es de aplicación al Sistema de Gestión de la Seguridad de la Información (SGSI) de **080 Formación**, cuyo alcance comprende los sistemas de información, servicios, procesos y activos que soportan la actividad de la organización definidos en el documento de categorización del sistema.

La Política resulta de obligado cumplimiento para todo el personal de la organización, incluidos directivos, empleados, personal temporal y contratistas, así como para terceros que tengan acceso a los sistemas de información o a la información incluida en el alcance del SGSI. El alcance incluye tanto los activos de información propios de la organización como aquellos gestionados o tratados por terceros en el marco de relaciones contractuales, con independencia del soporte o medio en el que se encuentren.

4. MISIÓN

Como parte de su política estratégica para el desarrollo de sus actividades, 080 Formación ha desarrollado e implementado un Sistema de Gestión Integrado (en adelante SGI), que integra los requisitos de calidad, medio ambiente, seguridad de la información y continuidad del negocio, incorporando los principios y controles del Esquema Nacional de Seguridad (ENS) para garantizar la protección de la información y de los servicios, la gestión de riesgos, la prevención de incidentes y la mejora continua, mediante un enfoque basado en el análisis, la evaluación y el tratamiento de los riesgos, así como en la revisión periódica de la eficacia de las medidas de seguridad implantadas.

La misión y visión de la organización están recogidos en la “Política Integrada de Gestión”, según normas ISO 9001, ISO 14001 e ISO 27001, aprobada por la dirección.

Los objetivos en materia de seguridad que **080 Formación** pretende garantizar con la presente Política serán:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.

- Implementar medidas de seguridad en función del riesgo.

- Formar y concienciar a los integrantes de la organización respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.

- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.

- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida.

- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.

- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.

- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.

- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

5. PRINCIPIOS RECTORES DE LA POLÍTICA

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la organización y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente

- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

- Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar

justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.

- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, dando una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.

- Existencia de líneas de defensa, la estrategia de seguridad de la organización se diseña e implementa en capas de seguridad.

- Vigilancia continua y reevaluación periódica: la organización implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.

- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

- Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

6. MARCO NORMATIVO

Las principales normas que afectan a esta Política son:

- 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 y por el que se deroga la Directiva 95/46/CE (RGPD).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

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

- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.

- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual.

- Resto de requisitos legales establecidos en los registros asociados a los procedimientos del sistema integrado PRO 13 y PRO 1.

7. ORGANIZACIÓN DE LA SEGURIDAD

La organización dispone de una estructura organizativa formal en materia de seguridad de la información, conforme a lo establecido en el Real Decreto 311/2022, garantizando la diferenciación de responsabilidades y la ausencia de conflictos de interés.

Se encuentran formalmente designados los roles de seguridad de la información en los registros derivados del PRO 3 Recursos humanos, del sistema integrado de gestión, definiendo para cada uno, las funciones y responsabilidades de su cargo, así como el procedimiento para su designación y renovación. En este sentido, el Responsable de Seguridad reporta directamente a la Dirección y dispone de la autoridad necesaria para supervisar el cumplimiento de las medidas de seguridad, pudiendo elevar incidencias o incumplimientos sin interferencias operativas.

La organización dispone asimismo de un Comité de Seguridad, como órgano colegiado de coordinación y seguimiento, que supervisa el estado de la seguridad, analiza riesgos e incidentes y promueve la mejora continua del sistema.

La designación de los responsables se realiza formalmente por la Dirección y queda debidamente documentada.

Los roles y responsabilidades en relación al SGSI son comunicados a las nuevas incorporaciones y recordados periódicamente a todo el personal de la organización.

En caso de conflicto o discrepancia entre los responsables definidos en materia de seguridad de la información, la resolución corresponderá a la Dirección, previo análisis en el seno del Comité de Seguridad, garantizando la adecuada ponderación de los riesgos y el cumplimiento de los requisitos establecidos en el Esquema Nacional de Seguridad.

8. TRATAMIENTO DE DATOS PERSONALES EN LA ORGANIZACIÓN

080 Formación trata datos de carácter personal de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD). La

organización está cumpliendo con todas las disposiciones del GDPR para el tratamiento de los datos personales de su responsabilidad, y manifiestamente con los principios descritos en el artículo 5 del GDPR, por los cuales son tratados de manera lícita, leal y transparente en relación con el interesado y adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

La organización garantiza que implementa políticas técnicas y organizativas apropiadas para garantizar las medidas de seguridad que establece el artículo 32 GDPR con el fin de proteger los derechos y libertades de los interesados.

9. GESTIÓN DE RIESGOS

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

- regularmente, al menos una vez al año.

- cuando se produzcan cambios en la información manejada.

- cuando se produzcan cambios en los servicios prestados.

- cuando ocurra un incidente grave de seguridad.

- cuando se reporten vulnerabilidades graves.

- cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de normativa de seguridad que aborde aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

11. OBLIGACIONES DEL PERSONAL

Todos los miembros de **080 Formación** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo

responsabilidad de la organización disponer los medios necesarios para que la información llegue a los afectados.

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

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

12. PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES

Cuando **080 Formación** preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación.

Cuando la organización utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las Guía de desarrollo.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que la organización pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los

responsables de la información y los servicios afectados antes del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará a la Dirección de la organización que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la organización adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema.

13. GESTIÓN DE INCIDENTES DE SEGURIDAD

La organización dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte a la organización para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

14. APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR/EFECTIVIDAD

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información, que deberá revisarla anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.

Área 080. Cualificación Profesional, S.L.
B18805457
Ctra. Celulosa S/N (N 232) CP.18613
Motril (Granada)

Bernardo Spa Vázquez