Política de Seguridad de la Información

PO01

CONTROL DE VALIDACIÓN

	REVISADO	APROBADO
NOMBRE:	Jordi Martí	Vicente Arteaga
FUNCIÓN:	Responsable del Sistema	Responsable de Seguridad
FECHA:	13/04/2026	13/04/2026

CONTROL DE VERSIONES

Versión	Autor	Fecha	Comentarios
1	JM	09/10/2025	Redacción inicial
2	JM	13/04/2026	Incorporación de principios de seguridad del Art. 12 ENS y revisión de estructura conforme a CCN-STIC 805.

Tabla de contenido

1 APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por el Responsable de Seguridad de la Información de ARCON, con la validación del Comité de Seguridad TIC.

Esta Política de Seguridad de la Información está vigente desde la fecha de aprobación y hasta que sea reemplazada por una nueva Política.

Este texto deroga al anterior, que fue aprobado el día 9 de octubre de 2025 por el Responsable de Seguridad de la Información.

2 INTRODUCCIÓN

ARCON 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 ARCON pueda cumplir con sus objetivos, desarrollar sus funciones y prestar los servicios para los cuales ha sido constituida, garantizando 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.

ARCON debe 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 pliegos de licitación para proyectos donde se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

3 ALCANCE

Esta política se aplica a todos los sistemas de información de ARCON, a las personas que conforman la organización y a los prestadores de servicios o proveedores de soluciones TIC de ARCON.

4 MISIÓN

La misión de ARCON es ofrecer soluciones integrales de control de accesos, seguridad y equipamiento especializado, trabajando con sectores como hospitality, sanidad, educación, sector público, residencial, retail, coworking y utilities. Sus principales líneas de negocio son:

- Soluciones de control de accesos y seguridad: cerraduras electrónicas, sistemas sin llave, control de acceso en la nube u on-premise.
- Equipamiento hotelero: cajas fuertes, cerraduras de hotel, minibares, señalética, etc.
- Herrajes técnicos, manillas, complementos arquitectónicos, puertas y automatismos.
- Servicios de asesoramiento y acompañamiento en todas las etapas del proyecto (desde diseño hasta implementación).

Los objetivos en materia de seguridad que ARCON 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 ARCON 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 transmitida 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 entidad 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 entidad se diseña e implementa en capas de seguridad.

Vigilancia continua y reevaluación periódica: la entidad implementa medios para 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 PRINCIPIOS DE SEGURIDAD — REQUISITOS MÍNIMOS (ART. 12 ENS)

De conformidad con el artículo 12.6 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, la política de seguridad se desarrollará aplicando los siguientes requisitos mínimos:

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos.
- h) Seguridad por defecto.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de actividad.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- o) Mejora continua del proceso de seguridad.

7 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 (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.
- Ley 24/2015, de 24 de julio, de Patentes; Ley 17/2001, de 7 de diciembre, de Marcas; Ley 20/2003, de 7 de julio, de Protección Jurídica del Diseño Industrial; Ley 3/1991, de 10 de enero, de Competencia Desleal; Reglamento (CE) n.º 6/2002 sobre los dibujos y modelos comunitarios.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

8 ORGANIZACIÓN DE LA SEGURIDAD

NOTA: este apartado puede completarse en estructura de mayor tamaño con otros roles vinculados a la ciberseguridad descritos en otras normas, Guías o recomendaciones publicadas.

8.1 COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad de la Información estará formado por el Responsable de la Información, el Responsable del Servicio, el Responsable de Seguridad de la Información y el Responsable del Sistema.

El Secretario del Comité de Seguridad de la Información será el Responsable de Seguridad de la Información, y tendrá las siguientes funciones:

- Convocar las reuniones del Comité.

- Preparar los temas a tratar, aportando documentación técnica y contextual para la toma de decisiones.
- Elaborar las actas de cada reunión.
- Asegurar la ejecución de las decisiones adoptadas por el Comité.

El Comité de Seguridad de la Información reportará a la Alta Dirección de ARCON.

El Comité de Seguridad de la Información tendrá las siguientes funciones:

- Revisar y aprobar la Política de Seguridad de la Información, así como las responsabilidades clave asociadas.
- Definir y promover la estrategia y planificación en materia de seguridad, proponiendo los recursos y presupuestos necesarios.
- Supervisar los cambios significativos en la exposición al riesgo de los activos de información, así como la implantación de controles adecuados.
- Aprobar las principales iniciativas destinadas a la mejora continua de la seguridad.
- Realizar el seguimiento de los incidentes relevantes en materia de seguridad de la información, de la elaboración y revisión de planes de continuidad, y del grado de cumplimiento y difusión de la Política de Seguridad.

8.2 ROLES: FUNCIONES Y RESPONSABILIDADES

8.2.1 RESPONSABLE DE LA INFORMACIÓN

- Tiene la potestad de establecer los requisitos de seguridad aplicables a la información bajo su responsabilidad.
- En caso de tratarse de datos personales, deberá considerar además lo establecido en la normativa vigente sobre protección de datos.
- Es el responsable de determinar y documentar el nivel de seguridad de la información.
- Tiene la potestad exclusiva de modificar dicho nivel, conforme a la política de clasificación vigente.

8.2.2 RESPONSABLE DEL SERVICIO

- Establece los requisitos de seguridad aplicables a los servicios que gestiona.
- Es responsable de definir los niveles de seguridad asociados a dichos servicios.

8.2.3 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

- Dirige y coordina las reuniones del Comité de Seguridad.
- Supervisa la aplicación de la estrategia de seguridad definida.

- Controla la implantación y cumplimiento de los procedimientos establecidos en la Política de Seguridad y su normativa de desarrollo.
- Supervisa los incidentes de seguridad registrados en la organización.
- Difunde internamente las obligaciones en materia de seguridad de la información.
- Colabora y supervisa las auditorías internas y externas necesarias para evaluar el cumplimiento normativo y legal.
- Asesora a todas las unidades organizativas en materia de seguridad de la información.

8.2.4 RESPONSABLE DEL SISTEMA

- Garantiza la correcta aplicación de medidas de seguridad sobre los activos y servicios tecnológicos que soportan la actividad de la organización.
- Es responsable del desarrollo, operación y mantenimiento del sistema de información durante todo su ciclo de vida.
- Define la arquitectura y la gestión del sistema, sus criterios de uso y servicios disponibles.
- Se asegura de que las medidas específicas de seguridad se integren dentro del marco general de la organización.
- Asigna funciones y responsabilidades al personal técnico para asegurar la correcta gestión de la seguridad operativa.
- Supervisa que los nuevos sistemas, y los cambios realizados sobre los existentes, cumplen con los requerimientos de seguridad establecidos.
- Define mecanismos de monitorización y gestión de incidentes de seguridad.
- Puede ordenar, de forma coordinada con los responsables implicados, la suspensión de un servicio o tratamiento de información si se detectan deficiencias graves que pongan en riesgo los requisitos de seguridad.

8.3 PROCEDIMIENTOS DE DESIGNACIÓN

Los miembros del Comité de Seguridad de la Información serán designados por la Alta Dirección.

El Responsable de la Información será designado a propuesta del Comité de Seguridad.

El Responsable del Servicio será designado a propuesta del Comité de Seguridad.

El Responsable de la Seguridad será designado a propuesta del Comité de Seguridad.

Los nombramientos podrán ser revisados cada dos años, pudiendo realizarse antes cuando el puesto quede vacante o por un incumplimiento reiterado de sus funciones, previo apercimiento. ARCON debe disponer de un mecanismo que permita la sustitución de los responsables designados en caso de ausencias de larga duración o aquellas de

menor duración pero que puedan provocar ineficiencias en las funciones de cada uno de ellos que afecten al sistema.

8.4 RESOLUCIÓN DE CONFLICTOS

En el caso de conflictos entre los diferentes responsables, el Comité de Seguridad de la Información podrá dirimir las discrepancias.

9 TRATAMIENTO DE DATOS PERSONALES EN LA ENTIDAD

ARCON trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento. ARCON deberá evaluar los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado.

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice el Delegado de Protección de Datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales.

10 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.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información

manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Delegado de Protección de Datos, y además se coordinarán los planes del tratamiento del riesgo.

11 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa/se integra junto con otras políticas de ARCON en diferentes materias:

- Control de accesos.
- Copias de seguridad.
- Clasificación y etiquetado de la información.
- Seguridad física.

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 ARCON que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en el repositorio documental.

12 OBLIGACIONES DEL PERSONAL

Todos los miembros de ARCON 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 ARCON a través del Comité de Seguridad y del área de personal de disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de ARCON 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 los miembros de ARCON, 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.

13 TERCERAS PARTES / PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES

Cuando ARCON 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 de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando ARCON 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 se tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las Guías 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 ARCON 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 que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. 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.

Cuando la entidad 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, debiendo también el Delegado de Protección de Datos emitir su parecer.

14 GESTIÓN DE INCIDENTES DE SEGURIDAD

ARCON 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 al organismo 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 del Estado o los juzgados.

15 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 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.