Política

Política de Seguridad de la Información

11/12/2024

Referencia: ICA-POL-PSI

Grupo ICA
La Rábida 27
28039 Madrid

Control de versiones

Versión	Responsable			Modificación
1.0	Autor:	Responsable de Seguridad	11/12/2024	Versión inicial Adaptación al ENS y norma ISO 27001
	Revisión:	Comité de Seguridad de la Información	11/12/2024	

Contenido

1. Introducción.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica, persigue tres objetivos fundamentales:

1. Alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital.
2. Introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios.
3. Facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Para ello, el Real Decreto en el capítulo III referido a la política de seguridad en sus artículos 12 a 27, se definen:

1. Los requisitos mínimos para permitir una protección adecuada de la información y los servicios a través de la organización e implantación del proceso de seguridad;
2. gestión de riesgos;
3. gestión de personal;
4. profesionalidad; autorización y control de los accesos;
5. protección de las instalaciones;
6. adquisición de productos de seguridad y contratación de servicios de seguridad;
7. mínimo privilegio;
8. integridad y actualización del sistema;
9. protección de la información almacenada y en tránsito;
10. prevención ante otros sistemas de información interconectados;
11. registro de la actividad y detección de código dañino;
12. incidentes de seguridad;
13. continuidad de la actividad; y mejora continua del proceso de seguridad.

La política de seguridad de la información (en adelante PSI), según el Real Decreto, es el documento que define el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

Cuando la provisión de las soluciones o la prestación de los servicios sujetos al cumplimiento del ENS sean realizadas por organizaciones del sector privado, se deberán utilizar estos mismos modelos, sustituyendo las referencias a los organismos públicos por las correspondientes a las entidades privadas certificadas.

ICA SL debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS.

1.1 Prevención

ICA SL debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello ***ICA SL*** debe implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, ***ICA SL*** debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

1.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

1.3 Respuesta

ICA SL debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

1.4 Conservación

Para garantizar la disponibilidad de los servicios críticos, ***ICA SL*** debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

2. Disposiciones generales.

2.1 Objetivos y misión de la entidad

I.C.A. Informática y Comunicaciones Avanzadas S.L. (en adelante ***ICA SL***) se creó el 26 de diciembre de 1983 según consta en la escritura con numero de protocolo 1536 de 1984. Tiene como actividad los Sistemas de la información que dan soporte a los servicios profesionales relacionados con la evolución y mantenimiento de sistemas de gestión informáticos y outsourcing.

ICA Transformación Digital, SLU (en adelante ***ICA SL***) se creó 2024 como una escisión de ***I.C.A. Informática y Comunicaciones Avanzadas S.L.***, siendo esta última su accionista único. Tiene como actividad el Desarrollo de software, aplicaciones y portales web y aplicaciones móviles, así como consultoría de transformación digital, digitalización de procesos, integración de sistemas y aplicativos y data intelligence.

Ambas sociedades utilizan el mismo Sistema de Gestión de Seguridad de la Información (SGSI) de modo que en la documentación del sistema se definirá ICA SL para referirse a actividades que incumben a ambas sociedades de manera compartida, y sólo cuando haya actividades específicas de una de las sociedades se hará referencia específica a la misma.

Estas funciones y objetivos son realizadas a través del órgano de Gobierno (Junta General y Órgano de Administración) de este organismo y de las unidades de negocio, departamentos que se creen.

2.2 Objeto

El presente documento tiene por objeto definir y regular la política de seguridad de las tecnologías de la información y comunicaciones de ***ICA SL***, qué se ha de aplicar en el tratamiento de los activos de tecnologías de la información y comunicaciones de su titularidad o cuya gestión tenga encomendada, conformando, junto a las disposiciones y documentos técnicos que la desarrollen, el marco regulador de seguridad TIC de ***ICA SL***.

Esta Política de seguridad define los siguientes aspectos:

- Objetivo y alcance de la Política de Seguridad.
- Modelo organizativo para la gestión de la Política de Seguridad y la protección de datos.
- Los roles, responsabilidades y funciones relacionados con la seguridad y la protección de datos.
- Implementación de las medidas técnicas y organizativas de seguridad que se desarrollan en normas y procedimientos de seguridad del ayuntamiento en diferentes niveles.

2.3 Ámbito de aplicación

La presente Política de Seguridad es de aplicación a todos los niveles de los sistemas de información que permiten a ***ICA SL*** prestar sus servicios de "*Diseño, desarrollo, mantenimiento e implantación de soluciones software*", "*Servicios profesionales relacionados con la evolución y mantenimiento de sistemas de gestión*" y "*Servicios profesionales de outsourcing*". Se aplicará a todos los sistemas y demás recursos TIC que den soporte a sus procesos y que afecten a los diferentes activos de información sustentados en ellos.

La Política de Seguridad se aplica también a todas las personas, indistintamente del colectivo o unidad organizativa a la que pertenezcan, que hagan uso de los recursos de las TIC.

2.4 Marco legal y regulatorio

El marco normativo en el que ***ICA SL*** y, en particular, la prestación de sus servicios electrónicos a sus clientes está integrado por las siguientes normas:

- 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.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Con carácter transitorio hasta finalizados los plazos establecidos en el RD 311/2022, Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- UNE-ISO/IEC 27001:2023 "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información Requisitos".
- ITS de Conformidad con el Esquema Nacional de Seguridad y del Informe del Estado de la Seguridad (BOE del 2 de noviembre de 2016): Instrucción técnica que establece los procedimientos para dar publicidad a la conformidad con el Esquema Nacional de Seguridad, así como los requisitos exigibles a las entidades certificadoras.
- Instrucción Técnica de Seguridad de Auditoría (BOE del 3 de abril de 2018): Instrucción técnica que establece las condiciones para la realización de las auditorías, ordinarias o extraordinarias, previstas en el artículo 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): Ley que adapta el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, completa sus disposiciones, y garantiza los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la Política de Seguridad

2.5 Compromisos

Conforme a los requisitos de la norma ISO 27001, ***ICA SL*** se compromete a:

- Cumplir los objetivos de seguridad de la información que se definen y revisan anualmente.
- Cumplir los requisitos aplicables a la seguridad de la información.
- Mejorar continuamente el sistema de gestión de la seguridad de la información.
- Comunicar dentro de la organización la Política de Seguridad de la información, que se gestiona como información documentada.
- Poner la Política de Seguridad de la información a disposición de las partes interesadas, según sea apropiado.

3. Principios de seguridad

3.1 Principios de la seguridad de la información

Los principios son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de tecnologías de la información y comunicaciones. Se establecen los siguientes de acuerdo con el artículo 5 del ENS:

- Seguridad como proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.

3.2 Declaración de la Política de Seguridad

La Política de Seguridad se concreta en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos y que inspiran las actuaciones en dicha materia. Se establecen los siguientes:

a) Todas las directrices de seguridad estarán alineadas y no entrarán en conflicto con lo establecido en la política de seguridad de las tecnologías de la información y comunicaciones de ***ICA SL***.
b) Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el 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 (Reglamento general de protección de datos).
c) Los activos de información se encontrarán gestionados, inventariados y categorizados, y estarán asociados a un responsable.
d) Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
e) Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
f) Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones y los servicios prestados a los ciudadanos deberán ser adecuadamente protegidos, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
g) Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

h) Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto. En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones 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.
i) Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
j) Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.
k) La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. Se 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 y deberán designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado.
l) Los sistemas de información se diseñarán y configurarán otorgando los mínimos privilegios necesarios para su correcto desempeño.
m) Cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten y la detección temprana de cualquier incidente que tenga lugar sobre los mismos.
n) Se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica deberá estar protegida con el mismo grado de seguridad que ésta.
o) Se protegerá el perímetro del sistema de información reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.
p) Con plenas garantías legales, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

4. Organización de la seguridad

4.1 Estructura organizativa de seguridad

La estructura organizativa para la gestión de la seguridad de la información en el ámbito particular de ***ICA SL*** está compuesta por los siguientes agentes:

- El Comité de Seguridad de la información (CSI) de ***ICA SL***.

La estructura organizativa será competente para mantener, actualizar y hacer cumplir, dentro del ámbito definido por la presente Resolución y de sus competencias, la Política de Seguridad.

4.2 El Comité de Seguridad de la Información (CSI)

El Comité de Seguridad de la Información (CSI) de ***ICA SL*** ejercerá las siguientes funciones:

- Definir, aprobar, implementar y control continuado de:
  - La Política de Seguridad de la Información y sus objetivos.
  - Los criterios de apreciación y aceptación de los riesgos de Seguridad de la Información.
  - Niveles y perfiles de riesgo aceptables (riesgo residual).
  - Planes de actuación vigentes en cada momento.

- Aprobar las acciones que se consideren oportunas ante modificaciones consideradas significativas en la valoración/apreciación de riesgos de los Activos de la entidad.
- Revisar y aprobar los documentos "Contexto para el SGSI" y el "Manual del SGSI".
- Revisar el análisis de incidencias de Seguridad del Sistema.
- Promover la mejora continua del SGSI.
- Aprobar el Informe de Revisión del SGSI.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Comité de Seguridad de la Información (CSI) se reunirá con carácter ordinario al menos cada doce meses y con carácter extraordinario cuando lo decida su Presidente y actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tiene encomendada.

El Comité de Seguridad de la Información (CSI) de la Entidad estará compuesto por los siguientes miembros:

- Presidente. Asumido por el Director Corporativo de ***ICA SL***. Tendrá voto de calidad en la toma de decisiones del Comité.
- Vocales. Asumido por aquellos que ostenten las funciones establecidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema, y el que ostente la función de Delegado de Protección de Datos establecidas según lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4.3 Responsable de Seguridad

Es la persona designada por el Comité de Seguridad, encargada de coordinar las actividades relacionadas con la obtención, tratamiento, almacenamiento y salvaguarda de la información. Reporta directamente al Comité de Seguridad. También nombrado como Responsable del SGSI.

Responsabilidades:

- El responsable de la Seguridad de la Información es la persona que se va a encargar de coordinar y aprobar todas las actuaciones en materia de seguridad dentro de ICA, de acuerdo a lo establecido en la Política de Seguridad de la Información.
- Convocar al Comité de Seguridad.
- Impulsar la cultura en Seguridad de la Información, gestionando y promoviendo la formación y concienciación en materia de seguridad.
- Establecer los requisitos de la información en materia de seguridad, esto es, determinar los niveles de Seguridad de la Información.
- Participar en la categorización de los sistemas y el análisis de riesgos.
- Resolver discrepancias y problemas que puedan surgir en la gestión de la seguridad.
- Mantener el nivel adecuado de Seguridad de la Información manejada y de los servicios prestados por los sistemas.
- Revisar y aprobar toda la documentación relacionada con la Seguridad del Sistema.
- Realizar o promover las auditorías periódicas para verificar el cumplimiento de los requisitos del mismo, así como realizar el seguimiento de las acciones correctivas y de mejora que se establezcan para resolver las desviaciones detectadas.
- Acompañar y facilitar a los auditores de certificación el acompañamiento por las instalaciones y el apoyar en la localización de documentación y registros del SGSI.
- Determinar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
- Determinar las excepciones cuando lo justifiquen las exigencias de proporcionalidad en cuanto a los riesgos asumidos en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que 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.
- Aprobar la Declaración de Aplicabilidad. Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente

que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto.
- Analizar los informes de autoevaluación y/o los informes de auditoría y elevar las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
- POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, con el apoyo de los órganos de dirección. Canaliza y supervisa, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

4.4 Responsable del Sistema

El Responsable del Sistema reportará, en materia de seguridad, al Responsable de la Seguridad.

Responsabilidades:

- Operar el sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
- Analizar las conclusiones del Responsable de la Seguridad sobre los informes de autoevaluación y/o los informes de auditoría para adoptar las medidas correctoras adecuadas.
- (Sólo en el caso de sistema de categoría ALTA) Visto el dictamen de auditoría, acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

4.5 Responsable de la Información

Responsabilidades:

- Determinar los requisitos (de seguridad) de la información tratada.
- Aprobar los niveles de seguridad de la información.
- Valorar las consecuencias de un impacto negativo sobre la seguridad de la información, atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de las personas.

4.6 Responsable del Servicio

Responsabilidades:

- Determinar los requisitos (de seguridad) de los servicios prestados.
- Aprobar los niveles de seguridad de los servicios.
- Definir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios, atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de las personas.

4.7 Delegado de Protección de Datos

El Delegado de Protección de Datos de ***ICA SL*** tendrá además de las funciones recogidas expresamente el 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 en la ley Orgánica 3/2018, de 5 de octubre, de protección de datos personales y garantías de los derechos digitales, las siguientes:

- La promoción y concienciación de una cultura de protección de datos dentro de ICA SL.
- Asesorar a las diferentes unidades orgánicas y administrativas en materia de protección de datos en general y en particular en los tratamientos a crear.
- Dictar normas internas interpretativas, aclaratorias y/o circulares o instrucciones en materia de protección de datos para todas las unidades Orgánicas, administrativas de la entidad.

- Dar respuesta a las cuestiones que los interesados le platean, ya sea a través su dirección de correo electrónico, que será pública, o por cualquier otro cauce legal, respecto al tratamiento de sus datos personales.
- Asesorar a los responsables de los tratamientos en la elaboración de los informes de evaluación que requiere la creación de los tratamientos, previa supervisión y comprobación de la conformidad con la normativa de las actividades del tratamiento.
- Colaborar con todos los servicios en la supervisión y actualización de los tratamientos creados y en el cumplimento del deber de información recogido en el artículo 11 de la Ley Orgánica 3/2018, de 5 de octubre, de protección de datos personales y garantías de los derechos digitales y en el artículo 13 del Reglamento de la UE.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Coordinar con los responsables de las diferentes Unidades administrativas las reclamaciones y requerimientos de actuación que lleguen por parte de ICA SL.
- Diseño e implantación de políticas de protección de datos.
- Poner en conocimiento de los responsables de los tratamientos y de las unidades administrativas, las vulneraciones de protección de datos que se produzcan y colaborar con ellos con el fin de solventar dichas vulneraciones.
- Colaborar con las unidades competentes en formación, en la implantación de programas de formación y sensibilización del personal municipal en materia de protección de datos.
- Cuantas otras funciones contribuyan al cumplimiento de la normativa en materia de protección de datos.

5. Resolución de conflictos

De acuerdo con el Principio de Jerarquía que rige en ***ICA SL***, en caso de conflicto entre los diferentes responsables y/o entre diferentes servicios, éste será resuelto por el superior jerárquico de los mismos.

En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad de la Información (CSI) de ***ICA SL***, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

6. Gestión de los riesgos

La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

El Responsable de Seguridad es el encargado de que se realice el preceptivo análisis de riesgos y se proponga el tratamiento adecuado, calculando los riesgos residuales.

El Responsable de Seguridad es el encargado de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

Los Responsables de la Información y del Servicio son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el Comité de Seguridad, a través de un Plan de Adecuación al Esquema Nacional de Seguridad.

Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la

aplicación de este elaboradas por el Centro Criptológico Nacional, así como todo lo referente al análisis de riesgo y de impacto en la protección de datos especificado en la Ley Orgánica 3/2018, de 5 de diciembre.

7. Documentación de desarrollo

Las medidas sobre la seguridad de la información, de obligado cumplimiento, se desarrollarán en cuatro niveles con diferente ámbito de aplicación, detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento de desarrollo se fundamenta en el nivel superior.

Su desarrollo se agrupará en las categorías de política, normativa, procedimientos y guías técnicas. Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación.

La Política de Seguridad de la Información de ***ICA SL***, constituida por el presente documento, es de obligado cumplimiento en todo el ámbito de aplicación.

La normativa establecerá el uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido, la responsabilidad del personal con respecto al cumplimiento o violación de la normativa, derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente. Será aprobada por el comité de seguridad correspondiente en cada caso.

Los procedimientos describirán la secuencia concreta de actividades que permiten satisfacer las obligaciones contenidas en las normas. Serán aprobados por el responsable de seguridad correspondiente en cada caso.

Las guías técnicas ofrecerán información sobre cómo actuar ante situaciones y tecnologías específicas. Serán aprobadas por la dirección ejecutiva de responsabilidad en la materia correspondiente en cada caso.

Los procedimientos y guías técnicas tendrán carácter de recomendaciones y serán desarrollados con arreglo a los ámbitos en materia de seguridad de la información que se establezcan.

Todo el personal de cada una de las direcciones y departamentos de ***ICA SL*** tendrá la obligación de conocer y cumplir, además de esta Política de Seguridad de la Información y todas las directrices generales, normas, procedimientos y guías técnicas de seguridad de la información que puedan afectar a sus funciones, aquellas que se desarrollen en el marco de cumplimiento general de ***ICA SL***.

El Comité de Seguridad de la Información (CSI) establecerá los mecanismos necesarios para compartir la documentación derivada de su desarrollo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación.

La documentación que ICA SL ha considerado necesaria para establecer, implementar y mantener el SGSI, comprende lo siguiente:

- Política de Seguridad de la información: Documento base para el Sistema de Gestión que recoge la aplicación de los requisitos de ENS y de las normas ISO/IEC 27001. Contiene las Políticas de Seguridad y de la Gestión de los Servicios y recoge los procesos clave correspondientes a la operativa interna.
- Procedimientos de Seguridad: Documentos que describen la operativa para garantizar la aplicación de las medidas y controles de seguridad que aseguran el mantenimiento y enriquecimiento del Sistema de Gestión de la Seguridad, y que, además proporcionan la pauta a seguir en las diferentes actividades realizadas.

Además de los documentos citados, la documentación del sistema podrá contar, bajo criterio del Responsable de Seguridad, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

El correspondiente titular de la Dirección que gestione cada procedimiento afectado será responsable dentro de su ámbito de actuación de mantener la documentación de actualizada y organizada.

El Responsable de Seguridad será responsable dentro de su ámbito de actuación de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos de acceso, a la misma y a la documentación responsabilidad de otras Unidades del Organismo.

Todos los registros generados se emiten y mantienen con el fin de demostrar la conformidad con los requisitos especificados y verificar el funcionamiento del SGSI.

La operativa seguida para la elaboración, revisión, aprobación, distribución, archivo y modificación de dichos documentos, así como la gestión de los registros se describen en el Procedimiento de Control de la Documentación del Sistema de Gestión de la Calidad.

8. Protección de datos de carácter personal

En lo referente a los datos de carácter personal que sean objeto de tratamiento, se adoptarán las medidas técnicas y organizativas que corresponda implantar atendidos los riesgos generados por el tratamiento una vez llevada a cabo la evaluación exigida por el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre.

Respecto a la protección de datos de carácter personal, el Responsable del Sistema asumirá las funciones de responsable del tratamiento.

ICA SL ha establecido la estructura Protección de datos nombrando la figura de Delegado de Protección de Datos Global, que actuará además en representación ante el Comité Técnico de Protección de datos de ***ICA SL***.

ICA SL realiza tratamientos de datos de carácter personal. El inventario de actividades de tratamiento actualizado con la finalidad de que los interesados puedan acceder al mismo para su consulta, siendo ***ICA SL*** responsable de su tratamiento.

ICA SL mantendrá actualizado el Registro de Actividades de Tratamientos y el documento de seguridad relacionado con los ficheros de su competencia que los traten, de conformidad con lo exigido en la normativa sobre protección de datos vigente en cada momento, así como por las normas, e instrucciones dictadas por el Delegado de Protección de Datos de ***ICA SL***.

Todos los sistemas de información de ***ICA SL*** que traten datos personales se ajustarán a los requisitos de seguridad definidos por los responsables de los tratamientos de los datos, de acuerdo con lo exigido por el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; la Ley Orgánica 3/2018, de 5 de diciembre; la Ley Orgánica 7/2021, de 26 de mayo; y las directrices y normas dictadas por los respectivos Delegados de Protección de Datos.

9. Formación y concienciación.

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados de ***ICA SL***, así como a la difusión entre los mismos de la Política de Seguridad de la Información y de su desarrollo normativo.

El Responsable de Seguridad de cada entidad se encargará de promover las actividades de formación y concienciación en materia de seguridad a través dentro de los Planes de Formación.

10. Terceras partes.

Cuando ***ICA SL*** preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la información. ***ICA SL***, definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que ***ICA SL***, lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando ***ICA SL***, utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad. De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto Real Decreto 311/2022, de 3 de mayo, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS 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 de seguir adelante.

11. Actualización permanente y revisiones periódicas de la política de seguridad de la información.

La presente política deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de Administración Electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.