POLÍTICA

Política de Seguridad de la Información

espublico.

Información general

Control documental

Clasificación	Público
Versión	4.0
Fecha creación	13/02/2017
Fecha última actualización	04/10/2023
Fichero	POL_PolíticaSeguridadInformación

Estado formal

Preparado por:	**Revisado por:**	**Aprobado por:**
Oficina de seguridad Fecha: 04/10/2023	Responsable de seguridad Fecha: 04/10/2023	Comité de seguridad Fecha: 04/10/2023

Control de versiones

Versión	**Descripción del cambio**	**Autor del cambio**	**Fecha del cambio**
1.0	Versión inicial aprobada de la Política.	Oficina de seguridad	13/02/2017
2.0	Revisión global anual. Adaptación conforme a modificaciones ENS 2015	Oficina de seguridad	07/02/2018
3.0	Revisión 2020. Generalización a todo esPublico.	Oficina de seguridad	06/03/2020
4.0	Revisión según RD 311/2022 e implantación del SGCN en esPublico.	Oficina de Seguridad	19/09/2022
5.0	Actualización referencia ISO 27001:2022. Sustitución SGSI por SIG	Oficina de Seguridad	04/10/2023

Índice

1. Introducción

En la actualidad "la información digital" se ha convertido en uno de los principales activos de cualquier compañía, de ahí la necesidad de protegerla adecuadamente.

Espublico Servicios Para La Administración S.A. ha impulsado la elaboración de una política de seguridad que sirva como guía para la protección de los Sistemas de Información de todo el grupo esPublico (en adelante también referido como "**esPublico**").

La seguridad de la información del grupo esPublico se asienta sobre un sistema integrado de gestión (en adelante, "SIG") cuyo objetivo principal es proteger los activos fundamentales para la organización: la información y los sistemas sobre los que se prestan los servicios.

Debido a que esta protección debe abarcar a todas las dimensiones de la seguridad (disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad), el SIG del grupo esPublico integra los siguientes sistemas:

- Sistema de gestión de **seguridad** de la información, conforme a la ISO/IEC 27001:2022 y al Esquema Nacional de Seguridad.
- Sistema de gestión de **privacidad** de la información, conforme a la ISO/IEC 27701:2019 y a la normativa nacional y europea en materia de protección de datos.
- Sistema de gestión de **continuidad de negocio**, conforme a la UNE-EN ISO 22301:2020.

Todos estos sistemas de gestión, junto con el de calidad (cuyos principios se recogen en su correspondiente política), se encuentran implantados de manera integrada en la totalidad del grupo esPublico y sometidos periódicamente a auditorías internas y externas de certificación para garantizar su correcto funcionamiento.

2. Compromiso del grupo esPublico

Las personas que forman el grupo esPublico, desde su Consejo de Administración y Alta Dirección hasta los empleados, están comprometidos con el mantenimiento y mejora continua del SIG.

Este compromiso abarca, especialmente, el cumplimiento de los requisitos legales y reglamentarios incluidos en el ámbito del SIG, y que forman parte del marco regulatorio en el que se desarrollan las actividades del grupo esPublico:

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

En particular, la Alta Dirección contribuye a la eficacia del SIG mediante su liderazgo y compromiso, el cual se refleja a través de su ejemplo, la comunicación de la importancia del SIG, el desarrollo de las políticas y objetivos estratégicos, el establecimiento de roles y responsabilidades en el ámbito de la seguridad de la información, así como la dotación de los recursos necesarios para la implantación y seguimiento efectivos del SIG.

3. Objetivos de la Política de Seguridad

Esta Política de seguridad de la información establece los principios y directrices para una protección adecuada de la información y los sistemas sobre los que se prestan los servicios de esPublico a sus clientes.

Los objetivos de esta Política de Seguridad de la Información son los siguientes:

a) Garantizar a sus clientes que los datos custodiados por esPublico serán gestionados de acuerdo con los estándares y buenas prácticas en seguridad TIC.

b) Aumentar el nivel de concienciación en materia de seguridad TIC allí donde es de aplicación esta Política, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.

c) Establecer las bases de un modelo integral de gestión de la seguridad TIC en la administración de esPublico, que cubra los aspectos técnicos, organizativos y procedimentales en un ciclo continuo de mejora.

d) Hacer patente el compromiso del grupo esPublico con la seguridad de la información mediante su apoyo al Comité de Seguridad dotándole de los medios y facultades necesarias para la realización de sus funciones.

e) Definir, desarrollar y poner en funcionamiento los controles metodológicos técnicos, organizativos y de gestión, necesarios para garantizar de un modo efectivo y medible la preservación de los niveles de confidencialidad, disponibilidad e integridad de la información aprobados por esPublico.

f) Garantizar la continuidad de los servicios ofrecidos por esPublico a sus clientes.

g) Crear y promover de manera continua una “cultura de seguridad” tanto internamente, a todo el personal, como externamente a los clientes y proveedores que permita asegurar la eficiencia y eficacia de los controles implantados y aumente la confianza de nuestros clientes.

4. Ámbito de aplicación

Esta Política será de aplicación y de obligado cumplimiento para todo el personal del grupo esPublico, así como terceras partes que presten servicio o manejen información responsabilidad de esPublico.

5. Principios de seguridad TIC

5.1. Principios básicos de la Política de seguridad TIC

La Política de seguridad TIC de esPublico se desarrolla con carácter general de acuerdo con los siguientes principios:

a) Principio de confidencialidad: los activos TIC deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

b) Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de sus procesos de tratamiento, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

c) Principio de disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los activos TIC y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

d) Principio de trazabilidad: se implantarán medidas para asegurar que en todo momento se pueda determinar quién hizo qué y en qué momento, con el fin de tener capacidad de análisis sobre los incidentes de seguridad detectados.

e) Principio de autenticidad: se deberán articular medidas para garantizar la fuente de información de la que proceden los datos y que las entidades donde se origina la información son quienes dicen ser.

f) Principio de gestión del riesgo: se deberá implantar un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TIC.

g) Principio de la seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema.

h) Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los activos TIC deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

i) Principio de concienciación y formación: se llevarán a cabo iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información se refiere. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

j) Principio de prevención, detección, respuesta y conservación: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC, así como, en caso de que produzcan, a restaurar la información y servicios afectados y garantizar la conservación de los datos e información.

k) Principio de vigilancia continua y reevaluación periódica: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico.

l) Principio de seguridad en el ciclo de vida de los activos TIC o líneas de defensa: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control .

m) Principio de diferenciación de responsabilidades: la responsabilidad de la seguridad de los sistemas estará diferenciada de la responsabilidad del servicio y de la información. Los roles y responsabilidades de cada una de estas funciones deberán quedar debidamente acotadas y reflejadas documentalmente.

5.2. Requisitos Mínimos de Seguridad

Esta Política de seguridad se establece además a través de la aplicación de los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad: La estructura organizativa para la gestión de la seguridad de la información será

competente para mantener, actualizar y hacer cumplir, la Política de Seguridad de la Información de esPublico, así como para garantizar la implantación del proceso de seguridad en la organización.

b) Análisis y gestión de los riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

c) Gestión del personal: 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.

d) Profesionalidad: La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. El personal de la empresa que atiende, revisa y audita la seguridad de los sistemas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables. Se exigirá, de manera objetiva y no discriminatoria, que los prestadores de servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

e) Autorización y control de los accesos: 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.

f) Protección de las instalaciones: 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.

g) Adquisición de productos o servicios de seguridad: En la adquisición de productos de seguridad podrá ser exigible la certificación de la funcionalidad de seguridad relacionada con el objeto de dicha adquisición, aplicando el principio de proporcionalidad y de profesionalidad.

h) Mínimo Privilegio: los sistemas de información deberán diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño.

i) Seguridad por defecto: La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

j) Integridad y actualización del sistema: Los sistemas de información de grupo esPublico serán diseñados y mantenidos bajo criterios técnicos, de eficiencia y de seguridad, teniendo en cuenta el proceso de autorización formal ante las modificaciones o alteraciones de los distintos componentes, equipos, software o cualquier elemento de dichos sistemas.

k) Protección de la información almacenada y en tránsito: Se establecerán mayores requisitos para proteger la información almacenada en entornos de mayor incertidumbre como equipos portátiles, dispositivos periféricos, soportes de información y comunicaciones en redes abiertas o de cifrado débil.

l) Prevención ante otros sistemas de información interconectados: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de los sistemas y sus conexiones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad y privacidad.

m) Registro de actividad y detección de código dañino: Se implantarán las medidas y herramientas necesarias para registrar las actividades de los

usuarios, así como detectar y clasificar las amenazas a través de la monitorización de los equipos, ya sean de usuario o servidores.

n) Incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

o) Continuidad de la actividad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de los procesos de negocio, de acuerdo con las necesidades de nivel de servicio comprometidas.

p) Mejora continua del proceso de seguridad: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

6. Organización de la seguridad TIC

6.1. Responsabilidad general

La preservación de la seguridad TIC será considerada objetivo común de todo el personal de esPublico, siendo responsables del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

En caso de incumplimiento de las directrices y normativas de seguridad indicadas en la presente Política y las obligaciones derivadas de ellas, el grupo esPublico se reserva el derecho de aplicar las medidas disciplinarias correspondientes establecidas en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, así como en el Convenio Colectivo que resulte de aplicación.

A continuación, debido a su relevancia en la implementación de la seguridad, se desarrollan los roles y responsabilidades asignados dentro del grupo esPublico para la correcta gestión de la seguridad.

6.2. Responsables

Responsable de seguridad

Es la persona encargada de las funciones de coordinación, gobierno, supervisión, formación y concienciación en materia de seguridad.

Su nombramiento será potestad del Comité de Seguridad de esPublico.

Responsable de información y servicio

Define los requisitos sobre el nivel de protección y seguridad de la información que se va a tratar, así como de los servicios prestados.

Responsable del sistema

Tiene la responsabilidad operativa de los recursos TIC. Se encarga de que se desarrolle, opere y mantenga el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

6.3. Comité de Seguridad TIC

Se crea el Comité de Seguridad de esPublico, de carácter transversal para la coordinación y gobierno en materia de seguridad en el ámbito del grupo.

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

Serán funciones propias del Comité:

a) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en seguridad TIC.

b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.

c) Elevación de propuestas de revisión del marco normativo de seguridad TIC al órgano competente para su reglamentaria tramitación.

d) Establecimiento de directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad TIC.

e) Supervisión y aprobación del nivel de riesgo y de la toma de decisiones en la respuesta a incidentes de seguridad que afecten a los activos TIC.

f) Definición y aprobación del modelo de relación con los Comités de Seguridad TIC de las entidades incluidas en el ámbito de aplicación de la Política.

g) Toma de decisiones en caso de contingencia que afecte a la seguridad de los sistemas de información o que suponga un riesgo para la continuidad de negocio de esPublico.

Las labores de soporte al Comité serán realizadas por el Responsable de Seguridad TIC y la Oficina de Seguridad TIC.

6.4. Oficina de Seguridad TIC

La Oficina de Seguridad TIC se corresponde con el departamento de Cumplimiento Normativo. Colaborará con las Áreas de Operaciones y Seguridad de esPublico Sistemas para el desempeño de sus funciones:

La Oficina de Seguridad TIC tendrá las siguientes atribuciones:

a) Definición del planteamiento técnico y operativo de los objetivos, iniciativas y planes estratégicos en seguridad TIC, de acuerdo con las directrices del Comité de Seguridad TIC.

b) Elaboración de propuestas relativas a la revisión del marco normativo de seguridad TIC.

c) Coordinación para el desarrollo de proyectos del grupo esPublico en materia de seguridad de la información.

d) Participación en el diseño de proyectos iniciados en cualquier área del grupo para la definición de los requisitos y especificaciones de seguridad que deben cumplir.

e) Participación en la gestión, control y coordinación en caso de incidencia que pueda afectar a la continuidad de negocio.

f) Elaboración de informes y propuestas de cumplimiento legal y normativo.

g) Elaboración de informes sobre el nivel de seguridad TIC de los activos.

h) Reporte al Comité Seguridad TIC de informes periódicos sobre el estado de la Seguridad TI de la organización.

La Oficina de Seguridad TIC se regirá por esta Política.

7. Desarrollo de la Política de Seguridad

7.1. Instrumentos del desarrollo

La Política de Seguridad de la Información de esPublico se desarrollará por medio de instrucciones de servicio y circulares que afronten aspectos específicos. Dichas instrucciones y circulares podrán adoptar alguna de las siguientes modalidades:

Se usarán los siguientes instrumentos:

- **Normativas de seguridad:** Uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.
- **Procesos:** Concretan los flujos de trabajo que deben seguirse para la realización de tareas, indicando lo que hay que hacer, paso a paso, pero sin entrar en detalles (no se incluirían por ejemplo nombres de proveedores, ni marcas comerciales, comandos o similar).
- **Instrucciones técnicas (IT) / Políticas de configuración:** Desarrollan los Procedimientos llegando al máximo nivel de detalle (pudiendo llegar a indicar por ejemplo, nombre de proveedores, marcas comerciales o comandos técnicos empleados para la realización de la tarea).

La normativa de seguridad estará disponible para todo el personal de la organización.

7.2. Aprobación de las normativas

En toda la organización, la aprobación de las normas de seguridad se hará de acuerdo con lo dispuesto en la presente Política.

7.3. Sanciones previstas por incumplimiento

Del incumplimiento de la Política de Seguridad de la Información y normativas o Instrucciones que la desarrollan podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en la Ley del Estatuto de los Trabajadores y en el Convenio Colectivo aplicable sobre régimen disciplinario de los empleados.

8. Concienciación y Formación

esPublico desarrollará medidas de concienciación y formación para todos sus empleados con el objetivo de adquirir conciencia y sensibilidad respecto a la seguridad de la información tratada en todas las actividades y servicios de esPublico.

9. Análisis y Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando ocurra un incidente grave de seguridad.

10. Clasificación de la información

Se desarrollará una Normativa de Clasificación de la Información de esPublico, de forma que se identifiquen los distintos tipos de información, en base a su sensibilidad, determinando las acciones permitidas y prohibidas sobre cada nivel de clasificación.

11. Datos de Carácter Personal

Será de aplicación lo contemplado en el RGPD y lo dispuesto en la legislación nacional a tales efectos.

Cada departamento se encargará de gestionar y mantener la seguridad referente a los datos de carácter personal incluidos en las operaciones de tratamiento que a tal efecto sean de su responsabilidad. Para ello, se impartirá formación en este sentido.

Todos los sistemas de información de esPublico se ajustarán a los niveles de seguridad requeridos por esta normativa.

12. Cumplimiento

12.1. Cumplimiento por parte del personal

Todo el personal de esPublico tiene la obligación de conocer y cumplir la presente Política, así como todas las normativas y procesos del SIG que puedan afectar a sus funciones, siendo cada persona responsable del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

esPublico, a través del Departamento de Cumplimiento Normativo, es responsable de la comunicación de esta Política y demás normativa , así como de disponer de los medios necesarios para que todo el personal las conozca de forma efectiva, en especial, las que puedan afectar a sus funciones.

Esta Política de seguridad, las normativas y procesos del SIG se encuentran disponibles para su consulta en la intranet de esPublico.

12.2. Cumplimiento por terceras partes

Las terceras partes que presten servicio a esPublico o manejen información responsabilidad de esPublico deberán cumplir con lo establecido en esta Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. En particular, las terceras partes deberán poner en conocimiento de esPublico cualquier incidencia de la que tengan conocimiento y que pueda afectar a un sistema de información y/o la información que se trata o los servicios que se prestan.

Se fomentará que el personal de terceros está adecuadamente concienciado en materia de seguridad y privacidad, al menos al mismo nivel que el establecido en esta Política.

13. Revisión de la Política

Esta política será revisada al menos una vez al año y siempre que haya cambios relevantes que afecten a la organización interna, con el fin de asegurar que ésta se adecua a la estrategia, necesidades u obligaciones de la organización.

La Política será aprobada por el Comité de Seguridad y difundida para que la conozcan todas las partes afectadas.

En caso de conflictos o diferentes interpretaciones de esta Política se recurrirá al Comité de Seguridad para su resolución.