PÚBLICO

CENTRO TECNOLÓGICO DEL NOTARIADO

Política General de Seguridad

v2.0

Control documental

Título del documento:	Política General de Seguridad
Tipo de documento:	Política
Nombre del fichero:	Política Seguridad Información v2.0.pdf
Versión:	2.0
Estado:	Aprobado
Confidencialidad:	Público
Fecha:	20/08/2024
Autor:	Oficina de Seguridad

Revisión, Aprobación		
Revisado por:	Responsable de Seguridad	Fecha: 01/10/2024
Aprobado por:	Comité de Seguridad	Fecha: 04/10/2024

Historial de cambios			
Versión	**Fecha**	**Descripción de la acción**	**Páginas**
0.1	04/02/2014	Primera versión de la política.	5
1.0	12/09/2012	Incorporación de modificaciones sugeridas durante su revisión.	5
1.1	06/03/2019	Cambio en el control documental para adaptarlo a los requisitos de la evaluación *Common Criteria*.	5
1.2	10/10/2019	Ajuste de la política de seguridad para dar cobertura al SGSI alineado a ISO27001.	6
1.2	06/11/2020	Revisión de la vigencia del documento. No es necesaria actualización	6
1.3	01/09/2021	Ajuste de la política para incorporar los requisitos de los sistemas de información afectados por el ENS.	Todo
1.4	23/01/2023	Actualización por necesidades de 27001:2022 y 27002:2022	Todo
2.0	20/08/2024	Adaptación a la nueva imagen corporativa. Añadidos apartados para la gestión de excepciones y el análisis de contexto.	Todo

Índice

1. Roles y Responsabilidades

Rol	Responsabilidad
Responsable SGSI / Responsable de Seguridad	Revisar los objetivos de seguridad y revisar que el presente documento se encuentre actualizado. Revisar los controles de seguridad y verificar que son asumibles por la Organización.
Dirección	Aprobar el presente documento. Verificar que la política de seguridad está alineada con negocio.
Toda la Organización	Velar por el cumplimiento de la política de seguridad.
Proveedores	Velar por el cumplimiento de la política de seguridad

2. Objetivos

El objetivo de esta política es proteger los activos de información del Centro Tecnológico del Notariado (CTNotariado), en adelante la Organización, de amenazas internas, externas, intencionadas o accidentales, minimizando el riesgo mediante una gestión formal de este; lo que desemboca en la implantación de controles que reduzcan su impacto potencial, tales como la prevención y respuesta ante incidentes.

Esta Política será de aplicación para todo el Sistema de Gestión de la Seguridad de la Información (SGSI). Adicionalmente, para los sistemas de información en el alcance del Esquema Nacional de Seguridad (ENS) se aplicará lo dispuesto en la "Política de Seguridad para los Sistemas de Información afectados por el ENS".

Por su carácter de Política General, es de obligado conocimiento y cumplimiento para todo el personal de la Organización de todas las áreas, departamentos y direcciones, así como en sus relaciones internas y con otras organizaciones y/o colaboradores.

La Dirección espera así mismo que esta política sea promovida de forma activa por todos los que trabajen o actúen en nombre y/o representación de la Organización.

3. Política de Seguridad de la Información

La Seguridad de la información es el conjunto de procesos y medidas, tanto técnicas como organizativas, destinadas a proteger y preservar la información en sus tres dimensiones principales, siendo éstas:

- Disponibilidad:
    - Los activos de información, y aquellos activos que los soportan, deben estar accesibles para los usuarios autorizados siempre que se necesiten (en la forma y tiempo requeridos).
    - La organización debe ser capaz de responder diligentemente a incidentes que afecten la disponibilidad de los activos.
- Confidencialidad:

    - Los activos, en particular la información, sólo deben ser accesibles a los usuarios autorizados.
    - Deben existir medidas que prevengan el acceso no autorizado, ya sea intencionado o accidental, a los activos.
- Integridad:
    - Se debe proteger la exactitud y completitud de la información y los procesos asociados, como procesos de tratamiento, comunicación y almacenamiento
    - Deben existir medidas que prevengan la modificación o destrucción, total o parcial, accidental o intencionada, de los activos.

Con este propósito, en relación a la seguridad de la información en la organización:

- El presente documento establece el compromiso para garantizar la seguridad de los activos de información de la Organización .
- Del mismo modo, el presente documento se compromete a cumplir los objetivos de seguridad indicados en el documento de objetivos del SGSI
- La seguridad de la información establecida debe asegurar que el SGSI consigue los resultados previstos por la Organización
- La seguridad de la información debe de cumplir con los requerimientos legales y normativos aplicables, y alinearse con los estándares y buenas prácticas internacionalmente reconocidos. Se toma como base el conjunto de estándares ISO 27000, en concreto los controles se han diseñado siguiendo las recomendaciones del estándar ISO 27002. Para los sistemas de información afectados por el ENS se añaden las medidas de seguridad definidas en el Anexo II del ENS de acuerdo con la clasificación del sistema.
- La seguridad de la información debe de entenderse como un proceso definido e integral orientado a la mejora continua y enmarcado dentro del ciclo de *PDCA* (Planificar, Hacer, Verificar y Actuar).
- La dirección de la Organización manifiesta su soporte a lo establecido en la presente política, así como a las medidas concretas que se deriven, con el objetivo de preservar la seguridad de los activos de información.
- La seguridad de la Información debe de trasladar los principios mencionados a un Cuerpo Normativo de Seguridad de la Información, que establecerá las directrices y medidas de Seguridad de la Información a cumplir en la Organización en sus diferentes ámbitos. Es por ello que la Organización dispone de las políticas, estándares, guías, normativas y procedimientos necesarios para dar cumplimiento a la presente política y sus objetivos descritos en la sección 6 de este documento.
- Los documentos de normativa de seguridad de la Organización detallan el conjunto de directrices y principios que se deben seguir para el alineamiento con los requerimientos de seguridad de la organización. La mayoría de los controles se alinearán con estos documentos.
- Todos los empleados internos y externos deben cumplir con la presente política, así como el conjunto de controles que la implementen. Se llevarán a cabo las acciones necesarias para su divulgación. El no cumplimiento de la presente política puede suponer medidas disciplinarias de diversa índole, siempre de forma proporcional a la infracción, lo que incluye la revocación de empleo en los casos más graves, en los que se hayan perpetrado acciones

que ataquen directamente a la confidencialidad, integridad o disponibilidad de los activos de la empresa

- El comité de seguridad revisará periódicamente la presente política, y velará por el desarrollo, implantación, mantenimiento y revisión de las políticas, estándares, guías, normativas y procedimientos que dan cumplimiento con la política.
- Todos los empleados deben notificar a su superior o al comité de seguridad cualquier violación de la política que detecten.

La Dirección de la Organización ha establecido las líneas de la Política de Seguridad de la información, al mismo tiempo que manifiesta su apoyo y compromiso en todo lo relativo a la seguridad de la información; aprobando, publicando y manteniendo la presente política, lo que incluye revisiones periódicas; y aplicable a toda la Organización. Cualquier excepción de lo establecido aquí, deberá ser autorizada formalmente por la Dirección.

4. Análisis del contexto

De manera continua la Organización identificará las necesidades y expectativas de las partes interesadas en su actividad y del entorno en el que ejerce sus actividades para determinar los requisitos de seguridad aplicables. Esta actividad se desarrollará de acuerdo a la “Norma de análisis de contexto”.

5. Gestión de riesgos

Todos los sistemas de información sujetos a esta política deberán disponer de un análisis de riesgos y de un plan de tratamiento de riesgos, en los que se evaluarán los riesgos a los que están sujetos los sistemas y las medidas de seguridad aplicadas para mitigarlos. Este análisis se realizará:

- Anualmente.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra una incidencia grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los criterios y las actividades del proceso de análisis de riesgos, el Comité de Seguridad de la Información aprobará una metodología y procedimientos para el análisis de riesgos.

6. Desarrollo de la Política de Seguridad de la Información

Esta política se desarrollará mediante normativas, guías y procedimientos de seguridad.

Toda esta documentación estará a disposición de todo el personal y entidades externas afectadas. Toda la normativa de seguridad estará publicada en la intranet corporativa, en particular, dentro de la página “Normativa de Seguridad” del espacio “Oficina de Seguridad” en del gestor de conocimiento Confluence. En este espacio se enlazarán las normativa y procedimientos, cuyos contenidos mínimos cubrirán los siguientes puntos:

- Normativa general que complementa o desarrolla el marco organizativo de la Seguridad (apartado 6.1 de la página “Normativa de Seguridad”): en el que se definen áreas o aspectos de la seguridad a tener en cuenta, caso del Teletrabajo, Firma electrónica, gestión de Recursos Humanos, gestión de soportes, entre otros.
- Gestión de Activos (apartado 6.2 de la página “Normativa de Seguridad”): que define como identificar los activos de la organización y definir las responsabilidades de protección adecuadas
- Control de Accesos (apartado 6.3 de la página “Normativa de Seguridad”): que define cómo limitar el acceso a los recursos de tratamiento para prevenir el acceso no autorizado, garantiza el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios
- Cifrado (apartado 6.4 de la página “Normativa de Seguridad”): para garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información
- Protección de las Instalaciones (apartado 6.5 de la página “Normativa de Seguridad”): que establece las directrices para prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.
- Seguridad de las Operaciones (apartado 6.6 de la página “Normativa de Seguridad”): para asegurar el funcionamiento correcto de las instalaciones de tratamientos de información, están protegidos contra el malware, evitar la pérdida de datos, registrar eventos y generar evidencias, asegurar la integridad del software en producción, reducir riesgos resultantes de la explotación de las vulnerabilidades técnicas y minimizar el impacto de las actividades de auditoría en los sistemas operativos.
- Comunicaciones (apartado 6.7 de la página “Normativa de Seguridad”): para asegurar la protección de la información en las redes y los recursos de tratamiento de la información
- Adquisición, desarrollo y Mantenimiento de Productos (apartado 6.8 de la página “Normativa de Seguridad”): para garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida
- Gestión de proveedores (apartado 6.9 de la página “Normativa de Seguridad”): para asegurar la protección de los activos de la organización que sean accesibles a los proveedores y mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.
- Gestión de Incidencias de seguridad (apartado 6.10 de la página “Normativa de Seguridad”): para asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad.
- Cumplimiento regulatorio (apartado 6.12 de la página “Normativa de Seguridad”): para evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

7. Gestión de excepciones

Toda exención o excepción de la aplicación de esta Política de Seguridad deberá ser solicitada por el correspondiente responsable del servicio, validada por el Responsable de Seguridad y aprobada, si procede, por el Comité de Seguridad.

Este procedimiento se desarrollará de acuerdo a la “Norma de Gestión de Excepciones de Seguridad” en la que se determinarán los procesos y tareas a seguir para el registro, la aprobación, la revisión y cancelación de las excepciones de seguridad.

CONSEJO GENERAL
DEL NOTARIADO