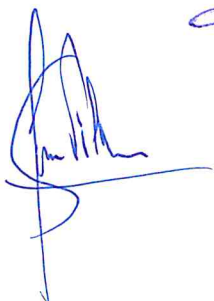


Losán

SISTEMA DE CUMPLIMIENTO NORMATIVO

Política de Seguridad IT

Aprobado:
Dirección General
Consejo de Dirección Corporativa



Fecha: 18/01/2024
Versión II

CONTROL MODIFICACIONES				
Versión	Fecha	Aprobador	Autor	Resumen de Cambios
I	01/03/2023	Dirección General	Comité de Cumplimiento	Original
II	18/01/2024	Dirección General	Comité de Cumplimiento	Cambio imagen corporativa

Índice:

- 1.- Aprobación y entrada en vigor
- 2.- Introducción
- 3.- Alcance
- 4.- Marco Normativo
- 5.- Cumplimiento de los principios de seguridad de la información
- 6.- Objetivos de seguridad de la información
- 7.- Datos de carácter personal
- 8.- Desarrollo de la Política de Seguridad de la Información
- 9.- Terceras partes

1.- Aprobación y entrada en vigor

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2.- Introducción

LOSÁN depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar 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 consecución de los objetivos.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en el proceso de diseño para proyectos de TIC.

3.- Alcance

Esta Política se aplicará a los sistemas de información de aplicación global y directa para todas las sociedades españolas que integran LOSÁN y que se incluyen en el Sistema de Cumplimiento Normativo, con independencia de su ubicación geográfica.

4.- Marco normativo

La base normativa que afecta al desarrollo de las actividades y competencias de LOSÁN en lo que a sistemas de información se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los mismos, está constituida por la normativa de protección de datos personales y demás normativa sectorial que pueda resultar de aplicación.

Las normas que constituyen dicho marco se encuentran recogidas en un registro al efecto, el cual se mantiene actualizado.

5.- Cumplimiento de principios de seguridad de la información

La presente Política tiene como objetivo preservar los tres conceptos básicos de la Seguridad de la Información. La confidencialidad previniendo la divulgación no autorizada de la información sobre nuestra organización. La integridad, supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.

El objetivo de la integridad es prevenir modificaciones no autorizadas de la información. La disponibilidad supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. El objetivo es necesario prevenir interrupciones no autorizadas de los recursos informáticos.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

Alcance estratégico: Para conformar un marco de trabajo estable y eficaz, la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la sociedad, y de esta forma estar integrada con el resto de las estratégicas.

Gestión de riesgos: La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables, siendo parte esencial del proceso de seguridad de la información. Gracias al despliegue de medidas de seguridad se conseguirá la reducción de estos niveles obteniendo un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.

Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

Seguridad integral: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.

Mejora continua: Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, se reevaluarán y actualizarán periódicamente todas las medidas adoptadas para adecuar su eficacia a la constante evolución de los riesgos. Una vez identificadas las vulnerabilidades, la organización deberá aplicar las medidas correctoras necesarias.

Seguridad por defecto: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

Además de aplicar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros.

6.- Objetivos de seguridad de la información

LOSÁN establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestión de activos de información: Los activos de información se encontrarán inventariados y categorizados y estarán asociados a un responsable
- Seguridad ligada a las personas: 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 su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- Seguridad física: 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.
- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. 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.
- Control de acceso: 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.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: 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.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.
- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

7.- Datos de carácter personal

LOSÁN solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

LOSÁN publicará en su página web su Política de Privacidad.

8.- Desarrollo de la Política de Seguridad de la Información

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al sistema de gestión de seguridad de la información.

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: constituido por la presente Política de Seguridad de la Información y el Código Telemático.

b) Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores.

c) Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

La revisión anual de la presente Política corresponde al Responsable de Seguridad de la Información proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

9. Terceras Partes

Cuando LOSÁN preste servicios a otras organizaciones, o maneje información de otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información. LOSÁN 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 la organización lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando LOSÁN utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y del Código de Telemático existente que atañe 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.

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 que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe deberá ser aprobado por la Dirección General, con carácter previo al inicio de la relación con la tercera parte.
