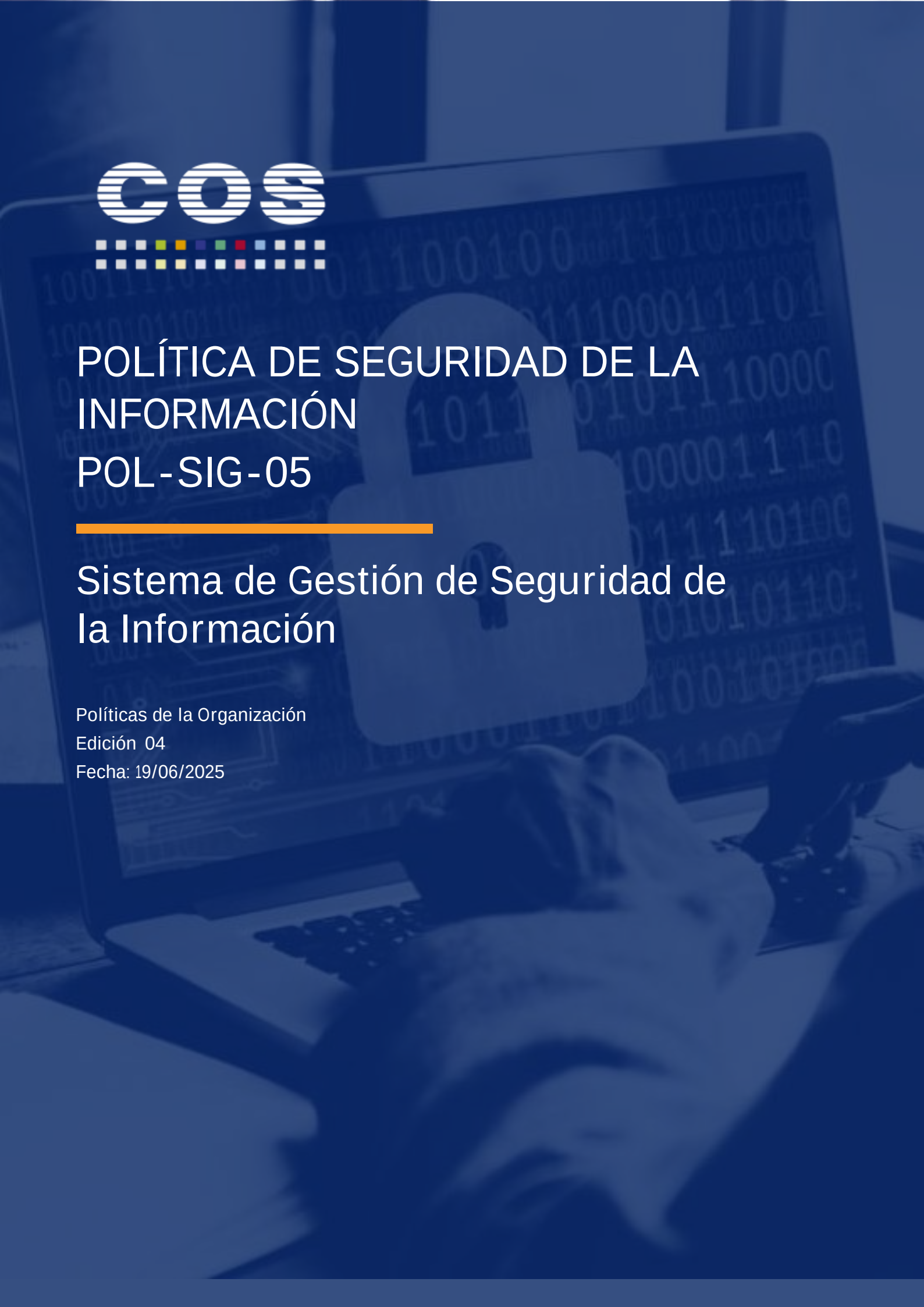
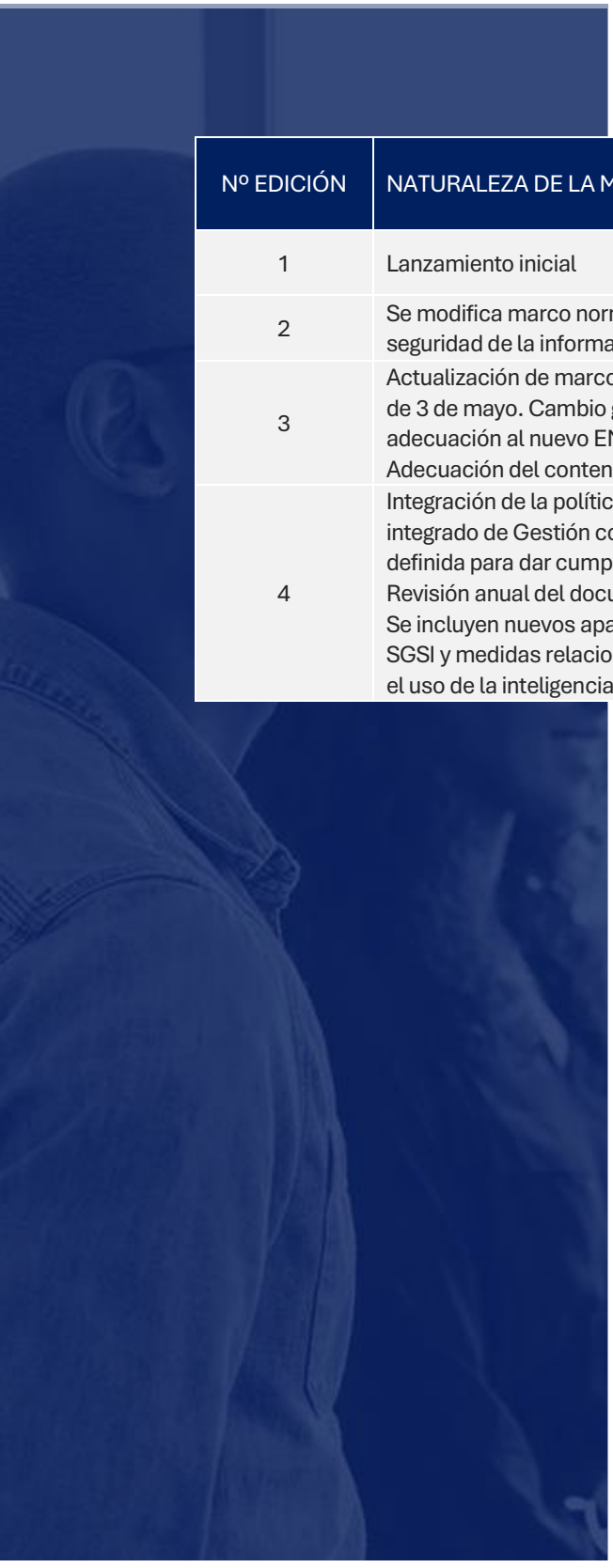


POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
POL-SIG-05

Sistema de Gestión de Seguridad de la Información

Políticas de la Organización
Edición 04
Fecha: 19/06/2025

Control de versiones



Nº EDICIÓN	NATURALEZA DE LA MODIFICACIÓN	FECHA
1	Lanzamiento inicial	10-11-2020
2	Se modifica marco normativo y apartado “Compromiso con la seguridad de la información”	14-02-2022
3	Actualización de marco normativo por nuevo Real Decreto 311/2022, de 3 de mayo. Cambio general del contenido del documento para la adecuación al nuevo ENS. Adecuación del contenido a ISO 27001:2022	25-09-2023
4	Integración de la política del seguridad de la información del Sistema integrado de Gestión con la Política de Seguridad de la información definida para dar cumplimiento al ENS. Revisión anual del documento. Se incluyen nuevos apartados: Términos y definiciones, Objetivos del SGSI y medidas relacionadas con la seguridad de los servicios cloud y el uso de la inteligencia artificial.	19/06/2025

Detalles del documento

Publicado por	COS MANTENIMIENTO S.A.
Área o Proceso	Seguridad de la Información
Nombre del documento	Política de Seguridad de la Información
Versión	4
Fecha	19/06/2025
Estado	Vigente
Autor	Responsable del SIG. Responsable de Seguridad
Revisado por	Comité de Seguridad de la Información
Aprobado por	Laura Gómez Moral Dirección General

Índice

CONTROL DE VERSIONES 2

OBJETO 5

ALCANCE 6

OBLIGACIONES DEL PERSONAL 6
INCUMPLIMIENTO DE LA PRESENTE POLÍTICA 6

TÉRMINOS Y DEFINICIONES 7

MISIÓN Y MARCO REGULATORIO 8

NUESTRA MISIÓN 8
MARCO REGULATORIO 8

LIDERAZGO Y COMPROMISO DE LA DIRECCIÓN 9

OBJETIVOS DEL SGSI 9

ORGANIZACIÓN DE LA SEGURIDAD 11

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN 11
RESPONSABLE DE LA INFORMACIÓN 12
RESPONSABLE DEL SERVICIO 12
RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN 12
RESPONSABLE DEL SISTEMA DE LA INFORMACIÓN 12
PROCEDIMIENTOS DE DESIGNACIÓN 13
FORMACIÓN Y CONCIENCIACIÓN 13

DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA 14

DATOS PERSONALES Y RIESGOS ASOCIADOS 15

DESARROLLO DE LA POLÍTICA DE SEGURIDAD 16

TERCERAS PARTES 19

APROBACIÓN Y REVISIÓN DE LA POLÍTICA 20

Objeto

El propósito de esta política es establecer los principios y directrices necesarias para garantizar la protección y gestión adecuada de la información en posesión de la organización. Esta política busca preservar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, minimizar los riesgos asociados a amenazas internas y externas, y cumplir con los requisitos legales, regulatorios y contractuales aplicables.

Esta política se encuentra alineada con las mejores prácticas establecidas por la Norma Internacional ISO/IEC 27001 y el RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Alcance

Esta política aplica a toda la información y a todos los sistemas de información propiedad, gestionados y operados por la organización, incluyendo aquellos provistos o gestionados por terceros. Es de **cumplimiento obligatorio** para todas las personas trabajadoras en COS, contratistas, personal temporal, socios comerciales y cualquier persona que tenga acceso a la información de la organización o a los recursos informáticos de la misma.

Obligaciones del personal

Todos y cada uno de los usuarios de los sistemas de información de COS son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros de COS tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad de la Organización.

Los miembros de COS recibirán formación 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 COS, 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.

Incumplimiento de la presente política

El incumplimiento de la presente Política podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

Términos y definiciones

- **SGSI**. Son las siglas del Sistema de Gestión de la Seguridad de la Información (regulado por la Norma UNE-ISO/IEC 27001), que es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **ENS**. Son las siglas del Esquema Nacional de Seguridad, Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- **Parte interesada**: Persona o grupo que tiene un interés en el desempeño o éxito de la organización.
- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser reveladas a personas y o empresas no autorizadas.
- **Integridad**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable en el momento que se requiera por la persona y o empresa autorizada
- **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a una persona y o empresa.
- **Autenticidad**: Propiedad de que una persona y o empresa que ha accedido y utilizado la información es lo que afirma ser.
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o **elemento** relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de riesgos**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Tratamiento del riesgo**: Proceso de gestión del riesgo mediante la implementación de controles y medidas que ayuden a evitarlo o mitigarlo.
- **Datos personales**: Cualquier información relacionada con una persona que permita identificarla o pueda servir para identificarla.

Misión y marco regulatorio

COS depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos de negocio. 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 a los servicios prestados.

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 implican que deben aplicar las medidas mínimas de seguridad, así como realizar un seguimiento continuo de los niveles de prestación de los servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La seguridad de la información 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.

Nuestra misión

COS es una compañía de servicios de tecnologías de información que opera en el mercado español, portugués y latinoamericano ofreciendo servicios especializados en la compra, venta, alquiler y mantenimiento de equipos informáticos multi-fabricante. Nuestra MISIÓN es mejorar continuamente nuestros servicios y soluciones tecnológicas para satisfacer las necesidades más exigentes de nuestros clientes, ayudándoles a focalizarse en su estrategia de negocio.

Marco regulatorio

Se toma como referencia básica en materia de Seguridad de la Información la normativa siguiente:

- Norma UNE-EN ISO 27001
- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.
- Ley 34/2002, de 11 de junio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley de Propiedad Industrial

Liderazgo y compromiso de la Dirección

La Dirección de COS manifiesta un fuerte compromiso con la gestión de la seguridad de la información y con el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI).

La Dirección de COS se compromete expresamente a:

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de la Organización.
- Asegurar que los recursos necesarios para el SGSI estén disponibles.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del SGSI.
- Asegurar que el SGSI consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI.
- Promover la mejora continua del Sistema de Gestión.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.
- Asegurar que los requisitos acordados con los clientes y otras partes interesadas se cumplen continuamente y sin excepción
- Cumplir todos los requisitos legales aplicables en materia de seguridad de la información y protección de datos de carácter personal.
- Asegurar que todos las personas trabajadoras y colaboradores de COS conocen sus funciones y obligaciones de seguridad y son responsables de cumplirlas.
- Formar y concienciar a todos los empleados en materia de seguridad de la información.

La presente Política constituye el marco de referencia mediante el cual COS define las directrices de protección eficaz de la Información gestionada y tiene los siguientes principios fundamentales:

- Confidencialidad. La información debe ser conocida exclusivamente por las personas autorizadas.
- Integridad. La información debe ser completa, exacta, válida y no sujeta a manipulaciones.
- Disponibilidad. La información debe ser accesible por los usuarios autorizados en todo momento y garantizar su persistencia ante cualquier eventualidad.
- Autenticidad. La información debe ser auténtica.
- Trazabilidad. Posibilidad de realizar seguimiento de los accesos a la información y sus cambios.

Objetivos del SGSI

Anualmente, la Dirección aprobará objetivos relacionados con el SGSI que serán cuantificables para evaluar el grado de consecución de los mismos y establecer las medidas oportunas en el caso de que no se alcancen.

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del SGSI.
- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, así como la protección de los datos personales.

- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
- Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará tomando en cuenta los siguientes elementos:

- Lo que se va a hacer.
- Los recursos necesarios.
- El responsable.
- Plazo de consecución.
- Indicadores para evaluar el resultado/cumplimiento

Todo ello quedará reflejado en el Programa de Gestión (COS-64) que la Dirección aprueba cada año junto a los Objetivos anuales.

Organización de la seguridad

La implantación de la Política de Seguridad en COS requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado.

Como parte de la presente Política, cada rol especifico debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

- Comité de Seguridad de la Información
- Responsable del Servicio
- Responsables de la Información
- Responsable de Seguridad de la Información
- Responsable del Sistema

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

Como principio básico los siguientes pares de funciones deberán de ser ejecutados por diferentes roles que no podrán recaer sobre la misma persona / equipo:

- Desarrollo de operación del sistema.
- Configuración y mantenimiento del sistema de operación.
- Auditoría o supervisión de cualquier otra función.

Comité de seguridad de la información

La seguridad de la Información es una responsabilidad organizativa que es compartida con la Dirección General. En consecuencia, la Dirección General de **COS** promueve la composición de un Comité de Seguridad de la Información, en aras de establecer una vida definida y el palpable apoyo a las iniciativas de seguridad.

Dicho Comité está compuesto los siguientes cargos y personas:

- Presidencia: Dirección General
- Responsable de Seguridad
- Asesor jurídico
- Director Financiero
- Director de Operaciones
- Director de Tecnología

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales;
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dichos activos;
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
- Principales incidencias en la Seguridad de la Información;
    - Elaboración y actualización de planes de continuidad
    - Cumplimiento y difusión de las Políticas de Seguridad

Responsable de la Información

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos
- Determina los niveles de seguridad de la información.

Responsable del Servicio

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad de la información.

Responsable de Seguridad de la Información

Responsable de la definición, coordinación, implantación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos de la Dirección General.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de COS.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
    - La estrategia de seguridad de la información definida por el Comité de Seguridad.
    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de COS y normativa de desarrollo.
- Supervisar (como responsable último) los incidentes de seguridad informática producidas en COS.
- Difundir en COS las normas y procedimientos contenidos en la Política de Seguridad de la Información de COS y normativa de desarrollo, así como las funciones y obligaciones de todo COS en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables tales como el RGPD.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de COS.

Responsable del Sistema de la información

Es responsable último de asegurar la ejecución de medidas para asegurar los activos y servicios de los Sistemas de Información, que soportan la actividad de **COS**, conforme a los objetivos estratégicos de **COS**.

Las funciones del Responsable del Sistema de la Información son las siguientes:

- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de COS, conforme a la estrategia de seguridad definida.
- Establecer la actuación de los Responsables Técnicos Informáticos, en los distintos entornos de seguridad que se designen.
- Garantizar la actualización del inventario de activos de Sistemas de Información de COS.
- Asegurar que existe el nivel de seguridad informática adecuado para cada uno de los activos inventariados, coordinando el correcto desarrollo, implantación, adecuación y operación de los controles y medidas destinados a garantizar el nivel de protección requerido.

- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en COS.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- Mantener y actualizar las directrices y políticas de seguridad de los Sistemas de Información y normativa asociada.

La relación de personas que desempeñan estas funciones quedará recogida en el correspondiente acta de designación, así como en la herramienta interna de RRHH, en la que se asociará el puesto a la persona que lo ostenta.

Procedimientos de designación

La designación se lleva a cabo en el seno del Comité de Dirección, quien, en caso necesario, podrá delegar en el responsable del Sistema de Gestión.

El nombramiento quedará reflejado en un acta, que deberá ser firmada por la Dirección (persona que designa) así como por la persona que recibe el nombramiento.

Tanto los nombramientos como la posible resolución de conflictos correrán a cargo de la Dirección Ejecutiva.

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

Formación y concienciación

Las acciones específicas de concienciación y formación relativas al ENS se gestionan, sin distinción con las del Sistema de Gestión de Seguridad de la Información, por el Departamento de RRHH.

La sistemática seguida por para la detección de necesidades de formación y concienciación y para darles curso se describe en el procedimiento “PR-SIG-07-Formación y competencia del personal”.

Directrices para la estructuración de la documentación de seguridad del Sistema

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad de la Información.

  Documento de obligado cumplimiento por todo el personal, interno y externo, de la Organización, recogido en el presente documento y aprobado mediante Decreto de la Organización.

- Segundo nivel: Normativas y Procedimientos de Seguridad.

  De obligado cumplimiento conforme al ámbito organizativo, técnico o legal correspondiente, desarrollados por COS en el marco de su Sistema de Gestión en los que se han incluido los aspectos específicos del ENS.
  Para facilitar la trazabilidad entre las medidas de seguridad requeridas por el ENS y su implantación en COS en el marco del SGSI, se ha procedido a mapear las medidas de seguridad aplicables del Anexo II con los controles del Anexo A de ISO 27001 de acuerdo con la Guía de Seguridad (CCNSTIC 825).
  La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Responsable de Seguridad bajo la supervisión del Responsable del Sistema Integrado de Gestión.

- Tercer nivel: Instrucciones Técnicas relativas a la seguridad de la información.

  Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.
  La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable del Sistema de Información correspondiente, bajo la supervisión del Responsable de Seguridad. En caso de que los procedimientos afectaran a varios sistemas de información será responsabilidad del Responsable de Seguridad el aprobarlos.

- Cuarto nivel: Informes, registros y evidencias electrónicas.

  Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.
  La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito.

- Otra documentación

  Se podrá seguir en todo momento procedimientos, normas o instrucciones STIC así como guías CCN-STCI de las series 400, 500, 600 y 800.

Datos personales y riesgos asociados

COS trata datos de carácter personal siempre y cuando sean adecuados, pertinentes y no excesivos y éstos estén relacionados con el alcance y los fines para los que se han obtenido.

Los riesgos derivados del tratamiento son contemplados en el análisis general de riesgos, tomando como referencia la normativa general de protección de datos vigente, así como las categorías de datos tratados.

Todos los sistemas de información de COS se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado Marco normativo , de la presente Política de Seguridad de la Información.

Desarrollo de la política de seguridad

COS implementa medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categorización del sistema en cada caso.

La presente política de seguridad se establece de acuerdo con los principios básicos del Sistema de Gestión de Seguridad de la Información y, en cumplimiento del artículo 12 del Real Decreto ENS, se desarrolla aplicando los siguientes **requisitos mínimos**:

- **Organización e implantación del proceso de seguridad.**

La seguridad es un proceso compuesto por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema. Se prestará máxima atención a la concienciación de las personas involucradas en el proceso y sus líderes jerárquicos, para así evitar cualquier situación que pueda poner en riesgo la implementación del proceso de seguridad.

- **Análisis y gestión de los riesgos.**

Una correcta identificación y gestión de los riesgos a los que se encuentran sometidos los activos de información que sustentan los servicios de COS es primordial para la correcta toma de decisiones por parte del Comité Ejecutivo.

La Metodología de Análisis y Gestión de Riesgos empleado por COS está basada en MAGERIT versión 3. El procedimiento interno paras la gestión de riesgos está descrito en el procedimiento interno "*PR-SIG-29 Metodología Análisis Riesgos SGSI"*.

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información gestionada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

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

- **Gestión de personal y profesionalidad**

Todos los miembros de COS dentro del alcance del SGSI son formados y sensibilizados de manera continua, según las necesidades de su puesto. El proceso de formación y capacitación del personal es gestionado por RRHH y está regulado por el procedimiento interno "*PR-SIG-07 Formación y competencia del personal*". Así mismo, anualmente se llevan a cabo acciones de concienciación y sensibilización desde el área de Seguridad Interna conforme al procedimiento "*PR-SIG-08 Concienciación del personal*"

- **Autorización y control de los accesos.**

COS ha implementado mecanismos de control del acceso al sistema de información, limitándose a aquellos estrictamente necesarios y debidamente autorizados. El control de accesos a los Sistemas de COS está regulado por el procedimiento interno "*PR-SIG-34 Control de accesos*".

- **Protección de las instalaciones.**

COS ha implementado mecanismos de control de acceso físico, evitando el acceso físico no autorizado, así como daños a la información y los recursos, a través de perímetros de seguridad, controles físicos y protecciones generales en diferentes áreas. Todo ello regulado por el procedimiento interno "*PR-SIG-36 Seguridad física"*.

- **Adquisición de productos y servicios**

Para la adquisición de productos o servicios, COS tendrá en cuenta que estos productos/servicios han certificado la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en los que los requisitos de proporcionalidad con respecto a los riesgos asumidos no lo justifiquen, a juicio del Responsable de Seguridad. Ello incluye la adquisición de servicios Todo ello queda regulado en el procedimiento interno "*PR-SIG-33 Gestión de terceros"*.

- **Mínimo privilegio**

Los sistemas se diseñarán de una manera que garantice la seguridad predeterminada conforme al "*PR-SIG-34 Control de accesos*" de la siguiente manera:

a) El sistema proporcionará la funcionalidad mínima necesaria para que la organización alcance sus objetivos.
b) Las funciones de operación, administración y registro de la actividad serán las mínimas necesarias, y deben garantizar que sólo sean accesibles por las personas, o desde lugares o equipos autorizados. Podrán ser requeridas cuando sea apropiado restricciones de tiempo y facultades de puntos de acceso.
c) Las funciones del sistema operativo que no sean de interés serán eliminadas o desactivadas.
d) El uso ordinario del sistema debe ser simple y seguro, por lo que un uso inseguro requiere un acto consciente por parte del usuario.

- **Integridad y actualización del sistema**

COS ha implementado controles y evaluaciones de seguridad regulares (incluidas las evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de seguridad de los sistemas en relación con las especificaciones de los fabricantes, vulnerabilidades y actualizaciones que les afectan, reaccionando diligentemente para gestionar el riesgo en vista de su estado de seguridad. Asimismo, solicitará la revisión periódica por parte de terceros para obtener una evaluación independiente.

- **Protección de la información almacenada y en tránsito**

COS ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando se encuentra en entornos inseguros (portátiles, móviles, tabletas, medios de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios de trabajo habituales. Además, se utilizarán mecanismos de encriptación autorizados por el CCN acorde al nivel de sensibilidad de la información a proteger en cada caso.

COS ha definido los procedimientos internos "PR-SIG-47 Protección de la información", "PR-SIG-43 Gestión de soportes", "PR-SIG-45 Gestión de dispositivos móviles" y "PR-SIG-46 Protección de equipos".

- **Prevención ante otros sistemas de información interconectados.**

COS ha implementado una estrategia de protección basada en múltiples capas, consistente en medidas organizativas, físicas y lógicas, de modo que cuando una de las capas falla, el sistema implementado permite una reacción adecuada a los incidentes que no han podido evitar, reduciendo la probabilidad de que el sistema se vea comprometido en su conjunto y minimizando el impacto final en él.

Se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

- **Registro de la actividad y detección de código dañino**

COS ha habilitado registros de la actividad del usuario al retener la información necesaria para monitorear, analizar, investigar y documentar actividades inadecuadas o no autorizadas, permitiendo identificar en todo momento a la persona que actúa. Todo ello con el único fin de lograr el cumplimiento del objeto de este Real Decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar, a la imagen de los afectados, y de acuerdo con la normativa de protección de datos personales o laborales, y otras disposiciones aplicables.

Igualmente todos los sistemas de COS están protegidos para la detección de código dañino, tal como describe el procedimiento interno "PR-SIG-46 Protección de equipos".

- **Incidentes de seguridad**

COS ha implementado un proceso integral de detección, reacción y recuperación ante incidentes de seguridad de la información: "PR-SIG-48 Gestión de incidentes de seguridad".

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, COS implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que ha identificado como necesario, mediante una evaluación de amenazas y riesgos.

COS establece mecanismos para responder eficazmente a los incidentes de seguridad y además:
- Designa puntos de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (INCIBE-CERT).

- **Continuidad de la actividad**

COS, como empresa proveedora de servicios, considera esencial la disponibilidad y continuidad de su actividad. Es por ello que, dentro del marco del Sistema Integrado de Gestión así como del ENS, define el procedimiento "PR-SIG-24 Disponibilidad y continuidad de los servicios" así como el "Plan de Continuidad de Negocio" o PCN.

El PCN es probado a intervalos regulares según el calendario de pruebas con la finalidad de verificar que en caso de desastre, la recuperación es conforme a lo descrito en dicho Plan.

- **Mejora continua del proceso de seguridad**

El proceso de seguridad es mejorado continuamente conforme a los procesos de mejora continua del Sistema Integrado de Gestión mediante la aplicación de los principios básicos del ciclo de Deming "PDCA".

Terceras partes

Las empresas y organizaciones externas que con ocasión de su colaboración con COS para la prestación de un servicio, accedan o gestionen activos de información de COS o de sus usuarios, directa o indirectamente (en sistemas propios o ajenos), comparten la responsabilidad de mantener la seguridad de los sistemas y activos del COS, por lo que deberán asumir las siguientes obligaciones:

- No difundir ninguna información relativa a los servicios proporcionados a COS sin autorización expresa para ello.
- Informar y difundir a su personal las obligaciones establecidas en esta Política.
- Aplicar las medidas estipuladas por RGPD en el tratamiento de los datos personales responsabilidad de COS que traten por razón de la prestación del servicio.
- Aplicar los procedimientos para la gestión de seguridad relacionados con los servicios proporcionados a COS. Especialmente se deben aplicar los procedimientos relacionados con la gestión de usuarios, tales como notificaciones de altas y bajas, identificación de los usuarios, gestión de contraseñas, etc., en el sentido descrito en la presente política y normativa reguladora que sea de aplicación.
- Notificar cualquier incidencia o sospecha de amenaza a la seguridad de algún sistema o activo de COS a través de los mecanismos que se determinen, colaborando en la resolución de las mismas relacionados con los sistemas, servicios o personal de la propia entidad.
- Implantar medidas en sus propios sistemas y redes para prevenir la difusión de virus y/o código malicioso a los sistemas de COS. Específicamente, cualquier equipo conectado a la red corporativa de COS debe disponer de un antivirus actualizado preferiblemente de forma automática.
- Implantar medidas en sus propios sistemas y redes para prevenir el acceso no autorizado a los sistemas de COS desde otras redes. Entre otros, se deben aplicar las actualizaciones de seguridad en sus sistemas y se debe mantener un sistema cortafuegos para proteger las conexiones desde Internet y otras redes no confiables.

COS se reserva el derecho de revisar la relación con la entidad externa en caso de incumplimiento de las anteriores obligaciones.

Aprobación y Revisión de la política

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma.

Así mismo, la Política de Seguridad será aprobada por la Dirección General, quién dotará al SGSI de todas las herramientas precisas para asegurar que es conocida, comprendida, desarrollada y mantenida al día por todos los niveles de la organización, así como comunicada a todas aquellas personas que trabajan en nombre de COS.