Política de Seguridad

04/04/2022

Revisiones

Revisiones				
Estado	**Revisión**	**Descripción del Cambio**	**Autores**	**Fecha efectiva**
Publicado	0	Publicación inicial	Antonio Serra Francisco Araujo	15/06/2018
Publicado	1	Actualización de los elementos de la norma ISO22301, modificaciones menores.	Antonio Serra	22/01/2019
Publicado	2	- Se añaden los requisitos mínimos de Seguridad referentes al artículo 11 del Real Decreto 3/2010. - Se añade la referencia a los Servicios afectados por el Plan de Continuidad. - Se añade la referencia a la LOPDPGDD y se elimina la referencia a la LOPD.	Antonio Serra	16/05/2019
Publicado	3	Se modifica el proceso de actualización de la Política para garantizar que se distribuye y publica la misma versión en todas las plataformas.	Antonio Serra	2/06/2020
Publicado	4	Revisión previa a auditoría ENS, sin cambios.	Antonio Serra	01/06/2021
Publicado	5	Revisión previa a auditoría ENS. Se añaden al marco normativo: - Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los	Antonio Serra	03/07/2021

		servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (eIDAS) - Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia		
Publicado	6	Modificaciones varias como parte del PAC de la auditoría	Antonio Serra	22/07/2021
Publicado	7	Revisión previa a las auditorias ISO27001/ISO22301, sin cambios.	Antonio Serra	04/04/2022

ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 22 de julio de 2018 por la Dirección General y el Comité de Seguridad. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política. Este texto anula el anterior, que fue aprobado el día 1 de juniuo de 2021 por la dirección.

2. INTRODUCCIÓN

Costaisa Group 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, autenticidad, trazabilidad, 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 implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

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 pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

3. PREVENCIÓN

Los departamentos deben 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 los departamentos deben 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, los departamentos deben:

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

4. DETECCIÓN

Dado que los servicios se puede 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 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 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.

5. RESPUESTA

Los departamentos deben:

1. Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
2. Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
3. 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).

6. RECUPERACIÓN

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

7. ALCANCE

Esta política se aplica a todos los sistemas TIC de Costaisa Group y a todos los miembros de la organización, sin excepciones. Para ver los alcances específicos de cada una de las certificaciones de las empresas del grupo consultar el documento CS_MNPR_AlcanceSGSI/SGCN.

8. MISIÓN, VISIÓN Y VALORES

8.1 Misión

Costaisa Group pretende desarrollar un negocio de continuidad para contribuir a mejorar el tejido industrial y productivo.

• Mediante la consultoría organizativa y tecnológica ayuda a las empresas clientes a conseguir mayor éxito en su negocio.
• Garantiza la contratación de profesionales con calidad de empleo y continuidad en el puesto de trabajo.
• Proporciona beneficios a sus accionistas.
• Contribuye a mejorar el tejido industrial mediante el diseño, desarrollo e implantación de soluciones organizativas y tecnológicas.

8.2 Visión

Costaisa Group pretende convertirse en la consultora de referencia en los ámbitos en los que opera, y quiere que sus clientes la consideren su socio organizativo y tecnológico para sus proyectos estratégicos de negocio.

8.3 Valores

• Proximidad y confianza: su principal valor son los profesionales que forman los equipos de trabajo junto con sus clientes ejerciendo una consultoría de proximidad y afianzando relaciones de confianza.
• Voluntad de mejorar día a día: la competitividad se gana trabajando hacia la mejora continua, por este motivo ha creado un Sistema de Gestión de la Calidad para ajustar nuestros procesos a las exigencias del mercado.
• Actitud de desafío: la meta es conseguir los objetivos de sus clientes.

9. MARCO NORMATIVO

9.1 Sistemas de Información

9.1.1 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.1.2 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

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.1.3 L 34/2002 de 11 Jul. (Servicios de la sociedad de la información y de comercio electrónico).

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.1.4 Ley 9/2014, de 9 de mayo, de Telecomunicaciones.

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.1.5 OM PRE/2740/2007 de 19 Sep. (Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información)

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.1.6 Esquema Nacional de Seguridad

- Real Decreto 951/2015, de 23 de octubre, de modificación 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.

- 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.

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.1.7 Norma ISO27001 de Seguridad en los Sistemas de Información

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.1.8 Norma ISO20000 de Gestión de Servicios TI

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.1.9 Norma ISO22301 de Continuidad de negocio

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.1.10 Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (eIDAS)

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.1.11 Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Responsable: Dirección Técnica
Asesor Legal: Across Legal

9.2 Propiedad Intelectual

9.2.1 Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

Responsable: Administración
Asesor Legal: Brugueras, García-Bragado, Molinero & Asociados

9.3 Recursos Humanos

9.3.1 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

Responsable: Recursos Humanos
Asesor Legal: Brugueras, García-Bragado, Molinero & Asociados

9.3.2 Ley 3/2012, de 6 de julio, de medidas urgentes para la reforma del mercado laboral

Responsable: Recursos Humanos
Asesor Legal: Brugueras, García-Bragado, Molinero & Asociados

9.3.3 Convenio colectivo de Oficinas y Despachos

Responsable: Recursos Humanos
Asesor Legal: Brugueras, García-Bragado, Molinero & Asociados

9.3.4 Ley de Prevención de Riesgos Laborales (Ley 31/1995, de 8 de noviembre).

Responsable: Recursos Humanos
Asesor Legal: Brugueras, García-Bragado, Molinero & Asociados

9.3.5 Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia

Responsable: Recursos Humanos
Asesor Legal: Brugueras, García-Bragado, Molinero & Asociados

9.3.6 Real Decreto 625/2014, de 18 de julio, por el que se regulan determinados aspectos de la gestión y control de los procesos por incapacidad temporal en los primeros trescientos sesenta y cinco días de su duración.

Responsable: Recursos Humanos
Asesor Legal: Brugueras, García-Bragado, Molinero & Asociados

10. PROCEDIMIENTOS DE DESIGNACIÓN

La relación completa de comités y funciones se puede encontrar en la Normativa de Seguridad. Los cargos de Responsable de la Información, Responsable del Servicio y Responsable de Seguridad de la Información serán nombrados por la Dirección a propuesta del Comité de Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.
El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

11. COORDINACIÓN Y RESOLUCIÓN DE CONFLICTOS

El Comité de Seguridad será el órgano competente para coordinar y resolver cualquier conflicto en lo referente a la seguridad de los SSII para cualquier empresa del Grupo Costaisa.

12. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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. La Política será aprobada por el Comité de Seguridad y difundida para que la conozcan todas las partes afectadas.
En caso de modificación de la Política, se deberá garantizar su actualización en todos los medios en los que está publicada, tanto a nivel interno (InstMan, Redmine) como externo (páginas web de las empresas del grupo).

13. DATOS DE CARÁCTER PERSONAL

Costaisa Group trata datos de carácter personal. El Documento de Seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de Costaisa Group se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

14. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá regularmente, al menos una vez al año o cuando:

1. Cambie la información manejada
2. Cambien los servicios prestados
3. Ocurra un incidente grave de seguridad
4. 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 manejados 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.

15. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos:

- ISO27001 Seguridad de la Información
- Esquema Nacional de Seguridad (ENS)
- ISO22301 Continuidad de Negocio
- ISO20000 Gestión de Servicios TI
- Reglamento General de Protección de Datos (RGPD)

La Normativa de Seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas

de información y comunicaciones. La documentación estará disponible en la BBDD Notes de Instrucciones y Manuales:

Los principios básicos son los siguientes:

a) Organización e implantación del proceso de seguridad.
Se desarrollará en la Normativa de Seguridad vigente publicada en Instman.

b) Análisis y gestión de los riesgos.
Se desarrollará en el análisis de riesgos realizado cada año para la revisión por la dirección del SGSI. La metodología aplicada se explica en la instrucción.

c) Gestión de personal.
Se desarrollará en la Normativa de Seguridad vigente publicada en Instman.

d) Profesionalidad.
Se desarrollará en la Normativa de Seguridad vigente publicada en Instman, y en los manuales de funciones pertinentes de cada área/departamento.

e) Autorización y control de los accesos.
Se desarrollará en la Normativa de Seguridad vigente publicada en Instman.

f) Protección de las instalaciones.
Se desarrollará en la Normativa de Seguridad vigente publicada en Instman.

g) Adquisición de productos.
Se desarrolla en el manual CS_MNPR_Procedimiento de adquisición de componentes.

h) Seguridad por defecto.
Se recoge en los distintos manuales de bastionado de Sistemas, y en la Normativa de Seguridad.

i) Integridad y actualización del sistema.
Se recoge en el manual SIMNPR01_20180219_QVM_Remediación_Vulnerabilidades, y en los distintos manuales y procedimientos de Sistemas.

j) Protección de la información almacenada y en tránsito.
Se desarrollará en la Normativa de Seguridad vigente publicada en Instman. Al tratarse de información relativa a la salud de las personas estará siempre cifrada, según los pertinentes manuales de Explotación y Sistemas.
En la Normativa de Seguridad y en el documento del alcance del ENS se especifican los responsables de cada tipo de información y los niveles de seguridad requeridos.

k) Prevención ante otros sistemas de información interconectados.
Se gestionará siguiendo los manuales de sistemas

l) Registro de actividad.
La herramienta corporativa QRadar recoge y gestiona todos los registros, según los pertinentes manuales de Sistemas.

m) Incidentes de seguridad.
Se desarrollará en la Normativa de Seguridad vigente publicada en Instman.

n) Continuidad de la actividad.
Se desarrollará en el Plan de Continuidad, ME_MNPR_Business Impact Analysis BIA y en la Normativa de Seguridad vigentes publicados en Instman. La relación de servicios que se incluyen dentro del alcance del mismo como servicios gestionables por la continuidad de negocio de la organización se encuentran en el manual M-2198 CS_MNPR_AlcanceSGSI/SGCN.

o) Mejora continua del proceso de seguridad.
Como parte del SGSI y del SGCN, el Sistema se revisa íntegramente como mínimo una vez al año siguiendo el ciclo de Deming (Plan, Do, Check, Act).

16. OBLIGACIONES DEL PERSONAL

Todos los miembros de Costaisa Group tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de seguridad disponer los medios necesarios para que la información llegue a los afectados.
Todos los miembros de Costaisa Group atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros, 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.

17. TERCERAS PARTES

Cuando Costaisa Group preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
Cuando Costaisa Group utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.
Cuando algún aspecto de la Política 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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.
El seguimiento del servicio de los proveedores se trata en CS_MNPR_Procedimiento de seguimiento de SLAs con proveedores.