POLÍTICA DE SEGURIDAD ENS

Control de versiones

Versión	Fecha	Descripción	Aprobación
4	31.01.2023	Se completa lo relativo a los niveles de seguridad y las directrices para el acceso a la documentación.	Representante del administrador único
3	01.06.2022	Adecuación al RD 311/2022	Representante del administrador único
2	01.02.2021	Actualización de los requisitos mínimos de seguridad	Consejero Delegado
1	23.10.2020	Redacción Inicial	Consejero Delegado

Índice

1 MISIÓN Y ALCANCE

La misión y visión de la organización están recogidos en la "*Política Integrada de los Sistemas de Gestión*" que está publicada en la web de la organización.

Como parte de su política estratégica para el desarrollo de sus actividades, CONTACTEL TELERSERVICIOS S.A. *(en adelante CONTACTEL)*, ha desarrollado e implementado un *Sistema de Gestión Integrado (en adelante SGI)* que abarca calidad, medioambiente, seguridad de la información y continuidad del negocio, y que se encuentra basado en el análisis, la prevención y la mejora continua.

2 MARCO REGULATORIO

2.1 Identificación

La sistemática utilizada por **CONTACTEL** para la identificación, análisis y cumplimiento de la legislación y normativa vigentes se desarrolla en el procedimiento interno "*SGI - Manual del SGI*".

2.2 Datos de carácter personal

En el ámbito de los datos de carácter personal, **CONTACTEL** ha realizado la adecuación a la "*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*".

2.3 Esquema Nacional de Seguridad

En el ámbito del Esquema Nacional de Seguridad, está política está integrada por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica *(en adelante ENS)*.
- 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.

3 PRINCIPIOS Y DIRECTRICES

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son los marcados en el *artículo 5* del ENS, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, de manera que las amenazas existentes no se materialicen o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

3.1 Prevención

CONTACTEL evita que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos tienen implementadas 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, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **CONTACTEL**:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, los servicios monitorizan 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 8* del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el *Artículo 9* del ENS.

Están establecidos mecanismos de detección, análisis y reporte que llegan a los responsables regularmente y cuando se produce una desviación significativa de los parámetros preestablecidos como normales.

3.3 Respuesta

Se dispone de mecanismos para responder eficazmente a los incidentes de seguridad. El punto de contacto para las comunicaciones con respecto a incidentes es soporte@contactel.es. El protocolo para el intercambio de información relacionada con el incidente se establece por medio de los procedimientos internos "*Soporte – P Gestión de Incidencias*" y "*27001 – Brechas de seguridad*".

Las comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias *(INCIBE-CERT)* se desarrollan en el procedimiento interno "*SGI – Comunicaciones*".

3.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, **CONTACTEL** dispone de un plan de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3.5 Requisitos mínimos de seguridad

a) Los responsables de velar por el cumplimiento de la política de seguridad están adecuadamente identificados y son conocidos por todos los miembros de la organización. *(Art. 13)*
b) El análisis y gestión de riesgos es parte esencial del proceso de seguridad y se mantiene permanentemente actualizado. *(Art. 14)*
c) La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información de la organización deben protegerla, por lo que están adecuadamente formadas e informadas sobre sus deberes, obligaciones y responsabilidades en materia de seguridad. *(Art. 15)*
d) El personal encargado de atender, revisar y auditar la seguridad de los sistemas dispone de la cualificación necesaria y cumplen con los requisitos de formación y experiencia que establece la organización. *(Art. 16)*
e) Los sistemas de información son protegidos contra accesos y alteraciones no autorizadas. *(Art. 17)*
f) Todos aquellos activos (sistemas de información, infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside, se transporta o se procesa información, están debidamente protegidos. *(Art. 18)*
g) Para la adquisición de productos de seguridad y/o contratación de servicios de seguridad, se atenderá a las directrices marcadas por el Centro Criptológico Nacional (CCN), priorizando en todo caso aquellos productos y/o servicios que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición. *(Art. 19)*
h) Todos los sistemas se diseñan y configuran de forma que garanticen el mínimo privilegio, proporcionando la funcionalidad imprescindible para lograr los objetivos de la organización. *(Art. 20)*
i) Todo elemento físico o lógico es autorizado previamente tanto a su instalación como a su modificación y son evaluados y monitorizados permanentemente con el fin de mantener un estado de seguridad de los sistemas óptimo. *(Art. 21)*
j) La información en formato físico o electrónico almacenada o en tránsito a través de entornos inseguros está debidamente protegida para garantizar su recuperación y conservación. *(Art. 22)*
k) Los sistemas de información están debidamente protegidos en todo su perímetro en general y en su conexión con redes públicas en particular. *(Art. 23)*
l) La monitorización y análisis de actividades indebidas o no autorizadas se realiza sobre la base de un registro de actividad respetuoso con el derecho al honor, intimidad personal y familiar y a la propia imagen de los usuarios, y de acuerdo con la normativa aplicable en protección de datos. *(Art. 24)*
m) La organización tiene debidamente implantados los procedimientos internos necesarios para una correcta gestión de los incidentes de seguridad. *(Art. 25)*
n) La organización dispone de un plan de continuidad del negocio y de un plan de copias de seguridad que garantizan la continuidad de los servicios. *(Art. 26)*
o) La Seguridad de la Información no es algo estático, está constantemente controlada y es periódicamente revisada dentro del ciclo de mejora continua PDCA de la organización. *(Art. 27)*
p) El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes la Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley

Orgánica 3/2018 de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales.

3.6 Niveles de seguridad

Los niveles de seguridad requeridos para los diferentes sistemas de información vienen determinados por la categorización del sistema. CONTACTEL desarrolla dicha categorización en el procedimiento interno "*ENS – Categorización de los Sistemas*".

CONTACTEL dispone de procedimientos internos donde se desarrollan las medidas de seguridad del ANEXO II del RD 311/2022 conforme al nivel de categorización vigente.

4 ORGANIZACIÓN DE LA SEGURIDAD

4.1 Roles y responsabilidades

La estructura organizativa, roles y responsabilidades de **CONTACTEL** están definidos en el procedimiento interno "*SGI – Funciones y Organigrama Contactel*". En el marco del ENS, la gestión de la seguridad de la información implica la existencia de una estructura organizativa que defina unas responsabilidades diferenciadas en relación a requisitos de información, requisitos del servicio y requisitos de seguridad, *(Art. 11)*.

CONTACTEL articula esta diferenciación en el ámbito del alcance del ENS según la guía *CCN-STIC 801 ANEXO B. ESTRUCTURAS POSIBLES DE IMPLANTACIÓN*, a través de los siguientes roles:

- *Gobierno:* Comité SGI.
- *Supervisión:* Responsable de Seguridad.
- *Operación:* Responsable del Sistema.

4.2 Coordinación, nombramiento y resolución de conflictos

La coordinación se lleva a cabo en el seno del Comité de Dirección que podrá delegar en el Comité del SGI.

Los nombramientos los establece la Dirección de la organización y se revisan cada 2 años o cuando un puesto queda vacante.

Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité del SGI y prevalecerá en todo caso el criterio de la Dirección.

5 FORMACIÓN Y CONCIENCIACIÓN

Las acciones específicas de concienciación y formación relativas al ENS se gestionan, sin distinción alguna, conjuntamente con las del SGI.

Dentro del marco del SGI, **CONTACTEL** desarrolla su metodología en el procedimiento "*SGI – Manual del SGI*".

6 ANÁLISIS Y GESTIÓN DE RIESGOS

Un correcto análisis, identificación y gestión de los riesgos a los que se encuentran sometidos tanto los datos personales que trata la organización como los activos de información que sustentan los servicios de **CONTACTEL**, es primordial para la correcta toma de decisiones de la Dirección.

La metodología de Análisis y Gestión de Riesgos adoptada por **CONTACTEL** está basada en *MAGERIT v3* y se desarrolla en el procedimiento interno *"27001 – Metodología apreciación del riesgo".* Para su aplicación, **CONTACTEL** emplea una herramienta propia.

7 DOCUMENTACIÓN DE SEGURIDAD

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

- *Primer nivel:* Política de seguridad de la Información.
- *Segundo nivel:* Normativas y procedimientos de seguridad.
- *Tercer nivel:* Informes, registros y evidencias electrónicas.

La aprobación de la documentación de seguridad depende de su nivel:

- Primer nivel: Alta Dirección
- Segundo nivel: Responsables de TI
- Tercer nivel: n/a

7.1 Acceso

Las directrices para conceder accesos a la documentación se desarrollan en el procedimiento interno "*27001 – Control de accesos"*.

7.2 Primer nivel: Política de seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, de la organización, recogido en el presente documento.

7.3 Segundo nivel: Normativas y procedimientos de seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente, desarrollados por **CONTACTEL** en el marco de su SGI en los que se han incluido los aspectos específicos del ENS para cumplir con los requisitos mínimos de seguridad que marca su *artículo 11*, tal y como indica la guía *CCN-STIC 825 ENS – ESQUEMA NACIONAL DE SEGURIDAD CERTIFICATIONES 27001*, apartado 5.1. *CUADRO RESUMEN*.

Para facilitar la trazabilidad entre las medidas de seguridad requeridas por el ENS y su implantación en **CONTACTEL** en el marco del SGSI, en la Declaración de Aplicabilidad del ENS se ha procedido a mapear las medidas de seguridad aplicables del Anexo II con los controles del

Anexo A de ISO 27001. Realizado de acuerdo con la guía *CCN-STIC 825 ENS – ESQUEMA NACIONAL DE SEGURIDAD CERTIFICATIONES 27001*.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Comité del SGI.

7.4 Tercer nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen evidencias generadas durante todas las fases del ciclo de vida de los sistemas de información, así como amenazas y vulnerabilidades de los sistemas de información.

7.5 Otra documentación

Se tendrán en cuenta, durante todo el ciclo de vida de los sistemas de información, los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC que publique el Centro Criptológico Nacional (CCN).

8 DOCUMENTACIÓN

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo a los requisitos generales del SGI que se desarrolla en el procedimiento interno "*SGI – Manual del SGI*".

9 PROCESO DE APROBACIÓN Y REVISIÓN

Esta *Política de Seguridad ENS* es aprobada por el representante del administrador único y es revisada junto a la *Política de los Sistemas de Gestión* de forma periódica o cuando las circunstancias técnicas u organizativas lo requieran.