Política de Seguridad de los Sistemas de Información

Versión 1.0

Calidad y Normativa
1-9-2023

Índice

1 OBJETIVO

El presente documento describe la Política de Seguridad de la Información (en adelante, Política) y persigue la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, que constituyen los tres componentes básicos de la seguridad de la información, estableciendo los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte a los procesos de negocio.

Esta Política de Seguridad de la Información es la base por la que se rige el Cuerpo Normativo de Seguridad de las empresas CENTRO ESPAÑOL DE SERVICIOS TELEMÁTICOS S.A. y LN DETER S.A., (**grupo CESTEL**, en adelante).

De este modo, el principal objetivo de la Política es definir los principios y las reglas básicas para la gestión de la seguridad de la información de manera que se garanticen la seguridad de la información y minimicen los riesgos en la información derivados de un impacto provocado por una gestión ineficaz de la misma.

2 ÁMBITO DE APLICACIÓN Y OBJETIVOS

Este documento es de aplicación para todos los trabajadores del **grupo CESTEL**, así como para los trabajadores externos que presten servicio a la misma.

El alcance de la presente Política abarca toda la información del **grupo CESTEL** con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente.

Los principales objetivos de esta política son los siguientes:

- ✓ Dar respuesta a las necesidades y expectativas de nuestros grupos de interés, en especial de nuestros clientes.
- ✓ Gestionar y controlar de forma eficaz de los procesos implicados, así como el análisis y gestión de los riesgos existentes.
- ✓ Cumplimiento con la legislación aplicable en materia de calidad y seguridad de la información que afecte a los activos de la empresa.
- ✓ Determinar y proteger de forma apropiada los activos relacionados con la información de clientes, empresa y resto de grupos de interés para evitar:
  - La pérdida o mal uso de los mismos.
  - Las pérdidas económicas o de imagen como empresa.
  - La paralización total o parcial de los procesos de negocio.
- ✓ Adaptarse a la evolución económica y tecnológica de los mercados.
- ✓ Concienciar, formar y motivar al personal, sobre la importancia y el desarrollo e implantación de un Sistema de Gestión integrado.
- ✓ Mejorar de forma continua.

3 VIGENCIA

La presente Política del **grupo CESTEL** ha sido aprobada por el departamento de **Calidad y Normativa**, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que **grupo CESTEL** pone a disposición de sus usuarios para el ejercicio de sus funciones.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte del **grupo CESTEL**.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa.

4 PRINCIPIOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La responsabilidad de la seguridad de un activo es del Propietario del activo, que puede delegar la administración de los mecanismos y medidas de seguridad en el Encargado del Tratamiento del activo.

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar al **grupo CESTEL**. Además, se establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- ✓ Alcance estratégico: La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos del **grupo CESTEL** de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.
- ✓ 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
- ✓ Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá 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.
- ✓ Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado.
- ✓ Seguridad por defecto: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto. **Grupo CESTEL** considera que las funciones de Seguridad de la Información deberán quedar integradas en todos los niveles jerárquicos de su personal. Puesto que la Seguridad de la Información incumbe a todo el personal del **grupo CESTEL**, esta Política deberá ser conocida, comprendida y asumida por todos sus empleados. Para la consecución de los objetivos de esta Política, **Grupo CESTEL** deberá establecer una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación. En el transcurso de este ciclo de mejora continua, **Grupo CESTEL** mantendrá la definición tanto del nivel de riesgo residual aceptado (apetito al riesgo) como de sus umbrales de tolerancia.

5 MARCO REGULATORIO

El marco normativo en materia de seguridad de la información en el que grupo CESTEL desarrolla su actividad, esencialmente, es el siguiente:

- ✓ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal.
- ✓ Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
- ✓ 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.
- ✓ Real Decreto 311/2022, de 3 de mayo, por el que se regula el 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 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- ✓ Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de
- ✓ comercio electrónico.
- ✓ Ley 59/2003, de 19 de diciembre, de firma electrónica.
- ✓ Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- ✓ 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.
- ✓ Guías CCN-STIC, 802, 807, 808, 809 y 825.
- ✓ Instrucciones Técnicas de Seguridad de conformidad con el Esquema Nacional de Seguridad (Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas) y de Auditoría de la Seguridad de los Sistemas de seguridad de la información.
- ✓ Ley orgánica 10/1995, de 23 de noviembre, del código penal.
- ✓ Información (Resolución de 27 de marzo de 2018 de la Secretaría de Estado de Función Pública).
- ✓ UNE - ISO/IEC 27002:2013 Código de buenas prácticas para la Gestión de la Seguridad de la información.
- ✓ UNE - ISO/IEC 27001:2013 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- ✓ UNE-EN-ISO 9001:2015 Sistemas de gestión de la calidad.

6 COMPROMISO DE LA DIRECCIÓN

Consciente de la importancia de la seguridad de la información, la Dirección del **Grupo CESTEL**, para llevar a cabo con éxito sus objetivos de negocio, está comprometida con:

- ✓ Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- ✓ Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- ✓ Impulsar la divulgación y la concienciación de esta Política entre los empleados del **grupo CESTEL** y todos aquellos implicados en el tratamiento de la información del **grupo CESTEL**.
- ✓ Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información
- ✓ Considerar los riesgos de seguridad de la información en la toma de decisiones.

7 ROLES Y RESPONSABILIDADES

Grupo CESTEL se compromete a velar por la Seguridad de todos los activos bajo su responsabilidad mediante las medidas que sean necesarias, siempre garantizando el cumplimiento de las normativas y leyes aplicables. **Grupo CESTEL** deberá nombrar una figura responsable de definir, implementar y monitorizar las medidas de ciberseguridad y seguridad de la información. Esta figura deberá establecerse desde un entorno de gobierno y gestión, será independiente de cualquier área organizativa reportando al órgano de gobierno.

7.1 COMITÉ DE SEGURIDAD CORPORATIVO Y DE LA INFORMACIÓN

Competencias:

- ✓ Elaborar y revisar la Política de Seguridad de la información del **grupo CESTEL**, que deberá ser aprobada por la Dirección de la entidad.
- ✓ Coordinar todas las funciones de seguridad de la organización.
- ✓ Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- ✓ Velar por el alineamiento de las actividades de seguridad a los objetivos de la organización.
- ✓ Coordinar los Planes de Continuidad de las diferentes áreas, para asegurar una actuación sin fisuras en caso de que deban ser activados.
- ✓ Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose gestionar un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- ✓ Recibir las inquietudes en materia de seguridad de la Dirección de la entidad y transmitirlas a los responsables departamentales pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, habrán de ser comunicadas a la Dirección.
- ✓ Recabar del Responsable de Seguridad informes regulares del estado de la seguridad de la organización y de los posibles incidentes. Estos informes, se consolidan y resumen para su comunicación a la Dirección de la entidad.
- ✓ Coordinar y dar respuesta a las inquietudes transmitidas a través del Responsables de seguridad.

- ✓ Definir, dentro de la Política de Seguridad de la información, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones.

- ✓ Informar regularmente del estado de la seguridad de la información a la Dirección.

- ✓ Promover la mejora continua del sistema de gestión de la seguridad de la información.

- ✓ Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.

- ✓ Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.

- ✓ Aprobar la Normativa de Seguridad de la información.

- ✓ Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.

- ✓ Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.

- ✓ Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.

- ✓ Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

- ✓ Aprobar planes de mejora de la seguridad de la información de la organización.

- ✓ Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

- ✓ Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

7.2 RESPONSABLE DE SEGURIDAD

El responsable de Seguridad del **grupo CESTEL** tendrá como como competencia las tareas de los siguientes roles:

- ✓ Responsable de Seguridad Corporativa (CSO).
  - Convoca al Comité de Seguridad Corporativa, recopilando la información pertinente.
  - Recaba las inquietudes de la Dirección de la entidad y de los responsables de seguridad departamentales, incorporándolas al Orden del Día del Comité de Seguridad Corporativa, para su examen y acciones pertinentes.
  - Es responsable, junto con los diferentes responsables de seguridad departamentales, de estar al tanto de cambios regulatorios o normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la entidad, debiendo informarse de las consecuencias para las actividades de la organización, alertando al Comité de Seguridad Corporativa y proponiendo las medidas oportunas de adecuación al nuevo marco.
  - Es el responsable de la toma de decisiones cotidianas entre dos reuniones del Comité de Seguridad Corporativa. Estas decisiones darán respuesta a propuestas de los responsables de seguridad departamentales, velando por la unidad de acción y la coordinación de actuaciones, especialmente en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres.

- ✓ Responsable de Seguridad (CISO)
  - Toma las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
  - En caso de servicios externalizados, la responsabilidad última la tiene siempre la entidad destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio.
  - Exige, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
  - Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización.
  - Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
  - Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciber incidentes que afecten a la organización y los servicios.

- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del RD-l 12/2018 y de su Reglamento de Desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.
- Se responsabiliza de la adquisición, de forma proporcionada a la categoría del sistema y nivel de seguridad, de productos de seguridad de las tecnologías de la información y comunicaciones que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición. Se considera la excepción de aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de la Seguridad.
- Determinar las medidas aplicables del Anexo II del ENS, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales.
- Determinar si deben ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del Responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.
- Elaborar y aprobar el documento de declaración de aplicabilidad.
- Realizar la evaluaciones de riesgos
- Determinar si alguna de las medidas del Anexo II deben ser reemplazadas por otras compensatorias y justificar documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan. Aprobar formalmente dicha documentación.
- Asegurarse que la utilización de infraestructuras y servicios comunes facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el ENS en condiciones de mejor eficiencia.
- Analizar los informes de autoevaluación y/o los informes de auditoría y elevar las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
- Convoca las reuniones del Comité de Seguridad de la Información.

- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

✓ Responsable de la Información
- Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Es propietario de los riesgos sobre la información.
- Valoración de las consecuencias de un impacto negativo sobre la seguridad de la información atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
- Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.
- Estas responsabilidades son indelegables.

✓ Responsable del servicio
- Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.
- Es propietario de los riesgos sobre los servicios.
- Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valoración las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
- Estas responsabilidades son indelegables.

7.3 RESPONSABLE DE INFORMACIÓN

El responsable de Información del **grupo CESTEL** tendrá como como competencia las tareas de los siguientes roles:

- ✓ Responsable del Sistema de la información
  - Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
  - Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
  - Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
  - Adoptar las todas las medidas de seguridad determinadas por el Responsable de la Seguridad de la Información, e informar a éste de su grado de implantación, eficacia e incidentes.
  - Proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

- ✓ Administrador de seguridad
  - La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
  - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
  - La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
  - La aplicación de los Procedimientos Operativos de Seguridad (POS).
  - Asegurar que los controles de seguridad establecidos son adecuadamente observados.
  - Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
  - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
  - Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
  - Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
  - Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

8 ESTRUCTURA DE LA DOCUMENTACIÓN

La documentación está compuesta por:

- Políticas
- Normativas
- Procedimientos
- Guías del CCN
- Guía de buenas prácticas.

Dicha documentación está disponible en la intranet de la organización, es gestionada por el Calidad y Normativa del grupo CESTEL y está sujeta a la política de la organización.