POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

1 Compromisos TREELOGIC 3
2 Alcance 4
3 Responsabilidades dentro de Esquema Nacional de Seguridad 4
4 Funciones del Comité de Seguridad de la Información 5
5 Funciones del Responsable de Seguridad 6
6 Funciones del Responsable del Sistema 7
7 Funciones de los Responsables de Información y Servicios 9
8 Funciones del Delegado de Protección de Datos 9
9 Seguridad como un proceso integral 10
10 Tratamiento de datos personales 12
11 Prevención, detección, respuesta y conservación de incidentes de seguridad 13
12 Resolución de conflictos 13
13 Terceros 14
14 Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados 14
15 Autorización y control de accesos 15
16 Protección de las instalaciones 15
17 Adquisición de productos de seguridad y contratación de servicios de seguridad. 15
18 Protección de la información almacenada y en tránsito 16
19 Registro de actividad y protección frente a código dañino 16
20 Legislación aplicable 17
21 Mejora continua en el proceso de seguridad 17
22 Control de Ediciones 18

1 COMPROMISOS TREELOGIC

TREE TECHNOLOGY S.A. (en adelante, **TREELOGIC**) como empresa intensiva en I+D, tecnología de la información y comunicación (TIC), ha ayudado a centenares de clientes a optimizar sus procesos y mejorar sus negocios. Centrados en los sectores de sanidad, en la administración pública, en servicios financieros, educación e industria, **TREELOGIC** ha venido desarrollando su actividad, prioritariamente en España, adquiriendo cada vez una mayor presencia en el ámbito europeo e internacional, siempre desde la transparencia y atendiendo a los más altos estándares éticos, tanto nacionales como internacionales.

TREELOGIC, plenamente consciente de la importancia que tienen la preservación de la disponibilidad, integridad, autenticidad, trazabilidad y confidencialidad de la información y los datos, tiene como objetivo o compromiso prioritario, establecido a través de la presente Política de Seguridad de la Información, asegurar la seguridad de los sistemas de información que dan soporte a los procesos de análisis, diseño, desarrollo, implantación, operación, mantenimiento y licenciamiento de soluciones software proporcionadas por la organización a entidades del sector público —incluyendo hospitales, universidades y organismos de investigación—, así como a empresas que prestan servicios a dichas entidades en el marco de relaciones contractuales o colaborativas. Estas soluciones comprenden aplicaciones avanzadas que pueden incorporar tecnologías como inteligencia artificial, y abarcan también servicios de soporte, formación y consultoría técnica especializada.

A través de su Sistema Integrado de Gestión basado en la Normativa ISO 27001 y el Real Decreto por el que se regula el Esquema Nacional de Seguridad, la Dirección adquiere un compromiso firme de satisfacer los requisitos contractuales, legales y reglamentarios aplicables al negocio y de mejorar su eficacia de forma y planificada.

El Comité de Seguridad de la Información aprueba el desarrollo del sistema de gestión, establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad y aquellos equivalentes dentro de la norma ISO 27001. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité.

Se ha establecido una metodología de gestión documental de forma transversal, de forma que ésta se encuentre gestionada, estructurada y disponible al personal conforme le sea de aplicación.

La edición inicial de esta política se aprueba por la alta dirección de **TREELOGIC**, correspondiendo la competencia de las labores de mantenimiento y actualización al comité de seguridad de la información, el cual se definirá mediante este documento con una periodicidad mínima de carácter anual.

2 ALCANCE

El ámbito de aplicación de la presente política se extiende a todos los miembros de **TREELOGIC** y tiene por objeto regular y procurar unas pautas con objeto de garantizar la seguridad de los sistemas de información que dan soporte a los procesos de análisis, diseño, desarrollo, implantación, operación y mantenimiento de soluciones software proporcionadas por la organización a entidades del sector público —incluyendo hospitales, universidades y organismos de investigación—, así como a las empresas que prestan servicios a dichas entidades en el marco de relaciones contractuales o colaborativas. Estas soluciones comprenden aplicaciones avanzadas que pueden incorporar tecnologías como inteligencia artificial (pero no es un requisito obligatorio); por ejemplo, en el ámbito sanitario, soluciones tecnológicas específicas tales como software de ayuda al triaje, sistemas de alerta temprana y seguimiento de casos de sepsis, plataformas para la gestión clínica y de datos hospitalarios, y herramientas de telemedicina; y, en el ámbito universitario, plataformas de gestión de la investigación y repositorios institucionales. Además, se incluyen proyectos de Compra Pública de Innovación (CPI) con énfasis en pruebas de concepto y prototipos que abordan retos específicos (p. ej., detección temprana de ciberataques o análisis de anomalías en infraestructuras críticas). En particular, se incorporan las especificaciones en los ámbitos de gestión de identidades, monitorización de criptotransacciones, ciberseguridad en entornos críticos, protección de datos e información, y seguridad de los datos y prevención de su uso malicioso. Al alcance también pertenecen los servicios de venta de licencias de productos de software (con o sin módulos IA), la instalación, integración, soporte y mantenimiento continuos de dichas soluciones, así como la formación especializada impartida al personal de la administración para el uso seguro de las plataformas y el cumplimiento de buenas prácticas.

3 RESPONSABILIDADES DENTRO DE ESQUEMA NACIONAL DE SEGURIDAD

La organización gestiona y organiza su seguridad conforme integra y garantiza el compromiso de todos los integrantes de la misma. Con objeto de garantizar esta máxima, establece una serie de roles con responsabilidades definidas y diferenciadas, asegurando la no concurrencia o conflicto de interese entre ellos.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información de la organización son responsables de la seguridad de la información, así como de los recursos y medios puestos a su disposición para el manejo de dicha información. En ellos recae la responsabilidad de un uso correcto, siempre de acuerdo a las atribuciones profesionales y competencias.

Como extensión a la estructura de seguridad, se establecerán relaciones de cooperación en materia de seguridad con las autoridades competentes, autonómicas o estatales, proveedores de servicios informáticos o de comunicación, así como organismos públicos y privados dedicados a promover la seguridad de los sistemas de información.

4 FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Atender las solicitudes, en materia de Seguridad de la Información, de la organización y de las diferentes áreas, informando regularmente del estado de la Seguridad de la Información.

Asesorar en materia de Seguridad de la Información.

Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.

Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello, se encargará de:

- Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.

- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y, en particular, en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Coordinación y supervisión de la realización de auditorías periódicas dentro del marco de ISO 27001, Esquema Nacional de Seguridad y protección de Datos con objeto de verificar el cumplimiento de los correspondientes requisitos tanto normativos como legales de aplicación conforme a las actividades de **TREELOGIC**.

5 FUNCIONES DEL RESPONSABLE DE SEGURIDAD

Es la persona responsable de la gestión y el mantenimiento del Sistema de Seguridad de la Información y de proporcionar ayuda y soporte a los propietarios de los activos de información para asegurar que se cumple la Política de Seguridad de la Información y que la información y los sistemas están adecuadamente protegidos. A continuación, se describen las responsabilidades principales del Responsable de Seguridad:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información, en su ámbito de responsabilidad.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Designar ejecuciones de análisis de riesgos, revisiones de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Validar los planes de continuidad, evaluación de los mismos así como la gestión de su eficiencia.
- Gestionar las revisiones externas o internas del sistema, incluyendo la recogida de indicadores específicos.
- Gestionar los procesos de certificación.
- Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.
- Asegurarse de que el sistema de gestión de la información es conforme con los requisitos de la norma internacional ISO 27001.

- Informar a la alta Dirección sobre el comportamiento del sistema de Gestión de Seguridad de la Información.
- Asegurar el cumplimiento de los derechos de propiedad intelectual, cumplimiento de los acuerdos de licenciamiento de herramientas software
- Destrucción segura de soportes de información una vez éstos dejan de estar en uso.
- Velar por la continuidad de los servicios prestados.
- Implementar medidas con objeto de evitar el robo, fraude o sustracción de información.
- Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y, en su caso, del Delegado de Protección de Datos y supervisar su despliegue.

La titularidad de esta figura se renovará de manera automática con carácter anual, aunque podrá ser modificada cuando, desde dirección, se considere necesario por cuestiones de personal, operativa o estrategia.

6 FUNCIONES DEL RESPONSABLE DEL SISTEMA

El responsable de Sistemas y comunicaciones es responsable de la seguridad de los sistemas. Entre sus obligaciones están:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborando los procedimientos operativos necesarios.
- 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 específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información de la Información.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Cuando la complejidad del sistema lo justifique el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

Adicionalmente, dentro de sus responsabilidades se encuentran:

- Gestionar todo el sistema y asegurarse que por directiva se cumplan las medidas implementadas.
- Administrar y gestionar las cuentas de los usuarios.
- Asegurarse de que sólo las personas autorizadas a tener acceso cuenten con él, siguiendo el principio de mínimo privilegio.
- Asegurarse de que los sistemas de información de **TREELOGIC** tienen los niveles de disponibilidad requeridos por la Organización.
- Incluir en los requisitos para nuevos desarrollos los aspectos de seguridad que sean de aplicación.

La titularidad de esta figura se renovará de manera automática con carácter anual, aunque podrá ser modificada cuando desde dirección se considere necesario por cuestiones de personal, operativa o estrategia.

7 FUNCIONES DE LOS RESPONSABLES DE INFORMACIÓN Y SERVICIOS

Entre sus funciones están:

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, previa propuesta al Responsable de Seguridad, y/o Comité de Seguridad de la Información. Aprobación de la categorización del sistema conjuntamente con el comité de seguridad.
- Aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.
- Informar sobre los derechos de acceso al Servicio y a la Información.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo.

La titularidad de estas figuras se renovarán de manera automática con carácter anual, aunque podrán ser modificadas cuando desde dirección se considere necesario por cuestiones de personal, operativa o estrategia. Cambios de relevancia, en los servicios o la información dentro del alcance de certificación, podrán desembocar en una revisión y actualización de estas figuras.

8 FUNCIONES DEL DELEGADO DE PROTECCIÓN DE DATOS

Corresponde al Delegado de Protección de Datos las funciones atribuidas a tal figura en el Reglamento UE 2016/679, de 27 de abril (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Tales funciones se ejercerán en los términos y condiciones y con el alcance señalados en la citada normativa. Actualmente estas funciones se encuentran transferidas a un tercero, el cual velará por el cumplimiento de todos los requisitos de aplicación, así como los controles específicos de aplicación referentes a datos personales de Real Decreto por el cual se regula el Esquema Nacional de Seguridad.

La titularidad de esta figura se renovará de manera automática con carácter anual, aunque podrá ser modificada cuando desde dirección se considere necesario por cuestiones de personal, operativa o estrategia.

9 SEGURIDAD COMO UN PROCESO INTEGRAL

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Los sistemas se encuentran diseñados de forma que garanticen la seguridad por defecto del siguiente modo:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue. De esta forma se minimiza la superficie de exposición o la probabilidad de que una vulnerabilidad en alguno de los elementos del sistema de información pudiese ser explotable.
- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario. Se ha de minimizar la probabilidad de fallo debido a errores de configuración debido a una elevada complejidad de la misma o la existencia de potenciales conflictos no controlados.

Este compromiso de la Dirección se articula mediante:

1. La participación de sus empleados/as y su influencia en sus respectivas áreas de responsabilidad.
2. El mantenimiento de las más estrictas normas éticas y profesionales, así como el empleo de códigos de buenas prácticas.
3. Concienciación desde la organización sobre aquellas prácticas que constituyen la base de un comportamiento que propicie la seguridad en los sistemas de información de igual manera de la prevención frente a amenazas, suplantaciones o bien otro tipo de engaños que los trabajadores pudiesen ser víctimas.
4. La dotación de los recursos humanos y materiales necesarios para su consecución, incluyendo la concienciación, el adiestramiento y la capacitación permanente del personal, tanto en materia de seguridad de información como en aquellas temáticas necesarias para el correcto desempeño de sus obligaciones.
5. La asignación de funciones y responsabilidades específicas que permitan mantener los compromisos de Seguridad de la Información establecidos, así como la definición de roles de las

personas Responsables de la información, Responsable de Seguridad, Responsable de Sistema TIC, Delegado/a de protección de datos, así como los responsables de los servicios, los activos que vienen desarrollados en la documentación de seguridad.

6. Que se han designado personas para dichos roles siguiéndose el principio de «separación de funciones», existiendo un acta específica de cada uno de los nombramientos, así como la creación de herramientas de resolución de conflictos de los entre dichos responsables, asimismo, se ha constituido un Comité de Seguridad de la Información según dispone el Real decreto por el que se regula el esquema Nacional de Seguridad.

7. La identificación, análisis, tratamiento y reevaluación de los riegos de seguridad de la información relacionados con sus servicios, sus activos y el negocio, mediante la aplicación de metodología reconocida basada en MAGERIT. Realizándose un análisis de riesgos, y que se prevé su revisión y aprobación al menos con carácter anual, o siempre que se den cambios sustanciales. La identificación, análisis, tratamiento y reevaluación de los riegos en materia de protección de datos de forma periódica además de siempre que se produzcan cambios de relevancia en materia de datos personales dentro de la organización, o bien se produzca una brecha de datos personales de acuerdo a la metodología establecida a este fin por parte de la Agencia Española de Protección de Datos.

   La identificación de estos riesgos y el tratamiento de estos tiene por objeto minimizar la posibilidad de que se produzca una brecha y la contención en caso de que tuviese lugar, reduciendo su impacto sobre la organización

8. La definición de un sistema de gestión de la seguridad, documentado en el que se intentan definir y procedimentar todas aquellas tareas que interrelacionan con la información y con un proceso regular de aprobación por la dirección, para ello se han tenido en cuenta las recomendaciones de protección descritas en el anexo II del ENS, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.

9. La gestión y el tratamiento responsable de los incidentes de seguridad de la información, previniendo su aparición o repetición, analizándose su causa e implantándose medidas correctoras. Se establece una metodología de gestión de incidentes, la cual implica procesos de aprendizaje derivado de la materialización de éstos, aplicable no solo al propio incidente que lo detona, sino a futuros incidentes con un número variable de elementos comunes, minimizándose de este modo el riesgo futuro.

10. La Revisión periódica y planificada del Sistema de Gestión, mediante auditorías, para incrementar su eficacia; mejorar la satisfacción de las partes interesadas; evaluar la eficacia y adecuación de

esta Política; y establecer, seguir y revisar objetivos de seguridad de la información medibles y coherentes con la misma.

11. Vigilancia en cuanto comportamientos anómalos, correlación de eventos, así como la evolución de posibles vulnerabilidades y deficiencias de configuración. Periódicamente se reevaluará las medidas de seguridad de acuerdo a los riesgos detectados y los sistemas de protección existentes, teniéndose en cuenta recomendaciones y alertas emitidas por organismos competentes y fabricantes.

10 TRATAMIENTO DE DATOS PERSONALES

La organización garantiza que el tratamiento de datos personales se realiza de forma lícita, leal, transparente y con sujeción a los principios de minimización, integridad y confidencialidad establecidos en la normativa vigente.

Únicamente se recogen y tratan los datos personales estrictamente necesarios para la prestación de los servicios contemplados dentro del alcance definido en esta política. Cualquier tratamiento adicional queda sujeto a evaluación previa de necesidad y proporcionalidad, conforme al principio de minimización de datos del artículo 5.1.c) del Reglamento (UE) 2016/679 (RGPD).

El detalle de finalidades, bases legales, destinatarios y plazos de conservación se encuentra documentado en los Registros de Actividades de Tratamiento (RAT), mantenidos actualizados como parte del Sistema Integrado de Gestión de la compañía. Asimismo, se dispone de una política de privacidad corporativa accesible a los interesados, donde se recogen los procedimientos para el ejercicio de derechos (acceso, rectificación, supresión, limitación, oposición y portabilidad), en cumplimiento de los artículos 12 a 22 del RGPD.

La organización se compromete a respetar en todo momento lo establecido en la legislación de protección de datos aplicable, en particular:

- El Reglamento (UE) 2016/679 (RGPD),
- La Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD),
- Así como las medidas aplicables del ENS en su Anexo II relativas a protección de datos y control de acceso.

11 PREVENCIÓN, DETECCIÓN, RESPUESTA Y CONSERVACIÓN DE INCIDENTES DE SEGURIDAD

Se dispone de un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema y aprendizaje sobre incidentes.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la organización implementa medidas de seguridad establecidas por el Real decreto por el cual se regula en Esquema Nacional de Seguridad, ISO 27001, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, se encuentran claramente definidos y documentados.

Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente

Medidas de reacción tomadas frente a incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- 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).
- Comunicación a partes interesadas de los incidentes de seguridad cuando éstas pudieran verse afectadas.
- Para garantizar la disponibilidad de los servicios, la organización dispondrá de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

12 RESOLUCIÓN DE CONFLICTOS

El Comité de Seguridad de la información se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los distintos roles de seguridad implicados.

13 TERCEROS

Cuando la organización preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información. **TREELOGIC** definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de actuaciones que lleve a cabo en materia de Seguridad en relación con otros organismos u organizaciones.

Cuando se haga uso de servicios de terceros o se ceda información a terceros, se les hará partícipe de esta Política de Seguridad de la Información y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad de la Información.

Cuando algún aspecto de esta Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS 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.

Si se considera necesario, **TREELOGIC** podrá requerir informes o cumplimentación de cuestionarios específicos a terceros con objeto de demostrar la garantía de los mecanismos de seguridad y no comprometer los sistemas de información que dan soporte a los servicios prestados o la información soportada en los mismos

14 EXISTENCIA DE LÍNEAS DE DEFENSA Y PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

La organización ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección protege el perímetro, en particular, si se conecta a redes públicas. En todo caso, se analizarán los riesgos derivados de la interconexión del sistema a través de redes con otros sistemas y se controlará su punto de unión.

15 AUTORIZACIÓN Y CONTROL DE ACCESOS

La organización implementa mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados. Se sigue la política de mínimo privilegio posible de forma que se realiza asignación de permisos y accesos a archivos de forma diferenciada mediante establecimiento de roles y políticas de acceso basadas en grupos de usuarios, ofreciendo un sistema de gestión de accesos robusto y diferenciado.

16 PROTECCIÓN DE LAS INSTALACIONES

La organización implementa mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas comunes y críticas. En caso de que estos sean transferidos a un tercero, se vela porque cumplan con todos los requisitos en materia de seguridad establecidos en el real decreto por el que regula el esquema nacional de seguridad que sean de aplicación.

Actualmente, dado que la fuerza de trabajo de **TREELOGIC** se encuentra en modalidad de teletrabajo, la exposición de amenazas relativas a los riesgos en instalaciones físicas se encuentra altamente minimizada y controlada.

17 ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD.

Se tendrá en cuenta, para la adquisición de productos, que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad. Dicha certificación vendrá respaldada por la inclusión de estos productos en la guía 105 CPSTIC publicada de manera periódica por el Centro Criptológico Nacional.

Todos aquellos terceros que provean servicios de seguridad a la organización, o bien accedan a los sistemas o la información de la organización, deberán acreditar la tenencia de certificado de acuerdo a

Esquema Nacional de Seguridad en, al menos, la misma categoría de la organización en el alcance de la prestación del servicio, evidenciando además de esto, el cumplimiento de los controles del RD 311/2022 que sean de aplicación.

18 PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

La organización implementa mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas disponen de copias de seguridad y se han establecido los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida, de los medios habituales de trabajo.

Se dispone de procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de la organización. De igual modo, se implementan mecanismos de seguridad adecuados a la naturaleza del soporte en que se encuentren los documentos, con objeto de garantizar que toda información en soporte no electrónico relacionada estará protegida con el mismo grado de seguridad que la electrónica.

Se dispone, así mismo, de planes de continuidad de negocio a fin de asegurar planes de actuación en aras de la continuidad del negocio de la organización dentro del marco de la norma ISO 27001 y el real decreto por el cual se regula el Esquema Nacional de Seguridad. En caso de activación de cualquier medida de continuidad, siempre se garantizará que los medios para la operación en degradado cumplen con todas las medidas de seguridad establecidas en los medios habituales de operación, no comprometiéndose en ningún caso los niveles de seguridad de los sistemas de información durante la operación en degradado.

La organización dispone de políticas de borrado de metadatos y otras propiedades de documentos, así como auditorías periódicas de los mismos a fin de asegurar que no se producen filtraciones de documentos publicados o de otro tipo de información incrustada en archivos electrónicos puestos a disposición del público.

19 REGISTRO DE ACTIVIDAD Y PROTECCIÓN FRENTE A CÓDIGO DAÑINO

La organización habilita registros de la actividad de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa mediante el uso de diversas soluciones, incluyendo un correlador de eventos. Todo ello con la finalidad exclusiva de lograr el cumplimiento del ENS, con

plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

Se dispone de una solución antivirus EDR desplegado sobre toda la infraestructura y endpoints, así como de procesos de actuación en caso de infección destinados a contener al máximo sus efectos mitigando el impacto producido sobre los sistemas de información.

20 LEGISLACIÓN APLICABLE

TREELOGIC establece, mediante el documento "Listado Legislación Aplicable", toda la legislación o normativa que le es aplicable en base a su actividad y localización geográfica, así como otros requisitos que la empresa suscriba y entre los que se encuentra, entre otros, Legislación general; Legislación del sector; Normas de Calidad, Medio Ambiente y Seguridad de la Información; Especificaciones; Legislación medioambiental; etc.

Esta documentación es controlada y archivada por el Responsable del Sistema.

21 MEJORA CONTINUA EN EL PROCESO DE SEGURIDAD

El proceso integral de seguridad implantado es actualizado y mejorado de forma continua. Para ello, se aplican los criterios y métodos reconocidos.

La Dirección de **TREELOGIC** reconoce que, para la consecución de este compromiso, es imprescindible la aportación y participación del personal de la empresa, su conocimiento y entendimiento, su sensibilización hacia la excelencia en la preservación de la seguridad de la información, en la satisfacción de terceras partes, en la eficacia y mejora continua del Sistema Integrado de Gestión y en la consecución de los objetivos y metas propuestos, por lo que difunde esta Declaración de la Política de Seguridad de la Información a todo el personal bajo su responsabilidad.

Periódicamente se realizan revisiones del sistema que lo soporta, tanto en las medidas propias de gestión, como aquellas de carácter técnico por parte de auditores independientes, garantizando de este modo la objetividad de la revisión realizada.

22 CONTROL DE EDICIONES

Edición	Fecha	Naturaleza de la edición
01	23/06/2025	Versión Inicial.