POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ENS

1. INTRODUCCIÓN

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica, persigue tres objetivos fundamentales:

- Alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital.
- Introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios.
- Facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Para ello, el Real Decreto en el capítulo III referido a la política de seguridad en sus artículos 12 a 27, se definen:

- Los requisitos mínimos para permitir una protección adecuada de la información y los servicios a través de la organización e implantación del proceso de seguridad;
- gestión de riesgos;
- gestión de personal;
- profesionalidad; autorización y control de los accesos;
- protección de las instalaciones;
- adquisición de productos de seguridad y contratación de servicios de seguridad;
- mínimo privilegio;
- integridad y actualización del sistema;
- protección de la información almacenada y en tránsito;

- prevención ante otros sistemas de información interconectados;
- registro de la actividad y detección de código dañino;
- incidentes de seguridad;
- continuidad de la actividad; y mejora continua del proceso de seguridad.

La política de seguridad de la información (en adelante PSI), según el Real Decreto, es el documento que define el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

Cuando la provisión de las soluciones o la prestación de los servicios sujetos al cumplimiento del ENS sean realizadas por organizaciones del sector privado, se deberán utilizar estos mismos modelos, sustituyendo las referencias a los organismos públicos por las correspondientes a las entidades privadas certificadas.

TERRANOVA está preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

1.1. Prevención

TERRANOVA evita, o al menos previene en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello TERRANOVA implementa 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, TERRANOVA:

- 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.

1.2. Detección

Dado que los servicios se pueden 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 10 del ENS.

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

1.3. Respuesta

TERRANOVA:

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

1.4. Conservación

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

2. OBJETIVOS Y MISIÓN DE LA ENTIDAD

Terranova fue creada para el desarrollo de productos de software para servicios públicos y está representada por un equipo de ingenieros, programadores y directivos que combinan su profesionalidad, creando aplicaciones específicas para la gestión interna de los procesos de empresas multiservicio, alineadas con el perímetro regulatorio proporcionado por ARERA.

En resumen, el objetivo de **Terranova** es crear aplicaciones que realmente apoyen y automatizen los procesos de las empresas multiservicio, en cumplimiento de las disposiciones legislativas, **sin necesidad de recurrir a la ayuda habitual de apoyo externo.**

Terranova, partiendo de estos supuestos:

- Es una empresa que presta servicios de diseño, desarrollo, mantenimiento, soporte, consultoría y personalización orientados a la implementación de productos de software para los mercados de energía, servicios públicos y medio ambiente, tanto en la nube como en entornos locales.
- Tiene personalidad jurídica propia y plena capacidad de obrar para administrar, adquirir, contratar, asumir obligaciones, así como renunciar y ejercer libremente toda clase de derechos y acciones ante las Administraciones públicas.
- En el nuevo marco de la administración electrónica, y para su correcto desarrollo, presta servicios a las propias administraciones y organismos públicos con los que colabora, y para ello, proporciona las mayores garantías para el correcto uso de las tecnologías por parte de las Administraciones Públicas.
- Establece objetivos de seguridad de la información encaminados a proteger con las mayores garantías, la integridad, la confidencialidad, la disponibilidad, la trazabilidad y la autenticidad de la información objeto de tratamiento dentro de sus competencias.
- Para garantizar una apropiada seguridad de la información, aplica las más adecuadas medidas de seguridad, en todos los Departamentos reforzando la prevención, detección y respuesta de incidentes de seguridad.
- Los sistemas de información y comunicación están protegidos contra potenciales amenazas que puedan poner en peligro la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información. A tal fin, adoptarán una estrategia de seguridad de la información que permita cumplir con los requisitos establecidos por el Esquema Nacional de Seguridad; aplicar un sistema de mejora continua, supervisar y garantizar unos adecuados niveles de servicios; seguir y analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes de seguridad con el fin de garantizar la continuidad de los servicios.
- Dentro del enfoque de la seguridad de la información como parte integral de los servicios prestados y de su funcionamiento interno, tiene una especial importancia la protección de datos personales, por lo que muchas de las medidas implantadas estarán encaminadas a proteger proactivamente dichos datos, velando por el cumplimiento de lo dispuesto en la legislación vigente en

materia de protección de datos personales dentro del marco normativo europeo y español.

2.1. Compromisos

Conforme a los requisitos de la norma del ENS, TERRANOVA se compromete a:

- Cumplir los objetivos de seguridad de la información que se definen y revisan anualmente.
- Cumplir los requisitos aplicables a la seguridad de la información.
- Mejorar continuamente el sistema de gestión de la seguridad de la información.
- Comunicar dentro de la organización la Política de Seguridad de la información, que se gestiona como información documentada.
- Poner la Política de Seguridad de la información a disposición de las partes interesadas, según sea apropiado.

3. PRINCIPIOS DE SEGURIDAD

3.1. Principios de la seguridad de la información

Los principios son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de tecnologías de la información y comunicaciones. Se establecen los siguientes de acuerdo con el artículo 5 del ENS:

- Seguridad como proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.

3.2. Declaración de la Política de Seguridad

La Política de Seguridad se concreta en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos y que inspiran las actuaciones

en dicha materia. Se establecen los siguientes:

- Todas las directrices de seguridad están alineadas y no entran en conflicto con lo establecido en la política de seguridad de las tecnologías de la información y comunicaciones de TERRANOVA.
- Se adoptan las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Los activos de información se encuentran gestionados, inventariados y categorizados, y están asociados a un responsable.
- Se implantan los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
- Los activos de información son emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas están suficientemente protegidos frente a amenazas físicas o ambientales.
- Se establecen los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones y los servicios prestados a los ciudadanos son adecuadamente protegidos, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- Se limita el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, queda registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme

a la actividad de la organización.

- Se contemplan los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto. En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos 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.
- Se implantan los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Se adoptan las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.
- La seguridad de los sistemas de información es atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. Se 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 y deben designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado.
- Los sistemas de información se diseñan y configuran otorgando los mínimos privilegios necesarios para su correcto desempeño.
- Cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requiere autorización formal previa. La evaluación y monitorización permanentes permiten adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten y la detección temprana de cualquier incidente que tenga lugar sobre los mismos.
- Se presta especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes

abiertas, que deberán analizarse especialmente para lograr una adecuada protección. Se aplican procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica es protegida con el mismo grado de seguridad que ésta.

- Se protege el perímetro del sistema de información reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.
- Con plenas garantías legales, se registran las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

4. ALCANCE DEL SISTEMA DE SEGURIDAD DE INFORMACIÓN BAJO EL ENS

Esta política es aplicable, dentro del marco del alcance del ENS, sin excepciones a: "Los sistemas de información que sustentan el Diseño, desarrollo, mantenimiento, soporte, consultoría y personalización orientados a la implementación de productos de software para los mercados de energía, servicios públicos y medio ambiente, tanto en la nube como en entornos locales."

5. MARCO LEGAL Y REGULATORIO APLICABLE

La legislación aplicable en el marco de la seguridad de la información es el definido en el Manual del Sistema de Gestión Integrado.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. Comité de Seguridad

El Comité de Seguridad de TERRANOVA está compuesto por:

- El Presidente de Garantía de Seguridad como Responsable de Seguridad
- El Responsable TIC como Responsable del Sistema
- El Propietario del Banco de Datos como Responsable de la Información
- El Propietario del Servicio (Jefe del Área de referencia) como Responsable del Servicio
- DPO

El Comité tiene las siguientes funciones:

- Promover la seguridad de los activos de información de TERRANOVA
- Validar, la documentación de seguridad elaborada por el Responsable de Seguridad,
- Proponer la aprobación de la clasificación de la información, conforme a lo que se indica más adelante
- Valorar y proponer la aprobación de toda la documentación de seguridad
- Diseñar la estructura de la documentación de seguridad
- Vigilar el cumplimiento de las obligaciones del Responsable del Registro de actividades, conforme las regula la normativa de protección de datos de carácter personal.
- Difundir entre el personal al que se refiere el ítem 2 del presente documento, el conocimiento de las obligaciones que le atañen y las consecuencias en que pudiera incurrir en caso de incumplimiento.

6.2. Responsable de la Información

El Responsable de la Información es habitualmente una persona que ocupa un alto cargo en la dirección de la organización. Este cargo tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

El/la Responsable de la información será designado/a por el Director de TERRANOVA y tiene como responsabilidad la ejecución de todas las medidas de seguridad adecuadas para TERRANOVA, incluida la elaboración de la documentación de seguridad. Este cargo se irá renovando automáticamente hasta que la Dirección General anuncie la sustitución de la persona que ocupa el cargo.

El/la Responsable de la información dispone de la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.

Determinar los niveles de seguridad de los servicios.

La Dirección de TERRANOVA garantizará que el/la Responsable de la información participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad de la información y a la protección de datos personales.

La Dirección de TERRANOVA respaldará al/a Responsable de la información en el desempeño de las funciones mencionadas en el artículo 39 del RGPD, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

La Dirección de TERRANOVA garantizará que el/la Responsable de la información no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. El/la Responsable de la información rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

Las personas interesadas podrán ponerse en contacto con el/la Responsable de la información por lo que respecta a todas las cuestiones relativas a la seguridad de la información y a la protección de datos personales.

El/la Responsable de la información estará obligado/a a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

El/la Responsable de la información podrá desempeñar otras funciones y cometidos. La Dirección General garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja (a veces se dice que 'se heredan los requisitos'), y suele añadir requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

El/la Responsable de la información tendrá como mínimo las siguientes funciones:

- Informar y asesorar al Director General y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del ENS y de otras disposiciones aplicables en materia de seguridad de la información y de

protección de datos, vigentes en España o en la Unión o de los Estados miembros;

- Supervisar el cumplimiento de lo dispuesto en el ENS, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable en materia de seguridad de la información y protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la seguridad de la información y supervisar su aplicación de conformidad con lo dispuesto en el ENS;

- Cooperar con las autoridades de control y los CERT.

- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento de datos personales, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El/la Responsable de la información desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Aunque la aprobación formal de los niveles corresponde al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad, así como también se escuchará la opinión del Responsable del Sistema.

6.3. Responsable del Sistema

Persona designada por la Dirección. La persona designada figurará en la documentación de seguridad del sistema de información. Este cargo se renovará automáticamente, salvo que se la persona designada cause baja en la organización o cambie de puesto de trabajo dentro de la propia organización.

Responsabilidades:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto

funcionamiento.

- Definir la topología y sistema de 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.

- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

6.4. Responsable de Seguridad

El/la responsable de seguridad será designado/a por el Director de DASS y tiene como responsabilidad la ejecución de todas las medidas de seguridad adecuadas para DASS, incluida la elaboración de la documentación de seguridad. Este cargo, se irá renovando automáticamente hasta que la Dirección General anuncie la sustitución de la persona que ocupa el cargo.

Con independencia de la obligación genérica referida a la implantación, coordinación y control de las medidas de seguridad, se enumeran a continuación, a título enunciativo, las funciones concretas del responsable de seguridad:

- Adoptar, con la mayor inmediatez, las medidas oportunas para subsanar cualquier anomalía que haya producido una incidencia e importar al Comité los impresos en que se hayan registrado las incidencias.

- Cuando las incidencias hayan afectado a Datos personales, el Responsable de Seguridad deberá comunicar inmediatamente la incidencia a la Responsable de Protección de Datos.

- Colaborar con el Director y el/la Responsable de Protección de Datos, en la comprobación de la correcta aplicación de los procedimientos de realización de copias de seguridad y recuperación de datos.

- Verificar que, en todo procedimiento de recuperación de datos que sea realizado por personal externo, se mantiene la más estricta confidencialidad sobre los datos de carácter personal objeto de tratamiento.

- Verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

- Custodiar y actualizar la relación de usuarios con acceso a los sistemas de información o que intervienen en los tratamientos de datos de carácter personal.

- Supervisar con la Responsable de Protección de Datos, el nivel de intervención, por los usuarios dados de alta, en las diferentes fases del ciclo de vida de los tratamientos de datos de carácter personal.

- Asignar a los nuevos usuarios el correspondiente código de usuario y una contraseña, dándoles las instrucciones para que cambien la contraseña asignada en un plazo no superior a veinticuatro horas, de tal forma que la contraseña pase a ser del exclusivo conocimiento del usuario.

- Borrar los identificadores de usuario y contraseñas cuando un usuario sea dado de baja.

- Autorizar expresamente a la persona que entregue para su salida, o reciba de terceros, soportes informáticos que contengan datos de carácter personal. La autorización la realizará de forma específica para cada recepción o entrega, mediante firma en el impreso correspondiente, o de forma genérica, también mediante autorización escrita.

- Conservar los impresos cumplimentados de entradas y salidas de soportes.

- Controlar los mecanismos establecidos para el registro de accesos, los cuales no podrán ser desactivados en ningún caso.

- Establecer y comprobar todos los procedimientos y estándares necesarios para la correcta aplicación de la normativa de seguridad.

6.5. Responsable del Servicio

El Responsable del servicio:

- Determinará los requisitos que deben ser tenidos en cuenta a la hora de prestar servicios a las administraciones y organismos públicos.
- Estará en contacto con el responsable por parte del cliente contratado por la administración u organismo público con el fin de consensuar los requisitos del servicio.
- Comunicará los requisitos del servicio a todo el personal de la organización implicado en la prestación del servicio.
- Velará por el cumplimiento de los requisitos del servicio y realizará un seguimiento exhaustivo de su cumplimiento por parte de la organización.

6.6. Administradores del sistema

Los administradores del sistema son designados por el responsable de seguridad y realizan tareas específicas de administración de servidores, de la red interna y distintas VPNs del proyecto. Este cargo se irá renovando automáticamente hasta que el responsable de seguridad anuncie la sustitución de la persona que ocupa el cargo.

6.7. Usuarios

Los usuarios / personal técnico, acceden a las aplicaciones con el perfil suficiente para desempeñar sus funciones profesionales, debido a la función asignada o del puesto de trabajo que despeñan y de la unidad administrativa en la que se encuadra.

7. CONCIENCIACIÓN Y FORMACIÓN

Se desarrollarán actuaciones de concienciación y formación. El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de la organización y a todas las actividades, de acuerdo con el principio de Seguridad Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Se va a incluir en el Plan de Formación, los cursos gratuitos publicados por el CCN-CERT en su plataforma ÁNGELES (ÁNGELES - Cursos STIC (cni.es) relacionados con la

seguridad de la información.

8. SEGURIDAD POR DEFECTO

Antes de realizar cualquier tipo de modificación de políticas, procedimientos o usos de nuevas herramientas aplicables a los servicios que se prestan a las Administraciones y organismos públicos en el marco del alcance del ENS, se tendrán en cuenta todos los aspectos de seguridad de la información requeridos por el ENS, y por cualquier otra legislación aplicable que resulte de aplicación, así como cualquier otro requisito de seguridad de la información requerido por cualquier Administración u organismo público que contrate cualquiera de los servicios enmarcados dentro del alcance del ENS.

9. PROCESO DE COORDINACIÓN Y RESOLUCIÓN DE CONFLICTOS Y RECLAMACIONES

En caso de conflicto entre los distintos perfiles de puesto integrados en el Comité de Seguridad, prevalecerán las instrucciones facilitadas por la Dirección General y, en su defecto por el Responsable de Seguridad de la Información.

10. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Cualquier elemento físico o lógico requiere la autorización del Responsable de Seguridad de la Información para poder proceder a su instalación en los sistemas de información de TERRANOVA.

Se realizan test periódicos de vulnerabilidades técnicas para comprobar el estado de la seguridad de los sistemas de información de TERRANOVA.

11. PREVENCIÓN ANTE OTROS SISTEMAS INTERCONECTADOS

Todos los intercambios de información y prestación de servicios con otros sistemas serán objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.

Y para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada, siguiendo la Guía de Seguridad CCN-STIC 811.

12. ENTRADA EN VIGOR Y PUBLICACIÓN

Esta Política se Seguridad de la Información es efectiva desde el día siguiente de su aprobación y hasta que no sea reemplazada por otra versión posterior, siendo de acceso público a través de la web de TERRANOVA.

Florencia, 16/04/2026

RESPONSABLE DE SEGURIDAD