POLÍTICA DE **SEGURIDAD DE LA INFORMACIÓN**

APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Gerencia de PRO-DATOS, el día 10 de Octubre de 2024
Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

INTRODUCCIÓN

PRO-DATOS depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad (confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad) de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, en pliegos de licitación y en contratos para proyectos de TIC.

El personal debe estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

PREVENCIÓN

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

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

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 actuaren consecuencia.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

RESPUESTA

PRODATOS deberá:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en la organización 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).

RECUPERACIÓN

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

ALCANCE

Esta Política será de aplicación y de obligado cumplimiento para toda la organización PRODATOS, a sus recursos y a los procesos afectados por el ENS, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Todos los miembros de PRODATOS, afectados por el alcance del ENS, tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad correspondiente, siendo responsabilidad de PRODATOS disponer los medios necesarios para que la información llegue al personal afectado.

MISIÓN

Ofrecer servicios de recogida y destrucción de documentos sensibles de las empresas u organismos mediante trituración de nivel 6, garantizando la máxima seguridad y confidencialidad en el manejo de información sensible. Nos especializamos en la destrucción de papel, planos, documentos, dibujos y así como soportes digitales como CD y DVD, proporcionando a nuestros clientes una solución integral y sostenible para la gestión de su documentación confidencial, en cumplimiento con las normativas vigentes UNE-EN 15713:2010, siendo respetuosos con el medio ambiente.

La Dirección de PRODATOS, ha establecido en su organización un Sistema de Gestión de la Seguridad de la Información basado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, atendiendo a los siguientes objetivos:

- Proporcionar servicios de destrucción mediante trituración de nivel 6 para garantizar que la información contenida en documentos y soportes digitales sea completamente irreconocible y no recuperable.
- Asegurar que todas las operaciones de recogida y destrucción cumplan con la normativa vigente en materia de protección de datos y confidencialidad, así como con los estándares establecidos en la ENS.

- Capacitar a todo el personal involucrado en el proceso de recogida y destrucción para que estén al tanto de las mejores prácticas en seguridad de la información y cumplan con los protocolos establecidos.
- Establecer un sistema de trazabilidad que permita registrar cada etapa del proceso de destrucción, proporcionando a los clientes informes claros y verificables que respalden la destrucción de sus documentos y soportes.

MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades de PRODATOS, y en particular la prestación de sus servicios electrónicos a la ciudadanía está integrado por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- UNE 15713 – Destrucción Segura de Material Confidencial. Código de Buenas Prácticas
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD).

COMITÉ DE SEGURIDAD DE LA INFORMACION

Responsable de la Información	Enrique del Olmo Benlloch
Responsable del Servicio	
Responsable de Seguridad	Marta del Olmo Maroto
Responsable de Sistemas	María Victoria del Olmo Maroto

ROLES: FUNCIONES Y RESPONSABILIDADES

- **RESPONSABLE DE LA INFORMACIÓN - RESPONSABLE DEL SERVICIO,** será quien determine los requisitos de los servicios prestados, en consonancia, tendrá las siguientes funciones:
  - Establecer y aprobar los requisitos de seguridad aplicables al servicio dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, previa propuesta del Responsable de Seguridad y/o Comité de Seguridad de la Información.
  - Aceptar los niveles de riesgo residual que afecten al Servicio.
  - Aprueba la Política de Seguridad de la Información
  - Emprende y dirige la política de seguridad de la información.
  - Aporta los recursos financieros para la Seguridad de la Información
  - Aprueba el Plan de continuidad de Negocio
  - Aprueba el sistema de gestión de la información

- **RESPONSABLE DE SEGURIDAD,** será quien tome las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios. Dispondrá de las siguientes funciones:
  - Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
  - Promover la formación y concienciación en materia de seguridad de la información.
  - Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad; identificar medidas de seguridad; determinar configuraciones necesarias; elaborar documentación del sistema.
  - Proporcionar asesoramiento para la determinación de la categoría del sistema en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información.
  - Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
  - Gestionar las revisiones externas o internas del sistema.
  - Gestionar los procesos de certificación.
  - Gestiona los incidentes de seguridad y las acciones correctivas correspondientes.
  - Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
  - Mantiene el Pan de Continuidad de Negocio.
  - Elabora, o participa en la elaboración, de los documentos de seguridad de Prodatos, en su caso.
  - Elabora los acuerdos para el tratamiento de datos por terceros.
  - 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.
  - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.

- **RESPONSABLE DE SISTEMAS**, dentro de sus áreas de actuación, tendrán asignadas las siguientes funciones:
  - 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.
  - Elaborar 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.
  - Prestar al Responsable de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
  - Colaborar, si así se le requiere, 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 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.
    - Dar de alta o baja los usuarios.
    - Lleva el registro de entrada y salida de soportes.

PROCEDIMIENTOS DE DESIGNACIÓN

La responsabilidad general de la seguridad de la información recaerá sobre el **Responsable de Seguridad**, siendo la responsabilidad última del Comité de Seguridad de la Información y de la Dirección como máximo Responsable del Sistema de gestión de seguridad de la información.

El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Dirección de PRODATOS y difundida para que la conozcan todas las partes afectadas.

DATOS DE CARÁCTER PERSONAL

PRO-DATOS trata datos de carácter personal. El documento de seguridad ANEXO I DESCRIPCION DE LOS TRATAMIENTO Y REGISTROS DE LAS ACTIVIDADES DEL TRATAMIENTO, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de PRO-DATOS se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de PRO-DATOS en diferentes materias:

- P03-01 Política de Contraseñas
- P03-02Política de Control de Accesos
- P04-01 Política de Uso aceptable de Activo
- P04-02 Política de Controles Criptográficas
- P06-01 Política de Uso aceptable de servicio en la nube

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la PRO-DATOS que necesiten

conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La Política de Seguridad de la Información estará disponible en la página web de la organización.

OBLIGACIONES DEL PERSONAL

Todos los miembros de PRO-DATOS tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.
Todos los miembros de PRO-DATOS atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año.

Se establecerá un programa de concienciación continua para atender a todos los miembros de PRO-DATOS, en particular a los de nueva incorporación.
Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo

TERCERAS PARTES

Cuando PRO-DATOS preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
Cuando PRO-DATOS utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en
materia de seguridad, al menos al mismo nivel que el establecido en esta Política.
Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

DIRECCION
10 de Octubre de 2024
Rev. 01