Política de Seguridad de la Información

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día **19 de marzo de 2025** por la Dirección General.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

SICOMORO SERVICIOS INTEGRALES, S.L. 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 disponibilidad, integridad o confidencialidad 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, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo a los artículos 6, 7, 8,9, 11 y12 del ENS (Real Decreto 311/2022, de 3 de mayo que modifica el Esquema Nacional de Seguridad (ENS)).

2.1. 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.

2.2. VIGILANCIA CONTINUA

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. Se deben establecer los procedimientos necesarios para garantizar la vigilancia continua y la evaluación periódica de los sistemas de información para detectar y corregir las vulnerabilidades en tiempo real. Articulo 6 capitulo II ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Capitulo II, sección 2.

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.

2.3. RESPUESTA

La Entidad ha establecido mecanismos para responder eficazmente a los incidentes de seguridad.

Se ha designado un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

Se han establecido protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. RECUPERACIÓN

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

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de la entidad y a todos los miembros de la organización, implicados en Servicios y Proyectos destinados al sector público, que requieran la aplicación de ENS, sin excepciones.

4. MISIÓN

Los principales objetivos que se persiguen son:

- Fomentar la relación electrónica del usuario con la Entidad o la de sus Clientes.
- Reducir tiempos de espera de atención al usuario.
- Acortar tiempos de espera en la resolución de trámites solicitados por el usuario.
- Desarrollar un sistema de gestión de información documental que facilite un rápido acceso del personal del servicio a la información solicitada por el usuario.

5. MARCO NORMATIVO

Esta política se enmarca en la siguiente legislación:

1. Real Decreto 311/2022, de 3 de mayo. Esta modificación tiene como objetivo actualizar y mejorar el ENS para adaptarlo a los nuevos retos y amenazas en materia de seguridad informática. Fue publicado en el BOE núm. 106, de 4 de mayo de 2022.
2. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
3. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
4. 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.
5. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
6. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
7. Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad TIC estará formado por: el Responsable de Seguridad GRPD, el Responsable del Departamento de Desarrollo, el Responsable del departamento de Administración, el Responsable del departamento de Sistemas/Soporte, el Responsable de Sistemas de Gestión ISO e ENS.

El Secretario del Comité de Seguridad TIC será el Responsable del departamento de Administración que se encargará de convocar las reuniones del Comité y levantar acta de las mismas.

El Comité de Seguridad TIC reportará a la Gerencia de la Entidad.

El Comité de Seguridad TIC tendrá las siguientes funciones:

- Coordinar y aprobar las acciones en materia de seguridad de la información.
- Impulsar la cultura en seguridad de la información.
- Participar en la categorización de los sistemas y el análisis de riesgos.
- Revisar la documentación relacionada con la seguridad del sistema.
- Resolver discrepancias y problemas que puedan surgir en la gestión de la seguridad.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Las responsabilidades del Responsable de Seguridad de la Información son:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos de los mismos.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

Las responsabilidades del Responsable del Sistema son:

- Gestionar el Sistema durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión el manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por la Dirección de la Entidad, a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política. Esta designación deberá ser aprobada por la dirección de la Entidad.

En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado. En el caso de que la entidad deba designar uno, este POC será designado por el comité de seguridad TIC de forma específica.

6.4. 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 la Entidad y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

La Entidad trata datos de carácter personal. El “Manual de Protección de Datos Personales”, al que tendrán acceso sólo las personas autorizadas, recoge los tratamientos afectados y los responsables correspondientes. Todos los sistemas de información de la Entidad se ajustarán a las medias de seguridad requeridos por su análisis de riegos y por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado “Manual de Protección de Datos Personales” y en la documentación de dicho sistema.

8. 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.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de la Entidad en diferentes materias:

- a) Política de gestión de riesgos.
- b) Política de gestión de personal.
- c) Políticas de adquisición y contratación.
- d) Políticas de protección de la información.

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

La política de seguridad estará disponible en la intranet y en la web corporativa de TICKAMORE.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de la entidad 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 la entidad atenderán a sesiones de concienciación en materia de seguridad TIC. Se establecerá un programa de concienciación continua para atender a todos los miembros de la entidad, 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.

11. TERCERAS PARTES

Cuando la Entidad 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 la Entidad 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.

En Zaragoza a 19 de marzo de 2025.

D. Santiago Castillón

Director SICOMORO SERVICIOS INTEGRALES, .S.L. (TICKAMORE)

Control del Documento

Fecha	Versión	Propuesto por	Aprobado por	Observaciones
22/03/2022	1	Ismael Trigo	Santiago Castillón	Aprobación Inicial
04/05/2023	2	Ismael Trigo	Santiago Castillón	Cambios actualización RD 3/2010 por RD 311/2022. Inclusión del principio de Vigilancia Continua en apartado 2.2. Otras actualizaciones de; Marco Normativo, desarrollo de políticas y detalle del comité TIC. Designación del POC punto 6.3. Cambio de Logotipo corporativo.