



Política de Seguridad

ENS

Sistema de gestión de la calidad

Tipo de documento:	Política		
Código de documento	Versión	Fecha	Elaborado por
PL.ENS.01	0	24/06/2024	Roberto Reta Salán
Estado del Documento	En vigor		

Gestión documental.

Control de versiones.

Edición	Fecha	Autor	Comentario
v.1	06/2023	Roberto Reta	Edición

Aprobado por:		Fecha
Nombre	José Castellanos	2 de julio de 2024
Firma		

Control de Revisiones.

Edición	Fecha Revisión	Autor	Observaciones
V 1.0			

Tabla de contenido

1	Aprobación y entrada en vigor	1
2	Introducción	1
2.1	Prevención	2
2.2	Detección	2
2.3	Respuesta.....	2
2.4	Recuperación	2
3	Misión.....	3
4	Alcance.....	4
5	Declaración de la política de seguridad de la información.....	4
6	Marco normativo.....	6
7	Organización de la seguridad	7
7.1	Comité de seguridad: Funciones y Responsabilidades	7
7.2	Roles: Funciones y Responsabilidades.....	8
7.2.1	Tareas.....	10
8	Procedimientos de designación.....	11
9	Política de seguridad de la información.....	11
9.1	Datos de Carácter Personal.....	11
9.2	Gestión de Riesgos	11
9.3	Desarrollo de la política de seguridad de la información.....	12
9.3.1	Política de Uso Aceptable	12
9.3.2	Seguridad de la gestión de recursos humanos.....	12

9.3.3	Seguridad física y del entorno.....	13
9.3.4	Áreas seguras.....	13
9.3.5	Seguridad de los equipos.....	13
9.3.6	Adquisición de productos:	13
9.3.7	Seguridad por defecto:	14
9.3.8	Integración y actualización del sistema:.....	14
9.3.9	Protección de la información almacenada y en tránsito:.....	14
9.3.10	Prevención ante otros sistemas de información interconectados:	15
9.3.11	Registro de actividad:	15
9.3.12	Gestión de comunicaciones y operaciones.....	16
9.3.13	Procedimientos operativos y responsabilidades	16
9.3.14	Protección frente a código malicioso y código móvil.....	16
9.3.15	Copias de seguridad.....	16
9.3.16	Gestión de la seguridad de la red.....	17
9.3.17	Gestión de soportes	17
9.3.18	Intercambio de información.....	17
9.3.19	Seguimiento.....	17
9.3.20	Control de accesos	17
9.3.21	Requisitos del servicio para el control de accesos	17
9.3.22	Gestión de accesos de los usuarios.....	17
9.3.23	Responsabilidades del usuario	18
9.3.24	Control de acceso a la red	18
9.3.25	Informática móvil y teletrabajo	18

9.3.26	Gestión de incidencias.....	18
9.3.27	Continuidad del servicio	18
9.3.28	Mejora continua del proceso de seguridad:	19
10	Obligaciones del personal.....	19
10.1	Terceras partes	19

1 Aprobación y entrada en vigor

Esta Política de Seguridad de la Información es efectiva desde la fecha de su aprobación por el Comité de Seguridad, hasta que sea reemplazada por una nueva Política.

2 Introducción

TIGLOO 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, confidencialidad, autenticidad, o trazabilidad 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 disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, 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 se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos y Reglamento Europeo de Protección de Datos, 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.

TIGLOO debe cerciorarse de que la seguridad de la información 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.

TIGLOO debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad y a la Ley Orgánica de Protección de Datos.

Esta Política de Seguridad sigue las indicaciones de la guía **CCN-STIC-805 del Centro Criptológico Nacional**, centro adscrito al Centro Nacional de Inteligencia.

2.1 Prevención

TIGLOO debe 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 se implementarán las medidas mínimas de seguridad determinadas por el ENS (311/2022), RGPD (679/2016) y la LOPD y GDD 03/2018, 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **TIGLOO** debe:

- 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 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua, para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS (*Prevención, detección, respuesta y conservación*). Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya prestablecido como normales.

2.3 Respuesta

TIGLOO:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos (definida como parte del proyecto donde se incluyen los teléfonos y correos electrónicos de contacto).
- Establecer protocolos de intercambio de información relacionada con incidentes con clientes y proveedores.

2.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, **TIGLOO** ha desarrollado planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

3 Misión

TIGLOO define la presente Política de Seguridad de la Información, de carácter obligatorio para empleados y empresas colaboradoras, teniendo como objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve a **TIGLOO** para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- **Disponibilidad:** propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- **Integridad:** propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- **Confidencialidad:** propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- **Autenticidad:** propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- **Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en **TIGLOO** serán:

- Velar por la seguridad de la información, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de contingencias y continuidad de la actividad que se definan para los distintos servicios ofrecidos por la organización.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

Esta Política de Seguridad:

- Se aprobará formalmente por la organización.
- Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Se comunicará a todos los empleados y empresas externas que trabajen con **TIGLOO**.

4 Alcance

La Política de Seguridad se aplica a toda la empresa y a sus activos de **“Los sistemas de seguridad de información de los procesos de HelpDesk y Operaciones que componen el Servicio Gestionado sobre las infraestructuras TI de clientes y ciberseguridad operado desde las oficinas centrales de SEIN TIC”**

A todos los departamentos, tanto a sus directivos como a empleados.

- A los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la organización.
- A bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- A la información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.
- A la información cedida dentro de un marco legal establecido, que será considerada como propia a efectos exclusivos de su protección.
- A todos los sistemas utilizados para administrar y gestionar la información, sean propios o alquilados o licenciados por la misma.

5 Declaración de la política de seguridad de la información

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de **TIGLOO**.

- En **TIGLOO** se reconoce expresamente la importancia de la información, así como la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad de la Institución, o al menos suponer daños muy importantes, si se produjera una pérdida total e irreversible de determinados datos.
- **TIGLOO** implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad, del RGPD y de la Ley Orgánica de Protección de Datos, y cumple con todos los requisitos legales aplicables.
- La información y los servicios están protegidos contra pérdidas de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Los controles serán proporcionales a la criticidad de los activos a proteger y a su clasificación.

- La responsabilidad de la seguridad de la información involucrada en la prestación de los servicios incluidos en el alcance del ENS es de la Dirección, que pondrá los medios adecuados, sin perjuicio de que los empleados o usuarios asuman su parte de responsabilidad respecto a los medios que utiliza, según lo indicado en las normativas y en los procedimientos complementarios. En el punto 7 "Organización de la Seguridad" de este mismo documento se describen las funciones y responsabilidades del Comité de Seguridad, que gestionará la seguridad de la información, y de sus miembros.
- Quienes desempeñen la función de Seguridad de la Información y otras de administración relacionadas, serán quienes administren la seguridad.
- Se ha identificado a los responsables de la información, que deberán promover el establecimiento de los controles y medidas destinadas a proteger los datos que la integran, especialmente los de carácter personal o críticos.
- Se establecerá dentro de la normativa un sistema de clasificación de la información, con diferentes niveles.
- Se establecerán los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y, en general, de cualquier activo de **TIGLOO**.
- Los aspectos específicos más relacionados con la información sobre datos personales están regulados por el conjunto de normas recogidas en este documento de seguridad y en la normativa interna o de otra índole a la que pueda remitir o que se cite.
- Quienes no cumplan lo determinado en estas normas y en los procedimientos complementarios podrán ser sancionados de acuerdo con la legislación laboral, o bien con sanciones personalizadas si están vinculados a **TIGLOO** bajo contratos no laborales, de acuerdo con las cláusulas que figuren en dichos contratos en este último caso.
- Deberán realizarse periódicamente evaluaciones de riesgos y, en función de las debilidades, determinar si es necesario elaborar planes de implantación o reforzamiento de controles.
- Se fomentará la difusión de información y formación en seguridad a empleados y colaboradores, previniendo la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar su posible existencia lo antes posible, y en caso de que existieren, procurándose una difusión muy restringida de las indagaciones.
- El personal de **TIGLOO** deberá conocer las normas, reglas, estándares y procedimientos relacionados con su puesto de trabajo, así como sus funciones y obligaciones, además de la separación de funciones y la revisión independiente de los registros, cuando sea necesario, de quién ha hecho qué, cuándo y desde dónde.
- Las incidencias de seguridad serán comunicadas y tratadas apropiadamente.

6 Marco normativo

Según la legislación vigente, las leyes aplicables a **TIGLOO** en materia de Seguridad de la Información son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica. BOE de 4 mayo de 2022.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- LOPD y garantías de los derechos digitales 03/2018
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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.
- Así mismo la legislación específica asociada está definida conforme registro AN_Legislación.

TIGLOO cumple con la legislación citada y con todos sus requisitos.

7 Organización de la seguridad

7.1 Comité de seguridad: Funciones y Responsabilidades

El Comité de Seguridad coordina la seguridad de la información en **TIGLOO**.

El **Comité de Seguridad** reportará a la organización.

El **Secretario del Comité de Seguridad** será el Responsable de Seguridad y tendrá como funciones:

- Convoca las reuniones del Comité de Seguridad.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Responsabilizarse de que se elaboren las actas de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El **Comité de Seguridad** tendrá las siguientes funciones:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de **TIGLOO** en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de los diferentes departamentos en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la organización.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de los Responsables de área, técnicos y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por **TIGLOO** y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de los diferentes departamentos en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de **TIGLOO**. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes departamentos.
- Priorizar 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 TIC 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.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Informar regularmente del estado de la seguridad de la información a la Dirección.

7.2 Roles: Funciones y Responsabilidades

En el caso de **TIGLOO** todas las responsabilidades recaen en los diferentes puestos que han sido nombrados en la organización por la Dirección; su renovación se deberá a la designación por parte de la Dirección de los diferentes cargos.

Las funciones y responsabilidades se detallan a continuación:

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.

Responsable de la Información

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

Responsable de Seguridad

- 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 este.
- 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.

Responsable de Sistemas:

- 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.
- 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 del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

7.2.1 Tareas

RINFO – Responsable de la Información

RSEG – Responsable de la Seguridad

RSERV – Responsable del Servicio

RSIS – Responsable de Sistemas

Tarea	Responsable
Garantizar el cumplimiento de los deberes de secreto y seguridad.	RINFO
Garantizar derechos LOPD/RGPD	RINFO
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o el Comité de Seguridad
Determinación de la categoría del sistema	RESER
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	RSEG
Implantación de las medidas de seguridad	RSEG
Aceptación del riesgo residual	RINFO + RSERV+RSEG (Comité de Seguridad)
Documentación de seguridad del sistema	RSEG
Política de seguridad	Elabora: comité de seguridad Aprueba : Organización
Normativa de seguridad	Elabora y aprueba: Comité de Seguridad
Procedimientos operativos de seguridad	Elabora y aprueba: RSEG Aplica: TIGLOO
Estado de la seguridad del sistema	Monitoriza: RSEG
Planes de mejora de la seguridad	Elaboran: RSIS + RSEG Aprueba: Comité de Seguridad
Planes de concienciación y formación	Elabora: RSEG Aprueba: comité de seguridad
Planes de continuidad	Elabora: RSIS Valida: RSEG Coordina y aprueba: comité de seguridad Ejercicios: RSER+RSEG
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	Elabora: RSIS Aprueba: RSEG

8 Procedimientos de designación

El procedimiento de Designación se detalla a continuación.

La Dirección nombra:

- Responsable de Seguridad, que reportará al Comité de Seguridad.
- Responsable del Servicio, que reportará al Comité de Seguridad.
- Responsable de la Información. Que reportará al Comité de Seguridad.
- R. Sistemas. Que reportará al Comité de Seguridad.

9 Política de seguridad de la información

Será misión del Comité de Seguridad 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 organización y difundida para que la conozcan todas las partes afectadas.

9.1 Datos de Carácter Personal

La Ley Orgánica de Protección de Datos y GDD 03/2018 (LOPD) y el RGPD 679/2016, tratan de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, y resulta de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

Todos los sistemas de información de **TIGLOO** se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal.

Para garantizar dicha protección, se han adoptado las medidas de seguridad que se correspondan con las exigencias previstas en la legislación de aplicación.

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con **TIGLOO**.

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

La gestión de riesgos quedará documentada en el informe de Análisis y Gestión de riesgos.

9.3 Desarrollo de la política de seguridad de la información

9.3.1 Política de Uso Aceptable

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de los equipos están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso intencionadamente. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus

9.3.2 Seguridad de la gestión de recursos humanos

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información confidencial.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede.

Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

9.3.3 Seguridad física y del entorno

Para que una seguridad lógica sea efectiva, es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa.

9.3.4 Áreas seguras

TIGLOO tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.

La totalidad de las instalaciones de **TIGLOO** cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen; en concreto un control de recepción e identificación del visitante y el acompañamiento del personal durante la estancia en las instalaciones.

9.3.5 Seguridad de los equipos

Los equipos informáticos son un activo importante del que depende la continuidad de las actividades, por lo que serán protegidos de manera adecuada y eficaz.

Los equipos informáticos de **TIGLOO** están protegidos contra posibles fallos de energía (ordenador portátil con batería, SAIs, etc.).

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones recomendadas por el suministrador. Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación. También será necesario adoptar las medidas de precaución necesarias en caso de los equipos deban abandonar las instalaciones para su mantenimiento.

9.3.6 Adquisición de productos:

TIGLOO establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

- a) Atenderán a las conclusiones del análisis de riesgos: [op.pl.1].
- b) Serán acordes a la arquitectura de seguridad escogida: [op.pl.2].
- c) Contemplarán las necesidades técnicas, de formación y de financiación de forma conjunta para:
 - La implantación inicial.
 - El mantenimiento a lo largo de la vida útil.

9.3.7 Seguridad por defecto:

Se aplicará la regla de «seguridad por defecto»:

1. Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
2. Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.
3. El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

9.3.8 Integración y actualización del sistema:

En las funciones de mantenimiento, se dispone de procedimientos para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

En la actualización del sistema, se mantendrá un control continuo de cambios realizados en el sistema, de forma que:

- a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.
- b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.
- c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.
- d) Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación

9.3.9 Protección de la información almacenada y en tránsito:

El responsable de sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.

Para ello:

- a) Se dispondrá de un registro de salida que identifique al transportista que recibe el soporte para su traslado.
- b) Se dispondrá de un registro de entrada que identifique al transportista que lo entrega.
- c) Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.
- d) Se utilizarán los medios de protección criptográfica (mp.si.2 criptografía) correspondientes al nivel de calificación de la información contenida de mayor nivel.
- e) Se gestionarán las claves según op.exp.10 protección de claves criptográficas.

9.3.10 Prevención ante otros sistemas de información interconectados:

Dos o más sistemas de información pueden comunicarse entre sí para intercambiar información o servicios. Se produce una interconexión de sistemas cuando

- Existe una conexión.
- Se habilitan flujos de comunicación entre los sistemas conectados.
- Esa conexión se produce entre sistemas con diferente responsable de seguridad o de diferente categoría (de acuerdo con el anexo I del ENS).

Cuando en TIGLOO se produzcan interconexiones de sistemas se atenderá:

- Al mínimo privilegio: para los usuarios y los procesos autorizados.
- Nodo auto protegido: cuando un nodo se conecta a otro, debe partir de la base de que el otro nodo no es fiable.
- Despliegue mínimo: En otras palabras, en el perímetro no habrá nada que no sea imprescindible. El objeto último es reducir la superficie de exposición a un ataque.

9.3.11 Registro de actividad:

TIGLOO protege los registros del sistema, de forma que:

- a) Determinando el periodo de retención de los registros.
- b) Se asegurará la fecha y hora. Ver
- c) Los registros no podrán ser modificados ni eliminados por personal no autorizado.
- d) Las copias de seguridad, se ajustarán a los mismos requisitos.
- e) Existe un procedimiento para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad.
- f) los registros están contemplados en los procesos de copias de seguridad garantizando las seguridades mencionadas

9.3.12 Gestión de comunicaciones y operaciones

9.3.13 Procedimientos operativos y responsabilidades

TIGLOO controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red de **TIGLOO** y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red existirán mecanismos para limitar los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del dominio. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo a estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

En algunos casos será necesario que distintas áreas estén lógicamente separadas del resto para evitar accesos no autorizados.

9.3.14 Protección frente a código malicioso y código móvil

Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de **TIGLOO**.

Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado por el Responsable de Seguridad y autorizado por el comité.

El Administrador del Sistema instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

9.3.15 Copias de seguridad

Los datos deben ser guardados en los servidores para asegurar que se realizan copias de seguridad habitualmente.

9.3.16 Gestión de la seguridad de la red

Los elementos de red (switch, router...etc.) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema.

Existirá una gestión gráfica de la red de forma que su mantenimiento pueda resultar más cómodo.

9.3.17 Gestión de soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a los ficheros de donde han sido extraídos.

9.3.18 Intercambio de información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, etc.).

9.3.19 Seguimiento

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos así como para recomendar cualquier cambio que se estime necesario.

9.3.20 Control de accesos

9.3.21 Requisitos del servicio para el control de accesos

La información debe estar protegida contra accesos no autorizados. El Responsable del Servicio definirá las necesidades de acceso a la información a dos niveles, para el conjunto de áreas y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

9.3.22 Gestión de accesos de los usuarios

El administrador del sistema es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.

Cada usuario deberá estar asociado a un perfil, de acuerdo a las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a información y sistemas que no le son necesarios para las competencias de su trabajo.

9.3.23 Responsabilidades del usuario

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

9.3.24 Control de acceso a la red

No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con **TIGLOO** para mantener el mismo nivel de seguridad que si fueran empleados de la propia organización.

9.3.25 Informática móvil y teletrabajo

Cuando los equipos o la información propiedad de **TIGLOO** están fuera de las instalaciones, es el empleado que los está utilizando el que debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

9.3.26 Gestión de incidencias

Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Responsable de Sistemas y de Seguridad, para que tome las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

9.3.27 Continuidad del servicio

Es imprescindible para **TIGLOO** establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad de la actividad en estos casos, **TIGLOO** establecerá planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del servicio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia que deberán probarse y actualizarse regularmente para comprobar su idoneidad.

La gestión de la continuidad del servicio se incorporará a los procesos de **TIGLOO** y será responsabilidad de una o varias personas dentro de la entidad.

9.3.28 Mejora continua del proceso de seguridad:

TIGLOO realiza una evaluación constante (objetivos e indicadores) y análisis de la respuesta a los incidentes, etc. de forma que se aprende de la experiencia, se corrigen defectos o debilidades y se busca la excelencia en la gestión del ENS. A fin de alcanzar una mejora continua.

10 Obligaciones del personal

Todos los miembros de **TIGLOO** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **TIGLOO** recibirán concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **TIGLOO**, 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.

10.1 Terceras partes

Cuando **TIGLOO** preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **TIGLOO** utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que atañe 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 roles y responsabilidades.

Es responsabilidad del responsable del SGSI asegurar que el contenido de esta plantilla responde a las necesidades de control y gestión documental que el SGSI necesita y diseñar, junto con el equipo de marketing, el formato del documento.