DESIC

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Sistema de Gestión de Seguridad de la Información

Nombre:	NS-01-Politica de seguridad de la información
Título:	Política de Seguridad de la Información
Edición:	V.3.
Clasificación:	Público
Estado:	Publicado
Fecha:	05/10/2022
Página:	1/22
Editado por:	Responsable de Seguridad de la Información
Revisado por:	Comité de Seguridad de la Información
Aprobado por:	Comité de Seguridad de la Información

1 **Copia controlada** **Nº** **1**

☐ **Copia no controlada**

DESIC

HOJA DE CONTROL			
Título	Política de Seguridad de la Información		
Entregable	NS-SGSI-01 Politica de seguridad de la información.docx		
Nombre del Fichero	NS-SGSI-01 Politica de seguridad de la información.docx		
Autor	Responsable de Seguridad de la Información		
Versión/Edición	V.3	**Fecha Versión**	05/10/2022
Aprobado por	Comité de Seguridad de la Información	**Fecha Aprobación**	05/10/2022
		Nº Total Páginas	22

REGISTRO DE CAMBIOS				
Versión	**Cambio**	**Responsable del Cambio**	**Área**	**Fecha del Cambio**
V.1.	Creación del documento	Responsable de Seguridad de la Información	SGSI	27/07/2019
V.2	Ampliación de la actividad Mejora de la redacción Modificación de responsabilidades para alineación con las responsabilidades ISO 27001 Modificación del alcance cambiando el existente en el ENS y en ISO 27001. Incorporación de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.	Responsable de Seguridad de la Información	ENS	08/02/2022
V.3.	Se modifica la política haciendo mención al nuevo Real Decreto del ENS.	Responsable de Seguridad de la Información	ENS	05/10/2022

DESIC

ÍNDICE

1. INTRODUCCIÓN

La Política de seguridad de la Información vigente hasta la fecha ha sido aprobada por la Junta Directiva de DESIC, S.L. el 08 de febrero de 2022.

Esta Política de Seguridad de la Información debe ser reemplazada por la presente política en su V.3. aprobada con fecha 5 de octubre del 2022 debido a la creación de un nuevo Real Decreto para el ENS.

La entrada en vigor de la presente Política de Seguridad de la Información de DESIC, S.L. sustituye cualquier otra que existiera a nivel de los diferentes departamentos o áreas de la organización.

2. OBJETIVOS Y MISIÓN DE LA ORGANIZACIÓN

DESIC, S.L. presta servicios de hosting, desarrollo y mantenimiento de software y SAS (software as a service) a empresas, entidades y administraciones públicas. Para prestar sus servicios hace uso de sistemas de información que deben ser protegidos de una forma efectiva y eficiente.

El ENS es una norma jurídica definida en el Real Decreto 311/2022, y es de aplicación obligatoria para todas las Administraciones Públicas y empresas privadas que presten servicios o provean de soluciones a entidades públicas, con el objetivo de generar confianza en dichos sistemas.

Para dar cumplimiento a dicha obligatoriedad DESIC, S.L. ha aprobado la presente política de seguridad de la información para la protección de su sistema de información en base al ENS y a la ISO 27001 conforme al alcance definido para el sistema de gestión de seguridad de la información para cada una de las normas a las que se ha hecho referencia (ISO 27001 y ENS)

3. OBJETIVOS Y MISIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

DESIC, S.L. ha establecido un marco de gestión de la seguridad de la información según lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS y en la norma ISO 27001, reconociendo como activos estratégicos la información y los sistemas que la soportan.

Uno de los objetivos fundamentales de la implantación de las normas que constituyen el marco de referencia es asentar las bases sobre las cuales el personal, colaboradores y clientes, así como terceras partes interesadas de DESIC, S.L., puedan acceder y prestar los servicios en un entorno de gestión seguro, anticipándose la organización a sus necesidades, y preservando sus derechos.

La Política de Seguridad de la Información protege la información de las amenazas a la que ésta puede verse sometida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y asegurando el eficiente cumplimiento de los objetivos y servicios de DESIC, S.L.

El marco de gestión de seguridad de la información abarca igualmente la protección de datos de carácter personal y tiene en cuenta lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, en adelante RGPD, así como lo contemplado en la legislación de carácter nacional en dicha materia, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos de Carácter Personal y garantía de los Derechos Digitales

La gestión de la seguridad de la información garantiza el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada del funcionamiento de los mismos.

Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

1. **Implementar el valor de la Seguridad de la Información en el conjunto de la Organización**, contribuyendo con la gestión de la seguridad a cumplir la misión y objetivos establecidos por DESIC, S.L.
2. Disponer de las **medidas de control necesarias para el cumplimiento de los requisitos legales, normativos y de nuestros clientes y partes interesadas** relativos a la seguridad de la información que resulten de aplicación como consecuencia de la actividad desarrollada, especialmente los relativos a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.
3. Asegurar el acceso, **integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información** y la prestación continuada de los servicios, estableciendo un plan de seguridad de la información que integre las actividades de prevención y minimización del riesgo de los incidentes de seguridad en base a los criterios de gestión del riesgo establecidos por DESIC, S.L y en el ENS y a la monitorización continuada de nuestra actividad.
4. **Proteger los activos de la información de DESIC, S.L. y los sistemas de información que la soportan** de todas las amenazas, ya sean internas o externas, deliberadas o accidentales, con el objetivo de garantizar la continuidad en la prestación de nuestros servicios y la seguridad de la información en las vertientes de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
5. Definir como marco de gestión de la seguridad y el compromiso de mejora continua utilizando como **referencia el ENS y la norma ISO/IEC 27001** para establecer el sistema de gestión de la seguridad de la información y la norma ISO/IEC 27002 como conjunto de buenas prácticas para la gestión de la seguridad de la información.
6. Garantizar que todas y cada una de las **personas que componen la organización de DESIC, S.L. contribuyen a la protección de la Seguridad de la Información**, aportando los medios necesarios para poder realizar las actuaciones pertinentes de cara a la gestión de los riesgos identificados, asegurando que el personal conozca y siga las normativas de seguridad de DESIC, S.L. y asumiendo la responsabilidad en materia de

concienciación y formación en materia de seguridad de la información como medio para garantizar el cumplimiento de esta política.

7. Extender nuestro compromiso con la seguridad de la información a nuestros clientes, colaboradores y proveedores, así como a terceras partes interesadas.

Esta Política de Seguridad asegura un compromiso manifiesto de la Dirección de DESIC, S.L., para su difusión, consolidación y cumplimiento.

4. ALCANCE

La presente Política de Seguridad de la Información del SGSI es aplicable y de obligado cumplimiento a quienes tengan acceso los recursos que hayan sido identificados como *"activos de información"* de DESIC, S.L. dentro del alcance establecido del sistema de gestión de la seguridad, a sus recursos y a los procesos afectados por el ENS, RGPD y LOPDGDD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Dichos requisitos de protección afectan a toda la información en soporte electrónico o soporte papel y a los sistemas de información propiedad de la organización o gestionados para la misma.

ALCANCE SGSI ENS

Los sistemas de información que dan soporte a los procesos de gestión documental y desarrollo y mantenimiento de aplicaciones según la declaración de aplicabilidad vigente.

ALCANCE SGSI ISO 27001

Los sistemas de información que dan soporte a los procesos de desarrollo de aplicaciones informáticas y apps, hosting, housing, gestión de sistemas y consultoría de negocio.

5. MARCO NORMATIVO

Se toma como marco normativo de referencia además del ENS y la ISO 27001:2013, a título ejemplificativo, sin carácter exhaustivo, la siguiente legislación:

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- 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.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- 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).
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Asimismo, resultarán de aplicación cuantas otras normas regulen la actividad de DESIC, S.L. en el ámbito de la prestación de sus servicios y aquellas otras dirigidas a asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos gestionados de sus clientes empresas, entidades y administraciones públicas en el ejercicio de su actividad y competencias.

6. AUTORIDAD SOBRE LA POLÍTICA Y REVISIÓN

El Comité de Seguridad tiene la autoridad para verificar el cumplimiento de la presente Política de Seguridad, la responsabilidad de hacer cumplir las directrices generales y actuaciones correspondientes contenidas en el mismo y la independencia para plantear acciones correctivas y preventivas necesarias para cumplir los objetivos del plan de tratamiento de riesgos y la mejora continua de la seguridad de la información. Este comité se reunirá al menos cada **6 meses.**

Es responsabilidad de todas las personas y departamentos implicados en los procesos o servicios incluidos en el alcance, el obligado cumplimiento de la presente Política de Seguridad. Para conseguir este propósito es necesaria la implicación y participación de todo el personal de DESIC.

DESIC, S.L. podrá requerir la participación de proveedores y terceros en la aplicación de las medidas de seguridad que se determinen como mínimos exigibles.

El Comité de Seguridad de la Información es responsable de la presente Política de Seguridad y deberá realizar la revisión de este documento con al menos una periodicidad anual para valorar la vigencia del presente texto o la necesidad de su actualización en base a nuevos riesgos aparecidos o nuevas necesidades de garantizar la seguridad de la información.

Esta política será revisada al menos una vez al año y siempre que haya cambios relevantes en la organización de DESIC, con el fin de asegurar que ésta resulta adecuada a la estrategia y necesidades de la organización.

La Política será propuesta y revisada por el Comité de seguridad de la Información del que forma parte la Dirección de DESIC, S.L.

En caso de conflictos o diferentes interpretaciones de esta política se recurrirá al Comité de Seguridad de la Información.

7. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información de DESIC, S.L. son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, acordes con las funciones desempeñadas.

Para una mejor respuesta ante incidentes de seguridad, DESIC, S.L. mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, proveedores de servicios informáticos o de comunicación, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

La asignación y delimitación de responsabilidades para asegurar que se implanta y satisfacen los objetivos propuestos en la presente política de seguridad requieren del establecimiento de unas determinadas funciones encargadas de los aspectos generales de gestión de la seguridad de la información.

La gestión de la seguridad de la información es responsabilidad específica de un conjunto de personas y comités con funciones concretas, definidas y documentadas que se describe en los párrafos siguientes.

7.1. ROLES Y RESPONSABILIDADES

7.1.1. Responsable de la Información

Le corresponde la potestad de establecer los requisitos de la información en materia de seguridad, es decir, la potestad de determinar los niveles de seguridad de la información.

Dicha potestad se ejercitará por la Junta Directiva de DESIC, S.L, quien determinará los requisitos de seguridad aplicables a la información bajo su responsabilidad y su nivel correspondiente.

Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

El Responsable de la Información es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

7.1.2. Responsable de los servicios/ departamentos

Son los roles que deben establecer los requisitos de seguridad aplicables a los servicios bajo su responsabilidad. Este rol estará ostentado por cada uno de los directores de los departamentos de DESIC. Ostentarán las siguientes responsabilidades específicas:

- Determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
- Velar por la inclusión de cláusulas de seguridad en los contratos con terceras partes y por su cumplimiento.
- Colaborar en el análisis de impacto de los incidentes que se puedan producir y plantear las estrategias y salvaguardas ante los mismos.
- Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

7.1.3. Responsable del tratamiento

De acuerdo con lo especificado en el RGPD y la LOPDGDD, la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Este rol, que recae sobre DESIC, S.L., representada por la figura del Gerente.

7.1.4. Delegado de Protección de Datos

Tiene asignadas las funciones contempladas en el art. 39 del Reglamento General de Protección de Datos.

La designación para el desempeño de este rol se efectuará por la Junta Directiva de DESIC.

7.1.5. Responsable de la Seguridad

El Responsable de la Seguridad de la Información tomará las decisiones necesarias para satisfacer los requisitos de seguridad establecidos por el responsable y de los servicios. Este rol lo ostentará el responsable del área de sanidad asumiendo las siguientes responsabilidades específicas:

- Determinar las medidas de seguridad necesarias para la protección de la información manejada y los servicios prestados y verificar que las establecidas son adecuadas en todo momento.
- Determinar la categoría del sistema y las medidas de seguridad que deben aplicarse.
- Informar a los Responsables de la Información y de los Servicios de las incidencias de seguridad.
- Reportar el estado de la seguridad al Comité de Seguridad de la Información.
- Impulsar o instar la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
- Llevar a cabo el seguimiento de la Política de Seguridad de la Información de manera operativa así como de la seguridad física y lógica de los recursos.
- Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

7.1.6. Responsable de los sistemas

El responsable de los sistemas de información será el encargado de aplicar las medidas de seguridad de índole tecnológica determinadas por el Responsable de la seguridad. Este rol lo asumirá el Responsable TIC de DESIC que será designado por la Junta Directiva, asumiendo las siguientes responsabilidades específicas:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- 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 de seguridad se integren adecuadamente en el marco general de seguridad.
- Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

7.1.7. Administrador del sistema

El administrador del sistema depende del responsable del sistema y será designado por la Dirección a propuesta del Responsable del Sistema, debiendo reportar ante éste.

Sus funciones más significativas son las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad (POS).
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de

información.

- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

7.1.8. Responsable de RRHH

Pertenece al Comité de Seguridad de la Información y cumplirá la función de implicar a todo el personal de la organización en el conocimiento y cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan, así como de los cambios que en aquellas se produzcan. Igualmente, se responsabilizará de la implementación de los compromisos de confidencialidad que deban suscribir los empleados y colaboradores y de la capacitación continua de los mismos en materia de seguridad. Este rol es desempeñado por el Responsable de RRHH y gestión de personal.

7.2. COMITÉS: FUNCIONES Y RESPONSABILIDADES

Tomando como base esta política, el documento de organización de la seguridad detalla la gestión interna del Comité de Seguridad de Tecnologías de la Información y Comunicación (STIC) y del Comité de Seguridad de la Información (SI), identificando a todos sus miembros y detallando las atribuciones de cada responsable así como los mecanismos de coordinación y resolución de conflictos.

7.2.1. Junta Directiva de DESIC

En materia de seguridad de la información, la Junta Directiva de DESIC tiene las siguientes funciones:

- Aprobar, como parte del Comité de Seguridad de la Información, la Política de Seguridad de la Información de DESIC y cualquier otra política sectorial complementaria de la anterior que permita el cumplimiento del ENS e ISO 27001 y el Reglamento General de Protección de Datos y normativa aplicable en materia de protección de datos.
- Aprobar el desarrollo organizativo propuesto por el Comité de Seguridad de la Información (Comité SI).
- Nombramiento y cese de los integrantes del Comité SI.
- Adoptar las medidas pertinentes, en materia de seguridad de la información, a propuesta del Comité SI.
- Nombrar al Delegado de Protección de Datos, a propuesta del Presidente del Comité SI, previo informe del Responsable de Seguridad.

7.2.2. Comité de Seguridad de la Información

El comité CSI tiene las siguientes funciones:

- Elaborar y proponer la política de seguridad de la organización de DESIC, para su posterior aprobación por la Junta Directiva.
- Velar por que la seguridad de la información sea parte del proceso de planificación de DESIC, S.L.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial referente a la seguridad de la información y a la protección de datos de carácter personal.
- Elaborar y proponer a la Junta Directiva el desarrollo organizativo que permita el

cumplimiento del ENS, ISO 27001, así como del Reglamento General de Protección de Datos y normativa complementaria.

- Recabar informes regulares del estado de seguridad de la información de la organización y de los posibles incidentes referentes a Tecnologías de Información y Comunicación (TIC); trasladando sus conclusiones a la Junta Directiva y al Comité STIC.
- Coordinar las actuaciones de seguridad y dar respuesta a las inquietudes de seguridad transmitidas a través de los responsables de los distintos departamentos.
- Promover la difusión y apoyo a la seguridad de la información dentro de la estructura orgánica de DESIC.
- Llevar a cabo acciones de concienciación, formación y motivación del personal afectado por esta Política, sobre la importancia de lo establecido en el marco de gestión de seguridad de la información y sobre su implicación en el cumplimiento de las expectativas de los departamentos, usuarios y y la protección de su información.
- Nombramiento y cese de los integrantes del Comité de Seguridad de Tecnologías de Información y Comunicación (Comité STIC).

Este comité está conformado por los siguientes roles:

- Gerente
- DPO
- Miembros de la Junta Directiva
- Responsables de los servicios/ departamentos o áreas de DESIC
- Responsable de Seguridad de la Información, que actuará como coordinador del Comité SI.
- Responsable de RRHH.

7.2.3. Comité de Seguridad de Tecnologías de Información y Comunicación (STIC)

Se crea el Comité STIC que eleva a la Junta Directiva todas sus propuestas. El Comité STIC tiene las siguientes funciones:

- Proponer al Comité SI la revisión de la Política de Seguridad de la Información, para su ulterior elevación a la Junta Directiva.
- Proponer al Comité SI las instrucciones y circulares que permitan la implantación del ENS e ISO 27001 en DESIC.
- Proponer criterios de seguridad: redactar, revisar y evaluar las normas técnicas y pautas de seguridad así como los procedimientos de notificación de incidentes de seguridad.
- Evaluar e informar sobre los riesgos de seguridad en los activos TIC y activos físicos.
- Velar por el alineamiento de las actividades de seguridad de la información y los objetivos de DESIC, llevando a cabo acciones orientadas a la mejora continua de los procesos de seguridad de la información.
- Velar porque la seguridad de la información sea parte del proceso de planificación de DESIC.

Estará formado por los siguientes roles:

- Responsable de Seguridad de la Información
- Responsable del Sistema, que actuará como coordinador del Comité STIC.
- Administrador del sistema, que actuará como secretario.

El coordinador del Comité STIC podrá incorporar a los técnicos y asesores que considere oportunos para el desarrollo de sus competencias.

7.3. PROCEDIMIENTOS DE DESIGNACIÓN DE LOS COMITÉS

Corresponde a la Junta Directiva el nombramiento y el cese de los componentes del Comité de Seguridad de la Información, para el ejercicio de las competencias definidas en la presente política.

La Presidencia del Comité recaerá en el responsable del área de DESIC que tenga las competencias en materia de Nuevas Tecnologías. La Junta Directiva podrá revisar los

nombramientos del Comité de Seguridad de la Información cuando estime oportuno.

Corresponde al Comité de Seguridad de la Información el nombramiento y el cese de los componentes del Comité STIC, a propuesta del Responsable del Sistema, quien desempeñará el rol de Coordinador de este Comité.

El Comité de Seguridad de la Información podrá revisar los nombramientos del Comité STIC a solicitud del Gerente, o tras la baja voluntaria o forzosa de cualquiera de sus miembros.

8. ÁMBITOS DE GESTIÓN CUBIERTOS POR LA POLITICA

8.1. ANÁLISIS Y GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando ocurra un incidente grave de seguridad.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

El nivel de riesgo máximo aceptable, se establecerá en base a la metodología elegida, Magerit.

El nivel máximo de riesgo aceptable se utilizará como objetivo de mejora en los planes de mitigación de riesgo que se desarrollen.

8.2. PLANIFICACIÓN

En este ámbito se contemplan las directrices relacionadas con la planificación de la seguridad dentro de DESIC, S.L., tanto en lo referente al análisis y gestión de los riesgos de seguridad de la información como en lo relativo a la planificación general de la seguridad de los sistemas de información de DESIC.

DESIC, S.L. establece su estrategia de protección de los sistemas de información en la constitución de múltiples capas de seguridad, compuestas por medidas de naturaleza organizativa, física y lógica, dispuestas de tal forma que si una de ellas falla, la seguridad del sistema en su conjunto no sea comprometida. Además, los sistemas de información se diseñan de forma que garanticen la seguridad por defecto, considerando expresamente la seguridad en su arquitectura. Con este fin, DESIC, S.L. tiene establecidas una serie de cláusulas contractuales que consideran expresamente la seguridad y valoran que los productos de seguridad informáticos y de comunicaciones sean acreedores de una certificación de seguridad *"Common Criteria"* para la funcionalidad para la que son utilizados.

8.3. CONTROL DE ACCESOS

Este dominio cubre las directrices de DESIC, S.L. relacionadas con el control de acceso a los sistemas de información, tanto en lo referente a la gestión de usuarios como en lo relativo a la gestión de permisos y mecanismos de autenticación. En términos generales, estas directrices establecen que el acceso a los sistemas de información debe estar controlado y limitado exclusivamente a los usuarios, procesos, dispositivos y sistemas de información que estén debidamente autorizados, de forma que se restrinja el acceso a las funciones permitidas.

Los identificadores de usuario utilizados en los sistemas de información se asignan de forma unívoca, de modo que cada identificador está asociado a un único usuario o proceso. Existe un procedimiento formal para gestionar las altas, bajas y modificaciones de usuario.

Los usuarios de DESIC, S.L. cuentan con soluciones de control de acceso a los sistemas de información que permiten limitar el acceso a la información, siendo los responsables de los servicios los que determinan dicha autorización. Estas autorizaciones se otorgan de acuerdo a los principios generales de mínimo privilegio, necesidad de conocer y capacidad de autorizar.

Los mecanismos de autenticación utilizados se encuentran definidos en el procedimiento de gestión de usuarios.

8.4. EXPLOTACIÓN

Dentro de este ámbito se recogen todas las directrices establecidas por DESIC, S.L. en relación a las medidas de seguridad a considerar durante la explotación de los sistemas de información. Aquí se contempla tanto la configuración segura de los sistemas como su mantenimiento, de modo que se gestione la seguridad a lo largo de todo el ciclo de vida de los sistemas de información.

Todos los sistemas de información de DESIC, S.L. son configurados inicialmente de forma

segura, de modo que proporcionan exclusivamente las funcionalidades mínimas necesarias, se limita el acceso a ellas y se configuran de forma que su uso natural sea sencillo y seguro por defecto.

La instalación de cualquier componente físico o lógico de un sistema de información requiere una autorización formal previa. Se mantiene un inventario actualizado de todos los componentes de los sistemas de información instalados y sus responsables. Una vez puestos en producción existe una sistemática de mantenimiento de los sistemas de información que estipula las tareas de mantenimiento a llevar a cabo, de acuerdo a las directrices de los fabricantes, y que regula la gestión de las actualizaciones de seguridad en función de la vulnerabilidad y el riesgo asociados.

Los incidentes de seguridad que se producen, y en particular los asociados con malware, son registrados y tratados diligentemente, utilizándose dichos registros para la optimización de las medidas de seguridad implantadas.

8.5. SERVICIOS EXTERNOS

En este ámbito se contemplan las directrices definidas por DESIC, S.L. en relación a la utilización de recursos externos a la organización, estableciendo como premisa general que DESIC, S.L. sigue siendo en todo momento responsable de los riesgos en que se incurra por el uso de los servicios externos utilizados, de forma que la organización debe adoptar las medidas necesarias para poder ejercer dicha responsabilidad y mantener el control de las funciones delegadas.

Se hará partícipes a los terceros de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

DESIC, S.L. exige, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

DESIC, S.L. regula contractualmente la utilización de recursos externos a la organización, estableciendo en dichos contratos las características del servicio, las responsabilidades de cada parte, la calidad mínima exigible y las consecuencias del incumplimiento del contrato. 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 de la Información 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, así como del responsable del tratamiento previsto en el RGPD y LOPDGDD, antes de seguir adelante.

En relación al seguimiento y gestión diaria de los servicios externos utilizados, DESIC, S.L. lleva a cabo un seguimiento periódico del cumplimiento de las obligaciones pactadas contractualmente, estableciendo con cada proveedor una sistemática específica para la coordinación del servicio, la monitorización de su calidad y la resolución de las desviaciones y conflictos que puedan surgir.

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

8.6. CONTINUIDAD

Dentro de este ámbito se recogen las directrices relacionadas con la continuidad de los servicios prestados por los sistemas de información de DESIC. Así, se establece como garantía básica que todos los sistemas de información disponen de copias de seguridad actualizadas periódicamente, y que la organización ha establecido los mecanismos necesarios para garantizar la continuidad de sus servicios informáticos y de comunicaciones en caso de pérdida de las infraestructuras originales. Estas copias de seguridad están en línea con el análisis de impacto de los servicios informáticos y de comunicaciones de DESIC, que identifica los requisitos de disponibilidad de cada servicio.

8.7. MONITORIZACIÓN

Este dominio cubre las directrices de DESIC, S.L. relacionadas con la monitorización tanto de los propios sistemas de información como del uso que los usuarios hacen de ellos. En términos generales, estas directrices establecen la obligatoriedad de registrar la actividad de los usuarios durante su uso de los sistemas de información, con el nivel de detalle necesario para identificar actividades indebidas o no autorizadas salvaguardando al mismo tiempo los derechos de los usuarios.

DESIC, S.L. tiene establecidas soluciones de monitorización de los sistemas que permiten supervisar su comportamiento y detectar/prevenir la intrusión en ellos. Así mismo, la organización cuenta con indicadores que permiten medir el grado de implantación, eficacia y eficiencia de las medidas de seguridad establecidas, tanto técnicas como organizativas y operativas.

8.8. INSTALACIONES E INFRAESTRUCTURAS

En este ámbito se contemplan las directrices definidas por DESIC, S.L. en relación a la protección de las instalaciones y las infraestructuras físicas, articuladas mediante el control de acceso físico y el acondicionamiento y protección frente a contingencias ambientales. En términos generales, estas directrices se resumen en que los sistemas de información se instalan en salas específicas y separadas, que deben permanecer cerradas, dotadas de mecanismos de control de acceso, como llaves o claves, cuya distribución debe estar controlada.

Los servidores y el equipamiento de red principal están instalados en los CPDs de DESIC. El acceso a estas salas está controlado y todos los accesos a estas salas se registran. Todos los visitantes (personal no autorizado por defecto, tanto propio de DESIC, S.L. como ajeno) son identificados previamente a dicho acceso.

Los CPDs de DESIC, S.L. están equipados con sistemas de control y acondicionamiento que velan por el buen funcionamiento del equipamiento albergado en ellos, siguiendo lo dispuesto en las normativas y procedimientos de control de acceso físico y lógico.

8.9. PERSONAL

Este ámbito contiene las directrices de DESIC, S.L. en materia de gestión del personal, y contempla todos los aspectos relacionados con la formación y capacitación, la concienciación y difusión y la gestión de sus deberes y obligaciones. DESIC, S.L. establece la obligación de que todo el personal afectado conozca sus deberes y obligaciones en materia de seguridad, y los respete en el ejercicio de sus funciones. Para ello, DESIC, S.L. se compromete a regular formalmente estos deberes y obligaciones y a formar al personal sobre ellos, de modo que la seguridad de los sistemas de información sea respetada, aplicada y supervisada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida.

DESIC, S.L. establece las funciones y obligaciones que en materia de seguridad son aplicables a cada puesto de trabajo, identificando las condiciones de confidencialidad a cumplir y las medidas disciplinarias asociadas en caso de incumplimiento.

DESIC, S.L. también establece los requisitos que debe cumplir todo el personal que sin pertenecer a la organización está relacionado con ella y afectado por esta Política, como es el personal perteneciente a empresas subcontratadas u otro tipo de colaboradores o socios.

Así mismo, DESIC, S.L. tiene un programa de formación y concienciación que garantiza que periódicamente todo el personal recibe la información necesaria para saber cómo realizar su trabajo de manera segura y cómo debe participar en la gestión de la seguridad de los sistemas de información y los incidentes que puedan producirse, con el fin de que ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas sean fuentes de riesgo para la seguridad.

8.10. EQUIPAMIENTO Y RESPONSABILIDADES DEL USUARIO

Dentro de este ámbito se recogen las directrices relacionadas con la gestión segura del equipamiento y material puesto a disposición de los usuarios, en relación tanto a las obligaciones de DESIC, S.L. al respecto como a las responsabilidades que los usuarios deben asumir durante su uso.

El personal debe velar porque el puesto de trabajo esté despejado, de modo que no haya más material sobre su mesa que el requerido para la actividad que se esté realizando en cada momento. Ese material se deberá guardar en un lugar cerrado, como armarios o cajones, cuando no se esté utilizando.

Los equipos portátiles, al tener la consideración de entornos inseguros, deberán contar con medidas de seguridad adicionales. Por una parte, estos equipos estarán equipados con un firewall personal, que limite su visibilidad y controle el acceso al equipo cuando se conecte a redes públicas. Por otra se habilitarán normativas para controlar los equipos portátiles que posee la organización, su responsable y su ubicación y para reportar incidentes relacionados con pérdidas o sustracciones de dichos equipos. Así mismo, sus usuarios también deberán limitar la información que contienen estos equipos, evitando, en la medida de lo posible, que contengan claves de acceso remoto a la red de DESIC.

8.11. COMUNICACIONES

Este dominio cubre las directrices de DESIC, S.L. relacionadas con la gestión de las redes de comunicaciones, principalmente de cara a su interconexión con redes ajenas, que en general tendrán la consideración de entornos inseguros. En general, estas directrices se resumen en la obligatoriedad de proteger el perímetro de la red, en particular si se conectan a redes públicas, y de controlar los puntos de interconexión, aplicando medidas de seguridad en función de los riesgos derivados de dicha interconexión.

DESIC, según lo dispuesto en la arquitectura de seguridad, dispone de cortafuegos que separan las redes internas del exterior, de modo que cualquier tráfico entre redes internas y externas debe atravesarlos, estando configurados de forma que sólo se permiten los flujos de datos previamente autorizados.

8.12. SOPORTES DE INFORMACIÓN

En este ámbito se contemplan las directrices definidas por DESIC, S.L. en relación a la protección de los soportes de información, entendidos como todo el equipamiento móvil electrónico y no electrónico sobre el que se almacena información de forma estática (papel, pen-drives, CDs, DVDs, cintas, discos, etc.), que tendrán la consideración de entornos inseguros. Estas directrices se pueden resumir en tener la precaución de adoptar las medidas de seguridad pertinentes para proteger la información almacenada en estos dispositivos durante su uso y transporte, y garantizar su conservación y recuperabilidad a largo plazo.

Todo el personal de DESIC, S.L. debe aplicar la debida diligencia y control a los soportes de información que permanezcan bajo su responsabilidad, garantizando que se cumplen las medidas de control de acceso físico y/o lógico aplicables y que se respetan unas exigencias ambientales mínimas apropiadas para su conservación.

Toda la información en soporte papel que haya sido causa o consecuencia de la información electrónica tratada por los sistemas de información deberá estar protegida con el mismo grado de seguridad que ésta, aplicando las medidas de seguridad apropiadas a la naturaleza del soporte en que se encuentren.

Los soportes de información electrónicos deberán estar etiquetados de forma que permitan identificar el nivel máximo de seguridad de la información contenida. Siempre que sea necesario su contenido deberá estar cifrado, y el responsable de sistemas deberá garantizar su control, registrando sus entradas y salidas y su eliminación segura.

8.13. APLICACIONES

Este ámbito contiene las directrices de DESIC, S.L. en materia de desarrollo y puesta en producción de aplicaciones, que regulan los principales aspectos a considerar desde el punto de vista de la seguridad en torno a estas actividades.

En relación a la puesta en producción de aplicaciones, DESIC, S.L. dispone de un entorno aislado en el que se llevan a cabo las pruebas, realizadas con datos previamente ofuscados. Estas pruebas contienen una parte funcional y otra parte de seguridad, en la que se verifica el cumplimiento de los criterios de aceptación en materia de seguridad y que su puesta en marcha no provoca deterioros en la seguridad de otros componentes del sistema de información afectado.

8.14. INFORMACIÓN

Dentro de este ámbito se recogen las directrices de DESIC, S.L. relacionadas con la protección de la información, relativas tanto a la protección específica de los datos de carácter personal de acuerdo a las exigencias del RGPD como a la protección general de toda la información gestionada por DESIC, S.L. en el ejercicio de sus funciones.

DESIC, S.L. cumple de forma escrupulosa las exigencias legales vigentes en materia de protección de datos de carácter personal, aplicando de manera global a esta información las medidas de protección preceptivas por dicha regulación, sin perjuicio de cumplir, además, otras medidas de seguridad adicionales en caso de que se considere necesario.

DESIC, S.L. clasifica la información en virtud de su naturaleza, identificando responsables de la información de acuerdo a lo establecido en la presente Política. Los criterios de clasificación y designación de responsables están identificados en el procedimiento correspondiente, en base a los cuales estos responsables podrán modificar dicha clasificación.

Como norma general de protección de la información, DESIC, S.L. establece la obligatoriedad de llevar a cabo copias de seguridad que permitan recuperar datos pasados. Así mismo, la organización establece la obligatoriedad de llevar a cabo procesos de limpieza de documentos, según los dispuesto en el procedimiento de borrado de metadatos.

9. DESARROLLO Y DESPLIEGUE DE LA POLÍTICA DE SEGURIDAD

9.1. INSTRUMENTOS DE DESARROLLO

La Política de Seguridad de la Información de DESIC se desarrollará por medio en una serie de documentos normativos en los que se recogerán políticas de seguridad específicas para los distintos ámbitos contemplados. Dichos documentos normativos podrán adoptar alguna de las siguientes modalidades:

- **Normas técnicas de seguridad (NS):** Uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.
- **Procedimientos generales (PG):** Incorporan procedimientos generales de actuación del sistema de gestión de seguridad de la información.
- **Guías de seguridad (G):** Tienen un carácter informativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos en los casos en los que no existan procedimientos precisos. Ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.
- **Procedimientos operativos de seguridad (POS o PS)**: Afrontan tareas concretas, indicando lo que hay que hacer, paso a paso, sin entrar en detalles de proveedores, marcas comerciales o comandos técnicos. Son útiles en tareas repetitivas.
- **Instrucciones técnicas (IT):** Desarrollan los POS llegando al máximo nivel de detalle, indicando proveedores, marcas comerciales y comandos técnicos empleados para la realización de las tareas.

En caso de que la normativa desarrollada afecte de manera general a los usuarios de los sistemas de información de DESIC, dicha afección deberá ser previamente aprobada por el Comité de Seguridad.

Las políticas, normativas y regulaciones específicas que se aprueban se notifican y difunden apropiadamente a todos los afectados.

A título ejemplificativo, no con carácter exhaustivo, se han aprobado en DESIC, S.L. siguientes normativas y procedimientos:

- Normativa general de utilización recursos y sistemas de información.
- Normativa de uso de correo electrónico.
- Normativa de acceso a internet.
- Normativa de creación y uso de contraseñas.
- Normativa para trabajar fuera de las instalaciones.
- Normativa de gestión de usuarios.
- Normativa de control de acceso lógico.
- Procedimiento de control de acceso físico.
- Procedimiento de clasificación y tratamiento de la información.
- Procedimiento de autorizaciones.
- Procedimiento de gestión de usuarios.
- Procedimiento de gestión de incidentes de seguridad.

La normativa técnica de seguridad estará disponible en la intranet de DESIC, S.L. 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.

9.2. SANCIONES PREVISTAS EN CASO DE INCUMPLIMIENTO

Del incumplimiento de la Política de Seguridad de la Información y normas que la desarrollan podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores y el Convenio Colectivo vigente en DESIC, S.L. en cada momento.

Fecha aprobación V.3.: 05 de octubre de 2022

Política revisada y versión V.3.

Firmado digitalmente por 45536676B DAVID MANUEL LEON (R: B35492784)
Fecha: 2022.10.07 15:58:04 +01'00'