1. OBJETO, APROBACIÓN Y ENTRADA EN VIGOR

1.1. Objeto

El objeto de este documento es integrar, establecer y revisar la POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN de KuFlow, definida a través del SOA y del mapa de riesgos de la organización.

Estas políticas han sido aprobadas el 11/04/2023 por medio de la Dirección de KuFlow, las cuáles a su vez han sido actualizadas a fecha de 11/04/2023 y aprobadas en el acta de revisión por la Dirección del mes de diciembre de 2023.

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

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

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

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

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 y 8 del ENS.

1.2. Fundamento jurídico y normativo

La presente política de seguridad de la información se ha elaborado de acuerdo al **artículo 12 ENS 311/2022 de 3 de mayo** que dice así:

***"Artículo 12. Política de seguridad y requisitos mínimos de seguridad**.*

1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

a) Los objetivos o misión de la organización.

b) El marco regulatorio en el que se desarrollarán las actividades.

c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

f) Los riesgos que se derivan del tratamiento de los datos personales.

…

6. La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

h) Mínimo privilegio.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de la actividad y detección de código dañino.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

ñ) Mejora continua del proceso de seguridad.

7. Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos".

Algunos de los preceptos recogidos en el citado artículo 12 del ENS 311/2022 de 3 de mayo se recogen en el documento denominado "Normativa de seguridad de la información" el cual es equiparable así mismo a la normativa de seguridad a pesar de su denominación de "política". Así mismo se ha utilizado como referencia para la presente política Política de Seguridad de la Información.

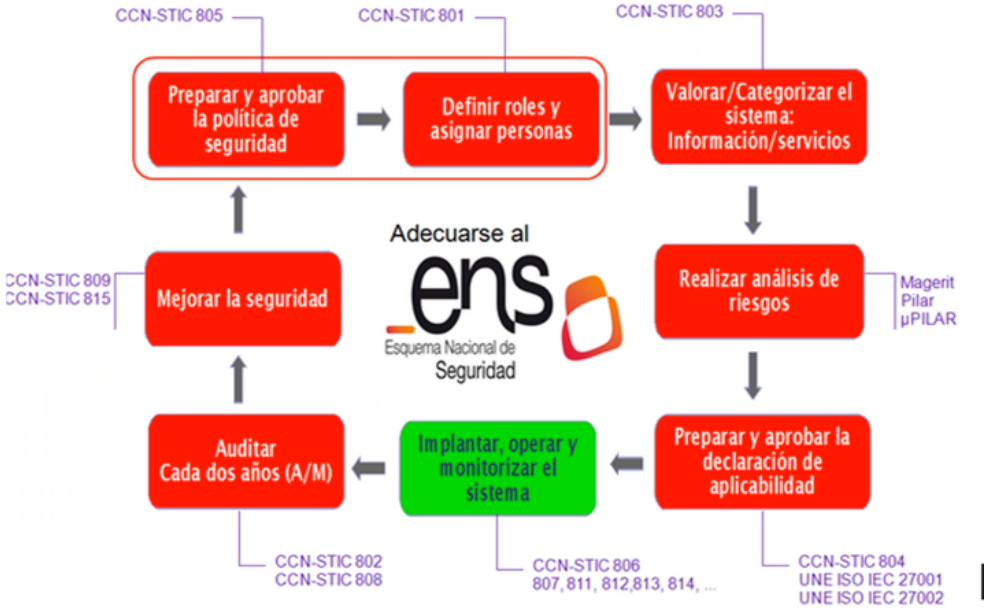
Esta Política de Seguridad ha sido desarrollada teniendo en cuenta los principios básicos y en base a los requisitos mínimos de seguridad establecidos por el Esquema Nacional de Seguridad (en adelante ENS) y conforme a lo exigido en el Anexo II del Real Decreto ENS, contemplando los requisitos exigidos en la sección [org.1].

La actual política de seguridad de la información se fundamenta en el Esquema Nacional de Seguridad (ENS) de 3 de mayo de 2022. Se han utilizado diversas guías de referencia como la "Guía de Seguridad de las TIC CCNSTIC 825" en la que se considera la relación del ENS con las normas ISO/IEC 27001 e ISO/IEC 27002 publicadas en 2005 y revisadas en 2013. Todo ello adaptado al ENS 311/2022 de 3 de mayo.

	ISO 27001:2013	**Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.**
Ontología	Norma internacional de seguridad, sin rango legal.	Regulación legal de carácter estatal, perteneciente al ordenamiento jurídico español derivado de la Ley 40/2015. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos
Carácter	certificación voluntaria	cumplimiento obligatorio
Ámbito de aplicación	Para cualquier sistema de Gestión de seguridad de la	Para los sistemas de información de las

	información.	Administraciones públicas comprendidos en el ámbito de aplicación de la Ley 40/2015, Ley 39/2015 y Real Decreto 203/2021
Modulación de las medidas	Según criterio del auditor	Regulado en función de los tipos de activos y los niveles de seguridad requeridos
Evidencia de cumplimiento o conformidad	Mediante certificación, expedida por un auditor autorizado, previa auditoría con resultado satisfactorio	Mediante declaración de conformidad legal, previa auditoría con resultado satisfactorio

Asimismo, se han tenido en cuenta otras guías tal y como aparecen en el siguiente mapa conceptual:



Por otro lado, el Anexo II del ENS 311/2022 modula los requisitos en función de la categoría del sistema de información.

El ENS requiere un sistema de gestión en:

- Anexo II (Medidas de seguridad), Marco operacional [op], Planificación [op.pl], Arquitectura de seguridad [op.pl.2]
- Anexo III (Auditoría de la Seguridad), Objeto de la auditoría; si bien la auditoría se requiere sólo para los sistemas de categoría MEDIA o ALTA.

1.3. Aprobación y entrada en vigor

La presente política de gestión integrada, ha sido adaptada a los requerimientos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Por todo ello, por medio del presente documento se procede a la aprobación de la presente política la cual incorpora la información relativa al ENS en su última versión del año 2022.

2. MISIÓN CORPORATIVA

Control ENS org.1.1

La **misión** como una declaración duradera de objetivos debe ser compartida por todos los miembros de la organización actual y también futuros, y en la definición y concepción de la misma debe jugar un papel clave los líderes de la entidad.

KuFlow tiene como **misión** "*proporcionar herramientas empresariales para que sus clientes puedan abordar automatización y orquestación de procesos de negocio*".

3. ALCANCE

Para conseguir nuestra misión apostamos por un Sistema de Gestión de la Seguridad de la Información para los servicios prestados por la compañía enumerados a continuación, tal y como está definido en el documento **Alcance del Sistema**:

"los sistemas de información que dan soporte a: los servicios de Software as a Service, los servicios de gestión de infraestructura interna y los servicios de implantación de proyectos, de acuerdo a la Declaración de Aplicabilidad vigente."

4. MARCO NORMATIVO

Control ENS org.1.2

La base normativa que afecta al desarrollo de las actividades y competencias de KuFlow en lo que a los servicios prestados entre otros ámbitos en la administración electrónica, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la legislación recogida en el documento denominado **Marco Regulatorio**.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica que de una u otra forma afectan a KuFlow derivadas de las anteriores comprendidas dentro del ámbito de aplicación de la presente Política.

El mantenimiento del marco normativo será responsabilidad de KuFlow. Incluyendo las instrucciones técnicas de seguridad y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el "Artículo 28.3".

Así mismo, KuFlow también será responsable de identificar las guías de seguridad del CCN, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

5. CATEGORIZACIÓN DEL SISTEMA

En el documento **Categorización del Sistema** de KuFlow compuesta por el **Inventario y Valoración de los Servicios y de la Información asociada a los mismos,** junto con su justificación, y la **categorización del sistema**, según lo establecido en el Anexo I del Real Decreto 311/2022 e 3 de mayo.

6. DECLARACIÓN DE APLICABILIDAD

Para dar cumplimiento a los requisitos mínimos establecido, KuFlow adoptará las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:

a) Los activos que constituyen los sistemas de información concernidos.
b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
c) Las decisiones que se adopten para gestionar los riesgos identificados.

Las medidas a las que se refiere el apartado 1 tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados. La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, del riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III. Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implantadas y las medidas del anexo II que compensan. El conjunto será objeto de la aprobación formal por parte del responsable de la seguridad. Una Guía CCN-STIC de las previstas en la disposición adicional segunda guiará en la selección de dichas medidas, así como su registro e inclusión en la Declaración de Aplicabilidad.

La Declaración de KuFlow se recoge en el documento **Declaración de Aplicabilidad**.

7. ROLES Y FUNCIONES DE SEGURIDAD

7.1. Roles de Seguridad

Control ENS org.1.3

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Delegado de Protección de Datos (DPD)
- Responsable de Seguridad
- Responsable del Sistema de Gestión de Seguridad de la Información

7.2. Comité de Seguridad de la Información

Control ENS org.1.4

KuFlow ha constituido un Comité de Seguridad de la Información está formado por los siguientes miembros:

- Presidente
- Miembros
    - Responsable de Seguridad
    - Delegado de Protección de Datos
    - Responsable del Sistema de Gestión de Seguridad de la Información

El Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiera a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos. Los Responsables de la Información y los Servicios serán convocados en función de los asuntos a tratar.

Con carácter opcional, otros miembros de KuFlow de la Dirección, podrán incorporarse a las labores del Comité, incluidos grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias de KuFlow con periodicidad semestral, previa convocatoria al efecto realizada por el Presidente de dicho Comité.

7.3. Responsabilidades asociadas al ENS

Control ENS org.1.4

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de los roles de seguridad ENS:

Funciones del Responsable de la Información y de los Servicios

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, previa propuesta al Responsable de Seguridad ENS, y/o Comité de Seguridad de la Información.
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

Funciones del Responsable de Seguridad

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

Funciones del Responsable del Sistema

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al Responsable de Seguridad de la Información y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.

Cuando la complejidad del sistema lo justifique, el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/as funciones concretas de las responsabilidades que se le atribuyen.

7.4. Funciones del Comité de Seguridad de la Información

Control ENS org.1.4

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando 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 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.
- Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.

- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

7.5. Procedimientos de designación

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política ha sido realizada por la Dirección de KuFlow y comunicada a las partes afectadas en una reunión presencial en la sede de la empresa.

Los miembros del Comité, así como los roles de seguridad serán revisados cada cuatro años o con ocasión de vacante.

7.6. Resolución de conflictos

El Comité de Seguridad de la Información, se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

8. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Control ENS mp.info.1

Tan sólo se recogerán datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

A la vista del 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) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos en KuFlow, a pesar de que no existe obligatoriedad en nombrar a esta figura dentro de la organización.

9. RELACIÓN CON TERCEROS

Cuando se preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. KuFlow definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de actuaciones que KuFlow lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando KuFlow utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad. De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogidas en el artículo 29 “Instrucciones técnicas de seguridad y guías de seguridad” del Real Decreto 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 modificado por el Real Decreto 951/2015 de 23 de octubre, y en consideración a la 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, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de **categorías MEDIA** o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS 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.

10. ESTRUCTURACIÓN DE DOCUMENTACIÓN DE SEGURIDAD

Control ENS org.1.5

Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso están especificadas en la **Política de Gestión de Información Documentada**.

11. ANÁLISIS DE RIESGOS

KuFlow, ha realizado un análisis de riesgos, según lo establecido en el Anexo II del Real Decreto en su sección [op.pl.1], conforme a lo establecido en el Perfil de Cumplimiento Específico de aplicación a KuFlow.

El análisis de riesgos se ha llevado a cabo de acuerdo al **Anexo III**, del ENS y ha sido realizado usando la metodología MAGERIT en su versión 3.0 (MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica).

El análisis de riesgos que se ha llevado a cabo en KuFlow está acorde al artículo 24 del reglamento de Protección de Datos, tal y como indica el artículo:

> *Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*
>
> *Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.*
>
> *La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.*

Asimismo, desde KuFlow se realiza una vigilancia continua y reevaluación periódica.

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

Todo ello se encuentra definido en el documento de **Política de Gestión de Riesgos**.

12. OTRAS CONSIDERACIONES Y CUMPLIMIENTO

KuFlow, para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en el que se recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral (artículo 6) y mínimo privilegio (artículo 20)

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad a KuFlow estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, por lo que los sistemas de información se diseñarán y configurarán otorgando los mínimos privilegios necesarios para su correcto desempeño del siguiente modo:

a) *El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.*

b) *Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.*

c) *Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.*

d) *Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.*

Vigilancia continua y reevaluación periódica (artículo 10) e integridad y actualización del sistema (Artículo 21)

KuFlow ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Gestión de personal (artículo 15) y profesionalidad (artículo 16)

Todos los miembros de KuFlow, dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros, 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.

El apartado relacionado con los artículos 15 y 16 del ENS se abordan en las Normas de seguridad de la información.

Gestión de la seguridad basada en los riesgos (artículo 7) y análisis y gestión de riesgos (artículo 14)

Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de 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 cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

Incidentes de seguridad (artículo 25), prevención, reacción y recuperación (artículo 8)

KuFlow ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, KuFlow implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

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

KuFlow establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.

- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- Para garantizar la disponibilidad de los servicios, KuFlow dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Existencia de líneas de defensa (artículo 9) y Prevención ante otros sistemas de información interconectado (artículo 23)

KuFlow ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Diferenciación de responsabilidades (artículo 11) y Organización e implantación del proceso de seguridad (artículo 13)

KuFlow ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de “ORGANIZACIÓN DE LA SEGURIDAD” del presente documento.

Autorización y control de los accesos (artículo 17)

KuFlow ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados. Esto se encuentra recogido en las políticas específicas.

Protección de las instalaciones (artículo 18)

KuFlow ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas. Esto se encuentra recogido en las políticas específicas.

Adquisición de productos de seguridad y contratación de servicios de seguridad

(artículo 19)

Para la adquisición de productos, KuFlow se tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

Protección de la información almacenada y en tránsito (artículo 22) y continuidad de la actividad (artículo 26)

KuFlow ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de KuFlow. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Registro de actividad y detección de código dañino (artículo 24)

KuFlow ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas,

permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

13. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información ha aprobado el desarrollo de un Sistema de Gestión de Seguridad de la Información, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad.

La presente Política de Seguridad se desarrollará en una serie de documentos normativos en los que se recogerán políticas de seguridad específicas para los distintos ámbitos contemplados, como los siguientes:

- Normativa de Seguridad
- Política de Gestión de Riesgos
- Política de Gestión de Cambios
- Política de Controles Criptográficos
- Gestión de Roles y Accesos
- Política de Autorizaciones
- Plan Director de Seguridad de la Información
- Procedimiento de Configuración de Seguridad y Bastionado
- Gestión de Información Documentada
- Gestión de Continuidad del Negocio
- Gestión de No Conformidades, Quejas e Incidentes

Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad.

El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité.

Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte de la dirección de la organización.