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.

1. MISIÓN Y OBJETIVOS DEL ORGANISMO

Desde **NEKI CREACTIVOS S.L. (NEKI)** queremos aportar la excelencia en proyectos de transformación digital. Nos comprometemos a ofrecer servicios profesionales integrales en toda la cadena de valor del software, incluyendo Consultoría IT, diseño y desarrollo de software personalizado, Marketing digital, y Ciberseguridad. Buscamos anticiparnos al futuro y definir los cambios necesarios para impulsar la eficiencia y el éxito de las empresas con las que colaboramos.

Aspiramos a ser la compañía tecnológica global de referencia nacional. Nos esforzamos por mantener y fortalecer nuestra excelencia técnica y capacidad de adaptación, permitiéndonos actuar de manera eficiente en un entorno empresarial en constante cambio. Buscamos ser reconocidos como líderes en la industria, tanto por nuestra innovación como por nuestra contribución al avance tecnológico.

Esta Política sienta las bases para que el acceso, uso, custodia y salvaguarda de los activos de información utilizados por NEKI 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 NEKI 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.

La presente política será:

- Aprobada por la Dirección de la organización y revisada periódicamente, así como ante cualquier cambio relacionado con la seguridad de la información.
- Comunicada a todo el personal interno y empresas externas colaboradoras.
- De carácter imperativo sobre toda la organización.

2. ALCANCE

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

2. MARCO NORMATIVO

Desde NEKI nos comprometemos a cumplir con la siguiente legislación vigente en materia de Seguridad de la Información:

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- 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. o 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 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información. o Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

3. ORGANIZACIÓN DE LA SEGURIDAD

3.1. Comité: Funciones y Responsabilidades

El Comité de Seguridad es el encargado de coordinar la seguridad de la información. Se encuentra formado por:

- Responsable del Servicio (Rafael Ferrer Sanchez).
- Responsable de la Información (Rafael Ferrer Sanchez)
- Responsable de Seguridad (Nacho Vilalta Esteban)
- Responsable del Sistema (Raul Novoa Mínguez)

El secretario del Comité de Seguridad será el responsable de Información y tendrá como funciones:

- Convocar las reuniones del Comité de Seguridad.
- Preparar 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 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 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 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. 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.

3.2. Roles: Funciones y Responsabilidades

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 del mismo.
- Gestionar la formación y concienciación en materia de seguridad.
- 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 del Sistema

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.

- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión 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.

3.3. Mecanismos de coordinación

Se celebrarán reuniones entre el Comité de Seguridad con periodicidad semestral, así como antes cualquier cambio sustancial en la organización susceptible de afectar a la seguridad de la información, o cualquier incidencia o emergencia relacionada con esta.

3.4. Procedimiento de designación

El personal integrante del Comité será designado por la Dirección.

6. CONCIENCIACIÓN Y FORMACIÓN

Desde NEKI trabajamos por garantizar la plena conciencia y el compromiso de todo el personal respecto a la seguridad de la información en todas nuestras actividades, de acuerdo con el principio de Seguridad Integral recogido en el Artículo 5 del ENS.

Toda la plantilla de la organización tiene 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/as.

Todo el personal de NEKI recibirá concienciación en materia de seguridad al menos una vez al año y se establecerá un programa de concienciación continua, dando especial importancia al personal 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.

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.

4. GESTIÓN DE RIESGOS

La organización realizará 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.
Los responsables de los sistemas deberán colaborar en el análisis y atender a las conclusiones de este.

Todo el personal de NEKI es responsable de informar sobre las debilidades e incidentes de seguridad de la información que se detectan oportunamente.

La gestión de riesgos quedará documentada en el informe de Análisis y Gestión de riesgos, conforme a lo establecido en el procedimiento de Análisis de riesgos de Seguridad de la Información.

5. DATOS DE CARÁCTER PERSONAL

La Ley Orgánica de Protección de Datos (LOPD) y el RGPD, 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.

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 NEKI.

NEKI dispone del Asesoramiento de un DPD y además garantiza el cumplimiento de la Ley Orgánica de Protección de Datos a través de sus procedimientos de aplicación, para ellos se dispone de un Registro de Actividades de Tratamiento de Datos en donde se identifica las responsabilidades como Responsable y como Encargado de Tratamiento de Datos.

7. AUTORIZACIÓN Y CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

El control del acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de NEKI y otras redes públicas o privadas.
- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.

8. PROTECCIÓN DE LAS INSTALACIONES

Los objetivos de esta política en materia de protección de las instalaciones son:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de NEKI.
- Proteger el equipo de procesamiento de información crítico de NEKI, colocándolo en áreas protegidas y protegido por un perímetro de seguridad definido, con las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección de esta en su traslado y permanecer fuera de las áreas protegidas, por mantenimiento u otros motivos.
- Controlar los factores ambientales que podrían perjudicar el buen funcionamiento del equipo de cómputo que alberga la información de NEKI.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus tareas habituales.
- Proporcionar protección proporcional a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de NEKI, como: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

El responsable de Seguridad, junto con los Titulares de la Información, según proceda, definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal de NEKI a las áreas restringidas bajo su responsabilidad. Los Propietarios de Información autorizará formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de NEKI cuando lo consideren apropiado.

Todo el personal de NEKI es responsable del cumplimiento de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas.

9. ADQUISICIÓN DE PRODUCTOS

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.

Por otro lado, se tendrá en cuenta la seguridad de la información en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.

10. SEGURIDAD POR DEFECTO

Desde NEKI consideramos estratégico para la entidad que los procesos integren la seguridad de la información como parte de su ciclo de vida. Los sistemas de información y los servicios deben incluir la seguridad por defecto desde su creación hasta su retirada, incluyéndose la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades en explotación estableciéndose la seguridad como un proceso integral y transversal.

11. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Desde NEKI nos comprometemos a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos o lógicos mediante la autorización previa a su instalación en el sistema. Dicha evaluación será llevada a cabo principalmente por la persona responsable de operaciones, quien evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de seguridad de los sistemas, en relación con 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 estos.

12. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

NEKI establece medidas de protección para la Seguridad de la Información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

13. PREVENCIÓN DE SISTEMAS DE INFORMACIÓN INTERCONECTADOS

NEKI establece medidas de protección para la Seguridad de la Información especialmente para proteger el perímetro, en particular, si se conecta a redes públicas, especialmente si se utilizan en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público.

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. Conexiones electrónicas disponibles para el público.

14. CONTINUIDAD DE LA ACTIVIDAD

NEKI con el objetivo de garantizar la continuidad de las actividades, establece medidas para que los sistemas dispongan de copias de seguridad y establece mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

15. MEJORA DE LA ACTIVIDAD

NEKI establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en el Esquema Nacional de Seguridad.

En Zaragoza a 11 de Septiembre de 2024
Asociados y Dirección General

Responsable del Servicio (Rafael Ferrer Sanchez). 	Responsable del Sistema (Raul Novoa Minguez) 
Responsable de Seguridad (Nacho Vilalta Esteban)