POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INDICE

Rev.	Descripción de los cambios	Fecha
1.0	Versión inicial.	15/03/2024

	Descripción de los cambios	Fecha
Elaborado	Responsable del SGSI	15/03/2024
Revisado	Comité de Seguridad	15/03/2024
Aprobado	Comité de Seguridad	15/03/2024

1. MISIÓN Y OBJETIVOS

La Dirección de *NIVI GESTIONES ESPAÑA* consciente del compromiso que contrae con sus clientes y la importancia del cuidado de la seguridad integral, ha establecido en su organización un Sistema de Gestión de la Seguridad de la Información basado en las normas ISO/IEC 27001 y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, teniendo en cuenta:

MISIÓN

Aportar soluciones efectivas a los problemas de cobro e impagos, poniendo al servicio de nuestros clientes nuestra dilatada experiencia en los servicios externalizados de recaudación internacional de créditos. Prestar un servicio basado en nuestro compromiso con la seguridad de la información y la mejora continua de nuestros sistemas de información potenciando la mejora continua.

VISIÓN

Satisfacer las necesidades de nuestros clientes, asegurando la confidencialidad de los datos gestionados por *NIVI GESTIONES ESPAÑA*, así como la disponibilidad de los sistemas de información, tanto en los servicios ofrecidos a los clientes como en la gestión interna, aportando una capacidad de respuesta ante situaciones de emergencia, y restableciendo el funcionamiento de los servicios críticos en el menor tiempo posible, evitando alteraciones indebidas en la información, promoviendo la concienciación y formación de nuestro equipo humano, así como fomentando la responsabilidad social, la seguridad, respeto al medio ambiente y la minimización de su impacto a través de la prevención de la contaminación como principal objetivo.

OBJETIVOS

La Dirección de *NIVI GESTIONES ESPAÑA* establece las siguientes directrices para su sistema de gestión de seguridad de la información:

- Los sistemas de información deben ser administrados con diligencia y estar protegidos contra amenazas de rápida evolución, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada o los servicios prestados.
- Garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con habilidad ante los incidentes.
- Cumplir con todo el articulado del Esquema Nacional de Seguridad (principios básicos y requisitos mínimos), para el nivel categorizado, 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.
- Cumplir con los requisitos aplicables de ISO/IEC 27001, así como toda la legislación aplicable en materia de Seguridad de la Información y Privacidad.
- Mejorar de forma continua nuestros Sistemas Integrados de Gestión.
- Gestionar los riesgos frente a amenazas y vulnerabilidades de manera eficiente.
- Concienciación, formación y motivación del personal de la organización, sobre la importancia del desarrollo e implantación del Sistema de Gestión de Seguridad de la Información y sobre su implicación en el

cumplimiento de las medidas de seguridad y los requisitos de los clientes y terceros relacionados con la protección de su información.

En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

- Organización e implantación del proceso de seguridad en la organización
- Gestión de la seguridad basada en los riesgos y análisis y gestión de los mismos
- Seguridad como un proceso integral y seguridad por defecto. Mínimo privilegio
- Gestión de personal y profesionalidad.
- Autorización y control de los accesos
- Protección de las instalaciones de la organización
- Adquisición de productos de seguridad y contratación de servicios de seguridad
- Protección de la información almacenada y en tránsito
- Reevaluación periódica, integridad y actualización del sistema.
- Líneas de defensa y prevención ante otros sistemas interconectados.
- Incidentes de seguridad, prevención, reacción y recuperación.
- Garantías sobre la continuidad del negocio
- Monitorización y Registros de actividad
- Mejora continua del Sistema de Información de Seguridad de la Información
- Velar por el cumplimiento de las políticas de seguridad de la información definidas e implantadas por la organización.

Estos objetivos se desarrollan en la organización mediante la aplicación de normas, procedimientos y controles que deberán permitir y asegurar la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada.

2. ALCANCE

NIVI GESTIONES ESPAÑA aplicará la presente Política de Seguridad de la Información sobre aquellos sistemas que están relacionados con el ejercicio de desarrollo de las aplicaciones utilizadas dentro de su actividad. De forma concreta, la presente Política de Seguridad es aplicable a:

"Los sistemas de información que soportan los servicios asociados a los procesos de negocio de servicios de notificación y cobro en extranjero de sanciones administrativas en outsourcing por cuenta de las administraciones públicas, cometidos por personas con domicilio fuera de España. Recuperación de deuda impagada de personas con domicilio fuera de España Identificación de titulares y conductores de vehículos con domicilio fuera de España de empresas de alquiler de coches, de acuerdo a la declaración de aplicabilidad vigente".

La presente Política de Seguridad de la Información no aplicará a aquellos sistemas de información no reflejados en este apartado.

Los centros de trabajo incluidos en el alcance son:

- Nivi Gestiones España S.L.: Oficinas ubicadas en Avenida América, 32-28922 Alcorcón, Madrid, España.
- Nivi SpA: oficinas ubicadas en Via O. da Pordenone, 20, 50127 Florencia, Italia.

3. MARCO NORMATIVO

El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales de 13 de diciembre
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016,
- Ley 39/2015 de 1 de octubre del Procedimiento Administrativo Común de las Administraciones
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- UNE-EN ISO/IEC 27001:2023: Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. (ISO/IEC 27001:2022).
- UNE-EN ISO/IEC 27002:2023: Seguridad de la información, ciberseguridad y protección de la privacidad. Control de la seguridad de la información. (ISO/IEC 27002:2022).
- Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad

Pueden ser de aplicación otras disposiciones y normativas que nuestra organización mantiene controladas en un listado de requisitos legales de aplicación en materia de seguridad de la información.

4. ORGANIZACIÓN DE LA SEGURIDAD

4.1. Comité: Funciones y Responsabilidades

NIVI GESTIONES ESPAÑA dispone de un Comité de Seguridad de la Información que tiene la finalidad de llevar a cabo la gestión del Sistema y velar por el correcto cumplimiento de las políticas y normas implantadas en la organización. El Comité está compuesto al menos por los siguientes responsables:

- Un miembro del Consejo de Administración
- Responsable de Seguridad
- Responsable de Sistemas
- Cualquier otro miembro que la dirección considere

El Comité de Seguridad de la Información alcanza a toda la empresa, es el mecanismo de coordinación y resolución de conflictos, que entre otras funciones tiene:

- Atender las solicitudes, en materia de Seguridad de la Información, de la organización 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 organización 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 posterior aprobación.

- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con Dirección.
- 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, ISO 27001 y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la compañía en materia de seguridad de la Información.
- Asegurar que los activos se gestionan conforme a los requisitos legales y regulatorios vigentes

El Comité, con pleno poder de decisión ejercerá de dueño de los riesgos detectados en los análisis de riesgos realizados en *NIVI GESTIONES ESPAÑA*. Para ello, se asegurará de la correcta realización del análisis de riesgos, el establecimiento del nivel de riesgo aceptable, la aprobación del plan de tratamiento de riesgos y la aceptación de los riesgos residuales (reevaluación de riesgos), todo ello, disponiendo de conocimientos sobre la metodología de análisis de riesgos utilizada en la organización.

El Comité se reunirá, al menos, una vez al año para verificar el correcto funcionamiento de los Sistemas de Gestión implantados en la organización. En caso de que el Comité lo considere oportuno, y debido a circunstancias que así lo requieran, se podrán convocar tantas reuniones extraordinarias como sea necesario. A las reuniones del Comité se podrán invitar a todas aquellas personas que se considere necesario, en función de los temas a tratar.

Las conclusiones acordadas en las reuniones del Comité quedan documentadas en un acta, la cual es aprobada o rectificada en el primer punto de la siguiente sesión del Comité, por todos los asistentes a la reunión y guardada como evidencia de la asistencia y registro del funcionamiento del mismo. Las actas se archivan como evidencia documental de las decisiones tomadas por parte del Comité.

La responsabilidad general de la seguridad de la información recaerá sobre el Responsable de Seguridad, siendo la responsabilidad última del Comité de Seguridad de la Información y de la Dirección como máximo Responsable del Sistema de gestión de seguridad de la información. El detalle de la composición del Comité de Seguridad de la Información, así como las obligaciones de cada rol en el ámbito de la seguridad de la información se determina en el acta de designación correspondiente.

4.2. Roles de Seguridad: Funciones y Responsabilidades

Siguiendo las recomendaciones de la GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-801), y en función de nuestro alcance y recursos, se definen los siguientes roles:

4.2.1. Responsable de la Información

El Responsable de la Información es habitualmente una persona situada en el nivel Directivo de la organización. Esta figura tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. 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).

El Responsable de la Información será el propietario de la misma y tendrá las siguientes funciones:

- Establecer y aprobar los requisitos de seguridad aplicables a la información dentro del marco establecido en el anexo 1 del Real Decreto 311/2022, de 3 de mayo, previa propuesta del Responsable de Seguridad y/o Comité de Seguridad de la Información.
- Valorar y asesorar al comité sobre los niveles de riesgo residual que afecten a la Información.

4.2.2. Responsable del Servicio

El Responsable del servicio tiene la potestad de establecer los requisitos del servicio en materia de seguridad la Información. Será quien determine los requisitos de los servicios prestados, en consonancia, tendrá las siguientes funciones:

- Establecer y aprobar los requisitos de seguridad aplicables al servicio dentro del marco establecido en el anexo 1 del Real Decreto 311/2022, de 3 de mayo, previa propuesta del Responsable de Seguridad y/o Comité de Seguridad de la Información.
- Valorar y asesorar al comité sobre los niveles de riesgo residual que afecten al Servicio.

4.2.3. Responsable de la Seguridad

El Responsable de Seguridad será quien tome las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios. Dispondrá de las siguientes funciones:

- 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 para posterior aprobación por parte del Comité de Seguridad.
- 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.
- Promover la creación de nuevas políticas y normativas en materia de seguridad que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar y mantener el documento de Declaración de Aplicabilidad y demás registros del Sistema de Gestión de Seguridad de la Información, con apoyo de otras áreas.

4.2.4. Responsable del Sistema

El Responsable del Sistema se encarga de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores que estén bajo su responsabilidad. Tendrá asignadas las siguientes funciones:

- 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, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento
- 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 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.
- Comunicar tan pronto como se tenga constancia de la misma al Responsable de Seguridad y Servicios, las violaciones de seguridad que afecten a datos personales.
- 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.

4.3. Designación y revisión de los roles de Seguridad:

Es función de la Dirección de *NIVI GESTIONES ESPAÑA* designar al:

- Responsable de la Información.
- Responsable del Servicio.
- Responsable de Seguridad.
- Responsable del Sistema.

Las figuras de responsable de Seguridad y Responsable del Sistema no pueden recaer en la misma persona, no debiendo existir dependencia jerárquica entre ambos. En caso contrario debe ser perfectamente justificado y aprobado por el Comité de Seguridad.

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad y por encima la decisión del Comité de Seguridad.

Por la presente, la Dirección de *NIVI GESTIONES ESPAÑA* asume la responsabilidad final y última del cumplimiento de la política.

5. REVISIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad de la Información 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 Dirección dentro de la reunión de Comité de Seguridad y difundida para que la conozcan todas las partes afectadas.

6. DATOS DE CARÁCTER PERSONAL

NIVI GESTIONES ESPAÑA solo recogerá 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.

Para garantizar el cumplimiento 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 su transposición 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 tomando 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 es de aplicación, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

Del mismo modo, se deberá de garantizar el cumplimiento de la Política de Protección de Datos establecida por la organización.

7. GESTIÓN DE RIESGOS

Todos los sistemas sujetos al alcance definido en esta Política deberán realizar un análisis de riesgos (incluidos los riesgos asociados al tratamiento de datos personales), 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 tipología de 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 de la Información establecerá una sistemática para los tipos de activos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8. OBLIGACIONES DEL PERSONAL Y DE TERCEROS

Todos y cada uno de los usuarios de los sistemas de información de *NIVI GESTIONES ESPAÑA* son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales.

Todos los miembros de *NIVI GESTIONES ESPAÑA* tienen la obligación de conocer y cumplir esta política de seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de la organización recibirán formación en materia de seguridad de la información y privacidad. Se establecerá un programa de concienciación continua para atender a todos los miembros de *NIVI GESTIONES ESPAÑA*, 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 incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

Cuando *NIVI GESTIONES ESPAÑA* preste servicios a clientes o maneje información de terceros, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información existentes (si hubiera) y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando *NIVI GESTIONES ESPAÑA* utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo

desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad y privacidad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Comité de Seguridad de la información antes de seguir adelante.

9. ESTRUCTURA DEL SISTEMA DE GESTIÓN

Esta Política de Seguridad de la Información es complementada con el Marco Normativo interno que incluye las políticas de seguridad, procedimientos y otras normativas internas de *NIVI GESTIONES ESPAÑA*. La seguridad de la información ha de ser entendida como un proceso integral que involucra a todos y cada uno de los intervinientes, así como a los diferentes elementos técnicos, materiales y organizativos involucrados en las actividades realizadas por la compañía. Es por ello que la documentación del sistema de gestión de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible y accesible en nuestras plataformas de consulta para personal externo e interno que le sea de aplicación.

La presente política de Seguridad de la Información se encontrará a disposición de todas las partes interesadas en la Web corporativa de NIVI GESTIONES ESPAÑA SL.

10. FIRMA DE APROBACIÓN

El Comité de Seguridad
Aprobado el 15 de Marzo de 2024