ESQUEMA NACIONAL DE SEGURIDAD (ENS)

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Sistema de Gestión de la Seguridad de la Información

Organización: BIODIVERSITY NODE

Código: PO-ENS-00

Versión: 1.0

Fecha: 15/10/2026

Clasificación: Pública

CONTROL DOCUMENTAL

REVISIÓN	FECHA	MOTIVO	PÁGINAS REVISADAS
1.0	15/10/2026	Emisión inicial del documento.	Todas

ÍNDICE

1. Declaración de principios
2. Política
3. Organización de la seguridad
4. Revisión de la Política de Seguridad
5. Datos de carácter personal
6. Gestión de riesgos
7. Obligaciones del personal
8. Terceras partes
9. Legislación aplicable

1. DECLARACIÓN DE PRINCIPIOS

BIODIVERSITY NODE es una organización dedicada a la prestación de servicios de consultoría ambiental para entidades públicas y privadas. Para ello, asumimos valores que consideramos esenciales para la consecución de nuestros objetivos, como es la preservación de la información y los datos personales, tanto propios como del resto de partes interesadas, y el desarrollo profesional y personal de todos los componentes de su equipo de trabajo.

Debido a nuestra actividad, en BIODIVERSITY NODE somos conscientes de que la información es un activo con un elevado valor para nuestra organización y requiere, por lo tanto, una protección y gestión adecuadas con el fin de dar continuidad a nuestra línea de negocio y minimizar los posibles daños ocasionados por fallos a la integridad, disponibilidad y confidencialidad de la información. Así mismo, tanto la legislación vigente relativa a la protección de datos personales (RGPD y LOPDGDD) como el compromiso de BIODIVERSITY NODE con nuestros clientes, que nos confían sus expedientes y su documentación técnica, nos hace especialmente sensibles al tratamiento de la información a la que tenemos acceso en el ejercicio de nuestra actividad.

Para ello, BIODIVERSITY NODE establece un conjunto de actividades de gestión que tienen como objetivo preservar los principios de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y conformidad regulatoria de la información. A su vez, estos principios se definen de la siguiente manera:

- Confidencialidad: es la propiedad que permite garantizar que el acceso a la información solamente puede ser ejercido por las personas autorizadas para ello.
- Integridad: es la propiedad de salvaguardar la exactitud y completitud de los activos de información.
- Disponibilidad: es la cualidad que garantiza que las personas autorizadas pueden acceder a la información y procesarla en cualquier momento en que sea necesario.
- Autenticidad: es la propiedad o característica consistente en que una entidad es quien dice ser, o bien que garantiza la fuente de la que proceden los datos.
- Trazabilidad: es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
- Conformidad Regulatoria: es la propiedad que asegura que la información es gestionada de acuerdo con los principios éticos, profesionales y legales establecidos por las regulaciones que son aplicables en cada contexto.

Los sistemas deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en 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, con el fin de garantizar la prestación continua de los servicios.

Esto implica que las distintas áreas de la organización 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 los servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las distintas áreas de la organización deben cerciorarse de que la seguridad es 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 identificarse e incluirse en la planificación, en la solicitud de ofertas y en los pliegos de licitación para proyectos de TIC.

La organización debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 8 del ENS.

Dentro del amparo de lo anterior se encuentra embebida la protección de la privacidad. Aunque la información técnica que gestiona la organización se refiere principalmente a datos ambientales y de distribución de especies, nuestros sistemas tratan también datos personales de empleados, clientes y proveedores y, por ello, la protección de la privacidad

se erige como un pilar esencial en el marco del SGSI y se constituye como una necesidad social que las empresas deben respetar y proteger, así como objeto de legislación y/o regulación específica en todo el mundo.

Objetivos generales

La Política de Seguridad proporciona las bases para definir y delimitar los objetivos y responsabilidades de las diversas actuaciones técnicas, legales y organizativas que se requieran para garantizar la seguridad de la información y la privacidad, cumpliendo el marco legal de aplicación y las políticas globales y específicas de la organización, así como los procedimientos definidos.

Estas actuaciones, desde el punto de vista de la seguridad y la privacidad, se seleccionan e implantan basándose en el análisis de riesgos y en el equilibrio entre el riesgo aceptable y el coste de las medidas.

El objetivo de la Política de Seguridad es fijar el marco de actuación necesario para proteger los recursos de información y datos frente a amenazas, internas o externas, deliberadas o accidentales.

La información y los datos pueden existir en una variedad de formatos, con soportes tanto electrónicos como en papel u otros medios, e incluyen a veces datos críticos acerca de las operaciones, estrategias o actividades de BIODIVERSITY NODE y de sus clientes, como los expedientes técnicos, los estudios ambientales y la información geográfica asociada a los proyectos. La pérdida, corrupción o sustracción de información, o de los sistemas que la gestionan, tiene un impacto elevado en nuestra organización.

BIODIVERSITY NODE está convencida de que una gestión eficaz de la seguridad de la información y de la privacidad es un elemento habilitador para que la organización comprenda completamente y actúe de modo adecuado ante los riesgos a los que la información está expuesta, así como para poder responder y adaptarse de manera eficiente a los crecientes requerimientos de organismos reguladores, leyes y, por supuesto, sus clientes, en particular las entidades del sector público con las que la organización colabora o a cuyas licitaciones concurre.

Compromiso de la Alta Dirección

El propósito del Sistema de Gestión de Seguridad de la Información es garantizar que los riesgos de la seguridad de la información y de la privacidad sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, asumible y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Para ello, la dirección declara el compromiso de BIODIVERSITY NODE para:

- Establecer como objetivo primordial la prestación del servicio de consultoría ambiental, preservando la información de la organización y de sus clientes con todas las medidas necesarias a su alcance.
- Aplicar el principio de mejora continua a todos los procesos de la organización, con el objetivo adicional de conseguir el mayor grado de satisfacción de los clientes.
- Asegurar el cumplimiento de los requisitos legales y reglamentarios que sean de aplicación (en particular, la relativa a la protección de los datos personales), así como los que la organización haya asumido de manera voluntaria.
- Potenciar la participación, la comunicación, la información y la formación del equipo profesional, con el objetivo de que se sienta partícipe del trabajo de la organización en su conjunto.
- Promover el compromiso de responsabilidad entre los componentes del equipo, de acuerdo con los requisitos de calidad, así como los relativos a la privacidad y seguridad de la información acordados tanto internamente como con los clientes, mediante acciones de formación y concienciación adecuadas y regulares.
- Asegurar la continuidad del negocio desarrollando planes de continuidad conformes a metodologías reconocidas.
- Realizar y revisar periódicamente un análisis de riesgos basado en métodos reconocidos, que permita establecer el nivel tanto de privacidad de los datos personales como de seguridad de la información a nivel general y de los proyectos y servicios en marcha, y minimizar los riesgos mediante el desarrollo de políticas específicas, soluciones técnicas y acuerdos contractuales con organizaciones especializadas.

- Mantener el compromiso de información a las partes interesadas.
- Seleccionar a los proveedores y subcontratistas en base a criterios relacionados con la privacidad y la seguridad de la información.

En lo que respecta de manera específica a la protección de los datos personales, BIODIVERSITY NODE se compromete a cumplir con los principios indicados en la legislación de referencia. Estos son:

- Principio de "Licitud, transparencia y lealtad": los datos deben ser tratados de manera lícita, leal y transparente para el interesado.
- Principio de "Finalidad": los datos deben ser tratados con una o varias finalidades determinadas, explícitas y legítimas; se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.
- Principio de "Minimización de datos": se aplicarán medidas técnicas y organizativas para garantizar que sean objeto de tratamiento únicamente los datos que resulten precisos para cada uno de los fines específicos del tratamiento, reduciendo la extensión del tratamiento y limitando a lo necesario el plazo de conservación y su accesibilidad.
- Principio de "Exactitud": se dispondrá de medidas razonables para que los datos se encuentren actualizados, y se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan.
- Principio de "Limitación del plazo de conservación": la conservación de los datos debe limitarse en el tiempo al logro de los fines que persigue el tratamiento.
- Principio de "Seguridad": se realizará un análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales tratados.
- Principio de "Responsabilidad activa o responsabilidad demostrada": se mantendrá diligencia debida de manera permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados, en base a un análisis de los riesgos que el tratamiento representa para esos derechos y libertades, de modo que pueda garantizarse y demostrarse que el tratamiento se ajusta a las previsiones del RGPD y de la LOPDGDD.

Asimismo, la dirección se compromete a dirigir, apoyar y supervisar el sistema de gestión de la seguridad de la información, según lo establecido en el Real Decreto 311/2022 y sus posteriores modificaciones, y a velar por que se alcancen los objetivos del mismo.

La dirección de BIODIVERSITY NODE se compromete a apoyar y promover los principios establecidos en esta Política, para lo que pide al personal de la organización que asuma y se atenga a las previsiones del sistema de gestión documentado para el ENS.

Desarrollo de la Política de Seguridad

Esta Política de Seguridad complementa las políticas de seguridad de BIODIVERSITY NODE en diferentes materias y se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular de aquellos que utilicen, operen o administren los sistemas de información y comunicaciones, a través del repositorio documental corporativo en SharePoint Online.

La documentación relativa a la seguridad de la información estará clasificada en tres niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad.
- Segundo nivel: normativas y procedimientos de seguridad.
- Tercer nivel: informes, registros y evidencias electrónicas.

Alcance

El alcance del Sistema de Gestión de la Seguridad de la Información queda definido como: «Los sistemas de información que dan soporte al servicio de Consultoría Ambiental, según declaración de aplicabilidad vigente».

BIODIVERSITY NODE opera bajo un modelo íntegramente remoto: no dispone de sede física de trabajo y la totalidad de la plantilla desarrolla su actividad en régimen de teletrabajo. Sus sistemas de información se sustentan en servicios en la nube (Microsoft 365 y Microsoft Azure), sin servidores propios ni perímetro de red corporativo.

Esta Política se aplicará a los sistemas de información de BIODIVERSITY NODE relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados, y con independencia de la naturaleza de su relación jurídica con BIODIVERSITY NODE. Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su normativa de seguridad derivada, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

2. POLÍTICA

Prevención

La organización debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, debe implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la organización debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, deben monitorizarse de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, según lo establecido en el artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 8 del ENS. Al no disponer la organización de perímetro de red propio, las líneas de defensa se articulan sobre la identidad, el dispositivo, la aplicación y los datos. Se establecerán mecanismos de detección, análisis y reporte, apoyados en las capacidades de detección y correlación de eventos de Microsoft Defender, que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

La organización debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones relativas a incidentes detectados por terceros o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente, incluyendo comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT), en particular el CCN-CERT y el INCIBE-CERT.

Recuperación

Para garantizar la disponibilidad de los servicios críticos, la organización debe desarrollar planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y de sus actividades de recuperación.

3. ORGANIZACIÓN DE LA SEGURIDAD

Esta política se aplica a todos los sistemas de BIODIVERSITY NODE y a todos los miembros de la organización, sin excepciones.

BIODIVERSITY NODE se compromete a prestar sus servicios cumpliendo con los requisitos establecidos en su Sistema de Gestión de la Seguridad de la Información, de modo que se garantice un servicio continuado conforme a los requisitos de disponibilidad, seguridad y calidad hacia los clientes.

Debido a nuestra actividad, en BIODIVERSITY NODE sabemos que la información es un activo con un elevado valor para nuestra organización y, sobre todo, para la de nuestros clientes, y requiere, por lo tanto, una protección y gestión adecuadas con el fin de dar continuidad a nuestra línea de negocio y minimizar los posibles daños ocasionados por fallos en la seguridad de la información.

Para ello, la organización:

- Protegerá adecuadamente la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de sus activos de información mediante la introducción de una serie de controles para gestionar los riesgos de seguridad relevantes.
- Priorizará la protección y salvaguarda de sus clientes y de la información de los clientes como una prioridad de negocio.
- Establecerá, implementará, monitorizará, mantendrá y mejorará continuamente su gestión de seguridad de la información como parte de su enfoque más amplio de gestión empresarial, y mantendrá la certificación acreditada a los estándares adecuados.
- Gestionará cualquier violación de la seguridad de la información de manera oportuna y responsable, e invertirá en estrategias adecuadas de detección, respuesta y remediación.
- A intervalos planificados, probará sus controles de seguridad de la información y sus respuestas a escenarios que puedan causar una amenaza a sus operaciones.
- Proporcionará los recursos adecuados a la organización para establecer, mantener y mejorar el entorno de seguridad según sea apropiado para el cambiante panorama de riesgos.
- Invertirá en las competencias del personal para llevar a cabo sus tareas, y proporcionará al personal la capacitación y la concienciación adecuadas y relevantes para su función y para la información a la que tiene acceso.
- Garantizará que sus proveedores y organizaciones asociadas hagan lo mismo, y que establezcan y hagan cumplir los estándares de seguridad a aquellos a quienes se transmita cualquier información.

Comité de Seguridad

Los integrantes del Comité de Seguridad serán designados en un acta fundacional (Acta de constitución del Comité de Seguridad), donde se indicará la persona designada y el cargo que deberá ostentar.

El secretario del Comité de Seguridad será el Responsable de Seguridad 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.
- Elaborar el acta de las reuniones.

- Responsabilizarse de la ejecución directa o delegada de las decisiones del Comité.

El Comité de Seguridad reportará a la Dirección. Dado el modelo de trabajo remoto de la organización, sus reuniones podrán celebrarse por medios telemáticos (Microsoft Teams), dejando constancia en el acta correspondiente.

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las inquietudes de la Alta Dirección y de las diferentes áreas de la organización.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que sean consistentes, estén alineados con la estrategia decidida en la materia y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Coordinar todas las funciones de seguridad de la organización.
- Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- Velar por el alineamiento de las actividades de seguridad con los objetivos de la organización.
- Coordinar los planes de continuidad de las diferentes áreas, para asegurar una actuación sin fisuras en caso de que deban activarse.
- Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose de gestionar un control y presentación regular del progreso de los proyectos y del anuncio de posibles desviaciones.
- Recibir las inquietudes en materia de seguridad de la Dirección de la entidad y transmitirlas a los responsables pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, se comunicarán a la Dirección.
- Recabar de los responsables y del proveedor de servicios TI informes regulares del estado de la seguridad de la organización y de los posibles incidentes, que se consolidan y resumen para su comunicación a la Dirección de la entidad.
- Coordinar y dar respuesta a las inquietudes transmitidas a través de los responsables de las distintas áreas.
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías pertinentes en materia de segregación de funciones.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de la seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos, velando en particular por la coordinación de las diferentes áreas de seguridad en la gestión de dichos incidentes.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la organización en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización, velando en particular por la coordinación de los diferentes planes que puedan realizarse en distintas áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

- Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación, velando en particular 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 surgir entre los diferentes responsables y/o entre distintas áreas de la organización.

Roles: funciones y responsabilidades

Se detallan a continuación las funciones de los responsables de la organización:

Responsable de la Información

- Responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- 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).
- Establecer los requisitos de la información en materia de seguridad.
- Determinar y aprobar los niveles de seguridad de la información.
- Aprobar la categorización del sistema con respecto a la información.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar la categorización del sistema con respecto a los servicios.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

Responsable de la Seguridad

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Aprobar la declaración de aplicabilidad.
- Canalizar y supervisar tanto el cumplimiento de los requisitos de seguridad del servicio que se presta o solución que se provee, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio (POC).
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

El Responsable de la Seguridad será el secretario del Comité de Seguridad, con las funciones indicadas en el apartado correspondiente de la presente política.

De conformidad con el principio de “segregación de funciones y tareas” recogido en el artículo 10 del ENS, el Responsable de la Seguridad será una figura diferenciada del Responsable del Sistema.

Responsable del Sistema

- 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 integran adecuadamente en el marco general de seguridad.
- Tener potestad para proponer la suspensión del tratamiento de una cierta información o de la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Supervisar las tareas de administración técnica encomendadas al proveedor externo de servicios TI, que actuará siempre bajo sus indicaciones y con la autorización previa de la organización.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

Responsable de Privacidad

- Coordinar todos los aspectos relacionados con la adecuación de las actuaciones de BIODIVERSITY NODE en materia de protección de datos de carácter personal. En caso de contar con un DPD designado, éste asumirá el rol de Responsable de Privacidad.
- Coordinar, junto con el Responsable de Seguridad, el cumplimiento del ENS con respecto a la protección de datos de carácter personal.

Procedimientos de designación

El Responsable de Seguridad será nombrado por el Comité de Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Igualmente, el resto de los cargos indicados en el apartado anterior será designado por el Comité de Seguridad mediante acta de reunión.

4. REVISIÓN DE LA POLÍTICA DE SEGURIDAD

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad y la propuesta de su revisión o mantenimiento, así como su revisión extraordinaria cuando se produzcan cambios significativos en la organización, en los sistemas de información o en el marco normativo aplicable. La Política será aprobada por la Alta Dirección y difundida para que la conozcan todas las partes afectadas.

5. DATOS DE CARÁCTER PERSONAL

BIODIVERSITY NODE, en la prestación de su servicio, no trata categorías especiales de datos personales. La información técnica asociada a los proyectos se refiere principalmente a datos ambientales y de distribución de especies, sin perjuicio del tratamiento de los datos personales propios de la gestión de personal, clientes, proveedores y expedientes.

La documentación relativa, a la que tendrán acceso solo las personas autorizadas, recoge los registros de actividad de tratamiento de datos afectados y los responsables correspondientes. Todos los sistemas de información de BIODIVERSITY NODE se ajustarán a los niveles de seguridad requeridos por la normativa, atendiendo a la naturaleza y finalidad de los datos de carácter personal.

6. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, conforme a la metodología MAGERIT v3, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

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

7. OBLIGACIONES DEL PERSONAL

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

Todos los miembros de BIODIVERSITY NODE atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de BIODIVERSITY NODE, en particular a los de nueva incorporación, con especial atención a las particularidades del trabajo en remoto: protección de credenciales, uso de la autenticación multifactor, custodia de los dispositivos y buenas prácticas al conectarse desde redes ajenas al control de la organización.

Las personas con responsabilidad en el uso, operación o administración de sistemas 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 se trata de su primera asignación como de un cambio de puesto de trabajo o de responsabilidades en el mismo.

8. TERCERAS PARTES

Cuando BIODIVERSITY NODE preste servicios a otras organizaciones públicas o privadas, o maneje información de otras organizaciones públicas o privadas (por ejemplo, la documentación que los clientes comparten a través de los espacios de SharePoint habilitados para cada proyecto), se les hará partícipes de esta Política de Seguridad, se establecerán canales para el reporte y la coordinación de los respectivos comités de seguridad, y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando BIODIVERSITY NODE utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. En particular, esta obligación alcanza a ALLBIT, en su condición de proveedor de servicios gestionados de Microsoft 365, y a cualquier otro proveedor con acceso a información o sistemas de la organización. 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, y se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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

9. LEGISLACIÓN APLICABLE

A continuación se detallan las leyes que se consideran aplicables al SGSI, junto con la indicación del área responsable de evaluar su impacto en la organización.

LEY / REGULACIÓN	RESPONSABILIDAD
Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.	Responsable de Seguridad
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD).	Responsable de Privacidad
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.	Responsable de Privacidad
Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.	Dirección
Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.	Dirección
Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.	Dirección
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.	Dirección
Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).	Dirección
Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.	Dirección
Ley 17/2001, de 7 de diciembre, de Marcas.	Dirección
Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza (eIDAS).	Dirección
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.	Dirección
Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas sobre inteligencia artificial.	Responsable de Seguridad
Ley 42/2007, de 13 de diciembre, del Patrimonio Natural y de la Biodiversidad.	Dirección
Ley 21/2013, de 9 de diciembre, de evaluación ambiental.	Dirección
Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente (incorpora las Directivas 2003/4/CE y 2003/35/CE).	Dirección

Documento de uso interno de BIODIVERSITY NODE. Su distribución fuera de la organización requiere autorización previa de la Dirección.