



POLÍTICA
SEGURIDAD DE LA
INFORMACIÓN
ENS
USO PÚBLICO



Firmado:

Elena Pita

Directora Fundación Biodiversidad



1. OBJETO Y CAMPO DE APLICACIÓN

Este documento describe la política de seguridad de la información seguida por Fundación Biodiversidad F.S.P. (FB) para dar cumplimiento a los requisitos establecidos en el Esquema Nacional de Seguridad.

Se aplica a todos los sistemas que dan soporte a las siguientes actividades:

- Conservación y recuperación de hábitats y especies
- Restauración de ecosistemas
- Gobernanza y participación
- Generación del conocimiento
- Divulgación y Sensibilización
- Gestión de convocatorias de ayudas.

Y en general todos los procesos informáticos y sistemas en el ámbito de la actividad de la FB.

2. REFERENCIAS

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.1. LA ORGANIZACIÓN

Los objetivos de la Fundación Biodiversidad son:

- La conservación y restauración de los ecosistemas y el uso sostenible de los recursos naturales.
- La lucha contra las causas de pérdida de biodiversidad.
- El desarrollo de alianzas estratégicas y trabajo con socios.

1.2. MISIÓN DE LA ORGANIZACIÓN.

Nuestra misión es contribuir a revertir la pérdida de biodiversidad. Esto exige impulsar actuaciones en varios ámbitos a la vez, para conservar los ecosistemas sanos, restaurar los ecosistemas degradados, promover un uso sostenible de la biodiversidad y frenar las causas de su deterioro.

La complejidad de los retos ambientales nos obliga a actuar en distintos ámbitos a la vez, estableciendo alianzas estratégicas y puentes con la ciencia, con la iniciativa privada y con la sociedad en su conjunto.

Esta política de seguridad de la información se ha desarrollado hasta completar un sistema de gestión que cumple con los requisitos establecidos en el Esquema Nacional de Seguridad, y que incluye los siguientes apartados:

- 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.
- o) Mejora continua del proceso de seguridad.

3.1. EL MARCO REGULATORIO EN EL QUE SE DESARROLLAMOS NUESTRAS LAS ACTIVIDADES.

Fundación Biodiversidad desarrolla su actividad en un marco regulatorio marcado por el cumplimiento de los requisitos establecidos en materia de protección de datos, telecomunicaciones, y propiedad intelectual.

En el desarrollo de nuestras actividades, estamos comprometidos con el cumplimiento de los requisitos legales establecidos en:

- 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
- Ley 50/2002, de 26 de diciembre, de Fundaciones
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (vigente en aquellos artículos que no contradigan el RGPD)
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- 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.
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- Ley 10/2021, de 9 de julio, de trabajo a distancia.



- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información en el sector público.
- RD 1495/2011, de 24 de octubre, que desarrolla la Ley 37/2007 sobre reutilización de la información del Sector público, para el ámbito del sector público estatal.
- **Ley 47/2003, de 26 de noviembre**, General Presupuestaria, en cuanto al régimen presupuestario, económico financiero, de contabilidad, y de control, sin perjuicio de las competencias atribuidas al Tribunal de Cuentas. Asimismo, las fundaciones del sector público están sometidas al control de la Intervención General de la Administración del Estado
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 38/2003, de 17 de noviembre, General de Subvenciones, en base a lo dispuesto en su Disposición adicional decimosexta para las Fundaciones del sector público.

3.2. LOS ROLES O FUNCIONES DE SEGURIDAD, DEFINIENDO PARA CADA UNO, SUS DEBERES Y RESPONSABILIDADES, ASÍ COMO EL PROCEDIMIENTO PARA SU DESIGNACIÓN Y RENOVACIÓN.

La información y el saber hacer de las personas son factores decisivos para la competitividad de Fundación Biodiversidad, y constituyen activos esenciales para el crecimiento y desarrollo de nuestra organización.

Por este motivo, se han establecido los siguientes roles de seguridad:

1. **Directora de FB.** Forma parte del Comité de Seguridad de la información y es el último responsable de las decisiones adoptadas por el mismo.
2. **Responsable de la información.** Esta figura recae en el Comité de Seguridad de la Información. Es el órgano encargado de determinar los requisitos de seguridad de la información tratada, aprobando los niveles de seguridad de la información. Entre sus funciones se incluye la aprobación de esta política de seguridad.
3. **Responsable del servicio.** Al frente de cada servicio ofrecido por Fundación Biodiversidad, los Coordinadores de área actúan como responsables de los mismos.

Valora las consecuencias de un impacto negativo sobre la seguridad de los servicios. Esta valoración se efectúa atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

4. **Responsable de seguridad.** Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Se trata de una persona jerárquicamente independiente del responsable del sistema.

Participa en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones seleccionando, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que 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 su juicio.

Las medidas del Anexo II del ENS, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del responsable de la Seguridad del sistema, habida cuenta del estado de



la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

Es el responsable de aprobar la declaración de aplicabilidad que incluya las medidas del Anexo II del Esquema Nacional de Seguridad.

Es el responsable de analizar y determinar las medidas compensatorias de forma justificada mediante su aprobación formal.

Analizar y supervisar los supuestos concretos de utilización de las infraestructuras y servicios comunes de la organización.

Analizar los informes de auditoría, y encargarse de que se adopten las medidas correctivas adecuadas. El responsable de seguridad de la FB es José Félix Infante

5. **Responsable de cada sistema de información.** Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el responsable de la Seguridad. El responsable del sistema es Alberto Fernández.

6. **Responsable de protección de datos.** Es la persona encargada de determinar los fines y los medios del tratamiento de la información que contenga datos de carácter personal, y se asegura de que se cumplen los requisitos establecidos en el reglamento general de protección de datos y la ley orgánica de protección de datos y garantía de los derechos digitales.

6.1. Estos roles son desempeñados por los miembros de la organización designados por el Comité de Seguridad sin una duración determinada hasta que decida su renovación.

6.2. En el caso de que durante la realización de alguna actividad se requiriese su coordinación o mediación en la resolución de un conflicto, éste será elevado al Comité de Seguridad para su resolución.

6.3. Para los demás puestos de trabajo se han establecido sus funciones y responsabilidades en sus perfiles de puesto de trabajo. No es necesario que forme parte del comité

El responsable de protección de datos está delegado en la empresa Dret en Xarxa.

3.3. LA ESTRUCTURA Y COMPOSICIÓN DEL COMITÉ PARA LA GESTIÓN Y COORDINACIÓN DE LA SEGURIDAD.

El Comité de Seguridad de la Información se encuentra compuesto por:

- Directora.
- Subdirector Jurídico financiero, y de Capital Humano
- Coordinador Asesoría Jurídica y Servicios Generales.
- Responsable de Seguridad.
- Responsable de Sistema.

El Comité de Seguridad realiza las funciones de responsable de la información, coordinación de las actividades desarrolladas por los cargos nombrados para garantizar la seguridad y actúa como máximo órgano de decisión con los otros miembros de la organización.

3.4. LAS DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA, SU GESTIÓN Y ACCESO.

La documentación del sistema de gestión está estructurada de forma piramidal, en cuya parte superior se encuentra esta política.



Un Manual, que describe cómo se da cumplimiento a los diferentes puntos del Esquema Nacional de Seguridad y que referencia a los documentos que desarrollan cada apartado.

Instrucciones Técnicas de Seguridad, que describen las políticas de seguridad aplicadas a los sistemas de la organización.

Por último, los registros que sirven como evidencia para demostrar el cumplimiento de los requisitos establecidos en el Esquema Nacional de Seguridad.

Los documentos se encuentran compartidos con los miembros pertinentes de la organización a través de las carpetas de red a las que pueden acceder en modo solo lectura y que administra el responsable de sistemas de seguridad.

3.5. LOS RIESGOS QUE SE DERIVAN DEL TRATAMIENTO DE LOS DATOS PERSONALES.

Durante el desarrollo de su actividad, Fundación Biodiversidad accede a información personal que es tratada conforme a los requisitos legales establecidos tanto en el reglamento general de protección de datos, como en la ley orgánica de protección de datos y garantía de derechos digitales.

En aquellos casos en los que se cuenta con un encargado de tratamiento, se establecen los acuerdos y condiciones que rigen la forma en la que deben ser tratados acorde a los riesgos detectados por el responsable de protección de protección, que evalúa el tratamiento que debe aplicarse en cada caso, y al que puede acceder para ejercer los derechos contemplados en la legislación a través de la dirección de correo electrónico dpo@fundacion-biodiversidad.es.

4. CONTROL DE EDICIONES

EDICION	MOTIVO DEL CAMBIO	FECHA
1	Primera elaboración de la política	27/11/2023

