



ÍNDICE

1. INTRODUCCIÓN	2
1.1 Objeto	2
1.2 Alcance	2
1.3 Misión de Cofides.....	2
1.4 Marco normativo	2
2. OBJETIVOS	3
2.1. Directrices de seguridad de la información y protección de datos personales.....	3
2.2. Principios y responsabilidades de seguridad de la información y protección de datos personales.....	5
3. ORGANIZACIÓN DE LA SEGURIDAD	7
3.1 Comité de Dirección y Estrategia	8
3.2 Comité de Seguridad de la información.....	8
3.3 Roles: Funciones y Responsabilidades	9
3.3.1 Responsable de seguridad de la Información.....	9
3.3.2 Responsable de la información	10
3.3.3 Responsable del Servicio.....	11
3.3.4 Responsable del Sistema.....	11
3.3.5 Delegado de protección de datos.....	12
3.3.6 Designación.....	12
3.4 Obligaciones de los usuarios.....	12
4. Protección de datos de carácter personal	13
4.1 Datos de carácter personal	13
4.2 Gestión de Riesgos.....	13
4.3 Cuerpo Normativo	14
4.4 Calificación de la información.....	14
4.5 Formación y concienciación	16
4.6 Vigencia y revisión	16
5. REGISTROS.....	16



1. INTRODUCCIÓN

1.1 Objeto

La finalidad de esta Política de Seguridad de la Información y protección de datos personales es establecer los principios y directrices a aplicar para gestionar la seguridad de la información y de los datos de carácter personal en COFIDES, de manera que garantice el cumplimiento de la normativa aplicable y se protejan adecuadamente sus activos de información a lo largo de su ciclo de vida atendiendo a sus dimensiones de seguridad (Confidencialidad, Integridad, Disponibilidad, Trazabilidad y Autenticidad), y afectará a toda la información tratada por medios electrónicos y a la información en soporte papel que COFIDES gestiona en el ámbito de sus competencias.

1.2 Alcance

Además de las obligaciones que se mencionan a lo largo de las políticas de seguridad, esta política aplica a todos los sistemas, servicios y activos de Tecnologías de la información y la comunicación (de ahora en adelante TIC) de COFIDES, así como a las actividades de tratamiento, siendo extensible a todos los usuarios de los sistemas de la información, sin excepciones, debiendo ser conocida y cumplida por todos los usuarios de los sistemas de información y/o la información, incluido el soporte físico, internos y externos, con independencia de la posición, cargo y responsabilidad dentro de la Organización.

1.3 Misión de COFIDES

Contribuir a la internacionalización de la economía española y al desarrollo sostenible mediante la prestación de servicios financieros.

1.4 Marco normativo

A continuación, se enumeran las principales normas de referencia identificadas y de aplicación general a Cofides:

- ✓ 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).
- ✓ Corrección de errores 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 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.
- ✓ Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, de conformidad con el 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 la libre circulación de esos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio.

- ✓ Ley 2/2011, de 4 de marzo, de Economía Sostenible.
- ✓ Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- ✓ Ley 17/2001, de 7 de diciembre, de Marcas.
- ✓ Real Decreto 687/2002, de 12 de julio, por el que se aprueba el Reglamento para la ejecución de la Ley 17/2001, de 7 de diciembre, de Marcas.
- ✓ Ley 10/2021, de 9 de julio, de trabajo a distancia.
- ✓ 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.
- ✓ 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.
- ✓ Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011.
- ✓ Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

2. OBJETIVOS

2.1. Directrices de seguridad de la información y protección de datos personales

Las directrices de seguridad de la información se tendrán siempre presentes en cualquier actividad relacionada con el tratamiento de datos personales, la gestión y el uso de los activos de información. Dentro de la Organización se han establecido las siguientes directrices:

- ✓ Alcance estratégico: La seguridad de la información contará con el compromiso y apoyo de todos los niveles directivos de forma que se coordine e integre con el resto de las iniciativas estratégicas de la Organización.
- ✓ Responsabilidad diferenciada: En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la



responsabilidad sobre la prestación de los servicios y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

- ✓ Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, y legales relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los tratamientos de datos y los sistemas de información y considerando para esta su protección de acuerdo con la normativa de aplicación y sus dimensiones de:
 - Confidencialidad (C): Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
 - Integridad (I): Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
 - Disponibilidad (D): Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
 - Trazabilidad (T): Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Autenticidad (A): Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- ✓ Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- ✓ Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- ✓ Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado. Las auditorías serán subcontratadas y coordinadas por Control y Auditoría Interna, por lo que formarán parte integrante de la planificación de esta área.
- ✓ Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.



2.2. Principios y responsabilidades de seguridad de la información y protección de datos personales

Las directrices de seguridad se concretan en los siguientes principios de obligado cumplimiento en la Organización:

- ✓ Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para garantizar y poder demostrar que el tratamiento es conforme a la normativa, teniendo en cuenta la naturaleza, el ámbito, el contexto, los fines del tratamiento y los riesgos a los que puede verse expuesto el tratamiento, de acuerdo con lo exigido por el Reglamento General de Protección de Datos. Gestión de activos de información: Los activos de información de la Organización se encontrarán inventariados y categorizados y estarán asociados a un responsable. La categorización de los activos se realizará de acuerdo con sus dimensiones de seguridad según las indicaciones recogidas en el documento "PR_ValoracionActivosServicios_Ed01.00", como resultado de la valoración de los distintos activos se establecerá el nivel de seguridad requerido de acuerdo con lo indicado en dicho documento.
- ✓ Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
- ✓ Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- ✓ Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- ✓ Control de acceso: Se aplicará una política de mínimo privilegio y se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la Organización.
- ✓ Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- ✓ Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro, gestión y resolución de los incidentes de seguridad. Se asegurará la notificación de aquellos incidentes que correspondan al Centro Criptológico Nacional (CCN-CERT) en los plazos y formas estipulados por el ENS.
- ✓ Gestión de la continuidad: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus



procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.

- ✓ Seguridad en la cadena de suministro: Se supervisarán y gestionarán los riesgos de seguridad derivados de las relaciones con proveedores y terceros que accedan a los activos de información de la organización, asegurando el cumplimiento de esta política y la normativa aplicable.
- ✓ Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de protección de datos y seguridad de la información, así como su verificación y auditoría.
- ✓ Se cumplirá con los principios de protección de datos personales determinados por la normativa vigente.
 - Principio de legitimidad en el tratamiento de datos personales: sólo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en el RGPD.
 - Licitud y lealtad en el tratamiento de datos: los datos de carácter personal serán tratados de manera lícita, leal y transparente.
 - Minimización: los datos de carácter personal tratados han de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
 - Exactitud: los datos de carácter personal serán exactos y para su actualización se adoptarán las medidas razonables necesarias para que se supriman o rectifiquen sin dilación los datos personales que resulte inexactos con respecto a los fines para los que se tratan.
 - Limitación del plazo de conservación: los datos de carácter personal serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines que justificaron su tratamiento.
 - Integridad y confidencialidad: los datos de carácter personal serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medida técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto incluso después de haber concluido su relación con COFIDES
 - Responsabilidad proactiva: COFIDES será responsable de cumplir con los principios estipulados en esta política, la legislación aplicable y debe ser capaz de demostrarlo cuando así lo exija la legislación aplicable.
 - Seguridad integral: La gestión de riesgo se establece como parte esencial del proceso de cumplimiento normativo de protección de datos para alcanzar las máximas garantías en la protección de los derechos y libertades de los titulares de los datos que se tratan en COFIDES, buscando un equilibrio y proporcionalidad entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de ocurrencia de los riesgos a los que están expuestos y la eficacia y coste de las medidas de seguridad aplicadas, el valor



de la información y los servicios afectados. A través de los análisis de riesgos de los tratamientos que se realicen y en el caso de alguno de estos tratamientos pueda afectar a derechos y libertades fundamentales, sometidos a Evaluación de impacto, COFIDES identificará, valorará y adoptará decisiones y tendrá en consideración las encaminadas a la preservación de la confidencialidad, la integridad y la disponibilidad de la información, así como la autenticidad, responsabilidad, fiabilidad y no repudio en relación con determinada información. Las medidas de seguridad adoptadas estarán sujetas a un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad de los tratamientos.

- Para la atención y gestión de los Derechos de los interesados COFIDES adoptará las medidas que correspondan para garantizar el adecuado ejercicio de los derechos de los interesados. Por ello, se establecerán los procedimientos internos que resulten suficientes para atender, con prontitud y cuando procedan, los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad y revocación del consentimiento ejercitados por los interesados o sus representantes legales.
- En la obtención y registro de datos personales COFIDES se compromete al tratamiento de datos obtenidos de fuentes legítimas y por tanto queda prohibidas la adquisición y obtención de datos personales de fuentes que no garanticen suficientemente su legítima procedencia o de fuentes cuyos datos hayan sido recabados o cedidos contraviniendo la normativa aplicable. Además, para la contratación de encargados del tratamiento COFIDES ha previsto la adopción de las medidas necesarias que garanticen el tratamiento de datos por los prestadores de servicios contratados y ayuden al responsable a demostrar el cumplimiento de las obligaciones legales.

Estos principios se aplican en el momento del diseño e implementación de todos los procedimientos que impliquen el tratamiento de datos personales, en todos los servicios prestados por COFIDES, en los contratos y u obligaciones que se formalicen y supongan tratamiento de datos personales, en la implantación de sistemas y plataformas de tratamiento de datos que permitan el acceso a datos tanto por parte del personal propio como de tercero. COFIDES promoverá los sistemas de información de los que es responsable, así como aquellos sobre los que decide realizar tratamientos de datos de su responsabilidad se diseñen y configuren de forma que garanticen la protección de datos por defecto.

3. ORGANIZACIÓN DE LA SEGURIDAD

La estructura organizativa para la gestión de la seguridad de la información en el ámbito de la Organización está compuesta por los siguientes agentes:

- ✓ El Comité de Dirección y Estrategia.
- ✓ El Comité de Seguridad de la Información.
- ✓ El responsable de seguridad, que en ningún caso dependerá del responsable del Sistema.
- ✓ Los responsables de la información.



- ✓ Los responsables del servicio.
- ✓ Los responsables del sistema.

Dichos nombramientos se registrarán en las Actas del Comité de Dirección y Estrategia.

En caso de existir conflictos relacionados con sus competencias en el ámbito de la seguridad de la información entre los distintos responsables designados, estos conflictos serán comunicados al Comité de Seguridad de la información desde el cual se evaluarán y se propondrán soluciones a los mismos. En caso de no ser aceptadas dichas soluciones por las partes implicadas se escalará la decisión final al Comité de Dirección y Estrategia.

3.1 Comité de Dirección y Estrategia

Su composición y funcionamiento se establece en la normativa interna de gestión de la Organización, y ejerce las siguientes funciones:

- ✓ Establecer y aprobar la estrategia de seguridad para la compañía y los objetivos de alto nivel a alcanzar.
- ✓ Establecer una estrategia de gestión de riesgos en materia de seguridad y el nivel de tolerancia al riesgo aceptado.
- ✓ Establecer, aprobar y promover una estructura organizativa para la implementación de la seguridad integral en toda la compañía y los recursos necesarios. Actuar como decisor final ante la resolución de conflictos entre los distintos responsables designados.

3.2 Comité de Seguridad de la información

El Comité Coordinador de Seguridad TIC, es el máximo responsable de seguridad de la información y servicios. Este comité tendrá la siguiente composición:

- ✓ La presidencia del Comité recaerá en un miembro de la alta dirección de la organización designado por el Comité de Gestión Ordinaria (distinto del Responsable de Sistemas y Tecnología, y del Responsable de Seguridad)
- ✓ El responsable de Sistemas y Tecnología.
- ✓ El responsable de Seguridad.
- ✓ El delegado de protección de datos participará con voz y sin voto siempre que se traten cuestiones relacionadas con el tratamiento de datos de carácter personal, emitiendo su opinión, que se hará constar.
- ✓ Responsables de áreas de servicio clave, cuando sea requerido.

Este comité, tendrá las siguientes funciones:

- ✓ Coordinar y aprobar las acciones en materia de seguridad de la información, lo que incluye la revisión de esta política de seguridad de la información.
- ✓ Impulsar la cultura en seguridad de la información. Garantizar la divulgación de la política y normativa de seguridad de la organización.



- ✓ Participar en la categorización de los sistemas y en el análisis de riesgos.
- ✓ Revisar y aprobar los análisis de riesgos de los sistemas de información y los planes de acciones para mitigarlos, así como dar seguimiento al cumplimiento de estos.
- ✓ Resolver discrepancias y problemas que puedan surgir en la gestión de la seguridad.
- ✓ Aprobar y revisar las normas y procedimientos de desarrollo de esta política.
- ✓ Velar por la correcta aplicación de las distintas políticas y procedimientos de seguridad.
- ✓ Actuar como núcleo del Comité de Crisis en la gestión de los incidentes de seguridad de la información.
- ✓ Ser destinatarios de los informes de auditoría de seguridad, evaluar los hallazgos y debilidades detectadas y proponer y realizar seguimiento de las acciones correctoras necesarias.

De modo habitual el comité se reunirá con una periodicidad trimestral, pudiendo mantener reuniones con menor periodicidad siempre que la importancia de los asuntos a tratar así lo aconseje. Cualquier miembro del comité puede solicitar la convocatoria de una reunión extraordinaria enviando para ello una comunicación vía correo electrónico a los demás miembros, siendo potestad del presidente del comité el aceptar la solicitud.

3.3 Roles: Funciones y Responsabilidades

3.3.1 Responsable de seguridad de la Información

Sus funciones serán las siguientes:

- ✓ Aconsejar a los responsables correspondientes, en la identificación de la información y los servicios, así como en la evaluación de los niveles de seguridad necesarios para la información y el servicio.
- ✓ Realizar y mantener la categorización del sistema de la Organización de acuerdo con los niveles (Bajo, Medio, alto) establecidos en el Anexo I del Esquema Nacional de Seguridad (RD 311/2022).
- ✓ Elaborar y mantener la política de seguridad.
- ✓ Definir la metodología y supervisar la realización periódica de los análisis de riesgos, que serán ejecutados por los Responsables de Información y validados por el Comité de Seguridad.
- ✓ Elaborar y mantener el documento de aplicabilidad del sistema.
- ✓ Establecer las medidas de seguridad a aplicar de acuerdo con el nivel de seguridad resultante.
- ✓ Elaborar los documentos con los procedimientos operativos de gestión de la seguridad, así como la normativa de uso de los medios que será aprobada por la dirección.
- ✓ Velar e impulsar el cumplimiento del cuerpo normativo definido de seguridad.



- ✓ Revisar la puesta en marcha de los procedimientos de gestión de seguridad, así como su evaluación en el transcurso del ciclo de vida de los sistemas de información.
- ✓ Promover la mejora continua en la gestión de la seguridad de la información.
- ✓ Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución y participar en la toma de decisiones en momentos de alerta.
- ✓ Impulsar la formación y concienciación de todo el personal en materia de seguridad de la información.
- ✓ Llevar a cabo acciones, como por ejemplo hacking ético, para medir periódicamente el grado de concienciación del personal.
- ✓ Elaborar los planes de mejora de la seguridad.
- ✓ Asumir las funciones explícitamente atribuidas a la figura del responsable de seguridad en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- ✓ Asimismo, el Responsable de Seguridad de la información actuará como punto de contacto (PoC) establecido para la seguridad de la información.

3.3.2 Responsable de la información

Los responsables de la Información tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos en materia de seguridad de la información que manejan. Si esta información incluyera datos de carácter personal el responsable del Servicio o responsable de la Información, según el caso, se encargará de velar por el adecuado cumplimiento de las obligaciones de COFIDES en calidad de responsable del tratamiento., además deberán tenerse en cuenta las medidas de seguridad que correspondiera implantar atendidos los riesgos generados por el tratamiento de acuerdo con lo exigido en la legislación vigente que sea de aplicación.

Las funciones de responsable de la Información recaerán inicialmente en los responsables de área o departamento propietario o responsable del tratamiento de la información, pudiendo una misma persona acumular las responsabilidades de la información de todos los activos de información que gestione, o designar personal a su cargo para que asuma parte de sus funciones, no implicando esta designación en ningún caso una declinación de responsabilidad.

Sus funciones serán las siguientes:

- ✓ Establecer los requisitos de la información en materia de seguridad. Si esta información incluyera datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.
- ✓ Identificar, evaluar y aprobar la información que sea tratada por la Organización.
- ✓ Determinar los niveles de seguridad de la información tratada y de los servicios prestados, respectivamente.



- ✓ Realizar, con el asesoramiento del responsable de Seguridad y del responsable del Sistema, los preceptivos análisis de riesgos y auditorías de seguridad, acordando con dichos responsables las salvaguardas a implantar.
- ✓ Aceptar los riesgos residuales calculados en el análisis de riesgos.

3.3.3 Responsable del Servicio

Los responsables del Servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos de los servicios en materia de seguridad. Si estos servicios incluyen datos de carácter personal, además deberán tenerse en cuenta las medidas que corresponda implantar atendidos los riesgos generados por el tratamiento, de acuerdo con lo exigido en la legislación vigente que sea de aplicación.

Las funciones de responsable del Servicio recaerán inicialmente en los responsables de área o departamento propietarios de los servicios considerados, pudiendo una misma persona acumular las responsabilidades de todos los servicios que gestione o designar personal a su cargo para que asuma parte de sus funciones, no implicando esta designación en ningún caso una declinación de responsabilidad.

Sus funciones serán las siguientes:

- ✓ Establecer los requisitos de los servicios en materia de seguridad.
- ✓ Identificar, evaluar y aprobar los servicios tecnológicos prestados por la Organización.
- ✓ Tomar en consideración el estado de seguridad de los servicios prestados.
- ✓ Comunicar al gobierno de la Organización la necesidad de suspender un servicio por aquellas violaciones de seguridad que hayan afectado al propio servicio.
- ✓ Trabajar en colaboración con el responsable de seguridad y los responsables de sistemas en el mantenimiento de los sistemas.

3.3.4 Responsable del Sistema

El responsable del Sistema es la persona cuya responsabilidad es desarrollar, operar y mantener los sistemas de información corporativos durante todo su ciclo de vida, así como elaborar los procedimientos e instrucciones técnicas operativas de aplicación a estos sistemas.

Sus funciones serán las siguientes:

- ✓ Implantar las medidas de carácter técnico estipuladas como necesarias por el responsable de seguridad.
- ✓ Implantar los planes de continuidad del servicio, asesorado por el responsable de Seguridad.
- ✓ La gestión, configuración y actualización, según corresponda, del *hardware* y *software* en el que se basan mecanismos y servicios de seguridad del sistema de información.



- ✓ La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluido el control de que la actividad desarrollada en el sistema cumple con el que está autorizado, en especial la de los usuarios genéricos y administradores o súper usuarios.
- ✓ Aplicar los procedimientos operativos de seguridad.
- ✓ Aprobar los cambios en la configuración actual del Sistema de Información.
- ✓ Asegurarse de que se cumplan los controles de seguridad establecidos estrictamente.
- ✓ Asegurarse de que se aplican los procedimientos aprobados para gestionar el sistema de información.
- ✓ Supervisar las instalaciones de *hardware* y *software*, sus modificaciones y mejoras para asegurar que la seguridad no sea comprometida.
- ✓ Monitorizar el estado de seguridad del sistema, siempre por las herramientas y mecanismos de gestión de eventos de seguridad y auditorías técnicas que se implementaron.

3.3.5 Delegado de protección de datos

COFIDES cuenta con un delegado de protección de datos, designado voluntariamente, que llevará a cabo las tareas establecidas por la normativa de aplicación, las recomendaciones de la AEPD y las directrices del Comité Europeo de protección de datos.

El Delegado de protección de datos cumplirá diligentemente con las obligaciones determinadas en los artículos 37 y siguientes del RGPD, y con las funciones previstas en el artículo 39 del RGPD, relativas a la información, asesoramiento, supervisión y colaboración con la autoridad de control.

3.3.6 Designación

La designación para los distintos roles se detalla a continuación:

- ✓ Los responsables de Área, o persona que designen, tendrán el rol de responsables de la Información y de responsables de Servicio.
- ✓ Los responsables de Sistemas y Tecnología y/o Técnico de sistemas tendrán el rol de responsable del Sistema.
- ✓ Se designará personal específico para desempeñar el rol de responsable de seguridad, con independencia jerárquica con respecto al responsable del Sistema.
- ✓ El delegado de Protección de Datos será designado por el Consejo de Administración.

Estos nombramientos serán revisados cada 2 años o cuando uno de los puestos quede vacante y aprobados por el Comité de Dirección y Estrategia.

3.4 Obligaciones de los usuarios

Todos los usuarios de los sistemas de la información 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 disponer los medios necesarios para que la información llegue a los afectados. Estas obligaciones se mantienen tanto en el período durante el cual se ocupa un puesto como posteriormente, en el caso de rescisión de la cesión o traslado a otro empleo.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para lo 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 manifiesto incumplimiento de la Política de Seguridad de la Información o de la normativa y los procedimientos derivados de ellas, pueden llevar al inicio de medidas disciplinarias adecuadas y, si es el caso, a otras medidas legales de aplicación.

4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

4.1 Datos de carácter personal

En lo referente a los datos de carácter personal que sean objeto de tratamiento por parte de la Organización, el responsable del Servicio o responsable de la Información, según el caso, se encargará de velar por el adecuado cumplimiento de las obligaciones de COFIDES en calidad de responsable del tratamiento, con el asesoramiento del Delegado de protección de datos y bajo su función supervisora.

En caso de conflicto entre los diferentes responsables, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

4.2 Gestión de Riesgos

Todos los sistemas sujetos a esta Política deben ser considerados durante la realización de los análisis de riesgos de seguridad de la información. Este análisis se repetirá:

- ✓ Regularmente, al menos una vez al año.
- ✓ Cuando cambie de modo relevante el nivel de clasificación de la información manejada.
- ✓ Cuando cambien de modo relevante los servicios prestados.
- ✓ Cuando ocurra un incidente grave de seguridad.
- ✓ Cuando se reporten vulnerabilidades graves.
- ✓ Cuando se produzcan cambios significativos en la arquitectura de los sistemas, la infraestructura tecnológica o las medidas de seguridad.

El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo las inversiones de carácter horizontal necesarias.



4.3 Cuerpo Normativo

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en niveles, según el ámbito de aplicación y el nivel de detalle técnico, de manera que cada norma se fundamente en las normas de nivel superior. Dichos niveles de desarrollo son los siguientes:

- ✓ Primero: Política de seguridad de la información y protección de datos. Está constituido por el presente documento y es de obligado cumplimiento.
- ✓ Segundo: Está constituido por el conjunto de documentos que desarrollan la política de seguridad y que sirven para indicar como se debe actuar. Los documentos relativos a este segundo nivel normativo serán objeto de aprobación por parte del Comité de Seguridad y son de obligado cumplimiento.
- ✓ Tercero: Procedimientos de seguridad de la información. Conjunto de documentos que describen explícitamente y paso a paso como realizar una cierta actividad. La responsabilidad de aprobación de estos procedimientos dependerá de su ámbito de aplicación.

Además de los documentos citados, la documentación de seguridad podrá contar con otros documentos, como recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

4.4 Calificación de la información

COFIDES establece un sistema de clasificación de la información, incluida aquella que contiene datos de carácter personal, que genera y gestiona, en función de su ámbito de difusión previsto y de las consecuencias que pudiera tener para la organización y para los titulares de los datos un eventual acceso no autorizado a la misma.

El sistema se estructura en los siguientes niveles de menor a mayor criticidad:

Información pública

Toda aquella información que, individual o juntamente con información de terceros, está destinada a su divulgación pública.

Respecto a este tipo de información:

- ✓ No existe ninguna restricción para el acceso a la información.
- ✓ El responsable de la información establece u ordena que se establezcan medidas para controlar su modificación o borrado.
- ✓ La distribución o puesta a disposición pública sólo se produce una vez comprobado por su responsable que los documentos no incorporan información de nivel de clasificación superior.

Información de uso interno

Aquella información cuya vocación es estar a disposición de toda la organización a través de los cauces habituales de comunicación disponibles, tales como sistemas de gestión documental o sistemas de compartición de ficheros y cualesquiera otros medios de difusión interna existentes. La información no es, en principio, accesible a terceras partes ajenas a



la organización salvo que necesiten acceder a ella para la realización de las funciones que tienen encomendadas.

La difusión de esta información fuera del ámbito de la organización no conlleva impacto relevante.

- ✓ El acceso a la información queda restringido a todas las personas en plantilla de la organización o a aquellos terceros que la requieran para el desempeño de las funciones encomendadas.
- ✓ En caso de que lo considere oportuno, el responsable de información de USO INTERNO puede establecer u ordenar que se establezcan limitaciones para controlar su reproducción, física o lógica, o su modificación.
- ✓ La información sólo puede ser procesada, almacenada o reproducida en las áreas propias o gestionadas por la organización salvo acuerdos explícitos con terceros.

Información confidencial

Aquella información, propia o de terceros, destinada a ser utilizada en un ámbito concreto o proyecto de COFIDES y cuya revelación no autorizada podría causar un impacto económico, un menoscabo considerable en la reputación de la organización, en la pérdida de su competitividad o bien en la confianza de los clientes y en los derechos de los titulares de datos.

En concreto, toda la información que contenga datos de carácter personal será clasificada como “confidencial” con especial relevancia en el caso de categorías especiales de datos.

- ✓ El acceso a la información queda restringido al personal de la organización y proveedores, que desempeñen sus funciones en el proyecto o área de actividad concreta al que pertenece la información. En cualquier caso, la autorización de acceso es concedida previamente por el responsable del área.
- ✓ El acceso a la información por parte de personas de plantilla de la organización y proveedores requiere la firma de un compromiso de confidencialidad. En el caso de acceso autorizado a terceros, es precisa también la existencia previa de los correspondientes acuerdos de confidencialidad y contratos de acceso a datos.
- ✓ El almacenamiento, proceso o reproducción de información queda limitado a las áreas en las que se desarrollan las actividades a las que pertenece la información. Se evita en especial, el almacenamiento o reproducción de la información en áreas o dispositivos destinados al acceso público.
- ✓ Se adoptan en todo momento las medidas necesarias para evitar el acceso no autorizado a la información, bien sea fortuita o deliberadamente, durante su utilización y reproducción.
- ✓ Para el almacenamiento de información en formato físico se utilizan armarios o cajones dotados de cerradura.
- ✓ El almacenamiento de información en formato digital en dispositivos removibles se hace en forma cifrada.
- ✓ El almacenamiento de información en formato digital en los discos duros de equipos portátiles y dispositivos móviles corporativos se hará en forma cifrada.



- ✓ El intercambio local o remoto de información por medio de redes privadas o públicas se hace aplicando mecanismos de cifrado. Incluyendo los documentos adjuntos al correo electrónico.

Cualquier información no clasificada se tratará por defecto como de Uso Interno

4.5 Formación y concienciación

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados de la Organización, así como a la difusión entre los mismos de esta política y de su desarrollo normativo.

El responsable de Seguridad se encargará de promover las actividades de formación y concienciación en materia de seguridad y de testear de forma periódica el grado de concienciación del personal.

Las acciones formativas y de concienciación relativas al tratamiento de datos serán supervisadas por el Delegado de protección de datos.

4.6 Vigencia y revisión

El presente documento se revisará por el Comité de Seguridad de forma periódica con una frecuencia mínima anual, con el fin de adaptarla a los cambios que puedan surgir en el modelo de negocio o en el contexto donde opere la Organización, garantizando en todo momento su efectiva implantación.

Será misión del Comité de Seguridad la revisión, difusión y mantenimiento de la Normativa de Seguridad de la Información derivada de este documento.

5. REGISTROS

Nombre de Registro	Información	Área responsable
PUBLICACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Dentro del Portal Corporativo de COFIDES, en ISONET	CI
COMUNICACIÓN DE LAS POLÍTICAS DE SEGURIDAD	Comunicación remitida a los trabajadores de COFIDES sobre la ubicación, en ISONET , de las políticas cuando se incorporan por primera vez a la empresa y cuando estas se actualizan.	CI
AUDITORÍAS PERIÓDICAS DE ANÁLISIS DE RIESGOS	Los propios informes de auditoría interna y planificación de puntos de control anuales.	CI