PLT-02 – POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO.

USO PÚBLICO

VERSIÓN	FECHA	MOTIVO
1.0	18.07.2022	Elaboración del documento. Escisión de Oesía
1.1	Mayo 2023	Integración documentación ENS y SGI (27701/22301)

ELABORADO POR	REVISADO POR	APROBADO POR
Responsable del SGSI	Subcomité de ciberseguridad (SGSI-CIBER).	Subcomité de Gestión de la Seguridad y Continuidad (SGSC)
Fecha: Mayo 2023	Fecha: Enero 2023	Fecha: Julio 2023

Índice

1 Introducción

El presente documento complementa y desarrolla la Política de Seguridad de la Información de GRUPO OESÍA (ORG.01-01 Política de Seguridad de la Información), para recoger los aspectos particulares relacionados con la seguridad de la información y continuidad de los servicios y procesos específicos que lleva a cabo el Centro de Operaciones de Seguridad de Cipherbit-Grupo Oesía, en adelante **CERT Cipherbit**, así como recoger los requisitos determinados que son exigidos por las distintas normas y regulaciones que le afectan, como puede ser:

- ISO 27001, Information technology — Security techniques — Code of practice for information security controls based on ISO 27002.
- ISO 22301, Protección y seguridad de los ciudadanos – Sistema de Gestión de la Continuidad del Negocio.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Las leyes 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Reglamento (UE) 2016/679 de 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 estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.

Estos contenidos específicos de la seguridad de la información y continuidad de negocio de los servicios y procesos implantados en un determinado ámbito de operación (CERT Cipherbit), son aprobados, por el **Subcomité de Gestión de la Seguridad y Continuidad (SGSC)** del ámbito en el que se constituye, por delegación del **Comité Operativo de Seguridad Corporativa**. Dicho subcomité aborda la seguridad, como un proceso delegado integral, constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información dentro de su alcance y tiene el mandato de garantizar que dicho proceso implantado será actualizado y mejorado de forma continua.

2 Objeto y ámbito de aplicación

Esta política se aplica a todos los sistemas de información de Cipherbit- Grupo Oesía que dan soporte a los servicios especificados que se incluyen en el ámbito de aplicación del SGI – CIBER implantados en la Organización por medio del **Subcomité de Ciberseguridad (SGSI-CIBER)** y que son descritos, en cada caso, en el documento ***MS-01_ Alcance del Sistema Gestión Integrado.***

También se hace extensible a todos los miembros de la Organización y terceros afectados por el SGI-CIBER, sin excepciones, debiendo ser conocida y cumplida por todo el personal interno y externo, independientemente del puesto, cargo y responsabilidad dentro de la misma.

3 Misión y visión de Cipherbit- Grupo Oesía

Cipherbit es una organización que en 2022 ha sido creada al amparo del GRUPO OESÍA y por tanto al ser una organización aún muy joven depende en su gran mayoría de la Organización matriz, es por ello que la historia de Cipherbit, es la historia de Oesía.

Cipherbit es la primera marca española específicamente dedicada a la ciberseguridad y desarrollo de productos de comunicaciones seguras (cifra) certificados por el Centro Criptográfico Nacional (CCN) y la OTAN.

Focalizándose en el entorno nacional e internacional de Fuerzas Armadas, Administraciones Públicas e infraestructuras críticas, reforzando de esta manera nuestra autonomía estratégica en ciberdefensa.

Cipherbit- Grupo Oesía apuesta por mantener su liderazgo a largo plazo y este compromiso por el crecimiento sostenido se materializa en la inversión continua y la maximización de la captación del talento, incorporando día a día a la organización los avances tecnológicos que lo hacen posible y para lo cual sigue diversas estrategias como:

- Inversión significativa en I+D+i.
- Modelo de alianzas y colaboración con partners y clientes.
- Mantener la calidad a un coste competitivo.
- Relación con Universidades, compromiso con Asociaciones y presencia en los principales Parques Tecnológicos.

Un compromiso y responsabilidad que adquiere con las personas, la sociedad, las empresas y los gobiernos, con la que define la actitud que caracteriza a sus profesionales que, unida a su talento, proporciona las premisas necesarias para ofrecer un servicio excelente, que aporta valor a los clientes y con el que conseguir, entre todas sus partes interesadas, un futuro sostenible.

4 Desarrollo de la Política

Cipherbit- Grupo Oesía sustenta la mayoría de sus actividades de negocio en Sistemas de Información, siendo estos un soporte básico para la operativa interna, la gestión de los servicios que proporciona y su desarrollo comercial. La información manejada por los diferentes sistemas y aplicaciones, así como la infraestructura de comunicaciones, constituyen, junto a las personas, el activo principal para el normal desarrollo de las operaciones de negocio.

Con este fin ha desarrollado esta Política de Seguridad de la Información y Continuidad de Negocio, que está constituida por la estructura organizativa, los recursos humanos y técnicos, los procesos, planes, procedimientos y protocolos relacionados con las medidas de prevención y respuesta frente a los riesgos de seguridad de naturaleza física, lógica y el cumplimento de la regulación normativa, aplicable y del buen gobierno corporativo.

Los requisitos y objetivos de seguridad de la información y continuidad de las operaciones, son determinados en base a los criterios derivados de las políticas de GRUPO OESÍA y las necesidades determinadas por los responsables de los activos de información y de los procesos de negocio, siendo su alcance todas las actividades relacionadas con la seguridad de la información y continuidad de las operaciones, con especial enfoque en la seguridad lógica. Su aplicabilidad abarca la prestación de aquellas actividades y servicios que lo son directamente por la seguridad de la propia Organización y también por terceros, siguiendo sus directrices e instrucciones y lo hace desde un enfoque avanzado, completo e integral.

El objeto de esta Política es alcanzar una protección adecuada de los activos de información y procesos de negocio de Cipherbit- Grupo Oesía, ajustada a las distintas necesidades y expectativas de las distintas áreas productivas, estableciendo alcances delimitados, implementados por Sistemas de Gestión que recojan las particularidades de cada área y contexto, siempre preservando los siguientes principios de la seguridad:

4.1 Principios integradores

Sin perjuicio de los principios básicos establecidos en la Política Corporativa de GRUPO OESÍA y otras normas de rango superior, esta política se desarrollará, con carácter general, de acuerdo a los principios enumerados a continuación que fundamentan su necesidad, naturaleza y cuyo establecimiento evidencia el liderazgo y el compromiso del Comité Ejecutivo de GRUPO OESÍA respecto del sistema de gestión de la seguridad de la información y continuidad de negocio:

a) **Principio de confidencialidad:** los sistemas de información deberán ser accesibles

únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

b) **Principio de integridad y calidad:** se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

c) **Principio de disponibilidad y continuidad:** se garantizará un nivel de disponibilidad en los sistemas de información y se dotarán los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

d) **Principio de Seguridad Integral:** se entenderá la seguridad como un proceso integral que incluya a todos los elementos técnicos, humanos, materiales y organizativos de los sistemas de información.

e) **Principio de gestión del riesgo:** se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.

f) **Principio de proporcionalidad en coste:** la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.

g) **Principio de concienciación y formación:** se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad de las tecnologías de la información de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

h) **Principio de prevención:** se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad de las tecnologías de la información.

i) **Principio de detección y respuesta:** los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente, a través de los mecanismos establecidos al efecto, a los incidentes de seguridad. Existirán mecanismos de

recuperación que permitan la restauración y recuperación de la información y de los servicios para que en el caso de un incidente de seguridad que inhabilite los servicios y sistemas, éstos puedan restablecerse.

j) **Principio de Líneas de defensa:** Se establecerá una estrategia que se componga de varias capas de seguridad, para que en el caso de que una de las capas falle, se dote al sistema de capacidad para ganar tiempo para reaccionar, de reducir las probabilidades de que se comprometa dicho sistema, así como de que, si es afectado, se pueda minimizar el impacto.

k) **Principio de mejora continua y reevaluación periódica:** se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad planificados anualmente y el grado de eficacia de los controles y medidas de seguridad de las tecnologías de la información implantados, al objeto de reevaluarlos y actualizarlos a la constante evolución de los riesgos y del entorno tecnológico de la Administración Pública, llegando a replantear la seguridad si se da el caso.

l) **Principio de seguridad de las tecnologías de la información en el ciclo de vida de los sistemas de información:** las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

m) **Principio de función diferenciada:** Siempre que sea posible se diferenciará al Responsable de la Información, el Responsable del Servicio y el Responsable de la Seguridad. El responsable de la información será el que determine los requisitos de tratamiento de la información, el responsable del servicio, los requisitos de los servicios prestados y el responsable de seguridad tomará las decisiones para que los requisitos de seguridad de información y de los servicios se satisfagan.

4.2 Requisitos mínimos de seguridad

Esta Política identifica y consagra los requisitos de seguridad del SGSI a desarrollar en el marco normativo, a continuación, se describen los requisitos del SGSI:

- Que identifique a los responsables de la **Organización e implantación del proceso de seguridad,** por el que se compromete a todos los miembros de la organización a tomar parte en la Seguridad, de modo que, todos conocerán la política.
- Que tenga en cuenta los criterios que determinan el **nivel de seguridad** requerido del SGSI, como resultado de la valoración y categorización del Sistema contemplada en el Informe de Valoración de los Servicios de Seguridad Gestionada.

- Que considere el **Análisis y Gestión de los Riesgos** mediante una metodología reconocida que mitigue o elimine las situaciones potencialmente peligrosas, justificando y ponderando las medidas en función de los riesgos.
- Mediante la **Gestión de personal,** con la publicación y divulgación de normas y procedimientos para que todo el personal esté al tanto de sus deberes y obligaciones referentes a la seguridad y se supervise que éstas se cumplan, teniendo especial consideración en llevar un control a través de un sistema de identificación de usuarios que identifique y trace quien tiene derechos de acceso o quien ha realizado alguna actividad.
- Que el personal que atienda, revise y audite la seguridad, sea determinado con criterios de **Profesionalidad** acordes a las tareas que se realizan y con la debida formación. La organización se asegurará de que su personal reciba la formación adecuada para sus funciones que garantice la seguridad de las tecnologías de la información que se relacionan con los sistemas.
- **Autorización y control de los accesos,** donde el acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.
- **Protección de las instalaciones**, donde los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso
- En la **adquisición de productos** de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se utilizarán, 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 juicio del responsable de Seguridad.
- Los sistemas deben diseñarse y configurarse de forma que garanticen **la seguridad por defecto**.
- **Integridad y actualización del sistema.** Por el que se conocerá en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.
- **Protección de la información almacenada y en tránsito.** Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.
- **Prevención ante otros sistemas de información interconectados,** donde se harán una especial atención a las conexiones a la res redes.

- **Registro de actividad** de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.
- **Incidentes de seguridad**. Se establecerá un sistema de detección y reacción frente a código dañino, así como los procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- **Continuidad de la actividad**. Se dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

4.3 Objetivos de la política

Esta Política establece el marco necesario para alcanzar la máxima eficiencia y las mejores prácticas que se desarrollarán por medio de normativa de seguridad que aborde aspectos específicos coordinando estas actividades y servicios, persiguiendo en todo caso los siguientes objetivos:

- **Evitar e impedir**, en la medida de lo posible, cualquier situación de riesgo que pueda interrumpir o limitar el continuo y correcto funcionamiento de la actividad de Grupo Oesía y, en caso de producirse dicha situación, minimizar y restablecer la normalidad funcional con la mayor rapidez posible mejorando la resiliencia.
- **Desarrollar un modelo eficaz** basado en un Sistema de Gestión de Seguridad de la Información y continuidad de negocio creado sobre normas nacionales e internacionales y capaces de operar con indicadores de desempeño y cumplimiento.
- **Lograr un nivel de seguridad óptimo y a la vez económicamente viable** para Grupo Oesía.

Es responsabilidad del **Subcomité de Ciberseguridad (SGSI-CIBER**) en su ámbito de actuación, por delegación del SGSC, promover y apoyar la implantación de las medidas técnicas y organizativas necesarias para minimizar los riesgos potenciales a los que se encuentra expuesta la información y los procesos operativos, dentro de su alcance, en la consecución de los objetivos estratégicos y tácticos del negocio.

4.4 Estructura documental

La organización de la gestión de la seguridad de los Sistemas de Información de Grupo Oesía, se basará en un cuerpo normativo sobre seguridad de la información y continuidad de negocio que será de obligado cumplimiento en todos los Sistemas de Gestión y se desarrollará en cuatro niveles según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior.

Dichos niveles de desarrollo normativo son los siguientes:

- **Primer nivel normativo:** Política Corporativa de Seguridad de la Información y Continuidad de Negocio de obligado cumplimiento por todo el personal, interno y externo, aprobada por la alta dirección.
- **Segundo nivel normativo:** Políticas Específicas de Seguridad de la Información, Manuales y Normas de Seguridad de los Sistemas de información que desarrollan con un mayor grado de detalle dicha Política dentro de un ámbito determinado (en el presente caso, la presente política de seguridad del SGSI-CIBER). Los Manuales y as Normas dan respuesta, sin entrar en detalles de implementación ni tecnológicos, a qué se puede hacer y qué no en relación a un cierto tema desde el punto de vista de la seguridad: qué se considera un uso apropiado o inapropiado, las consecuencias derivadas del incumplimiento, entre otros aspectos.
- **Tercer nivel normativo:** Los Procedimientos Generales de los Sistemas de Gestión y los Procedimientos Operativos de los Sistemas de Información e Instrucciones Técnicas. Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la Organización, y los procesos internos en ella establecidos.
- **Cuarto Nivel:** Informes, registros y evidencias. Son documentos de carácter técnico que pueden estar soportados en formatos normalizados que recogen el resultado y las conclusiones de un estudio, una actividad o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

Además de los documentos citados anteriormente, la documentación de seguridad del SGSI-CIBER, podrá contar, bajo criterio de su Responsable, con otros documentos de carácter no vinculante como pueden ser recomendaciones, buenas prácticas, informes y otros datos de interés. El control documental se adecuará conforme lo estipulado en los documentos NRM-01- Control de la Documentación y PGS-01 Gestión de Documentación.

Esta normativa 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 de comunicaciones incluidos en el SGI-CIBER, según el nivel de conocimiento que por su desempeño requieran.

4.5 Revisión de la Política

La **revisión anual** de esta Política de Seguridad de la Información, así como la propuesta de modificación o mantenimiento de la misma, le corresponde al Subcomité de Gestión de CIBER **(SGSI-CIBER)**. La revisión de esta Política será **aprobada** por el Subcomité de Gestión de la Seguridad y Continuidad (**SGSC**), para su ratificación por el Comité Operativo de Seguridad Corporativa y convenientemente difundida para que la conozcan todas las partes afectadas.

5 Marco Normativo

La identificación de las leyes, normativas y regulaciones que son aplicables a la actividad de Cipherbit- Grupo Oesía para las distintas áreas de negocio y que afectan a la seguridad de la información, es un requisito fundamental para alcanzar sus objetivos de negocio, siendo una actividad que debe desarrollarse de forma continuada, para poder recoger todos los cambios que puedan producirse y las distintas necesidades que afectan a cada área de negocio.

Por tanto, Cipherbit- Grupo Oesía desarrollará los procedimientos adecuados con los que identificar y aplicar los requisitos legales, normativos, regulatorios y contractuales que puedan afectar a la gestión y operación de sus servicios. La relación completa de leyes, normativas, regulaciones y otras obligaciones contractuales identificadas para cada sistema de gestión de la Seguridad de la Información implantado, se podrán consultar en el documento ***RGS-18.01 Listado Marco Regulatorio*** correspondiente**.**

6 Organización de la seguridad

Cipherbit- Grupo Oesía, consciente que el mantenimiento y gestión de la seguridad de los Sistemas de Información va íntimamente ligada al establecimiento de una estructura organizativa que promueva y supervise la aplicación de los objetivos de seguridad fijados, establece su estructura mediante la identificación y definición de diferentes funciones y responsabilidades en materia de gestión de la seguridad de los sistemas de información y de la continuidad de las operaciones, que la soporte. La estructura y funcionamiento de la organización de la seguridad de los Sistemas de Información queda detallada en el documento ***NRM-02 Organización Roles y Responsabilidades.***

6.1 Estructura organizativa y designaciones

Para la estructura organizativa de la gestión de la seguridad de la información en el ámbito del SGSI-CIBER se adopta un modelo delegado que está compuesta por los siguientes agentes:

- Responsable de la Información
- Responsable del Servicio
- Responsable de Seguridad de Cipherbit
- Responsable del Sistema (Responsable del SGSI-CIBER)
- Administrador de sistemas Cipherbit
- Responsable/s de Servicios SOC
- Administrador de Seguridad TI
- Responsable de Auditoría Interna
- Subcomité de Gestión de Seguridad y Continuidad
- Subcomité de Ciberseguridad (SGSI-CIBER)

Los Roles y Responsabilidades se encuentran definidos en el documento NRM-02 Organización Roles y Responsabilidades

6.1.1 Designaciones

- La designación del Responsable de la Información recaerá sobre la Dirección de Cipherbit
- La designación del Responsable del Servicio recaerá sobre la Dirección de Cipherbit
- La designación del Responsable de Seguridad recaerá sobre el Subcomité de Gestión de Seguridad y Continuidad
- La designación del Responsable del Sistema recaerá sobre el Subcomité de Gestión de Seguridad y Continuidad
- La designación de /los Responsable/s de Servicios SOC recaerá sobre el Responsable del Sistema
- La designación de los miembros del Subcomité de Gestión de Seguridad y Continuidad
- La designación de los miembros del Subcomité de SGSI-Ciber
- La designación del Responsable de Auditoría interna recaerá sobre el Departamento de Calidad del Grupo Oesía
- EL Administrador de Seguridad TI será nombrado por el Responsable de Seguridad.

Los miembros que conforman el Subcomité de Seguridad y Continuidad serán:

Miembros permanentes:

- CISO (Responsable de Seguridad corporativa)
- COO Cipherbit (Responsable de Información y Servicio Cipherbit)

- Dir. Cifra
- Dir. Ciberseguridad
- PMO Cipherbit
- Gerente SOC (Responsable SGI)

Miembros optativos:

- Responsable Calidad
- Responsable SI (Arquitectura y medios TIC)
- SSGG
- DPO
- Talento
- Compras

Los miembros que conforman el Subcomité de SGI-Ciber serán:

Miembros permanentes:

- Gerente SOC (Responsable SGI)
- Responsable de Seguridad Cipherbit
- Responsables de Servicios SOC
- Consultor Normativo

6.2 Resolución de conflictos

El SGSI-CIBER será operado y mantenido siguiendo los principios de buena fe y diligencia por parte de sus responsables. En caso de producirse conflictos de competencias, será el **Responsable del SGSI-CIBER** el encargado de resolver, en primera instancia dichos conflictos.

Será el **SGSC** quién se ocupe de mediar en aquellos conflictos que por envergadura, complejidad o atribuciones quede fuera de las competencias del Responsable del SGSI-CIBER, y en aquellos casos que los conflictos se produzcan entre distintos Sistemas de Gestión.

El **Responsable de Seguridad Corporativa** será quien se ocupe de resolver aquellos conflictos que por cualquier causa no pueda ser resuelto por el SGSC o en aquellos conflictos que surjan entre el SGSC y el Subcomité SGSI-CIBER.

La máxima instancia en la resolución de conflictos dentro del ámbito de la gestión de la seguridad de la información del Grupo Oesía será el **Comité Operativo de Seguridad Corporativa**.

7 Gestión del riesgo

La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

El Responsable de Seguridad junto al Responsable de Sistemas, son los encargados de realizar los preceptivos análisis de riesgos y de seleccionar las salvaguardas a implantar, siguiendo las pautas de la metodología para el análisis y gestión de riesgos implantada y que es descrita en el documento ***PGS-03 Metodología de Análisis y Gestión de Riesgos***.

El Responsable de la Información y el Responsable del Servicio son los responsables de los riesgos sobre la información y sobre el servicio, respectivamente, y por tanto de aceptar los riesgos residuales calculados en el análisis y de realizar su seguimiento y control sin perjuicio de la posibilidad de delegar esta función.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse una vez al año de forma ordinaria y de manera extraordinaria, cuando se produzcan cambios en la información, en los servicios, ocurran incidentes significativos de seguridad o sean identificadas vulnerabilidades graves. Dicha revisión, le corresponde al Responsable de Seguridad, con la colaboración del Responsable del Sistema del mismo ámbito, quienes presentarán un informe al Responsable del SGSI-CIBER, para su presentación y evaluación por el SGSC.

8 Obligaciones del personal

Todos los **profesionales de Cipherbit- Grupo Oesía** que, de forma directa o indirecta, accedan o hagan uso de los servicios de Ciberseguridad que estén sustentados por el SGSI-CIBER, tienen la obligación de conocer y cumplir esta norma de Seguridad de la Información y Continuidad de Negocio, así como la normativa que la desarrolle, siendo responsabilidad del Comité Operativo de Seguridad Corporativa, disponer los medios necesarios para que la información llegue a todos.

El **incumplimiento** manifiesto de la Política de Seguridad de la Información y continuidad de Negocio o la normativa y procedimientos derivados de ésta, podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

9 Terceras partes

Toda **persona ajena a Cipherbit-Grupo Oesía** que de forma directa o indirecta, accedan o hagan uso de los servicios de Ciberseguridad que estén sustentados por el SGSI-CIBER, tienen la obligación de conocer y cumplir esta norma de Seguridad de la Información y Continuidad de Negocio, así como la normativa que la desarrolle y les sea de aplicación, siendo responsabilidad del Subcomité de Ciberseguridad (SGSI-CIBER), disponer los medios necesarios para que la información llegue a los mismos, en especial:

- En el caso de que Cipherbit- Grupo Oesía utilice servicios de terceros (por ejemplo, personal externo de proveedores) o transfiera información a terceros (por ejemplo, clientes o potenciales clientes) vinculados al SGSI-CIBER, se les hará partícipes de esta Política de Seguridad y de la normativa de Seguridad desarrollada que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la normativa que le aplique, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.
- En el caso de que Cipherbit- Grupo Oesía preste servicios relativos al SGSI-CIBER a otras organizaciones o entidades, se les hará partícipes de esta Política de Seguridad de la Información y Continuidad de Negocio, tratando de establecer canales para reporte y coordinación de los respectivos Comités de Seguridad que pudieran existir y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

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. Cipherbit- Grupo Oesía podrá contar con empresas y organismos externos que ayuden a mejorar sus sistemas de seguridad, mediante la contratación de auditorías, asistencias técnicas o trabajos y desarrollos especializados.

10 Concienciación y formación

Lograr la plena conciencia respecto a que la Seguridad de la Información y Continuidad de Negocio afecta a todo el personal de la organización y a todas sus actividades, de acuerdo al principio de seguridad integral, constituye un objetivo de primer orden para Cipherbit- Grupo Oesía. A estos efectos, GRUPO OESÍA, desde el patrocinio del Comité de Operativo de Seguridad Corporativa, propondrá y organizará, sesiones formativas y de concienciación para que todos los empleados y otras partes interesadas externas, tengan una sensibilidad adecuada respecto a los riesgos que acechan en el manejo de los sistemas de información que operan.

El SGSC aprobará una Política de Formación y Concienciación en el tratamiento seguro de la información y operación de los procesos, que implementará el SGSI-CIBER, con los siguientes objetivos:

- Capacitación sobre la protección de la información de datos de carácter personal, orientada a los responsables de los datos y hacia los usuarios con privilegios sobre los mismos.
- Capacitación sobre la política, normas y procedimientos de seguridad implantados y los riesgos existentes, así como los relacionados con el aseguramiento de los procesos y operaciones.

11 Auditoría

El SGSI-CIBER será objeto de una auditoría regular ordinaria, interna y externa, que verifique el cumplimiento de los requerimientos de cada una de las normas que dan cumplimiento, según lo establecido en los requisitos de los propios esquemas de gestión. Asimismo, con carácter extraordinario, deberá realizarse dicha auditoría siempre que se lleven a cabo modificaciones sustanciales en los sistemas de información que puedan repercutir en el cumplimiento de las medidas de seguridad requeridas.

Los informes de auditoría quedarán a disposición del SGSC que los evaluarán para su presentación al Comité Operativo de Seguridad Corporativa. Estos informes serán utilizados como medida del desempeño de la operación y mantenimiento del SGSI-CIBER y base para su mejora continua.

12 Aprobación y entrada en vigor

El texto de esta Política de Seguridad de la Información y Continuidad de Negocio es aprobado el día **23 de abril de 2019** por el SGSC y es efectiva desde esta fecha hasta que sea reemplazada por una nueva Política de la Seguridad de la Información y Continuidad de Negocio. En consecuencia, este texto anula la anterior Política de Seguridad de la Información y Continuidad de Negocio de igual rango vigente, aprobada por el mismo órgano en fecha anterior.

*El texto de esta Política ha sido revisado y actualizado a fecha **30 de Junio de 2023**.

13 Conocimiento del personal de Cipherbit- Grupo Oesía y terceras partes

El conocimiento, observancia y respeto de la presente Política es vinculante para toda la plantilla de Cipherbit Grupo Oesía vinculadas al SGSI-CIBER y terceras partes, cuando de forma directa o indirecta, accedan o hagan uso de los servicios de Ciberseguridad que estén sustentados por dicho SGSI-CIBER.

14 Referencias

Para la elaboración de la presente Política se ha tomado en consideración la siguiente información:

- ISO 27002 Information technology – Security techniques – Code of practice for information security management.
- ISO 27001 Information technology – Security techniques – Information Security Management Systems – Requirements.
- ISO 22301 Protección y seguridad de los ciudadanos – Sistema de Gestión de la Continuidad del Negocio.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Seguridad (ENS) en el ámbito de la Administración Electrónica.
- RGS-18.01 Listado Marco Regulatorio
- ORG-01.01 Política de Seguridad de la Información

Cipherbit SL

Calle Marie Curie, 19

28251 – Madrid,

Teléfono: 91 309 86 00, Fax: 91 375 82 16

http://www.oesia.com