ESQUEMA NACIONAL DE SEGURIDAD

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POL.01

Versión: 1.1

24.09.2024

CONFIDENCIAL

CONTROL DE VERSIONES

VERSIÓN	FECHA:	MODIFICACIÓN
1.0	09.09.2024	Versión inicial del documento
1.1	24.09.2024	Estandarización del formato

RUTA DE APROBACIÓN

VERSIÓN	REALIZADO POR:	REVISADO POR:	APROBADO POR:
1.0	Responsable de Seguridad	Comité de Seguridad	Dirección
	Fecha: 07.09.2024	Fecha: 07.09.2024	Fecha: 07.09.2024

RESPONSABILIDAD

DISTRIBUCIÓN	ARCHIVO	ACTUALIZACIÓN
Responsable de Seguridad	Responsable de Seguridad	Dirección

ÍNDICE DE CONTENIDOS

1. CONTEXTO 5
2. OBJETIVOS 6
3. ALCANCE 7
4. MARCO NORMATIVO 7
5. PRINCIPIOS 8
5.1. SEGURIDAD COMO PROCESO INTEGRAL 8
5.2. GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS 8
5.3. PREVENCIÓN, DETECCIÓN Y RESPUESTA 8
5.4. EXISTENCIA DE LÍNEAS DE DEFENSA 9
5.5. VIGILANCIA CONTINUA Y REEVALUACIÓN PERIÓDICA 9
5.6. DIFERENCIACIÓN DE RESPONSABILIDADES 9
6. REQUISITOS 9
6.1. ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD 9
6.2. GESTIÓN DE RIESGOS 9
6.3. GESTIÓN DE PERSONAL 9
6.4. PROFESIONALIDAD 10
6.5. AUTORIZACIÓN Y CONTROL DE ACCESOS 10
6.6. PROTECCIÓN DE LAS INSTALACIONES 10
6.7. ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD 10
6.8. MÍNIMO PRIVILEGIO 10
6.9. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA 11
6.10. PROTECCIÓN DE INFORMACIÓN ALMACENADA Y EN TRÁNSITO 11
6.11. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS 11
6.12. REGISTRO DE ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO 11
6.13. INCIDENTES DE SEGURIDAD 11
6.14. CONTINUIDAD DE LA ACTIVIDAD 12
6.15. MEJORA CONTINUA 12
7. ENFOQUE DE RIESGOS 12
8. ESTRUCTURA 12
8.1. MARCO ORGANIZATIVO 12
8.2. MARCO OPERACIONAL 13
8.3. MEDIDAS DE PROTECCIÓN 13
9. INSTRUMENTOS DE DESARROLLO 14
9.1. NIVEL I: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 14
9.2. NIVEL II: ESTÁNDAR DE SEGURIDAD DE LA INFORMACIÓN 14
9.3. NIVEL III: PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN 15
9.4. NIVEL IV: INSTRUCCIONES ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN 15

10. ORGANIZACIÓN DE LA SEGURIDAD **15**
10.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN **15**
10.1.1. COMPOSICIÓN 16
10.1.2. CONVOCATORIA Y REPORTE 16
10.1.3. FUNCIONES 16
10.2. FUNCIONES Y RESPONSABILIDADES **17**
10.2.1. RESPONSABLE DE LA INFORMACIÓN 17
10.2.2. RESPONSABLE DEL SERVICIO 18
10.2.3. RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN 18
10.2.4. RESPONSABLE DEL SISTEMA 19
10.2.5. ADMINISTRADOR DE SEGURIDAD DEL SISTEMA 20
10.2.6. USUARIOS 20
10.3. PROCEDIMIENTO DE DESIGNACIÓN **21**
10.4. PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS **21**
11. OBLIGACIONES DEL PERSONAL **21**
12. TERCERAS PARTES **21**
13. DATOS DE CARÁCTER PERSONAL **22**
14. REVISIÓN **22**
15. SANCIONES APLICABLES **22**
16. APROBACIÓN Y ENTRADA EN VIGOR **22**

1. CONTEXTO

La presente Política de Seguridad de la Información se formaliza con el objeto de dar cumplimiento a los preceptos legales recogidos en el **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS)**, en el ámbito de la Administración Electrónica, y constituye la piedra angular para el **Marco de Gobierno y Gestión de la Seguridad de la Información** formalizado para las distintas entidades que conforman el **GRUPO EULEN** (en adelante, **GRUPO EULEN**).

La finalidad del **ENS** es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de la identificación e implantación de medidas que permitan garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, otorgando a los ciudadanos y a las Administraciones Públicas, el posible ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El **ENS**, en su **artículo 12**, establece la obligación de disponer de una Política de Seguridad, especificando los principios básicos y los requisitos mínimos que debe cumplir la misma.

Esta Política de Seguridad de la información sigue las pautas, instrucciones e indicaciones consideradas por la ***guía CCN-STIC-805*** **del Centro Criptológico Nacional**, centro adscrito al Centro Nacional de Inteligencia.

GRUPO EULEN hace uso de los sistemas **TIC (Tecnologías de la Información y Comunicaciones)** para alcanzar los objetivos estratégicos que han sido formalizados por los órganos de gobierno (en adelante, la **Dirección**). En consecuencia, estos sistemas deben ser administrados con diligencia, tomando las medidas de seguridad adecuadas para proteger la información frente a daños accidentales o deliberados.

La información constituye para la práctica totalidad de los procesos de negocio y los servicios prestados por **GRUPO EULEN**, el hilo conductor imprescindible para la ejecución de los mismos con garantías de eficiencia y calidad, alcanzando, con ello, el cumplimiento de los objetivos estratégicos formalmente establecidos.

Las **dimensiones principales de seguridad de la información** que deben ser garantizadas en la ejecución de cualquier proceso son:

- **Confidencialidad:** Garantiza que la información solo se encuentra accesible a personas, entidades o procesos autorizados.
- **Integridad:** Garantiza que la información solo se genera, modifica y elimina por personas, entidades o procesos autorizados.
- **Disponibilidad:** Garantiza que la información se encuentra accesible cuando las personas, entidades o procesos autorizados lo precisan.

Por otro lado, se presentan otras dimensiones de seguridad, tales como la **autenticación de las partes**, el **no repudio** o la **trazabilidad** que, de igual forma, deben ser garantizadas cuando el valor de seguridad de la información en el contexto del proceso de negocio o el servicio que esté siendo prestado, así lo precise.

Esto implica que la organización y su personal debe aplicar las medidas mínimas de seguridad exigidas por el **ENS**, así como realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar las vulnerabilidades alertadas, y preparar una respuesta efectiva a los incidentes para garantizar las dimensiones de seguridad señaladas con anterioridad.

GRUPO EULEN debe garantizar que la seguridad es parte integral de cada etapa del ciclo de vida de los sistemas TIC, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición, y las actividades propias de explotación.

La Política de Seguridad de la Información se basa en la adopción de principios claros y bien definidos que aseguren el cumplimiento de las directrices estratégicas, los requerimientos legales, así como los contractuales formalizados con terceros y, por tanto, se constituye como el instrumento principal en el que se apoya **GRUPO EULEN** para la utilización segura de las tecnologías de la información y comunicaciones.

La normativa (estándares, procedimientos e instrucciones de seguridad) que emane de la Política de Seguridad de la Información de **GRUPO EULEN** pasará a formar parte de la misma una vez haya sido divulgada, siendo de obligado cumplimiento para la totalidad de los empleados y terceras partes que hagan uso de la información propiedad de **GRUPO EULEN**, o de alguno de sus clientes.

Los empleados serán responsables de la seguridad de la información que procesan en el desempeño de sus funciones, y deberán conocer, comprender y cumplir las directrices y normas relativas a la seguridad de la información, velando por la correcta aplicación de las medidas de protección habilitadas.

El acceso a la información por parte de los empleados se limitará al estrictamente necesario para el correcto desempeño de las funciones formalmente asignadas garantizando, con ello, la atención de la política de mínimo privilegio. Por tanto, los responsables de cada una de las direcciones tendrán en cuenta todas las medidas de seguridad de índole técnica y organizativa implantadas para definir y mantener los privilegios adecuados de acceso a la información de sus procesos, en función de las actividades de cada puesto de trabajo.

El incumplimiento de las directrices de la Política de Seguridad de la Información podría dar lugar a la aplicación de sanciones administrativas internas, además de las previstas en la normativa vigente.

La **Dirección** de **GRUPO EULEN** asegurará que esta Política de Seguridad de la Información es entendida e implantada en todas las direcciones, facilitando los recursos técnicos y humanos necesarios para la consecución de los objetivos definidos en este marco de actuación.

2. OBJETIVOS

La Política de Seguridad de la Información queda establecida como el documento de alto nivel que formaliza las distintas directrices de actuación en materia de seguridad adoptadas por **GRUPO EULEN**, y que serán desarrolladas en mayor detalle en la correspondiente normativa de seguridad (estándares, procedimientos e instrucciones de seguridad) elaborada a tales efectos.

Bajo esta premisa, por tanto, la Política de Seguridad de la Información contempla los siguientes objetivos principales:

- Dar cumplimiento a la normativa legal de aplicación en el ámbito de la seguridad de la información.
- Contribuir a cumplir con la misión y objetivos estratégicos formalizados por **GRUPO EULEN**.
- Alinear la seguridad de la información con los requerimientos demandados por los servicios prestados mediante la formalización y ejecución del proceso de análisis y evaluación de los riesgos a los que se encuentran expuestos los distintos activos de información, alcanzando la definición de una estrategia para la mitigación de los riesgos relacionados con el entorno de la seguridad de la información.

- Garantizar la protección adecuada de los distintos activos de información en función del grado de sensibilidad y criticidad alcanzado por los mismos (valor de seguridad de los activos de información según las distintas dimensiones consideradas).
- Facilitar el dimensionamiento de los recursos necesarios para la correcta implantación de las medidas de seguridad de índole técnica y organizativa recogidas en la normativa de seguridad documentada a tales efectos.
- Fomentar el uso de buenas prácticas en materia de seguridad de la información, así como crear una cultura de seguridad en el contexto de la estructura organizativa de **GRUPO EULEN**.
- Impulsar la definición, implantación y mantenimiento de un Plan de Continuidad de Negocio.
- Establecer los mecanismos de revisión, monitorización, auditoría y mejora continua con el objeto de mantener los niveles de seguridad oportunos demandados por los servicios prestados por **GRUPO EULEN**.

3. ALCANCE

Esta Política de Seguridad es de aplicación sobre la totalidad de las entidades que conforman el **GRUPO EULEN.**

GRUPO EULEN aplicará la presente Política de Seguridad de la Información sobre todos aquellos sistemas de información y de comunicaciones que se encuentren relacionados con la prestación de servicios que pudieran afectar el ejercicio de derechos y el cumplimiento de deberes por parte de los ciudadanos, mediante el uso de medios electrónicos, así como con el acceso a la información o al procedimiento administrativo a través de tales medios.

4. MARCO NORMATIVO

La formalización de la Política de Seguridad de la Información, así como la normativa de seguridad que se derive de la misma, tendrá en consideración e integrará la siguiente normativa legal aplicable a la actividad principal desarrollada en las distintas entidades que conforman el **GRUPO EULEN**:

- Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD – Reglamento General de Protección de Datos), 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.
- Ley Orgánica, 3/2018, de 5 de diciembre de 2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, Ley 3/2018).
- Ley 34/2002, de 11 de julio, de servicios de sociedad de la información y comercio electrónico.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto RD 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Y demás disposiciones concordantes y de desarrollo de las mencionadas anteriormente.

5. PRINCIPIOS

Con el objeto de garantizar el cumplimiento de los objetivos de seguridad identificados con anterioridad, la **Política de Seguridad de la Información** formaliza la aplicación de determinados principios de seguridad.

5.1. SEGURIDAD COMO PROCESO INTEGRAL

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información utilizados como soporte para la ejecución de los procesos de negocio. En este sentido, por tanto, todas las actividades de seguridad serán ejecutadas bajo esta perspectiva, evitando cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en la ejecución de los procesos de negocio, y la de los responsables jerárquicos con el objeto de evitar que el desconocimiento, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad de la información.

5.2. GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno de información controlado, minimizando los riesgos hasta niveles aceptables formalizados por la Dirección.

La reducción del riesgo hasta tales niveles se alcanzará mediante la aplicación de medidas de seguridad, de forma equilibrada y proporcionada a la naturaleza de la información tratada, los servicios a prestar y los riesgos a los que estén expuestos los distintos activos de información utilizados.

5.3. PREVENCIÓN, DETECCIÓN Y RESPUESTA

La seguridad de la información debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar las vulnerabilidades existentes, y lograr que las amenazas no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información o los servicios prestados.

Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección estarán orientadas a la alerta temprana de cualquier escenario de materialización de amenazas.

Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5.4. EXISTENCIA DE LÍNEAS DE DEFENSA

Se deberá garantizar que la estrategia de protección queda conformada por múltiples capas de seguridad, dispuestas de forma que, cuando una de las capas se vea comprometida, se pueda reaccionar

adecuadamente frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que puedan propagarse.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

5.5. VIGILANCIA CONTINUA Y REEVALUACIÓN PERIÓDICA

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de seguridad de los activos de información permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

5.6. DIFERENCIACIÓN DE RESPONSABILIDADES

La responsabilidad de la seguridad de la información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información.

6. REQUISITOS

El desarrollo de la **Política de Seguridad de la Información** deberá permitir el cumplimiento de determinados requisitos de seguridad.

6.1. ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD

La seguridad deberá comprometer a todos los miembros de la organización.

6.2. GESTIÓN DE RIESGOS

El proceso de gestión de riesgos estará conformado por las actividades de análisis y tratamiento de los riesgos garantizando la aplicación del principio de proporcionalidad.

6.3. GESTIÓN DE PERSONAL

El personal, propio o ajeno, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.

Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

El significado y alcance del uso seguro de los activos de información se concretará y plasmará en unas normas de seguridad específicas.

6.4. PROFESIONALIDAD

La seguridad de la información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases del ciclo de vida de los sistemas de información: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y decomisión.

Las entidades terceras que presten servicios de seguridad deberán contar con profesionales cualificados, así como niveles idóneos de gestión y madurez en los servicios prestados.

Se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

6.5. AUTORIZACIÓN Y CONTROL DE ACCESOS

El acceso controlado a los sistemas de información deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

6.6. PROTECCIÓN DE LAS INSTALACIONES

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.

6.7. ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD

La adquisición y desarrollo de nuevos componentes, así como la contratación de servicios de seguridad, estarán sujetos a un proceso formal de autorización y serán coherentes con el análisis de riesgos, la arquitectura de seguridad existente y el principio de proporcionalidad. Este proceso contemplará globalmente las necesidades técnicas, financieras y de formación del personal encargado de su despliegue, puesta en producción, gestión y operación posteriores.

En cuanto al criterio de selección de estos productos y servicios, se deberá optar por los productos y servicios establecidos en la guía del CCN-CERT Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC). Asimismo, en el caso de los servicios, se requerirá que la empresa proveedora esté certificada en el Esquema Nacional de Seguridad.

6.8. MÍNIMO PRIVILEGIO

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) Los sistemas de información proporcionarán la funcionalidad imprescindible para que se alcancen los objetivos competenciales o contractuales.
b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados, pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
c) Se eliminarán o desactivarán mediante el control de la configuración las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario de los sistemas de información ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

6.9. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

La inclusión de cualquier elemento físico o lógico en el registro de activos de información, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas de información atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

6.10. PROTECCIÓN DE INFORMACIÓN ALMACENADA Y EN TRÁNSITO

Se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

6.11. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

Se protegerá el perímetro de los sistemas de información, especialmente, si se conecta a redes públicas, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad. En todo caso, se analizarán los riesgos derivados de la interconexión de los sistemas de información con otros sistemas, y se controlará su punto de unión.

6.12. REGISTRO DE ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO

Se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello, se llevará a cabo en cumplimiento de las disposiciones legales de aplicación en este ámbito de actuación.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de la normativa legal de aplicación, se podrá analizar las comunicaciones entrantes y salientes, y únicamente para fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación del servicio, evitar la distribución malintencionada de código dañino, así como otros daños.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

6.13. INCIDENTES DE SEGURIDAD

Se dispondrá de procedimientos de gestión de incidentes de seguridad, así como cauces de comunicación a las partes interesadas, y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad de los sistemas de información.

6.14. CONTINUIDAD DE LA ACTIVIDAD

Los sistemas de información dispondrán de copias de seguridad, y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

6.15. MEJORA CONTINUA

El proceso integral de seguridad de la información implantado deberá ser actualizado y mejorado de forma continua.

7. ENFOQUE DE RIESGOS

Los sistemas que conforman el alcance de la presente Política de Seguridad de la Información se encuentran sujetos a un análisis y evaluación de riesgos, con el objeto de identificar las amenazas a las que se encuentran expuestos, evaluar el impacto asociado a la materialización de tales amenazas, y determinar las situaciones de riesgos que podrían derivarse.

El resultado de este análisis y evaluación de riesgos permitirá la identificación y proposición de las medidas de seguridad oportunas como estrategia para la mitigación de los mismos.

Este análisis de riesgos atiende a las siguientes características principales:

- Está basado en la aplicación de normas y metodologías de gestión de riesgos reconocidas como buenas prácticas a nivel nacional e internacional.
- Establece una valoración de referencia para la información y los servicios prestados, de tal forma, que se obtengan resultados homogéneos en la ejecución de las actividades inherentes al análisis de riesgos.
- Se ejecuta con periodicidad anual, o cuando se presentan los siguientes escenarios:
    - Modificación sustancial de la información gestionada, los servicios prestados, o los sistemas que actúan como soporte para la prestación de tales servicios.
    - Identificación de nuevos vectores de ataque, amenazas o vulnerabilidades asociadas al sistema.
    - Presencia de un incidente grave de seguridad.

El **Comité de Seguridad de la Información** liderará la ejecución periódica del análisis de riesgos, planificando los recursos técnicos, humanos y económicos necesarios a tales efectos.

8. ESTRUCTURA

El desarrollo de la Política de Seguridad de la Información incluirá, basándose en el análisis y evaluación de riesgos efectuado, aspectos específicos de la Seguridad de la Información, tales como las medidas de seguridad indicadas en el **ENS**.

Estas medidas de seguridad quedarán agrupadas en **tres niveles diferenciados de seguridad** según queda establecido en el **ENS**.

8.1. MARCO ORGANIZATIVO

Orientado a administrar la seguridad de la información en el contexto de la estructura organizativa de **GRUPO EULEN**, así como establecer un Marco de Gestión para controlar su implementación.

Partiendo de la presente Política de Seguridad de la Información se desarrollará el resto del marco normativo de seguridad según se detalla en el capítulo referido a los ***instrumentos de desarrollo***.

8.2. MARCO OPERACIONAL

Constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

- **Planificación:** mediante análisis de riesgos, controlando la arquitectura de seguridad y la adquisición de nuevos componentes, entre otros aspectos.
- **Control de acceso:** orientado a controlar el acceso lógico a la información.

- **Explotación:** medidas para la gestión de la seguridad en explotación; partiendo del inventario de activos y controlando la gestión de incidentes, gestión de cambios, gestión de la configuración, registros de actividad, entre otros.
- **Servicios externos:** medidas de seguridad orientadas a garantizar que los proveedores de servicios contratados por **GRUPO EULEN**, o que, de alguna manera, se presten bajo el control y/o la dirección de **GRUPO EULEN**, cumplan las políticas y normas de seguridad de la información establecidas.
- **Continuidad del servicio:** acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.
- **Monitorización del sistema:** orientado a garantizar la disponibilidad de las actividades diarias y proteger los procesos críticos frente al impacto provocado por situaciones de desastre.

8.3. MEDIDAS DE PROTECCIÓN

Para la protección de activos concretos, según su naturaleza, con el nivel requerido para cada dimensión de seguridad.

- **Protección de las instalaciones e infraestructuras:** destinado a impedir accesos no autorizados, daños e interferencias a las instalaciones e infraestructuras de **GRUPO EULEN**.
- **Gestión del personal:** orientado a reducir los riesgos de error humano o uso inadecuado de las instalaciones y equipamientos.
- **Protección de los equipos:** medidas para la protección física y medioambiental de los equipos.
- **Protección de las comunicaciones:** dirigido a garantizar el intercambio seguro de la información, y los accesos a través de redes de comunicaciones.
- **Protección de los soportes de información:** con el objeto de preservar la información que contienen estas unidades de almacenamiento externo.
- **Protección de las aplicaciones informáticas:** orientado a mantener la visión de seguridad durante todo el ciclo de vida asociado al desarrollo y mantenimiento de las mismas.
- **Protección de la información:** cumpliendo lo dispuesto en el **Reglamento General de Protección de Datos**, la **Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales**, así como cualquier otra legislación de aplicación en función de la naturaleza de la información.
- **Protección de los servicios:** definiendo las medidas necesarias para mantener la seguridad de los servicios de TI.

9. INSTRUMENTOS DE DESARROLLO

La normativa de seguridad establecida por **GRUPO EULEN** se estructura en los siguientes niveles relacionados jerárquicamente:

a) Nivel I: Política de Seguridad de la Información
b) Nivel II: Estándares de Seguridad de la Información
c) Nivel III: Procedimientos de Seguridad de la Información
d) Nivel IV: Instrucciones específicas de Seguridad de la Información

Esta estructura jerárquica permite adaptar con eficiencia los niveles inferiores a los cambios en el entorno operativo de **GRUPO EULEN**.

El personal de **GRUPO EULEN** tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todos los estándares y procedimientos de seguridad que puedan afectar al desempeño de sus funciones.

La normativa de seguridad estará disponible para todos los usuarios y, en particular, para aquéllos que utilicen, operen o administren los sistemas de información y de comunicaciones considerados en el alcance.

9.1. NIVEL I: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Recogida en el presente documento, ha sido aprobada formalmente por la **Dirección**, y detalla las directrices de actuación de **GRUPO EULEN** en materia de seguridad de la información con el objeto de contribuir al cumplimiento de la misión y visión formalizadas por la **Dirección**.

9.2. NIVEL II: ESTÁNDAR DE SEGURIDAD DE LA INFORMACIÓN

El segundo nivel desarrolla la Política de Seguridad de la Información mediante la identificación de los objetivos de seguridad considerados para los distintos **dominios de seguridad**:

- Seguridad relativa a los recursos humanos
- Gestión de activos de información
- Control de accesos
- Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Relación con proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información para la gestión de la continuidad del negocio
- Cumplimiento

Los objetivos de seguridad y, por ende, las medidas de seguridad que deben ser implantadas sobre los distintos activos de información para garantizar las dimensiones de seguridad de la información en los distintos procesos de negocio y servicios prestados por **GRUPO EULEN**, se encuentran, de igual forma, clasificados en **tres niveles de seguridad**, según las exigencias consideradas en cada caso (valores de seguridad alcanzados para los activos de información que actúan como soporte para la ejecución de los procesos y la prestación de los servicios).

El estándar de seguridad deberá ser aprobado por el **Comité de Seguridad de la Información** con carácter previo a su formalización y divulgación.

9.3. NIVEL III: PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

El tercer nivel está constituido por procedimientos técnicos y organizativos de actuación que **recogerán el conjunto de actividades de control que deben ser ejecutadas con el objeto de dar cumplimiento a los objetivos de seguridad formalizados a través del estándar de seguridad documentado**.

Estas pautas de actuación serán de aplicación específica según los distintos dominios de seguridad considerados y detallados en el nivel de estándar de seguridad ***(Nivel II)***.

Los procedimientos de seguridad deberán ser aprobados por el **Responsable de Seguridad** con carácter previo a su formalización y divulgación.

9.4. NIVEL IV: INSTRUCCIONES ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Las instrucciones específicas de seguridad serán documentadas con el objeto de detallar la aplicación de un procedimiento de seguridad específico para un activo de información concreto y, por tanto, presentará el detalle de las tareas a ejecutar en el contexto de dicho activo de información para dar cumplimiento a las actividades de control recogidas en el procedimiento de seguridad del cual deriva dicha instrucción.

Las instrucciones específicas de seguridad de la información, aun cuando forman parte de la normativa de seguridad de **GRUPO EULEN**, serán documentadas según el consenso alcanzado por el **Responsable de Seguridad** y el **Responsable del Sistema**, en función de la complejidad de entendimiento en lo relativo a la aplicación de lo establecido en el procedimiento para un activo de información concreto.

Las instrucciones específicas de seguridad de la información serán aprobadas por el **Responsable de Seguridad** tras el consenso alcanzado con el **Responsable del Sistema**.

10. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad en **GRUPO EULEN** queda establecida mediante la identificación y definición de las diferentes funciones y responsabilidades consideradas en esta materia, así como la implantación de la estructura organizativa asociada, diferenciando tres bloques principales de responsabilidad:

- La especificación de las necesidades o requisitos de seguridad.
- La operación del sistema de información que se atiene a tales necesidades o requisitos.
- La función de supervisión de acuerdo con el principio básico de consideración de la seguridad como una función diferenciada.

10.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Actúa como máximo órgano de control, supervisión y armonización en materia de seguridad de la información.

El **Comité de Seguridad de la Información** pertenecerá a los órganos de gobierno de la organización.

10.1.1. COMPOSICIÓN

El **Comité de Seguridad de la Información** está conformado por los siguientes miembros permanentes:

- **Responsable de Seguridad** (en calidad de secretario)
- **Responsable del Servicio**
- **Responsable del Sistema**

El **Comité de Seguridad de la Información** no es un comité técnico, sin embargo, recabará regularmente del personal técnico propio o externo, la información pertinente para la toma de decisiones o emisión de una opinión determinada. Este asesoramiento, se determinará en cada caso, pudiendo materializarse de diferente formas:

- Apoyándose en un asesoramiento externo.

- Conformando grupos de trabajo especializados internos, externos o mixtos.
- Asistiendo a seminarios u otro tipo de entornos formativos o de intercambio de experiencias.

10.1.2. CONVOCATORIA Y REPORTE

El **Comité de Seguridad de la Información** se reunirá con periodicidad trimestral, salvo excepciones debidamente justificadas de las que se deriven reuniones extraordinarias.

La convocatoria será efectuada por el **Responsable de Seguridad** que, de igual forma, aportará la información precisa para el tratamiento de las diferentes cuestiones incorporadas en el orden del día.

Como resultado de estas reuniones, el **Responsable de Seguridad** formalizará el acta de reunión correspondiente con las conclusiones principales alcanzadas, y la remitirá a los distintos órganos de gobierno afectados, y a los miembros integrantes del **Comité de Seguridad de la Información**, asumiendo la responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

10.1.3. FUNCIONES

- Colaborar con los órganos de gobierno en la definición de la estrategia de seguridad de la información.
- Definir formalmente y, una vez aprobada por la **Dirección**, divulgar la Política de Seguridad de la Información y la normativa de seguridad (estándares, procedimientos e instrucciones) que se derive de la misma.
- Revisar anualmente la Política de Seguridad de la Información, y proponer las modificaciones que estime oportunas.
- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Informar regularmente a la **Dirección** sobre el estado de seguridad alcanzado para los distintos procesos y servicios incorporados en el alcance.
- Informar a la **Dirección** con relación al orden del día planteado en las distintas reuniones periódicas mantenidas por este Comité, así como las conclusiones alcanzadas en el transcurso de las mismas.
- Aprobar las iniciativas que estime oportunas para mejorar la seguridad de la información, especialmente, las actividades de ejecución periódica relacionadas con el análisis de riesgos y la auditoría de seguridad.
- Monitorizar los principales riesgos aceptados por la organización e identificar posibles actuaciones, procediendo a la priorización de las mismas con el objeto de garantizar que los esfuerzos son consistentes.
- Dar respuesta a las inquietudes o consultas transmitidas a través de los responsables de las distintas direcciones de **GRUPO EULEN**.
- Monitorizar los incidentes de seguridad de mayor relevancia notificados por el **Responsable de Seguridad**.
- Supervisar que los aspectos de seguridad se tienen en cuenta en todos los proyectos TIC aprobados (desde su especificación inicial hasta su implantación), garantizando una visión homogénea en el tratamiento de los riesgos, así como el cumplimiento del principio de seguridad por diseño.
- Promover la ejecución de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.

- Ejecutar el proceso de designación de roles y responsabilidades para la estructura organizativa establecida en materia de seguridad, y resolver los conflictos que pudieran surgir a este respecto, elevando a los órganos de gobierno aquellos casos en los que no cuente con suficiente autoridad para la toma de decisiones.

10.2. FUNCIONES Y RESPONSABILIDADES

La asignación de funciones y responsabilidades en materia de seguridad se encuentra debidamente alineada con las competencias funcionales formalizadas en el contexto de la estructura organizativa de **GRUPO EULEN**.

10.2.1. RESPONSABLE DE LA INFORMACIÓN

La función de **Responsable de la Información** asume las siguientes responsabilidades principales:

- Actuar como **propietario de los riesgos** a los que se encuentra expuesta la información.
- Establecer los requisitos de la información en materia de seguridad (de forma conjunta con el **Responsable Interno del Tratamiento**, en el caso de que se presenten escenarios de tratamiento de datos de carácter personal).
- Determinar los niveles de seguridad de la información (valoración de las distintas dimensiones de seguridad para la información), y mantener actualizados estos niveles, valorando los impactos derivados de los incidentes que afectan a la seguridad de la información, conforme con lo establecido en el **ENS**.
  Para la ejecución de esta actividad, podrá actuar de forma coordinada con el **Responsable del Servicio**, el **Responsable de Seguridad** y el **Responsable del Sistema**.
- Ejecutar, de forma coordinada con el **Responsable del Servicio**, y contando con la participación del **Responsable de Seguridad**, los preceptivos análisis de riesgos, así como selección de las salvaguardas que se deban implantar como estrategia de mitigación de tales situaciones de riesgo para la información.
- Aceptar los niveles de riesgo residual alcanzados como resultado de la implantación de la estrategia de mitigación definida para las situaciones de riesgo identificadas.
- Efectuar el seguimiento, monitorización y control de los riesgos identificados.
- Actuar como responsable último de los incidentes de seguridad acaecidos sobre la información, para la cual, actúa como propietario.

El **Responsable de la Información** remitirá al **Responsable del Servicio** el resultado de las tareas ejecutadas en el ámbito de sus responsabilidades, al menos una vez al año o a petición del mismo, reportando el resultado en formato adecuado para la integración de la información.

El **Responsable de la Información** habrá sido designado en el contexto de los órganos de gobierno encargados de la definición de la misión de la organización y los objetivos estratégicos que se derivan, así como la supervisión con relación a la consecución de los mismos.

10.2.2. RESPONSABLE DEL SERVICIO

La función de **Responsable del Servicio** asume las siguientes responsabilidades principales:

- Actuar como propietario de los riesgos a los que se encuentra expuesto el servicio.

- Establecer los requisitos del servicio en materia de seguridad, y que derivan, de forma directa, de los requisitos alcanzados para la información (de forma conjunta con el **Responsable Interno del Tratamiento**, en el caso de que se presenten escenarios de tratamiento de datos de carácter personal).
- Determinar los niveles de seguridad del servicio (valoración de las distintas dimensiones de seguridad del servicio), y mantener actualizado estos niveles, valorando los impactos derivados de los incidentes que afectan a la seguridad del servicio, conforme con lo establecido en el **ENS**. Para la ejecución de esta actividad, podrá actuar de forma coordinada con los **Responsables de la Información**, el **Responsable de Seguridad** y el **Responsable del Sistema**.
- Ejecutar, de forma coordinada con los **Responsables de la Información**, y contando con la participación del **Responsable de Seguridad**, los preceptivos análisis de riesgos, así como selección de las salvaguardas que se deban implantar como estrategia de mitigación de tales situaciones de riesgo para la información afectada en la prestación del servicio.
- Aceptar los niveles de riesgo residual alcanzados como resultado de la implantación de la estrategia de mitigación de las situaciones de riesgo identificadas.
- Ejecutar seguimiento, monitorización y control de los riesgos identificados.
- Colaborar con el **Responsable de Seguridad** y el **Responsable del Sistema** en el mantenimiento de los sistemas catalogados según pautas facilitadas por el **ENS**.

El **Responsable del Servicio** remitirá al **Responsable de Seguridad** el resultado de las tareas ejecutadas en el ámbito de sus responsabilidades, al menos, una vez al año o a petición del mismo, reportando el resultado en formato adecuado para la integración de la información.

El **Responsable del Servicio** habrá sido designado en el contexto de la dirección ejecutiva encargada de la aplicación de los procesos oportunos para alcanzar la consecución de los objetivos estratégicos definidos por los órganos de gobierno.

10.2.3. RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

La función de **Responsable de Seguridad de la Información** asume las siguientes responsabilidades principales:

- Elaborar y mantener actualizada la Política de Seguridad de la Información, así como el cuerpo normativo formalizado en materia de seguridad de la información.
- Determinar formalmente la categoría de los sistemas de información en función de los niveles de seguridad identificados por los **Responsables de la Información** y **Responsables de Servicios**.
- Participar, de forma coordinada con los **Responsables de la Información** y los **Responsables de Servicios**, en los preceptivos análisis de riesgos, proponiendo los correspondientes indicadores de riesgos críticos para su aprobación por parte de los mismos.
- Formalizar la Declaración de Aplicabilidad para los distintos sistemas de información.
- Gestionar la seguridad de la información y los servicios prestados por los sistemas TIC en su ámbito de responsabilidad mediante el uso oportuno de las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica instalados en tales sistemas.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución y cierre.
- Planificar la ejecución de las auditorías periódicas de seguridad que permitan verificar el cumplimiento de las obligaciones de **GRUPO EULEN** en materia de seguridad de la información.

- Planificar la formación y concienciación de los usuarios sobre los riesgos que se derivan del uso inapropiado de las tecnologías de la información y comunicaciones.
- Elaborar informes periódicos de seguridad para los **Responsables de la Información** y los **Responsables de Servicios**, incluyendo los incidentes más relevantes acaecidos en el periodo analizado, y el cumplimiento o desviación con relación a los márgenes de riesgo residual identificados (indicadores de riesgos críticos).
- Analizar los informes periódicos recibidos por parte de los **Responsables de la Información** y los **Responsables de Servicios** con el objeto de adoptar las decisiones oportunas en materia de seguridad de la información.
- Convocar al **Comité de Seguridad de la Información** conformando el orden del día, así como aportando la información puntual precisa para el proceso de toma de decisiones (actuaciones de seguridad que se han llevado a cabo, incidentes principales acaecidos, y estado actual de la seguridad en términos de riesgo).
- Distribuir las actas de reunión del **Comité de Seguridad de la Información** con el detalle de las conclusiones alcanzadas, siendo responsable de la ejecución directa o delegada de las mismas.
- Reportar a la **Dirección** y órganos de gobierno con relación a las conclusiones alcanzadas en las reuniones del **Comité de Seguridad de la Información**.

Se garantizará la segregación de funciones oportuna entre la figura del **Responsable de Seguridad** y cualquier otra función relacionada con la prestación de servicios.

El **Responsable de Seguridad** habrá sido designado en el contexto de los órganos de gobierno.

10.2.4. RESPONSABLE DEL SISTEMA

La función de **Responsable del Sistema** asume las siguientes responsabilidades principales:

- Desarrollar, operar y mantener el sistema durante todo su ciclo de vida (análisis de especificaciones, diseño, desarrollo o adquisición, construcción, instalación, configuración, operación y mantenimiento), incorporando la visión oportuna de seguridad en todas las fases.
- Decidir, conjuntamente con el **Responsable de Seguridad**, las medidas (basadas en tecnologías de seguridad) que aplicarán para la correcta protección de la información y los servicios, así como las posibles actualizaciones precisas en la arquitectura de seguridad existente.
- Implementar las medidas de seguridad identificadas.
- Investigar, conjuntamente con el **Responsable de Seguridad**, los incidentes de seguridad que afecten al sistema.
- Colaborar en la ejecución de los análisis de riesgos en seguridad efectuados sobre el sistema.
- Definir e implantar los planes de contingencia asociados al sistema, ejecutando las pruebas pertinentes con el objeto de obtener garantías sobre la recuperación de la información y los servicios frente a situaciones de desastre.
- Decidir, conjuntamente con los **Responsables de Información**, los **Responsables de Servicios** y el **Responsable de Seguridad**, la suspensión en el tratamiento de cierta información o prestación de servicio, frente a escenarios de deficiencia grave de seguridad que pudieran afectar al cumplimiento de los requisitos formalmente establecidos.

10.2.5. ADMINISTRADOR DE SEGURIDAD DEL SISTEMA

La función del **Administrador de Seguridad del Sistema** asume las siguientes responsabilidades principales:

- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema.
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema.
- Gestionar las autorizaciones concedidas a los usuarios del sistema, en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Aplicar los procedimientos operativos de seguridad aprobados según normativa de seguridad.
- Aprobar los cambios en la configuración vigente del sistema de información.
- Monitorizar que los controles de seguridad establecidos se cumplen estrictamente.
- Supervisar que los procedimientos aprobados para gestionar el sistema están siendo aplicados convenientemente.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para garantizar que la seguridad no está comprometida y que, en todo momento, se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Comunicar al **Responsable de Seguridad** y el **Responsable del Sistema** cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

10.2.6. USUARIOS

Los usuarios asumen las siguientes responsabilidades principales:

- Tener conocimiento y dar cumplimiento a la Política de Seguridad, así como la normativa de seguridad que se deriva de la misma y que sea de aplicación en el desempeño de sus funciones.
- Colaborar en la notificación al **Responsable de Seguridad** de todo incidente que se detecte relativo a la seguridad de la información.
- Utilizar los servicios informáticos únicamente para el propósito establecido, y según las normas consideradas a tales efectos.

10.3. PROCEDIMIENTO DE DESIGNACIÓN

El **Responsable de la Información**, el **Responsable del Servicio** y el **Responsable de Seguridad** habrán sido designados por los órganos de gobierno mediante la formalización de las actas de nombramiento oportunas.

Este nombramiento se hará efectivo durante un periodo de dos (2) años o hasta que el puesto quede vacante por cualquier causa justificada.

La designación del **Responsable del Sistema**, y los **Administradores de Seguridad del Sistema** se hará efectiva según la estructura organizativa formalizada por **GRUPO EULEN** para el Gobierno y Gestión de los Sistemas de Información.

10.4. PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS

Atendiendo a la estructura jerárquica establecida por **GRUPO EULEN**, en caso de conflicto, éste deberá ser resuelto por el superior jerárquico identificado según el escenario que se presente.

11. OBLIGACIONES DEL PERSONAL

Todo el personal de **GRUPO EULEN** tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa que se derive de la misma, siendo responsabilidad del **Comité de Seguridad de la Información** disponer los medios necesarios para que la información llegue a los afectados.

Todo el personal de **GRUPO EULEN** atenderá a una acción continua de concienciación en materia de seguridad. Se establecerá un programa continuo de acciones de concienciación para atender a todo el personal de **GRUPO EULEN**, en particular a los de nueva incorporación.

El personal deberá usar el procedimiento para la notificación de incidentes de seguridad habilitado a tal efecto en caso de detectar un posible incidente.

Las personas con responsabilidad en la operación o administración de sistemas recibirán la formación oportuna para la gestión segura de los mismos.

12. TERCERAS PARTES

Cuando **GRUPO EULEN** requiera de la participación de terceras partes para la prestación de un servicio, les hará participes de la normativa de seguridad que sea de consideración en el contexto de dicha colaboración, quedando estos sujetos a las obligaciones establecidas en dicha normativa y, formalmente, a los requisitos de seguridad identificados para el alcance de los servicios externalizados.

Se formalizarán los procedimientos específicos de reporte y resolución de incidentes que pudieran presentarse durante la prestación del servicio.

Cuando algún aspecto de la normativa de seguridad no pueda ser satisfecho por una tercera parte, se requerirá la autorización del **Responsable de Seguridad** previa identificación de los riesgos en que se incurre y la forma de tratarlos, no siendo posible la formalización de la contratación con carácter previo a la obtención de dicha autorización.

13. DATOS DE CARÁCTER PERSONAL

La formalización de la Política de Seguridad de la Información, así como la normativa de seguridad que se derive de la misma, tendrá en consideración e integrará la normativa legal vigente aplicable en materia de protección de datos de carácter personal.

GRUPO EULEN ha formalizado los Registros de Actividades de Tratamiento con el detalle de los **Responsables Internos de Tratamiento** para las distintas entidades que conforman dicho grupo.

14. REVISIÓN

La Política de Seguridad de la Información será revisada anualmente por el **Responsable de Seguridad** o cuando exista un cambio significativo (enfoque de la gestión de la seguridad, circunstancias del negocio, cambios legales, cambios en el ambiente técnico, recomendaciones realizadas por autoridades de control, tendencias relacionadas con amenazas y vulnerabilidades, etc.) que obligue a ello.

En el caso de que se obtenga una nueva versión de la Política de Seguridad de la Información, se precisará la aprobación formal del **Comité de Seguridad de la Información** con carácter previo a su divulgación.

15. SANCIONES APLICABLES

El incumplimiento o violación, debidamente acreditado, de las directrices recogidas en la Política de Seguridad de la Información o en las prácticas de actuación y medidas de seguridad recogidas en la normativa de seguridad derivada de ésta, podría dar lugar a la aplicación de sanciones administrativas internas, además de las previstas en la normativa vigente.

16. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 09 de Septiembre de 2024 por la Dirección.

Esta Política de Seguridad de la Información es efectiva desde el día siguiente al de su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

Su entrada en vigor supone la derogación de cualquier otra Política que existiera a tales efectos.

La Dirección