POLÍTICA

SEGURIDAD DE LA INFORMACIÓN

POL.01

versión 1.0

31.10.2025

PÚBLICO

CONTROL DE VERSIONES

VERSIÓN	FECHA:	MODIFICACIÓN
1.0	31.10.2025	Versión inicial del documento

RUTA DE APROBACIÓN

VERSIÓN	REALIZADO POR:	REVISADO POR:	APROBADO POR:
1.0	Responsable de Seguridad	Dirección	Dirección
	Fecha: **31.10.2025**	Fecha: **31.10.2025**	Fecha: **31.10.2025**

RESPONSABILIDAD

DISTRIBUCIÓN	ARCHIVO	ACTUALIZACIÓN
Dirección	Responsable de Seguridad	Dirección

INDICE DE CONTENIDOS

1. CONTEXTO

La presente **Política de Seguridad de la Información** constituye la piedra angular para el **Marco de Gobierno y Gestión de la Seguridad de la Información** formalizado para las entidades relacionadas a continuación (en adelante, **GRUPO NEGRATÍN**):

- **INSTALACIONES NEGRATÍN, S.L**
- **NEGRATÍN GLOBAL SERVICES, S.L**

GRUPO NEGRATÍN 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, adoptando 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 NEGRATÍN**, 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.

GRUPO NEGRATÍN 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 NEGRATÍN** para la utilización segura de las tecnologías de la información y comunicaciones.

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 NEGRATÍN**, 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.
- 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.
- 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.

3. ALCANCE

GRUPO NEGRATÍN aplicará la presente **Política de Seguridad de la Información** sobre todos aquellos sistemas de información y de comunicaciones que se vean afectados por el ámbito de aplicación del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI).

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 de **GRUPO NEGRATÍN**:

- **Reglamento (UE) 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 la Sociedad de la Información y de Comercio Electrónico (en adelante, LSSICE).**
- **Texto Refundido de la Ley de Propiedad Intelectual, aprobado mediante el Real Decreto Legislativo 1/1996, de 12 de abril de 1996.** Esta normativa ha sido modificada por varias leyes, incluyendo la **Ley 21/2014**, que traspone el contenido de las directivas europeas a la legislación española, y la **Ley 2/2019**, que incorpora la **Directiva 2014/26/UE** y la **Directiva (UE) 2017/1564**.
- 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.

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 baja.

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. 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 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.

6.8. 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.

6.9. 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.

6.10. 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.

6.11. 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.

6.12. 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.

6.13. 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.

6.14. 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.

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 que deben ser implantadas en el contexto de los distintos activos de información.

8.1. MARCO ORGANIZATIVO

Orientado a administrar la seguridad de la información en el contexto de la estructura organizativa, 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 NEGRATÍN**, o que, de alguna manera, se presten bajo el control y/o la dirección de **GRUPO NEGRATÍN**, 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.
- **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 TIC.

9. INSTRUMENTOS DE DESARROLLO

La normativa de seguridad establecida por **GRUPO NEGRATÍN** 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 NEGRATÍN**.

El personal de **GRUPO NEGRATÍN** tendrá la obligación de conocer y cumplir, además de la **Política de Seguridad de la Información**, todos los estándares, procedimientos e instrucciones 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 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 específicos 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 específicos 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 NEGRATÍN**, 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 específicos 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 NEGRATÍN**, serán documentadas según el consenso alcanzado por el **Responsable de Seguridad** y el **Responsable de Sistemas**, 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 de Sistemas**.

10.ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad en **GRUPO NEGRATÍN** 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.

10.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

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

10.1.1. FUNCIONES

- Atender las inquietudes de la **Dirección** y de los **Responsables de Servicios**.
- Informar regularmente del estado de la seguridad de la información a la **Dirección**.
- Promover la mejora continua del **Modelo de Gobierno y Gestión de la Seguridad**.
- Promover la ejecución de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar su alineamiento con los objetivos de seguridad formalizados por la **Dirección**, evitando duplicidades.

- Resolver los conflictos de interés que puedan presentarse entre los diferentes responsables y/o entre diferentes unidades organizativas, elevando a **Dirección** aquellos casos en los que no tenga suficiente autoridad para decidir.
- Elaborar (y revisar regularmente) la **Política de Seguridad de la información** para que sea aprobada por la **Dirección**.
- Identificar los objetivos de seguridad precisos para su posterior aprobación por la **Dirección**, si procede.
- Aprobar los estándares de seguridad de la información elaborados por el **Responsable de Seguridad**.
- Elaborar y aprobar los requisitos de formación y cualificación de los roles identificados desde el punto de vista de seguridad de la información.
- Aprobar los planes de mejora continua de la seguridad de la información. En particular, velar por la coordinación de diferentes planes que puedan plantearse en diferentes áreas.
- Monitorizar los principales riesgos residuales asumidos por la **Dirección** y recomendar posibles actuaciones a tales efectos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones a tales efectos. En particular, velar por la coordinación de las diferentes áreas en la gestión de incidentes de seguridad de la información.
- Velar para que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación (garantías de seguridad por diseño).

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 NEGRATÍN**.

10.2.1. RESPONSABLE DE SERVICIO

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

- Actuar como propietario de los riesgos a los que se encuentra expuesto el servicio.
- Determinar y mantener actualizados los niveles de seguridad del servicio, valorando los impactos derivados de los incidentes que afectan a la seguridad de la información.
  Para la ejecución de esta actividad, podrá actuar de forma coordinada con el **Responsable de Seguridad** y el **Responsable de Sistemas**.
- Garantizar los niveles de seguridad del servicio.
- Ejecutar el análisis de riesgos de seguridad del servicio con la participación del **Responsable de Seguridad**, así como seleccionar las medidas de índole técnica y organizativa necesarias como estrategia de mitigación de los escenarios de riesgo identificados.
- Efectuar el seguimiento, monitorización y control de los escenarios de riesgo identificados.

10.2.2. RESPONSABLE DE SEGURIDAD

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

- Participar en la elaboración de la **Política de Seguridad de la Información** para la revisión por parte del **Comité de Seguridad de la Información** y aprobación por la **Dirección**.
- Elaborar y aprobar los **procedimientos e instrucciones de seguridad**.

- Velar por el mantenimiento actualizado del cuerpo normativo de seguridad y los registros asociados.
- Formalizar y divulgar la normativa de seguridad que emana de la **Política de Seguridad de la Información**.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Elaborar los Planes de Formación y Concienciación del personal en materia de seguridad, siendo éstos aprobados por el **Comité de Seguridad de la Información**.
- Monitorizar el correcto cumplimiento de los objetivos de seguridad formalizados por la **Dirección**.
- Recopilar los requisitos de seguridad de los **Responsables de Servicios**.
- Determinar formalmente la categoría de los sistemas de información en función de los niveles de seguridad identificados por los **Responsables de Servicios**.
- Colaborar con los **Responsables de Servicios** en la ejecución del análisis de riesgos.
- Elaborar la **Declaración de Aplicabilidad** como resultado del análisis de riesgos.
- Elaborar el **Plan de Tratamiento de Riesgos** para su consideración y aprobación por el **Comité de Seguridad de la Información** y **Dirección**.
- Aprobar las directrices propuestas por el **Responsable de Sistemas** para considerar la seguridad durante todo el ciclo de vida de los activos (principio de seguridad por defecto).
- Colaborar con el **Delegado de Protección de Datos** en la identificación de las medidas de seguridad precisas en materia de protección de datos personales.
- Liderar las reuniones del **Comité de Seguridad de la Información**.
- Facilitar periódicamente al **Comité de Seguridad de la Información** un reporte de actuaciones en materia de seguridad, de incidentes relevantes acaecidos y del estado de la seguridad (en particular del nivel de riesgo residual al que quedan expuestos los distintos servicios identificados).
- Exponer a la **Dirección** las necesidades y propuestas identificadas en materia de seguridad como estrategia para la mitigación de los riesgos.

10.2.3. RESPONSABLE DE SISTEMAS

La función de **Responsable de Sistemas** asume las siguientes responsabilidades principales:

- Desarrollar, operar y mantener los sistemas de información durante todo su ciclo de vida según especificaciones formalizadas, verificando su correcto funcionamiento.
- Garantizar que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Acordar la suspensión de la prestación de un servicio determinado si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con el **Responsable del Servicio** afectado y con el **Responsable de Seguridad** antes de ser ejecutada.
- Controlar la implantación de las medidas de seguridad que aplican para proveedores de TI durante las etapas de desarrollo, instalación y prueba de los sistemas.
- Determinar la configuración autorizada de hardware y software que debe ser aplicada en los sistemas.
- Delimitar las responsabilidades de las distintas funciones involucradas en el mantenimiento, explotación, implantación y supervisión de los sistemas.

- Elaborar procedimientos de seguridad de forma conjunta con el **Responsable de Seguridad**.
- Establecer planes de contingencia, llevando a cabo la planificación de ejercicios periódicos para que el personal se familiarice con tales planes.
- Aprobar los cambios que afecten a la seguridad del modo de operación de los sistemas.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento de los sistemas.
- Monitorizar el estado de la seguridad de los sistemas, y reportarlo periódicamente o ante incidentes de seguridad relevantes al **Responsable de Seguridad**.

10.2.4. DELEGADO DE PROTECCIÓN DE DATOS

La función del **Delegado de Protección de Datos** asume las siguientes responsabilidades principales:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de datos de las obligaciones que les incumben en virtud del **RGPD** y de otras disposiciones de protección de datos de la Unión o Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el **RGPD**, de otras disposiciones de protección de datos de la Unión o los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías.
- Ofrecer el asesoramiento oportuno con relación a las evaluaciones de impacto relativas a la protección de datos y supervisar su aplicación de conformidad con el **artículo 35** del **RGPD**.
- Cooperar con la autoridad de control (**Agencia Española de Protección de Datos**, en adelante, **AEPD**).
- Actuar como punto de contacto de la **AEPD** para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el **artículo 36** del **RGPD**, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Revisión de contratos de prestación de servicios en vías de formalización con proveedores (Encargados del Tratamiento) con el objeto de evaluar la idoneidad de las cláusulas referidas en materia de protección de datos.
- Revisión de formularios de recogida de datos con el objeto de confeccionar las cláusulas pertinentes de protección de datos que permitan la correcta atención del Principio de Transparencia.
- Asistencia en las actividades que se derivan para una correcta notificación y gestión de las brechas de seguridad (escenarios de violación de la seguridad de los datos personales) que pudieran presentarse.
- Comunicación de las novedades jurídicas (principalmente, directivas emitidas por la **AEPD** o el **Comité Europeo de Protección de Datos**) que pudieran impactar sobre las actividades de tratamiento existentes.
- Atención de las consultas de tipo técnico, organizativo o legal que pudieran presentarse en materia de protección de datos personales con relación a los distintos procesos de tratamiento existentes, y recogidos en el Registro de Actividades de Tratamiento.

10.2.5. ADMINISTRADOR DE SEGURIDAD

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

- Implantar y mantener las medidas de seguridad aplicables a los sistemas de información.

- Asegurar que los controles de seguridad establecidos se cumplen estrictamente.
- Informar al **Responsable de Seguridad** y **Responsable de Sistemas** de 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.
- Configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.
- Aprobar los cambios en la configuración vigente de los sistemas de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que, en todo momento, se ajustan a las autorizaciones pertinentes.
- Gestionar las autorizaciones concedidas a los usuarios de sistemas, en particular, los privilegios otorgados, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Aplicar los procedimientos de seguridad.
- Monitorizar el estado de seguridad de los sistemas de información mediante el uso de las herramientas de gestión de eventos e incidentes de seguridad y mecanismos de auditoría técnica implementados.

10.2.6. USUARIOS

Los usuarios asumen las siguientes responsabilidades principales:

- Conocer y cumplir la **Política de Seguridad de la Información**, 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.
- Colaborar en la notificación al **Delegado de Protección de Datos** de toda brecha que se detecte relativa a la seguridad de los datos personales.
- Utilizar los activos de información para el propósito establecido.
- Atender los acuerdos de confidencialidad de la información derivados de la formalización de su relación laboral con la entidad.

11.TERCERAS PARTES

Cuando **GRUPO NEGRATÍN** 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 éstos 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.

12.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.

13.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 de la **Dirección** con carácter previo a su divulgación.

14.APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado 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