# Política de seguridad

## PKF Attest

## 1. APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información ha sido revisada por el Comité de Seguridad de la Información con fecha de 17 de diciembre de 2024, siendo efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

## 2. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información será examinada en las revisiones del sistema por la Dirección, a través del Comité de Seguridad de la Información, siempre que se produzcan cambios significativos, como mínimo, una vez al año.

## 3. MISIÓN

PKF Attest asume su compromiso con la seguridad de la información, comprometiéndose a su adecuada gestión, con el fin de ofrecer las mayores garantías de seguridad.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

PKF Attest se sirve de los sistemas TIC (Tecnologías de Información y Comunicaciones) para prestar sus servicios. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, autenticidad, trazabilidad o confidencialidad de la información tratada o los servicios prestados.

En ese sentido, mediante el desarrollo de un SGSI, PKF Attest pretende garantizar la confidencialidad, integridad y disponibilidad de sus servicios. Por ello, en materia de seguridad de la información PKF Attest considera los siguientes principios básicos:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

## Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, PKF Attest implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.
Para garantizar el cumplimiento de la política, PKF Attest:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo el análisis de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

## Detección

PKF Attest establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el artículo 10 del ENS (vigilancia continua y reevaluación periódica).
Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

## Respuesta

PKF Attest establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Desarrollar una reacción adecuada frente a los incidentes, reduciendo al máximo la probabilidad de que el sistema sea comprometido en su conjunto.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

## Recuperación

Para garantizar la disponibilidad de los servicios, PKF Attest, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

## 4. ALCANCE

La presente Política se aplicará a todo el Grupo PKF Attest, y vinculará a todo su personal, independientemente de la posición y función que desempeñe.

Todo el personal de PKF Attest, así como personal externo que colabore con PKF Attest, tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

## 5. OBJETIVOS

Se establecen como objetivos de la seguridad de la información los siguientes:

- Garantizar, asegurar e implementar las medidas de seguridad adecuadas y necesarias sobre todos los recursos, procesos, funciones y servicios relacionados directa e indirectamente con usuarios internos y externos, y con clientes, proveedores, partners u otros terceros, con la finalidad de asegurar la disponibilidad, confidencialidad, integridad, trazabilidad, autenticidad de la información, y la conformidad con la legislación aplicable.
- Garantizar la calidad y protección de la información y los servicios.
- Disponer de los medios necesarios para que los diferentes usuarios de los servicios y procesos de PKF Attest hagan buen uso de la información, sistemas de la información y recursos utilizados en el desarrollo de sus funciones, obligaciones y responsabilidades, así como los que no comprometan la seguridad de la información de PKF Attest.
- Desplegar y controlar la seguridad física logrando que los activos de información se encuentren en áreas seguras y protegidos.
- Establecer la seguridad en la gestión de comunicaciones y operaciones mediante los procedimientos y herramientas necesarias logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida, conforme a su nivel de sensibilidad y de criticidad.
- Limitar el acceso a los activos mediante controles de acceso a usuarios, procesos y servicios, por medio de mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo, asegurando la trazabilidad del acceso y auditando su uso.
- Implementar y mantener los procesos de mejora continua para favorecer la eficiencia y eficacia de las medidas de seguridad de la información, evaluando periódicamente los riesgos mediante procesos de auditoría definidos para su identificación y mitigación.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Reducir al máximo las posibilidades de que se produzcan incidentes de seguridad y minimizar el impacto de estos en caso de que se produjeran.
- Garantizar la prestación continuada de los servicios de acuerdo con las necesidades de nivel de cada servicio.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación de seguridad y privacidad.

- Adoptar las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.
- Alinearse con las mejores prácticas y estándares de ámbito internacional en materia de seguridad de la información y/o ciberseguridad vigentes en cada momento.

## 6. MARCO NORMATIVO

PKF Attest tiene identificada la legislación que es de aplicación. El cumplimiento de la normativa legal y reglamentaria aplicable a todos los niveles, así como la voluntad de adaptarse a futuras normas y requisitos del cliente es un compromiso y una responsabilidad de la organización.

A continuación, se realiza un extracto del marco normativo en que se desarrollan las actividades de PKF Attest:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en la materia.
- Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011.

Para más información, revisar el documento SGSI.PR14.01 Cumplimiento requisitos legales y contractuales.

# 7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## Comité de Seguridad de la Información

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

- La persona responsable de los servicios
- La persona responsable de la información
- La persona responsable de la seguridad de la información
- La persona responsable del sistema
- La persona delegada de protección de datos

Con carácter opcional, otros miembros PKF Attest podrán incorporarse a las labores del Comité, incluidos grupos de trabajo especializados ya sean de carácter interno, externo o mixto.

El secretario o la secretaria del Comité de Seguridad será la persona responsable del sistema, que se encargará de convocar las reuniones del Comité y levantar acta de ellas.
El Comité de Seguridad tendrá las siguientes funciones:

- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Revisar regularmente la Política de Seguridad de la Información para su aprobación.
- Aprobar la Normativa de Seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

- Aprobar planes de mejora de la seguridad de la información de la organización.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

## Funciones y responsabilidades

### Responsable de la Información

Serán funciones del responsable de la Información:

- Establecer y mantener actualizada la clasificación de la información tratada en los sistemas, atendiendo a su nivel de sensibilidad.
- Definir los requisitos de seguridad necesarios para la información en función de su clasificación y asegurarse de que sean implementados en los sistemas correspondientes.
- Supervisar la seguridad de la información gestionada en el sistema, colaborando con el Responsable del Sistema y el Responsable de Seguridad.
- Garantizar que la gestión de la información se ajusta a las disposiciones legales, reglamentarias y organizativas aplicables.
- Participar en la identificación, gestión y resolución de incidentes de seguridad relacionados con la información.

### Responsable del Servicio

Serán funciones del responsable del servicio:

- Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a los Servicios.
- Supervisar el desarrollo, mantenimiento y operación del servicio, verificando que se ajusta a los niveles de seguridad acordados.
- Coordinarse con el responsable de Seguridad, el responsable del Sistema y el Responsable de la Información para garantizar una gestión integral de la seguridad en el servicio.
- Participar en la identificación y resolución de incidentes de seguridad que afecten al servicio, y reportar dichos incidentes según los procedimientos establecidos.
- Asegurar que el servicio cumple con las normativas internas y externas aplicables.
- Colaborar en la identificación, análisis y gestión de los riesgos que puedan afectar al servicio, informando de forma oportuna sobre aquellos que puedan tener un impacto significativo.

### Responsable de la Seguridad

Serán funciones del Responsable de Seguridad:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los incidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Realizar el análisis y evaluación de Riesgos de los activos de PKF Attest, junto con los responsables de los mismos.
- Elaborar el documento de Declaración de Aplicabilidad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad TIC.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Hacer seguimiento del cumplimiento de las medidas y normas de seguridad y acuerdos de nivel de servicio por parte de los proveedores de servicios TIC
- Gestionar, coordinar y reportar los incidentes de seguridad que afecten a los sistemas de información, asegurando su correcta resolución y adoptando las medidas preventivas necesarias.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.

### Responsable de Sistema

Serán funciones del Responsable del Sistema:

- Desarrollar, operar y mantener del Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Elaborar los procedimientos operativos necesarios.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.

- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el responsable del Seguridad y/o Comité de Seguridad TIC.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al responsable de Seguridad o a quién éste determine.
- Implantar los planes de continuidad del servicio, asesorado por la persona Responsable de Seguridad.
- Además, el responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

### Delegado de Protección de Datos

Serán funciones del Delegado de Protección de Datos:

- Informar y asesorar a PKF Attest, y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas de PKF Attest, 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 correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.
- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.
- El Delegado de Protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
    - ✓ Recabar información para determinar las actividades de tratamiento.
    - ✓ Analizar y comprobar la conformidad de las actividades de tratamiento.
    - ✓ Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento. Recabar información para supervisar el registro de las operaciones de tratamiento.
    - ✓ Asesorar en el principio de la protección de datos por diseño y por defecto.
    - ✓ Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
    - ✓ Priorizar actividades en base a los riesgos.
    - ✓ Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

### Resolución de Conflictos

En el caso de conflicto entre las diferentes partes, este se resolverá por el superior jerárquico de estas. En ausencia del anterior prevalecerá la decisión de la persona responsable de seguridad.

### Procedimientos de designación

- La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política, se realizará por un Socio de PKF Attest.
- El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

### Obligaciones del personal

Todas las personas usuarias de los sistemas de la información de PKF Attest tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a las personas afectadas.

Se establecerá un programa de concienciación continua para atender a todos las personas usuarias de los sistemas de la información, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que a necesiten para realizar su trabajo.

La formación será obligatoria antes de asumir una responsabilidad, tanto se es su primera asignación o se trata de un cambio de puesto de trabajo o de responsabilidades en este.

El manifiesto incumplimiento de la Política de Seguridad de la Información o de la normativa y los procedimientos derivados de ellas, pueden llevar al inicio de medidas disciplinarias adecuadas y, se es el caso, a otras medidas legales de aplicación.

## 8. PROTECCION DE DATOS, FORMACIÓN Y GESTIÓN

### Datos personales

PKF Attest solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas oportunas, tales como el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la

evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

## Gestión de riesgos

Todos los sistemas afectados por la presente Política de Seguridad de la Información están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de la Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal. El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

## Desarrollo de la Política de Seguridad de la Información

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas).

Corresponde al Comité de Seguridad de la Información su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma. El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: constituido por la presente Política de Seguridad de la Información y Manual del Sistema Gestión Seguridad de la Información

b) Segundo nivel normativo: constituido por las Normativa Interna de Seguridad para el correcto uso de los sistemas de información

c) Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al Comité de Seguridad la aprobación de la Política de Seguridad de la Información, la Normativa Interna y de los restantes documentos, siendo también responsable de su difusión para que la conozcan las partes afectadas.

## Terceras partes

Cuando PKF Attest preste servicios a otros organismos o maneje información de otros organismos, se les hará participe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando PKF Attest utilice servicios de terceros o ceda información a terceros, se les hará participe de esta Política de Seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

## Cambio climático

PKF Attest ha realizado el análisis de los servicios prestados por la organización, así como su operativa habitual para la prestación de los mismos no encontrando aspectos que puedan influir en el cambio climático del planeta más allá de los generados por los sistemas de climatización y emisiones de vehículos que prestan servicio a la organización, en ambos casos dentro de los requisitos legales establecidos.

Se han analizado los requisitos de las partes interesadas sin hallar ninguno específicamente relacionado con el cambio climático.

En base a ambos análisis se concluye la no necesidad de aplicar medidas más allá de los requisitos legales estándar establecidos.

## Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas.

Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.

b) Revisión de los servicios e información y su categorización.

c) Ejecución con periodicidad anual del análisis de riesgos.

d) Realización de auditorías internas o, cuando procedan, externas.

e) Revisión de las medidas de seguridad.

f) Revisión y actualización de las normas y procedimientos.

## 9. HISTÓRICO DE MODIFICACIONES

| Versión | Fecha | Revisado por | Aprobado por | Modificación |
|---|---|---|---|---|
| 1 | Abril 21 | Resp. Seguridad | Comité Seguridad | Edición inicial |
| 2 | Sept 21 | Resp. Seguridad | Comité Seguridad | Modificación tras auditoría interna |
| 3 | 11.03.22 | Resp. SGSI | Comité Seguridad | Modificación alcance (PKF Attest ITCà PKF Attest) |
| 4 | Dic. 24 | Resp. SGSI | Comité Seguridad | Adecuación ENS 311/2022 |