Política de seguridad

PKF Attest

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 ITC→ PKF Attest)

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 11 de marzo de 2022, siendo efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

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.

INTRODUCCIÓN

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 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.

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.

PRINCIPIOS Y DIRECTRICES EN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PKF Attest ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral y seguridad por defecto

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas y en las condiciones autorizadas.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Reevaluación periódica e integridad y actualización del sistema

PKF Attest ha implementado controles y evaluaciones regulares de la seguridad para conocer en todo momento el estado de la seguridad del sistema en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Gestión de personal y profesionalidad

Se establecerá un programa de concienciación continua para atender a todos los miembros, 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 la necesiten para realizar su trabajo.

Gestión de la seguridad basada en los riesgos y análisis y gestión de riesgos

Todos los sistemas afectados por esta Política de Seguridad deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos cada una vez al año.
- Cuando cambien la información manejada y/o los servicios prestados de manera significativa.

- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El responsable de 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.

Incidentes de seguridad, prevención, reacción y recuperación

PKF Attest ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

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

Líneas de defensa y prevención ante otros sistemas interconectados

PKF Attest ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Función diferenciada y organización e implantación del proceso de seguridad

PKF Attest ha organizado su seguridad mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas.

Autorización y control de los accesos

PKF Attest ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones

PKF Attest ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos, PKF Attest tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

Protección de la información almacenada y en tránsito y continuidad de la actividad

PKF Attest ha implementado mecanismos para proteger la información almacenada o en tránsito. Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de la información y servicios producidos en el ámbito de las competencias de PKF Attest. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos.

Registros de actividad

PKF Attest ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, laboral, y demás disposiciones que resulten de aplicación.

Cumplimiento requisitos legales

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.

Mejora continua

La mejora continua se desarrolla en el marco de un Sistema de Gestión, el cual la Dirección se compromete a liderar acorde a la norma ISO 27001, garantizando la idoneidad, adecuación y eficacia del Sistema.