Política de Seguridad de la información

Kairōs

Elaborado por:	Aprobado por:
Responsable del sistema Fecha: 29 - 11 - 2023	CEO Fecha: 29 - 11 - 2023

CONTENIDO

1. APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información es efectiva desde la fecha de su aprobación por el Comité de Seguridad y validada por la Dirección, hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

La Dirección del Grupo Kairós ("Kairós DS") en el marco de su competencia general e indelegable de determinar las políticas y estrategias generales de la sociedad, y previa revisión y propuesta por parte de la Comisión competente, ha decidido establecer e implantar **un Sistema de Gestión de Seguridad de la información, basado en los requisitos de la norma:**

- **UNE-EN ISO 27001:2023, y**
- **el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.**

Kairós DS depende de los sistemas de Tecnologías de Información y Comunicaciones (TIC) para alcanzar sus objetivos. 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, confidencialidad, autenticidad, o trazabilidad de la información tratada o los servicios prestados.

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.

Los sistemas de Kairós DS deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos y Reglamento Europeo de Protección de Datos e ISO 27001:2023, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Kairos DS trabaja en pos de que la seguridad de la información sea una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos tecnológicos y de consultoría de transformación.

Kairós DS trabaja y se prepara para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad, a la Ley Orgánica de Protección de Datos e ISO 27001:2023.

Esta Política de Seguridad sigue las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

2.1. Prevención

Kairós DS debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se implementarán las medidas mínimas de seguridad determinadas por el ENS, RGPD, la LOPD e ISO 27001:2023, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, Kairós DS debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua, para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya preestablecido como normales.

2.3. Respuesta

Kairós DS establecerá mecanismos para responder eficazmente a los incidentes de seguridad, designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en otras disciplinas, áreas, equipos o en otros organismos, y finalmente, establecerá protocolos de intercambio de información relacionada con incidentes con clientes y proveedores.

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, Kairós DS ha establecido planes de contingencia de los sistemas de información como parte de su plan general de continuidad del negocio y actividades de recuperación.

3. MISIÓN

Nuestra misión es ayudar a nuestros clientes en el lanzamiento, aceleración de productos y soluciones en el entorno digital / innovación, así como los proyectos de gestión de cambio organizacional, en definitiva, les ayudamos a reinventarse en el entorno digital.

En coherencia con la misión, nuestra visión consiste en ser la empresa de referencia en proyectos de gestión de cambio y construcción de soluciones en el nuevo entorno competitivo digital.

Para dirigir y orientar el Sistema de Gestión de Seguridad de la Información implantado, la cultura de nuestra organización se asienta sobre los siguientes objetivos y principios de actuación:

- Crear y mantener una cultura de seguridad de la información que sea asumida por la totalidad de nuestros empleados, haciéndola extensible a nuestra cadena de suministro, y que además garantice la continuidad del negocio y la seguridad de la información en todas sus dimensiones según el nivel de riesgo de nuestros activos, necesidades y recursos.
- Adoptar un comportamiento de mejora continua de la gestión de seguridad de la información en todos los aspectos de la organización.
- Proporcionar un marco de referencia para establecer y revisar los objetivos de la organización en materia de calidad y seguridad de la información.
- En todo momento, la política de gestión será implementada, mantenida y comunicada a todo el personal de la organización, estando a disposición de nuestros grupos de interés.
- Proteger la información que procesan y a la que acceden nuestros trabajadores, para evitar su pérdida, alteración, destrucción o uso indebido. Garantizando la confidencialidad, integridad y disponibilidad de la información. Siendo responsabilidad de estos de reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que utilicen.
- Garantizar que los servicios **Kairos DS** estén disponibles según sea necesario para el negocio y asegurar un mínimo impacto en el mismo en el caso de una interrupción temporal.
- Plasmar la filosofía y compromiso ético y social de **Kairos DS** en el Código de Conducta.
- Todo el personal de **Kairos DS** deberá asistir a las sesiones de concienciación en materia de seguridad, las cuales se establecerán en el plan de formación y concienciación anual.
- Las terceras partes que estén relacionadas con la gestión, mantenimiento o explotación de los servicios y sistemas de **Kairos DS** serán partícipes de esta Política de Seguridad de la Información. Las terceras partes quedarán obligadas al cumplimiento de esta política y a las normativas que se puedan derivar de ella.
- Las terceras partes podrán desarrollar sus propios procedimientos operativos para satisfacer esta Política y puedan reportarlas.

4. ALCANCE

Esta Política será de aplicación y de obligado cumplimiento para los equipos y servicios provistos por Kairós DS, a sus recursos y a los procesos afectados, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Así como los *Sistemas de Información que soportan los procesos y los* ***SERVICIOS DE CONSULTORÍA Y DESARROLLO RELACIONADOS CON LA TRANSFORMACIÓN DIGITAL DE NUESTROS CLIENTES****, según la declaración de aplicabilidad vigente.*

Desde **Kairos DS**, se ha constituido la política de nuestro Sistema de Seguridad de la Información como un pilar básico para establecer y revisar los objetivos de seguridad de la información, y así conseguir la plena satisfacción de nuestros clientes.

Por esta razón, y con el fin de alcanzar los objetivos marcados, la Dirección adopta el compromiso de dedicar a esta tarea todo su potencial económico, tecnológico y humano. De tal forma que la organización de la empresa, su política de inversiones, el desarrollo de nuevos métodos y los recursos humanos, estén orientados prioritariamente a garantizar el cumplimiento de los requisitos exigibles por el cliente y por la legislación vigente aplicable en materia de seguridad de la información.

Está Política de Seguridad:

- Será aprobada formalmente por la dirección de Kairós DS.
- Será revisada regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Será comunicada a todos los empleados y partes interesadas qué trabajan y están en contacto con nosotros.

5. DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El presente sistema de gestión de la seguridad de la información es aplicable a los sistemas de seguridad de la información que dan soporte a las actividades desarrollo, comercialización, consultoría y soporte relacionados con la:

- Prestación del servicio de consultoría en materia de transformación digital y tecnologías de la información.
- Soporte a los servicios de administración de sistemas y Hosting de acuerdo a las necesidades del cliente.
- Prestación de servicios de consultoría de oficina técnica (PMO).
- Desarrollo de aplicaciones e integración de sistemas.
- Servicio de desarrollo y mantenimiento de aplicaciones (AMS).
- Servicios corporativos de soporte técnico Help Desk, RRHH, CRM y ERP.
- Servicios de consultoría tecnológica, gestión de proyectos y actividades.

según declaración de aplicabilidad vigente en Ed. 1 Rev. 0 de fecha 14/02/2024.

6. MARCO NORMATIVO

Según la legislación vigente, las leyes aplicables a Kairós DS en materia de Seguridad de la Información son:

- UNE-EN ISO/IEC 27001:2023. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica. BOE de 29 de enero de 2010.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- 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.
- LOPD y garantías de los derechos digitales 03/2018.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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.

Kairós DS cumple con la legislación citada y con todos sus requisitos.

7. ORGANIZACIÓN DE LA SEGURIDAD

Con el objeto garantizar la continua idoneidad, adecuación, efectividad de la dirección y apoyo a la seguridad de la Información de acuerdo con los requisitos de negocio, legales, estatutarios, reglamentarios y contractuales, así como establecer una estructura definida, aprobada y compresible para implementación, operación y gestión de la seguridad de la información dentro de Kairós DS se han establecido una serie de roles, funciones y responsabilidades de los mismos.

7.1. Comité de Seguridad

Funciones:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos en materia de seguridad de la información.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- 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 y están alineados con la estrategia de ciberseguridad.
- Evitar duplicidades y garantizar la segregación de las funciones.
- 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.
- Elaborar (y revisar regularmente) las normativas de seguridad de la información para que sean aprobadas por la Dirección.
- Aprobar la política de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de los administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Supervisar la evaluación y gestión del riesgo.

- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de los diferentes planes que puedan realizarse en diferentes áreas.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles mejoras.
- Velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover y garantizar la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la entidad en materia de seguridad de la información.
- Priorizar las actuaciones en materia de seguridad de la información cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los servicios.

7.2. Responsable de Seguridad (CISO)

- Prevención, detección y análisis de amenazas.
- Respuesta ante incidentes de seguridad.
- Supervisión y gestión de la arquitectura, auditorías de seguridad, así como el control del acceso a la información.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles mejoras.
- Velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover y garantizar la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la entidad en materia de seguridad de la información.
- Encargado de la formación y concienciación en materia de seguridad de la información de todos los empleados.
- La definición de la normativa de seguridad y su cumplimiento.

7.3. Responsable del SGSI

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación e instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.

- Elaborar y aprobar la documentación de seguridad del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

7.4. Responsable de la Información

- Garantizar el correcto uso de la información y, en consecuencia, su adecuada protección.
- Asumir la responsabilidad final por cualquier error o negligencia que resulte en un incidente de confidencialidad o integridad.
- Definir los requisitos de seguridad aplicables a la información.
- Establecer los niveles de seguridad correspondientes a la información.
- Aprobar de manera formal el nivel de seguridad asignado a la información.

8. PROCEDIMIENTOS DE DESIGNACIÓN

La Dirección nombra:

- Responsable de Seguridad, que reportará al Comité de Seguridad.
- Responsable del Sistema, que reportará al Comité de Seguridad.
- Responsable de la Información, que reportará al Comité de Seguridad.

9. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la organización y difundida para que la conozcan todas las partes interesadas.

9.1. Datos de Carácter Personal

La Ley Orgánica de Protección de Datos (LOPD) y el RGPD, tratan de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, y resulta de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

El documento de seguridad que regula la normativa de protección de datos “POLÍTICA GLOBAL DE SEGURIDAD Y PROTECCIÓN DE DATOS” y “POLÍTICA DE PROTECCIÓN DE DATOS EN SITUACIONES DE TRABAJO A DISTANCIA” recoge los tratamientos correspondientes.

Todos los sistemas de información de Kairós DS se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en las mencionadas Políticas.

Para garantizar dicha protección, se han adoptado las medidas de seguridad que se correspondan con las exigencias previstas en la legislación de aplicación. Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con Kairós DS.

9.2. Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán someterse a un análisis de riesgos, evaluando las amenazas y riesgos a los que están expuestos. Este análisis se realizará en los siguientes casos:

- De manera regular, al menos una vez al año.
- Cuando se produzcan cambios en la información gestionada.
- Al modificarse los servicios ofrecidos.
- Tras la ocurrencia de un incidente de seguridad grave.
- Al detectarse vulnerabilidades críticas.

Para garantizar la coherencia en los análisis de riesgos, el Comité de Seguridad establecerá un marco de referencia para valorar los distintos tipos de información y servicios. Además, el Comité fomentará la asignación de recursos necesarios para cubrir las necesidades de seguridad de los sistemas, promoviendo inversiones transversales. La gestión de riesgos será documentada en el informe de Análisis y Gestión de Riesgos.

9.3. Desarrollo de la política de seguridad de la información

9.3.1. Política de Uso Aceptable

Los activos de información son prioritarios para el desarrollo de los procesos de Kairós DS y el adecuado cumplimiento de sus funciones.

Por lo que es responsabilidad del usuario:

- Salvaguardar los activos asignados a él ante cualquier alteración o modificación no autorizada, además de cualquier daño o destrucción que límite su disponibilidad para el adecuado desarrollo de sus actividades.
- Reportar cualquier fallo, mal funcionamiento o uso inadecuado detectado en los activos de información al departamento de soporte de IT.
- Reportar cualquier necesidad de protección o mejora de los activos de información al departamento de soporte de IT.
- Usar los activos de información únicamente para propósitos del negocio.

9.3.2. Seguridad de la gestión de recursos humanos

La seguridad relacionada con el personal es esencial para mitigar riesgos de errores humanos, robos, fraudes o uso indebido de instalaciones y servicios. Todos los empleados deberán firmar un acuerdo de confidencialidad para prevenir la divulgación no autorizada de información confidencial.

Las políticas y procedimientos de seguridad serán comunicados regularmente a todos los trabajadores y, cuando sea necesario, también a usuarios externos.

Al finalizar la relación laboral o contractual con empleados o proveedores de servicios, se revocarán sus permisos de acceso a instalaciones e información, y se solicitará la devolución de cualquier tipo de información o equipo que se les haya proporcionado para el desempeño de sus funciones.

9.3.3. Seguridad física y del entorno

Para que la seguridad lógica sea efectiva, es fundamental que las instalaciones cuenten con medidas adecuadas de seguridad física, evitando así accesos no autorizados y cualquier tipo de daño o interferencia externa.

- Accesos: Kairós DS ha tomado las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones. Además, todas ellas cuentan con las barreras físicas necesarias para asegurar que los recursos albergados; en concreto un control de acceso se realiza mediante una tarjeta y se realiza un acompañamiento del personal ajeno durante la estancia en las instalaciones.
- Equipos: Los equipos son un activo clave para asegurar la continuidad de las actividades, por lo que deben ser protegidos de manera eficaz. Los equipos informáticos de Kairós DS cuentan con medidas de protección frente a posibles fallos de energía, como portátiles con baterías y sistemas de alimentación ininterrumpida (SAIs).

  Es esencial mantener los equipos en óptimas condiciones para asegurar su correcto funcionamiento y garantizar la confidencialidad, integridad y, especialmente, la disponibilidad de la información. Esto incluye someterlos a las revisiones recomendadas por el proveedor. Solo el personal autorizado podrá acceder a los equipos para su reparación. Además, se deben adoptar las medidas de precaución necesarias cuando los equipos deban salir de las instalaciones para su mantenimiento.

9.3.4. Gestión de comunicaciones y operaciones

Se han establecido las directrices para garantizar la protección de la información en las redes e infraestructura de apoyo para el procesamiento de información de Kairós DS, siendo de aplicación a todo el personal de Kairós DS, a todos proveedores con acceso a los activos de información de Kairós DS y a todas las instalaciones y recursos de Kairós DS incluidos en el alcance del SGSI.

Así mismo, queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de Kairós DS. El Administrador del

Sistema instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, worms (gusanos), troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

Los datos deben ser guardados en la nube para asegurar que se realizan copias de seguridad habitualmente.

Los elementos de red (switch, router...etc.) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema. Existe una gestión gráfica de la red de forma que su mantenimiento sea más cómodo.

9.3.5. Control de accesos

Kairós DS ha establecido un protocolo de gestión para el Control de Accesos que permitirá evitar fugas de información y accesos no autorizados. Así mismo, los permisos de usuarios deben asignarse mediante roles o grupos, otorgando a cada rol o grupo un conjunto de permisos sobre el acceso lógico a los sistemas, y siguiendo la regla de mínimos privilegios posibles (need to know / need to use / deny all), en función de las necesidades de cada puesto de trabajo. Especialmente importante es el registro de los usuarios de los sistemas de información que contienen información confidencial de Kairós DS.

Esta regla debe ser aplicable a:

- Aplicaciones.
- Redes.
- Servicios web.
- Correo electrónico.
- Servicios de comunicaciones y mensajería instantánea.
- Acceso a equipos y a aplicaciones remotas.
- Transferencia de ficheros.
- Acceso a redes de intercambios de ficheros, entre otros servicios.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de Kairós DS están obligados a conocer y cumplir con esta Política de Seguridad de la Información. Es responsabilidad del Comité de Seguridad asegurar que la información llegue a todas las personas afectadas.

Anualmente, todos los miembros de Kairós DS recibirán una capacitación sobre concienciación en seguridad. Se ha implementado un programa de concienciación continua que abarca a todos los miembros de la organización, con especial atención a aquellos de nueva incorporación.

Las personas responsables del uso, operación o administración de los sistemas de la información recibirán la formación necesaria para asegurar un manejo seguro de dichos sistemas, en función de las necesidades de su puesto. Esta formación será obligatoria antes de asumir cualquier responsabilidad, ya sea por primera vez, por un cambio de puesto o por una reasignación de responsabilidades.

11. PARTES INTERESADAS

Cuando Kairós DS preste servicios a otros organismos o maneje información de estos, se les informará sobre la Política de Seguridad de la Información. Se establecerán canales de reporte y coordinación entre los respectivos Comités de Seguridad, así como procedimientos para la gestión y respuesta ante incidentes de seguridad.

Si Kairós DS utiliza servicios de terceros o transfiere información a ellos, estos terceros serán informados tanto de la Política de Seguridad como de la Normativa de Seguridad aplicable a dichos servicios o información. Las terceras partes estarán obligadas a cumplir con las disposiciones establecidas en esta normativa, aunque podrán desarrollar sus propios procedimientos operativos para cumplir con estos requisitos. Además, se establecerán procedimientos específicos para el reporte y resolución de incidencias. Se garantizará que el personal de las terceras partes esté adecuadamente formado en seguridad, al menos al nivel requerido por esta Política.

Si alguna disposición de la Política no puede ser cumplida por una tercera parte, se requerirá un informe del Responsable de Seguridad que detalle los riesgos asociados y las medidas de tratamiento. Este informe deberá ser aprobado por los responsables de la información y los servicios afectados antes de continuar con las actividades.