



KUO- ENS- PL 01
POLÍTICA DE SEGURIDAD – ENS



ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR.....	3
2. INTRODUCCIÓN.....	3
2.1. Prevención.....	3
2.2. Detección	4
2.3. Respuesta.....	4
2.4. Recuperación	4
3. MISIÓN	5
4. ALCANCE.....	6
5. DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.....	6
6. MARCO NORMATIVO	8
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.....	8
7. ORGANIZACIÓN DE LA SEGURIDAD.....	9
7.1. Comité de seguridad	9
7.2. Roles: Funciones y Responsabilidades.....	9
▪ Procedimientos de designación	11
▪ Revisión de la Política de Seguridad	11
8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	11
8.1. Datos de Carácter Personal	12
8.2. Gestión de Riesgos.....	13
8.3. Desarrollo de la política de seguridad de la información.....	13
8.3.1. Política de Uso Aceptable	13
8.3.2. Seguridad de la gestión de recursos humanos	14
8.3.3. Seguridad física y del entorno.....	14
8.3.6. Gestión de comunicaciones y operaciones.....	15
8.4. Control de accesos	17
9. OBLIGACIONES DEL PERSONAL	18
10. TERCERAS PARTES	19

1. APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información es efectiva desde la fecha de su aprobación, el 28/07/2022, y actualizada a ENS MEDIO el **01/04/2024** por el Comité de Seguridad, hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

SECURITY SERVICES KUO; S.L. depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) 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 prontitud a los incidentes.

Los sistemas TIC 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. 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, 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.

SECURITY SERVICES KUO; S.L. debe cerciorarse de que la seguridad de la información es 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 de TIC.

SECURITY SERVICES KUO; S.L. debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad) y a la Ley Orgánica de Protección de Datos.

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

SECURITY SERVICES KUO; S.L. 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 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, RGPD y la LOPD, 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **SECURITY SERVICES KUO; S.L.** 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 debido a incidentes es preciso monitorizar la operación de manera continua, para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según las líneas de defensa establecidas en el artículo 9 del ENS.

Se establecerán así 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 prestablecido como normales.

2.3. Respuesta

SECURITY SERVICES KUO; S.L.:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos.
- Establecer protocolos de intercambio de información relacionada con incidentes con clientes y proveedores.

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, **SECURITY SERVICES KUO; S.L.** ha desarrollado planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

3. MISIÓN

SECURITY SERVICES KUO; S.L. define la presente Política de Seguridad de la Información, de carácter obligatorio para empleados y empresas colaboradoras, teniendo como objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando frente a los incidentes que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve a **SECURITY SERVICES KUO; S.L.** para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- **Disponibilidad:** propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- **Integridad:** propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- **Confidencialidad:** propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- **Autenticidad:** propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- **Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en **SECURITY SERVICES KUO; S.L.** serán:

- Velar por la seguridad de la información, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de contingencias y continuidad de la actividad que se definan para los distintos servicios ofrecidos por la organización.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

Esta Política de Seguridad:

- Se aprobará formalmente por la organización.
- Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Se comunicará a todos los empleados y empresas externas que trabajen con **SECURITY SERVICES KUO; S.L.**

4. ALCANCE

La Política de Seguridad se aplica a toda la empresa y a sus activos de información:

- A todos los departamentos, tanto a sus directivos como a empleados.
- A los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la organización.
- A bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- A la información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.
- A la información cedida dentro de un marco legal establecido, que será considerada como propia y afectos exclusivos de su protección.
- A todos los sistemas utilizados para administrar y gestionar la información, sean propios o alquilados o licenciados por la misma.

5. DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de **SECURITY SERVICES KUO; S.L.**

- En **SECURITY SERVICES KUO; S.L.** se reconoce expresamente la importancia de la información, así como la necesidad de suprotección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad de la Institución, o al menos suponer daños muy importantes, si se produjera una pérdida total e irreversible de determinados datos.
- **SECURITY SERVICES KUO; S.L.** implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad, del RGPD y de la Ley Orgánica de Protección de Datos, y cumple con todos los requisitos legales aplicables.
- La información y los servicios están protegidos contra pérdidas de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Los controles serán proporcionales a la criticidad de los activos a proteger y a su clasificación.
- La responsabilidad de la seguridad de la información involucrada en la prestación de los servicios incluidos en el alcance del ENS es de la Dirección, que pondrá los medios adecuados, sin perjuicio de que los empleados o usuarios asuman su parte de responsabilidad respecto a los medios que utiliza, según lo indicado en las normativas y en los procedimientos complementarios. En el punto 7 “Organización de la Seguridad” de este mismo documento se describen las funciones y responsabilidades del Comité de Seguridad, que gestionará la seguridad de la información, y de sus miembros.
- Quienes desempeñen la función de Seguridad de la Información y otras de administración relacionadas, serán quienes administren la seguridad.
- Se ha identificado a los responsables de la información, que deberán promover el

establecimiento de los controles y medidas destinadas a proteger los datos que la integran, especialmente los de carácter personal o críticos.

- Se establecerá dentro de la normativa un sistema de clasificación de la información, con diferentes niveles.
- Se establecerán los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y, en general, de cualquier activo de **SECURITY SERVICES KUO; S.L.**
- Los aspectos específicos más relacionados con la información sobre datos personales están regulados por el conjunto de normas recogidas en este documento de seguridad y en la normativa interna o de otra índole a la que pueda remitir o que se cite.
- Quienes no cumplan lo determinado en estas normas y en los procedimientos complementarios podrán ser sancionados de acuerdo con la legislación laboral, o bien con sanciones personalizadas si están vinculados a **SECURITY SERVICES KUO; S.L.** bajo contratos no laborales, de acuerdo con las cláusulas que figuren en dichos contratos en este último caso.
- Deberán realizarse periódicamente evaluaciones de riesgos y, en función de las debilidades, determinar si es necesario elaborar planes de implantación o reforzamiento de controles.
- Se fomentará la difusión de información y formación en seguridad a empleados y colaboradores, previniendo la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar su posible existencia lo antes posible, y en caso de que existieren, procurándose una difusión muy restringida de las indagaciones.
- El personal de **SECURITY SERVICES KUO; S.L.** deberá conocer las normas, reglas, estándares y procedimientos relacionados con su puesto de trabajo, así como sus funciones y obligaciones, además de la separación de funciones y la revisión independiente de los registros, cuando sea necesario, de quién ha hecho qué, cuándo y desde dónde.
- Las incidencias de seguridad serán comunicadas y tratadas apropiadamente.

6. MARCO NORMATIVO

Según la legislación vigente, las leyes aplicables a **SECURITY SERVICES KUO; S.L.** en materia de Seguridad de la Información son:

Ley / Regulación	Responsabilidad
Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas	Asesoría Jurídica
Ley 40/2015, de 1 de octubre, establece y regula las bases del régimen jurídico de las Administraciones Públicas, los principios del sistema de responsabilidad de las Administraciones Públicas y de la potestad sancionadora, así como la organización y funcionamiento de la Administración General del Estado y de su sector público institucional para el desarrollo de sus actividades	Asesoría Jurídica
Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.	Asesoría Jurídica
Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal	Asesoría Jurídica
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	Asesoría Jurídica
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	Asesoría Jurídica
Ley 34/2002 de Servicios de la Sociedad de la Información (LSSI)	Asesoría Jurídica
Ley 22/11, de 11/11/1987, de Propiedad Intelectual	Asesoría Jurídica
Ley 17/2001, de Marcas	Asesoría Jurídica
REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE	Asesoría Jurídica
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.	Asesoría Jurídica

SECURITY SERVICES KUO; S.L. cumple con la legislación citada y con todos sus requisitos.

7. ORGANIZACIÓN DE LA SEGURIDAD

7.1. Comité de seguridad

El Comité de Seguridad, en cumplimiento con el Real Decreto 311/2022, de 4 de mayo, por el que se regula el Esquema Nacional de Seguridad, se ha constituido a fecha de 28 de julio del 2022, siendo integrantes como:

- Responsable del Sistema y del Servicio: Mirian Andrés
- Administradora y Responsable de seguridad, de la información: M^a Begoña Jausas

Las funciones de este Comité, en relación al Sistema de ENS, pasarán por:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de **SECURITY SERVICES KUO; S.L.** en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de los diferentes departamentos en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la organización.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de los Responsables de área, técnicos y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por **SECURITY SERVICES KUO; S.L.** y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de los diferentes departamentos en la gestión de incidentes de seguridad de la información.
- 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 **SECURITY SERVICES KUO; S.L.**. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes departamentos.
- 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, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Informar regularmente del estado de la seguridad de la información a la Dirección.

7.2. Roles: Funciones y Responsabilidades

En el caso de **SECURITY SERVICES KUO; S.L.** la mayor parte de las responsabilidades recaen en la gerencia, al ser una empresa unipersonal. Las funciones y responsabilidades de la misma se detallan a continuación dividiéndose entre cada una de las figuras detalladas en el art. 11 del Real Decreto 311/2022:

Responsable de la Información

- Responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Establecer los requisitos de la información en materia de seguridad.
- Determinar y aprobar los niveles de seguridad de la información.
- Aprobar la categorización del sistema con respecto a la información.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar la categorización del sistema con respecto a los servicios.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

Responsable de la Seguridad

Sus funciones serán las siguientes

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Aprobar la declaración de aplicabilidad.
- Canalizar y supervisar, tanto el cumplimiento de los requisitos de seguridad del servicio que se presta o solución que provee, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio (POC).
- Los que se vayan indicando en los documentos dentro del alcance del ENS.



El Responsable de la Seguridad será el secretario del Comité de Seguridad con las funciones indicadas en el apartado 3.5.1 de la presente política.

Responsable del Sistema

Sus funciones serán las siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Potestad para proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

Responsable de Privacidad

Sus funciones serán las siguientes:

- Coordinar todos los aspectos relacionados con la adecuación de las actuaciones de KUO SPAIN en materia de protección de datos de carácter personal.
- Coordinar, junto con el Responsable de Seguridad, el cumplimiento del ENS con respecto a la protección de datos de carácter personal.

▪ Procedimientos de designación

El Responsable de Seguridad será nombrado por el Comité de Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Igualmente, el resto de los cargos indicados en el apartado anterior será designado por el Comité de Seguridad mediante acta de reunión.

▪ Revisión de la Política de Seguridad

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

8. 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 afectadas.

8.1. 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 “Documento de Seguridad de la LOPD/RGPD” se puede encontrar en su carpeta correspondiente. Dicho documento recoge los tratamientos correspondientes.

En lo que respecta de manera específica a la protección de los datos personales, KUO SPAIN se compromete a cumplir con los principios indicados en la legislación de referencia. Estos son:

- Principio de “licitud, transparencia y lealtad”. Los datos deben ser tratados de manera lícita, leal y transparente para el interesado.
- Principio de “finalidad”. Los datos deben ser tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otro lado, se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.
- Principio de “minimización de datos”. Aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad.
- Principio de “exactitud”. Disponer de medidas razonables para que los datos se encuentren actualizados, se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan.
- Principio de “limitación del plazo de conservación”. La conservación de los datos debe limitarse en el tiempo al logro de los fines que persigue el tratamiento.
- Principio de “seguridad” Realizar un análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten.
- Principio de “responsabilidad activa” o “responsabilidad demostrada”. Mantener diligencia debida de manera permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados en base a un análisis de los riesgos que el tratamiento representa para esos derechos y libertades, de modo que podamos garantizar y demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.

- Dirigir, apoyar y supervisar el sistema de gestión de la seguridad de la información, según lo establecido en el RD 311.2022 y posteriores modificaciones y buscar se alcancen los objetivos del mismo.

La dirección de KUO SPAIN se compromete a apoyar y promover los principios establecidos en esta Política, para lo que pide al personal de la empresa que asuma y se atenga a las previsiones del sistema de gestión documentado para el ENS.

8.2. Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis y Gestión de riesgos.

8.3. Desarrollo de la política de seguridad de la información

8.3.1. Política de Uso Aceptable

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de los equipos están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.

- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso intencionadamente. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus osimilares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causarmolestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que puedallegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus.

La documentación relativa a la Seguridad de la Información estará clasificada en tres niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de seguridad.
- Segundo nivel: Normativas y procedimientos de seguridad.
- Tercer nivel: Informes, registros y evidencias electrónicas.

8.3.2.Seguridad de la gestión de recursos humanos

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información confidencial.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede.

Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

8.3.3.Seguridad física y del entorno

Para que una seguridad lógica sea efectiva, es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa.

8.3.4. Áreas seguras

SECURITY SERVICES KUO; S.L. tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.

La totalidad de las instalaciones de **SECURITY SERVICES KUO; S.L.** cuentan con las barreras físicas necesarias para asegurar los recursos que estas alberguen; en concreto un control de recepción e identificación del visitante (solicitándose su nombre completo e identificación de la empresa de la que proviene, en su caso) y el acompañamiento del personal durante la estancia en las instalaciones.

8.3.5. Seguridad de los equipos

Los equipos informáticos son un activo importante del que depende la continuidad de las actividades, por lo que serán protegidos de manera adecuada y eficaz.

Los equipos informáticos de **SECURITY SERVICES KUO; S.L.** están protegidos contra posibles fallos de energía (ordenador portátil con batería, etc.).

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones recomendadas por el suministrador. Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación. También será necesario adoptar las medidas de precaución necesarias en caso de los equipos deban abandonar las instalaciones para su mantenimiento.

8.3.6. Gestión de comunicaciones y operaciones

8.3.7. Procedimientos operativos y responsabilidades

SECURITY SERVICES KUO; S.L. controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red de **SECURITY SERVICES KUO; S.L.** y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red existirán mecanismos para limitar los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del dominio. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo a estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

En algunos casos será necesario que distintas áreas estén lógicamente separadas del resto para evitar accesos no autorizados.

8.3.8. Protección frente a código malicioso y código móvil

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 **SECURITY SERVICES KUO; S.L.**

Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado por el Responsable de Seguridad y autorizado por el comité.

El Administrador del Sistema instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, 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.

8.3.9. Copias de seguridad

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

8.3.10. Gestión de la seguridad de la red

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.

Existirá una gestión gráfica de la red de forma que su mantenimiento pueda resultar más cómodo.

8.3.11. Gestión de soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes que pudieran contener información sensible que a los ficheros de donde han sido extraídos.

8.3.12. Intercambio de información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, fax, etc.).

8.3.13. Seguimiento

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para

asegurar el cumplimiento con la política establecida y los procedimientos operativos, así como para recomendar cualquier cambio que se estime necesario.

8.4. Control de accesos

8.4.1.1. *Requisitos del servicio para el control de accesos*

La información debe estar protegida contra accesos no autorizados. El Responsable del Servicio definirá las necesidades de acceso a la información a dos niveles, para el conjunto de áreas y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

8.4.1.2. *Gestión de accesos de los usuarios*

El administrador del sistema es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.

Cada usuario deberá estar asociado a un perfil, de acuerdo a las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a información y sistemas que no le son necesarios para las competencias de su trabajo.

8.4.1.3. *Responsabilidades del usuario*

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado, así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

8.4.1.4. *Control de acceso a la red*

No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con **SECURITY SERVICES KUO; S.L.** para mantener el mismo nivel de seguridad que si fueran empleados de la propia organización.

8.4.1.5. *Informática móvil y teletrabajo*

Cuando los equipos o la información propiedad de **SECURITY SERVICES KUO; S.L.** están fuera de las instalaciones, es el empleado que los está utilizando el que debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

8.4.1.6. *Gestión de incidencias*

Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios

de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Servicio de Informática para que tome las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

8.4.1.7. Continuidad del servicio

Es imprescindible para **SECURITY SERVICES KUO; S.L.** establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad de la actividad en estos casos, **SECURITY SERVICES KUO; S.L.** establecerá planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del servicio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia que deberán probarse y actualizarse regularmente para comprobar su idoneidad.

La gestión de la continuidad del servicio se incorporará a los procesos de **SECURITY SERVICES KUO; S.L.** y será responsabilidad de una o varias personas dentro de la entidad.

9. OBLIGACIONES DEL PERSONAL

Todos los miembros de **SECURITY SERVICES KUO; S.L.** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **SECURITY SERVICES KUO; S.L.** recibirán concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **SECURITY SERVICES KUO; S.L.**, 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. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.



10. TERCERAS PARTES

Cuando **SECURITY SERVICES KUO; S.L.** preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **SECURITY SERVICES KUO; S.L.** utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que atañe 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.

Cuando algún aspecto de la Política 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.