Manual de Políticas Seguridad de la información

DEPARTAMENTO DE CALIDAD GRUPO SURESTE

Clasificación de la información	DIFUSIÓN LIMITADA
Ámbito de difusión	Partes implicadas y con responsabilidades en el presente procedimiento
Propietario	Dirección

1. OBJETIVO Y ALCANCE DEL MANUAL DE POLÍTICAS DE SEGURIDAD

Este documento recopila todas las políticas de Seguridad de la Información que aplican en Grupo Sureste.

2. ÁMBITO DE APLICACIÓN

El presente documento aplica a todo el personal y sistemas de gestión de Grupo Sureste, que está integrado por las siguientes sociedades:

- Sureste Seguridad, SL B30376982
- Sureste Facility Services, SL B73435018
- Grupo Sureste Central Office, SL B73937757

El presente documento se mantendrá en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

3. NORMAS Y DOCUMENTOS DE REFERENCIA

- UNE-ISO/IEC 27001 Requisitos de sistemas de Gestión de Seguridad de la Información (ISO27001)
- UNE-ISO/IEC 27002: Código de buenas prácticas para controles de Seguridad de la Información (ISO27002)
- 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- RGPD)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Real Decreto 311/2022 de Esquema Nacional de Seguridad.

4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN (PSI)

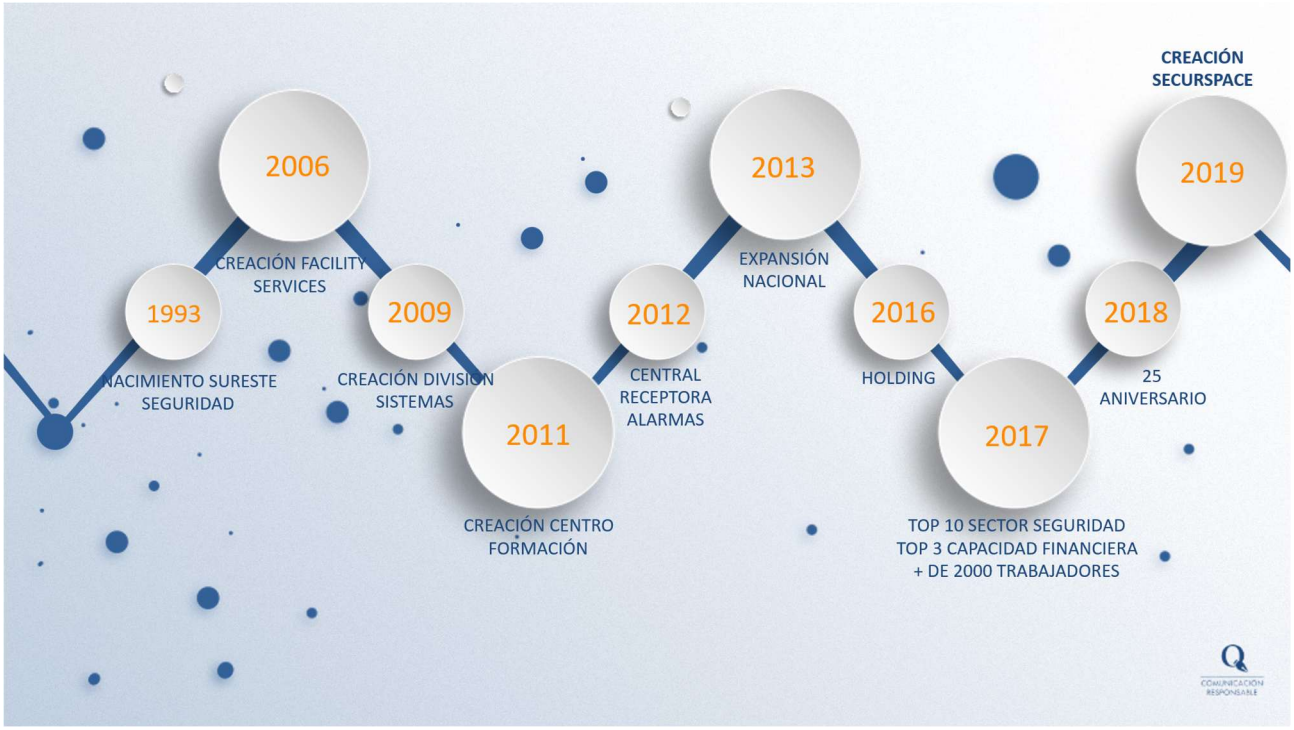
INTRODUCCIÓN

Han transcurrido 30 años desde el inicio de nuestra andadura, un camino largo, no exento de dificultades y de aprendizaje constante. Éxitos y fracasos que al final son el patrimonio empresarial de un gran equipo humano que ha sabido afrontar con profesionalidad retos y proyectos enriquecedores.

Nuestra principal premisa ha sido la de mantener esa esencia que ha sido el motor que nos ha permitido llegar a esta primera meta de nuestra andadura, cumplir 30 años en el sector,

siendo un referente a nivel nacional, convirtiéndonos en un holding sólido y solvente que garantiza día a día servicios de la máxima calidad. Y con un reto importante para este 2023, la certificación ENS que radica en garantizar la seguridad de todos los sistemas que interactúan, sin dejar resquicios para fugas de información y vulnerabilidades.

En nuestra larga trayectoria profesional, la especialización ha sido la prestación de servicios de seguridad física, ha dado como fruto una serie de divisiones dentro del área de seguridad física. Aplicación de diferentes parámetros de actividad, de control y desarrollo de los servicios, así como de estándares de calidad, que definen cada una de ellas.



En definitiva, Sureste Seguridad, S.L. es una empresa dedicada a:

A. La vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como de las personas que pudieran encontrarse en los mismos.

B. El acompañamiento, defensa y protección de personas físicas determinadas, incluidas las que ostenten la condición legal de autoridad.

C. La instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o centros de control o de vigilancia.

D. La explotación de centrales para la conexión, recepción, verificación y, en su caso, respuesta y transmisión de las señales de alarma, así como la monitorización de cualesquiera señales de dispositivos auxiliares para la seguridad de personas, de bienes muebles o inmuebles o de cumplimiento de medidas impuestas, y la comunicación a las Fuerzas y Cuerpos de seguridad competentes en estos casos.

En Sureste Seguridad, S.L. disponemos de una amplia solvencia técnica, profesional y financiera, para abordar proyectos de envergadura, avalados por nuestra dilatada experiencia en la prestación de servicios de seguridad. Esta solvencia ha permitido que en los últimos años nos hayamos posicionado dentro de las 10 empresas más importantes del sector y siendo miembros la patronal del sector APROSER, Asociación Profesional de Compañías Privadas de Servicios de Seguridad.

Nuestra presencia en el ámbito público y privado es importante, teniendo clientes de la talla de Metro de Madrid, Aeropuertos de Aena en: Málaga, Granada, Valencia, Reus, Zaragoza, Murcia, Girona), servicio de vigilancia en el Ministerio de Defensa, Renfe en Cataluña, Carrefour en el Levante, el Servicio Murciano de Salud, Correos en Canarias, …

Sureste Seguridad, S.L. ofrece servicios donde las expectativas y los requisitos de los clientes son muy exigentes y además redundan el servicio que reciben los ciudadanos.

El sector de la vigilancia privada requiere que el enfoque de concepción de los procesos y sistemas de información evolucionen y se adapten a un mundo cada vez más competitivo y cambiante.

Nuestra experiencia nos permite desarrollar proyectos para grandes empresas y corporaciones, estableciendo el control de los procesos y la centralización de la información durante todas las fases del servicio, desde la planificación, realización y evolución, etc..

Sureste Seguridad, S.L. trabaja con los sistemas TIC (Tecnologías de Información y Comunicaciones) para prestar sus servicios. A tenor de ello los sistemas deben ser administrados 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.

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 TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, 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 mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, 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.

SURESTE SEGURIDAD, S.L. está preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

PRINCIPIOS Y DIRECTRICES

✓ PREVENCIÓN

SURESTE SEGURIAD, 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 implementa las medidas mínimas de seguridad determinadas por el ENS, 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, SURESTE SEGURIAD, S.L.

Autoriza los sistemas antes de entrar en operación.

Evalúa regularmente la seguridad, incluyendo evaluaciones 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

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios se monitorizan 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.

Se establecen mecanismos de detección, análisis y reporte que llegan a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

✓ RESPUESTA

SURESTE SEGURIDAD, 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.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias

✓ RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, SURESTE SEGURIDAD, S.L ha desarrollado un Plan de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

ALCANCE

Esta Política se aplica a los sistemas TIC de SURESTE SEGURIDAD, S.L que se encuentran dentro del alcance del Esquema Nacional de Seguridad y a todos los miembros de la organización, sin excepciones. También se aplica sobre personal en prácticas y personal externo que puedan participar en los procesos de negocio de manera directa o indirecta.

La Política de Seguridad es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

1. Primer nivel: Política de Seguridad de la Información: Constituye el primer nivel la Política de Seguridad de la Información, recogida en el presente texto. La Política de Seguridad requiere la aprobación por parte del Responsable de Seguridad

2. Segundo nivel: Normativa de Seguridad de la Información: El segundo nivel desarrolla la Política de Seguridad de la Información mediante instrucciones específicas que abarcan un área o aspecto determinado de la seguridad de la información. Las Instrucciones se estructurarán en normativas y son aprobadas por el Responsable de seguridad.

3. Tercer nivel: Procedimientos de Seguridad de la Información: El tercer nivel está constituido por directrices de carácter técnico o procedimental que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios.

Los procedimientos son aprobados por el Responsable de Seguridad de la Información.

El personal de SURESTE SEGURIDAD tiene la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Instrucciones y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones.

La Política, las Normativas y los Procedimientos de Seguridad de la información están disponibles en la Intranet de la organización.

MISIÓN

En SURESTE SEGURIDAD, S.L. somos conscientes que todas las empresas tienen diferentes necesidades y problemáticas a solucionar.

Es por esto que, como expertos, nos apoyamos en nuestro conocimiento y bagaje profesional, para ofrecer soluciones que cubran estas necesidades rentabilizando al máximo las inversiones.

ORGANIZACIÓN DE LA SEGURIDAD

Mediante la estructuración de nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión se base en los siguientes documentos:

Documentos Internos: los generados por el propio sistema de gestión.

Documentos Externos: documentos necesarios para el correcto desarrollo del SGSI, no elaborados por la SURESTE SEGURIDAD. S.L.. como: legislación, normas, guías CCN STIC etc. Y además existen dos tipos de registros:

Registros internos: los generados por el propio SGSI.

Registros externos: registros recibidos del exterior (clientes, administración, proveedores, ...)

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

CONSTITUCIÓN

El Comité de Seguridad de la Información, en adelante el "Comité", asume los roles de Responsable de la Información y Responsable del Servicio.

El Comité presenta estructura orgánica y está formado por delegados de las partes interesadas en la óptima gestión de la Seguridad de la Información. La postura oficial del Comité ante cuestiones sometidas a votación será delimitada por mayoría simple.

FUNCIONES Y RESPONSABILIDADES

- El Comité de Seguridad de la Información reportará a la Alta Dirección sus propuestas y decisiones en aquellas áreas que le competen. El Comité tendrá las siguientes funciones:
- Atender las inquietudes de los socios y de los diferentes departamentos de la empresa.
- Informar regularmente del estado de la seguridad de la información a los socios de la empresa.
- 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, 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 Junta General de Socios.
- 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 respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad 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 la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- 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.

ROLES Y RESPONSABILIDADES

- ROLES

Los roles del Esquema Nacional de Seguridad se asignan de la siguiente forma:

FIGURA RESPONSABLE	ROL	FUNCIONES Y RESPONSABILIDADES
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Responsable de la información	Tratamiento / Protección de la información
	Responsable del servicio	Definir requisitos de seguridad de los servicios prestados
RESPONSABLE DE SEGURIDAD	Responsable de la Seguridad	Responsable del Cumplimiento ENS
RESPONSABLE DEL SISTEMA	Responsable del sistema	Mantenimiento y continuidad de los Sistemas

		Monitorización y configuración de medidas de Seguridad

- FUNCIONES Y RESPONSABILIDADES

El **Comité de Seguridad** como responsable de la información será el propietario de la misma y tendrá las siguientes funciones;

- Clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), dentro del marco establecido en el Anexo I del ENS.

  Trabajar en colaboración con el responsable de seguridad y el del sistema en el mantenimiento de los servicios de administración electrónica catalogados.

- Apoyar la realización de los análisis de riesgos y valorar las diferentes opciones de gestión del riesgo a implantar.

- Valorar y decidir, junto con los responsables de los Servicios, los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes que puedan tener acceso a información de los procedimientos administrativos que gestiona y realizar el seguimiento de su cumplimiento

El Comité de Seguridad como responsable del servicio será quien determine los requisitos de los servicios prestados, en consonancia, tendrá las siguientes funciones:

- Establecer los requisitos del servicio en materia de seguridad, o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.

- Clasificar los servicios conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), dentro del marco establecido en el Anexo I del ENS.

- Atender a los requisitos de seguridad de la información, tales como disponibilidad, accesibilidad, interoperabilidad, etc. que se demanden en la prestación de los servicios.

- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes que puedan afectar a sus servicios y realizar el seguimiento de su cumplimiento

El **Responsable de Seguridad** será quien tome las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios. Dispondrá de las siguientes funciones:

- Supervisar el cumplimiento de la presente Política, de sus normas y procedimientos derivados.

- Asesorar en materia de seguridad a los integrantes del Comité de Seguridad que así lo requieran.
- Coordinar la interacción con otros organismos especializados.
- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
- Establecer las medidas de seguridad adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
- Asesorar, en colaboración con los Responsables de los Sistemas, los Responsables de los Servicios y de la Información, en la realización del análisis y gestión de riesgos, elevando el informe resultante al Comité de Seguridad.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones Comité de Seguridad en materia de seguridad.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
- Elaboración y revisión de la normativa de seguridad Comité de Seguridad.
- Aprobación de los procedimientos de seguridad elaborados por el Responsable del Sistema.

El **Responsable del Sistema**, dentro de sus áreas de actuación, tendrán asignadas las siguientes funciones:

- Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Elaborar procedimientos técnicos de seguridad de los sistemas de información.
- Elaborar planes de continuidad de los sistemas de información.
- Colaborar para la realización del análisis de riesgos de los sistemas de información de los que es responsable.

- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.

- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información

El Comité Seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por él.

Las funciones y responsabilidades listadas en este apartado podrán ser delegadas tal como estipula la Guía de Adecuación 801 sobre Responsabilidades y Funciones en el Esquema Nacional de Seguridad.

En caso de conflicto entre los diferentes responsables, éste será resuelto por el Comité de seguridad.

Todo usuario tendrá la obligación de reportar los incidentes en materia de seguridad utilizando las directrices marcadas por la SURESTE DE SEGURIDAD, S.L.

Está política se complementa con el resto de políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

PROCEDIMIENTOS DE DESIGNACIÓN Y RENOVACION

El Responsable de Seguridad de la Información será nombrado por la Alta Dirección a propuesta del Comité de Seguridad de la Información. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Los roles de Seguridad a nivel transversal serán nombrados por la Alta Dirección, a propuesta del Comité de Seguridad, y pasarán a formar parte del mismo.

Los roles de seguridad específicos de cada área serán nombrados por la Alta Dirección a propuesta del Comité de Seguridad, pero podrá delegar su nombramiento en los Directores de dichas áreas. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

DATOS DE CARÁCTER PERSONAL

SURESTE SEGURIDAD sólo 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. Estas medidas, recogidas en la documentación de seguridad que da cumplimiento a la normativa vigente, se integrarán en los procedimientos y su correspondiente gestión documental de la Seguridad de la Información de SURESTE SEGURIDAD.

En su compromiso con la Protección de Datos SURESTE SEGURIDAD ha nombrado a una persona externa como Delegado de Protección de Datos.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, REVISIÓN Y MEJORAS.

Esta Política de Seguridad de la Información complementa las otras políticas de SURESTE SEGURIDAD entre las que figuran la de Calidad y Medio Ambiente y de cumplimiento de la normativa de protección de datos.

La Política de Seguridad se desarrollará por medio de normativa y procedimientos de seguridad que afronten aspectos específicos siguiendo los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

h) Mínimo privilegio.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de la actividad y detección de código dañino.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad.

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Anualmente se revisará esta Política, así como los procedimientos, medidas de seguridad, análisis de riesgo y plan de tratamiento. De esta revisión se extraerán y tratarán aquellas mejoras que sean necesarias o convenientes para el desarrollo del Sistema de Seguridad e la Información. El Comité establecerá en sus reuniones y a través de las actas de las mismas las decisiones adoptadas tras las revisiones del SI, así como las mejoras implantadas, los responsables de su implantación y los recursos asignados para llevarlas a cabo

TERCERAS PARTES

Las terceras partes relacionadas con SURESTE SEGURIDAD, dentro del alcance, firman con la empresa un acuerdo que protege la información intercambiada.

Cuando SURESTE SEGURIDAD utilice servicios de terceros o ceda información a terceros, además de trasladarles las obligaciones contractuales adquiridas con el cliente, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

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.

OBLIGACIONES DEL PERSONAL

Todos los miembros de SURESTE SEURIDAD 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 TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de SURESTE SEGURIDAD. atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. 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. 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

16.1. Comunicación de la política

La distribución de las Políticas y sus modificaciones se realizará a través de la página web de la Organización.

El Responsable de calidad debe asegurarse de que todos los empleados de Grupo Sureste, como también los participantes externos correspondientes, estén familiarizados con estas Políticas.

16.2. Apoyo a la implementación del SGSI

A través del presente, dirección declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

16.3. Sanciones

Cualquier violación premeditada o negligente de las políticas y normas de seguridad y que suponga un potencial daño, consumado o no a Grupo Sureste, será sancionada de acuerdo a los mecanismos habilitados en el convenio de Empresa y en la normativa legal, contractual y corporativa vigentes.

Todas las acciones en las que se comprometa la seguridad de Grupo Sureste y que no estén previstas en esta política, deberán ser revisadas por la Dirección Ejecutiva y por el Comité de seguridad para dictar una resolución sujetándose al criterio de la empresa y la legislación prevista.

Las acciones disciplinarias en respuesta a los incumplimientos de las Políticas de Seguridad de la Información son atribución de la Dirección Ejecutiva de Grupo Sureste y de los órganos de gobierno según la legislación aplicable.

16.4. Aprobación y revisión de la política de seguridad de información

Es labor del personal implicado la revisión periódica de la PSI y de la PENS y su comunicación a la dirección para su aprobación, así como la puesta en conocimiento de la misma al resto de la organización.

La PSI y la PENS se revisará periódicamente, **no superando el plazo de un año**, además, se realizará una revisión como respuesta a cambios relevantes en el entorno de la organización, circunstancias de negocio, condiciones legales y/o del entorno técnico, así como tras la detección de oportunidades de mejora de esta política.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN SUMINISTRADORES

Ponemos en conocimiento de nuestros proveedores la existencia de Directrices de Seguridad de la Información establecidas en nuestra organización para mostrar el compromiso de Grupo Sureste en la protección y garantía de los principios de: confidencialidad, integridad, autenticidad y disponibilidad de la información manejada en la Corporación.

Trabajamos bajo un Sistema de Gestión de Seguridad de la Información, cuyo alcance no sólo afecta al uso de los activos, sino que se extiende a todas las personas y terceros en el conocimiento y cumplimiento de estas Directrices estructuradas acorde a las normas ISO/IEC 27001:2013 y el Real Decreto 311/2022. Tanto la Política como las Directrices de Seguridad de la Información, están en línea con el 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 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDyGDD)

Esta regulación en materia de seguridad incide en los siguientes campos de la organización:

Acceso a las instalaciones. En la que se regulan las normas de acceso, haciendo especial mención a los accesos a áreas seguras y regulación del acceso a personas ajenas a la organización.

Acceso a la red corporativa. Los recursos corporativos son protegidos con los medios de seguridad técnicos necesarios para asegurar la protección de la información, ya sea desde las propias instalaciones o de forma externa. El acceso y el uso de la información están reguladas por normas enfocadas a la protección con especial atención a información sensible o confidencial.

Uso de los activos. Las personas que accedan a información de Grupo Sureste, se comprometen a hacer un uso racional y velar por el cuidado de los equipos proporcionados por la organización para el desempeño de sus funciones y tareas. En este sentido se describen normas de actuación y se aplican configuraciones encaminadas a la protección de la información contenida en estos dispositivos.

Uso de Internet. Especial atención se realiza en la regulación del uso de Internet, correo electrónico y almacenamiento en la nube a usos profesionales con el objetivo de minimizar riesgos que puedan producirse con un uso no regulado de dichas herramientas.

Gestión de incidencias. Ayudar a detectar posibles problemas que puedan poner en peligro la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los servicios o activos que soportan.

Continuidad de negocio. Todos los medios implantados para la disponibilidad y continuidad del negocio irán en línea con los requerimientos de los esquemas ISO certificados en la organización.

Propiedad intelectual. Protegida con el compromiso del personal de Grupo Sureste conforme a las normas de confidencialidad de la Organización.

La violación de las Política y la Normativa de Seguridad está sujetas a sanción de acuerdo a los mecanismos habilitados en la legislación vigente.

Tanto las Políticas como la Normativa de Seguridad son revisadas periódicamente para alinearlas con las necesidades de la organización.

La Gerencia conoce la importancia de estas Políticas y participa activamente en la revisión de las mismas.

6. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

La seguridad de la información se integrará en los métodos de gestión de proyectos para asegurar que los riesgos en seguridad de la información se identifican y se contemplan en el proyecto, exigiendo que se consideren los objetivos en seguridad de la información, que se evalúen los riesgos en una fase temprana del proyecto y que aplique a todas las fases de desarrollo del mismo, teniendo en consideración:

a) El enfoque del riesgo: Se realizará una evaluación de riesgos de seguridad de la información en una fase temprana del proyecto para identificar los controles necesarios.

b) Responsabilidad proactiva: La seguridad de la información se aplicará a todas las fases del proyecto, identificando para la realización de la misma los controles necesarios para la consecución de la misma.

16.1. Privacidad y protección de datos desde el diseño y por defecto

La organización tomará medidas organizativas y técnicas para integrar garantías que permitan aplicar de forma efectiva los principios del RGPD en el mismo momento en que se diseña un tratamiento, un producto o servicio que implique el tratamiento de datos personales. Esto implica que en las primeras fases de diseño de un nuevo proyecto o actividad de tratamiento será necesario incluir una etapa de estudio de las implicaciones en protección de datos y cómo minimizar riesgos para la entidad y para los derechos y libertades de las personas de las que se traten sus datos, y en particular su derecho a la protección de datos.

Los responsables deben adoptar medidas que garanticen que solo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.

Cualquier nuevo tratamiento de información susceptible de tratar datos de carácter personal, requerirá una aprobación previa por parte del Comité de seguridad y en todo caso la puesta en conocimiento del Delegado de Protección de Datos.

7. ORGANIZACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN

16.1. Organización interna

Se distinguirán y asignarán roles y responsabilidades en seguridad de la información. Las responsabilidades podrán delegarse, sin que ello implique que deje de ser responsable de las mismas.

La funciones y áreas de responsabilidad se segregarán para reducir posibilidad de incidentes en seguridad de la información.

Se establecerá contacto con las autoridades y con grupos de interés especial.

La seguridad de la información deberá tratarse dentro de la gestión de cualquier proyecto, independientemente de su naturaleza.

16.2. Uso de dispositivos móviles

El uso de dispositivos móviles para el tratamiento de datos en la organización está permitido según el puesto de trabajo del personal empleado, que utilizará sus credenciales para el acceso a dicha información.

Por defecto, se optará por usar el modelo de movilidad empresarial COBO (Company Owned Business Only). Esto implica que los usuarios no podrán hacer un uso privado de los dispositivos móviles facilitados por la entidad.

Los usuarios se responsabilizarán del cuidado de los dispositivos que le entregue la organización comprometiéndose al cumplimiento de las políticas y normativa que aplique. De forma general, no se puede tener información privada o confidencial en los dispositivos móviles de la organización.

El uso de dispositivos móviles personales para el desempeño de las funciones en la organización (BYOD Bring Your Own Device) será excepcional. Los datos de la organización que se almacenan, transfieren o procesan en BYOD siguen perteneciendo a la organización, y mantiene el derecho a controlar (ver, editar y borrar) todos los datos de la organización que se encuentran almacenados, transferidos o procesados en BYOD, aunque no sea propietaria del dispositivo.

16.3. Teletrabajo

El teletrabajo se realizará garantizando que las medidas de seguridad, como mínimo, equivalentes a las medidas de seguridad en local y garantizando la confidencialidad de la comunicación.

El teletrabajo requiere de autorización previa.

El procedimiento para su gestión se desarrollará en un procedimiento independiente.

8. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

Los empleados y contratistas que puedan acceder a información o sistemas de la organización deberán entender sus responsabilidades en seguridad de la información y ser adecuados para las funciones para las que se consideran. Para ello se realizarán actuaciones de investigación de antecedentes de acuerdo a las leyes, normas y códigos éticos que nos apliquen y proporcional a las necesidades del negocio y de forma que se asegure que es confiable para el puesto al que se le designa.

El personal deberá ser informado y concienciado del tratamiento de su información personal, así como de sus obligaciones de confidencialidad durante y después del empleo y de la obligación del cumplimiento de la normativa de seguridad y protección de datos. Periódicamente, cuando se produzcan cambios en la normativa, o si como consecuencia de las revisiones o auditorías efectuadas se detectaran carencias en la aplicación de las políticas y procedimientos de seguridad, los usuarios serán notificados.

Si el personal provoca una brecha de seguridad o un incidente con los datos personales de la entidad, la organización podrá iniciar un proceso disciplinario, cuya respuesta valorará la naturaleza y gravedad de la violación, el impacto, la reincidencia y la formación recibida y compromisos asumidos.

Se protegerá los intereses de la organización en cualquier proceso de cambio de puesto de trabajo o finalización del empleo retirando los activos entregados y los permisos de acceso que sean pertinentes, tan pronto como sea posible, una vez que se conozca la finalización de un puesto de trabajo o el cambio.

9. ACTIVOS DE INFORMACIÓN

16.1. Responsabilidad sobre los activos de información

Cualquier activo de información susceptible de ser usado por el personal empleado debe ser previamente inventariado, identificando su responsable, analizando su relevancia en el ciclo de vida de la información de la organización y los riesgos que su uso conlleva. El Propietario del activo será el responsable de aplicar la seguridad adecuada al mismo atendiendo al análisis de riesgos del activo, y el cumplimiento de la normativa de seguridad.

Las medidas de seguridad aplicables a los soportes que contengan información se ajustarán a la confidencialidad de la información que contienen.

La persona que se encuentre a cargo de información proceso de revisión o tramitación, ya sea previo o posterior a su registro y archivo, deberá custodiarla e impedir en todo momento que pueda acceder persona no autorizada.

16.2. Política de Clasificación, etiquetado y manipulación de la información

Clasificación de la información

A continuación, se detalla la clasificación de la información relativa a los tratamientos realizados por la organización, la aplicación de las medidas de seguridad se realizará en base a dicha clasificación:

1. PÚBLICA: Cualquier material de la empresa sin restricciones de difusión. Por ejemplo, información publicada en la página web o materiales comerciales, …

2. DIFUSIÓN LIMITADA: La información de difusión limitada, normalmente es de uso interno, pero puede ser compartida entre los usuarios (contratados y subcontratados que hayan firmado acuerdo de confidencialidad), y puede ser compartida entre las partes interesadas (clientes, proveedores, etc.) con algún tipo de contrato o acuerdo marco de colaboración.

A título meramente enunciativo, dentro del grado de clasificación "Difusión limitada" encontramos: documentos que forman el marco documental del Sistema de Gestión de Seguridad de la Información, procedimientos de operación y otra documentación interna.

3. CONFIDENCIAL: Esta información debe ser únicamente compartida entre personal seleccionado que necesite ser conocedor de la misma.

A título meramente enunciativo, dentro del grado de clasificación "Confidencial" encontramos: modos de operación o "know-how", procesos, técnicas, estrategias, mejoras, invenciones (sean o no patentables), trabajos de autor, planes de desarrollos técnicos, de negocio, financieros, de clientes, de proveedores, de marketing y de producto, previsiones, los salarios y términos de retribución de los empleados, listas de clientes y proveedores, contratos o conocimientos de clientes o futuros clientes o proveedores o futuros proveedores de la Corporación o cualquier compañía vinculada a GRUPO SURESTE y cualquier otra información concerniente a los productos, servicios, negocios, investigación o desarrollo de GRUPO SURESTE, de todas las sociedades vinculadas así como cualquier información que el trabajador haya recibido de forma confidencial por parte de GRUPO SURESTE o por cualquier sociedad vinculada a ésta.

Por su parte, los datos de carácter personal bajo el ámbito de aplicación de la legislación vigente en materia de protección de datos, son considerados Información Clasificada – Confidencial.

Toda información no identificada de otra forma debe entenderse como difusión limitada.

Sin importar el nivel de clasificación de la información, ésta ha de estar siempre accesible por la Dirección de Grupo Sureste.

La clasificación de la información es un acto formal, y no puede ser realizada por los usuarios. Sólo pueden proponerla, y elevarla para aprobación, al Comité de Seguridad. Esta estructura organizacional es quién decide sobre la clasificación, así como de su desclasificación en etapas posteriores.

Etiquetado de la información y Manipulación de la información.

- Clasificación de la información.

10. POLÍTICA DE CONTROL DE ACCESO

El acceso a la información, en todo lo que no esté específicamente permitido, se regirá por el principio de "la necesidad de conocer/usar" es decir los usuarios tendrán acceso únicamente a la información o recursos necesarios para su tratamiento que precisen para el desarrollo de sus funciones. Si no está expresamente permitido se debe entender por prohibido dicho acceso.

El acceso a la información atenderá igualmente a:

- Las limitaciones de acuerdo a la política de clasificación de la información
- Los acuerdos con terceros (contratos, acuerdos de nivel de servicio, NDAs, etc.)

- La legislación aplicable, en concreto a normativa de protección de datos de carácter personal.
- Los derechos y restricciones de acceso a los distintos roles de usuarios.

El control de acceso se realizará mediante la aproximación basada en roles, vinculando los derechos de acceso a las funciones desempeñadas en la organización.

La identificación de los usuarios con acceso a los sistemas de información se realizará de forma inequívoca y personalizada, verificando su autorización. La información de autenticación es confidencial, personal e intransferible, y su distribución y almacenamiento deberá garantizar esa confidencialidad. El usuario es responsable de la confidencialidad de la información de autenticación, prohibiéndose expresamente el acceso al sistema utilizando el identificador y la contraseña de otro usuario. En todo caso, la responsabilidad sobre el acceso realizado recaerá siempre sobre el usuario que tuviera asignado el identificador y la contraseña utilizada.

Para aquellos accesos a sistemas, aplicaciones o equipos que se encuentren dentro del alcance del Esquema Nacional de Seguridad la identificación y el acceso se realizará además de con el identificador y contraseña con un doble factor de autenticación.

El acceso físico a las instalaciones de Grupo Sureste estará restringido. El personal no autorizado para acceder a las instalaciones, en caso de necesitar acceder, requerirá estar acompañado en todo momento por personal autorizado.

11. CRIPTOGRAFÍA

16.1. Certificados Digitales Públicos

Todo sitio o servicio accesible desde Internet cuya URL incluya dominios de Grupo Sureste deberá estar protegido mediante certificado que proteja el acceso al servicio mediante SSL, o protocolo equivalente. Esto incluye las webs públicas del grupo además de cualquier servicio de acceso público que requiera validación por el Empleado, Colaborador o Cliente mediante HTTPS y FTPS.

16.2. Certificados Digitales Privados

En caso de crear y habilitar una VNP, todo empleado, colaborador o proveedor con dicho acceso mediante VPN al entorno corporativo dispondrá de un certificado privado nominativo asignado, que valida su acceso al entorno de forma remota vía VPN. El certificado no se podrá ceder a nadie y tendrá una validez máxima 12 meses

12. SEGURIDAD FÍSICA Y DEL ENTORNO

Se debe evitar la pérdida, daño, robo o compromiso de los activos y la posible interrupción de las actividades de Grupo Sureste. Se debe proteger los equipos de amenazas físicas y ambientales.

Se debe prevenir el acceso físico no autorizado a las instalaciones y a los recursos de tratamiento de información, a la vez se garantiza el acceso a los usuarios autorizados.

Los usuarios limitarán la posibilidad de acceso no autorizado a los equipos de los que son responsables o usuarios, asegurando no dejar los equipos desatendidos sin la protección adecuada y teniendo un entorno de trabajo despejado de papeles, soportes extraíbles de información y un escritorio de sistema equivalentemente limpio.

13. SEGURIDAD EN LAS OPERACIONES

El personal estará obligado a cumplir con todos los procedimientos e instrucciones de trabajo que describan los procesos operacionales de la organización y que les sean comunicados.

14. SEGURIDAD EN LAS COMUNICACIONES

Las comunicaciones que permitan el intercambio de información deben garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales. Para ello el Responsable de Seguridad Técnico definirá las pautas para garantizar la seguridad de los servicios de red de Grupo Sureste, tanto públicos como privados, teniendo en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.
- Revisar periódicamente su configuración.

16.1. Intercambio de información. Mensajería y Correo electrónico

Cuando se realicen acuerdos entre organizaciones para el intercambio de información digital y software, se especificarán el grado de sensibilidad de la información del Organismo involucrado y las consideraciones de seguridad sobre la misma.

Se prohíbe la comunicación de información confidencial fuera de la organización salvo aprobación expresa por parte del comité de seguridad una vez aplicadas las medidas de seguridad que recomiende.

Las cuentas de mensajería o correo electrónico de la organización nunca se considerarán personales o privadas.

No se autoriza la creación de cuentas de correo electrónico fuera del dominio de la organización, salvo autorización del comité de seguridad, quién se encargará de tener posibilidad de acceso a las mismas.

Se prohíbe la utilización de las herramientas de mensajería y del correo electrónico corporativo para usos personales o particulares. Se consideran herramientas de trabajo, y como tal podrán ser revisadas en caso de incidencia, y desviado en caso de ausencia o baja del trabajador, sin necesidad de previo aviso.

El correo electrónico no puede ser empleado para la transmisión de datos protegidos ni para fines diferentes a los establecidos para el correcto desarrollo de sus funciones laborales.

Todo el personal o terceros que accedan a la información de la organización tendrán que aceptar un acuerdo de confidencialidad y no revelación de la información a la que puedan tener acceso.

15. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO.

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. Durante el análisis y diseño de los procesos que soportan estas aplicaciones, se deben identificar los requerimientos de seguridad para incorporar durante las etapas de desarrollo e implementación.

Dado que los analistas y programadores tienen el conocimiento de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas

personas u otras que puedan operar sobre los sistemas, las bases de datos y plataformas de software de base y, en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, sistemas operativos y software de base en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que, en general, los aplicativos se asientan sobre este tipo de software.

La organización controlará que todo software o sistema de información desarrollado interna o externamente cumplan con los lineamientos de desarrollo seguro, tales como:

- Control de Cambios en los sistemas/software.
- Principios de Construcción Seguros.
- Ambientes de desarrollo seguro.
- Pruebas de seguridad.
- Pruebas de aceptación.
- Protección de datos de prueba.

16. RELACIÓN CON PROVEEDORES

Los proveedores o cualquier otro usuario que pueda acceder a la información que no sea pública, estará obligado igualmente a firmar los compromisos de confidencialidad.

En el caso de que el servicio implique el tratamiento de datos personales se deberá establecer un contrato de encargo de tratamiento que establezca las finalidades del tratamiento y las condiciones en las que el mismo se ha de realizar por parte del prestador.

16.1. COMPROBACIÓN PREVIA

La organización elegirá únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas. En caso de que implique tratamiento de datos personales, deberá ser conforme a la legislación de protección de datos, garantizando los derechos de los interesados y la confidencialidad de dicho tratamiento. Para ello se solicitará con carácter previo a la contratación, certificación expedida por terceros de confianza que acredite el cumplimento de la normativa, o bien muestra del último informe de auditoría, o una declaración responsable. Con carácter excepcional se puede sustituir por un control realizado por el responsable.

Esta comprobación previa no será aplicable en el caso de que los servicios vayan a ser prestados en la sede de la organización, y sujetos a la normativa implantada por ésta.

Cualquier contratación que implique el tratamiento de datos personales deberá comunicarse al delegado de protección de datos para efectuar el control de esta relación y en su caso anotarlo en el registro de actividades de tratamiento.

16.2. CONTRATACIÓN

La contratación de terceros deberá realizarse incluyendo las especificaciones legales previstas en la normativa de protección de datos.

La cadena de subcontrataciones deberá disponer de garantías equivalentes a las que se le exijan al proveedor.

Cualquier contratación que implique el tratamiento de datos personales será comunicada al DPO de Grupo Sureste en el correo electrónico dpo@gruposureste.es para la redacción y seguimiento del mismo.

16.3. SUPERVISIÓN Y REVISIÓN

Todos los incidentes de seguridad relacionados con el trabajo del proveedor deben ser elevados inmediatamente a la persona responsable, que será diferente dependiendo del tipo de incidencia.

16.4. FINALIZACIÓN DE SERVICIO DEL PROVEEDOR

Cuando finalice la relación contractual, se deberán tener en cuenta los siguientes aspectos:

- ✓ Se deben eliminar los derechos de acceso para los empleados del proveedor de acuerdo a la Política de control de acceso.
- ✓ El propietario del contrato debe asegurarse de que todo el equipamiento, software o información en formato electrónico o papel sea devuelto.

17. GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

Cualquier usuario, si tiene conocimiento de incidencia de seguridad de la información, es responsable de la comunicación de la misma. Si la incidencia puede constituir un riesgo para los derechos y libertades de las personas se comunicará una violación de seguridad de datos de carácter personal al Delegado de Protección de Datos.

En caso de que las incidencias tengan tal relevancia que pueda afectar a seriamente a la organización se evaluará la activación de planes de continuidad de negocio, garantizando en todo caso la continuidad de la seguridad de la información.