# MARCO ORGANIZATIVO

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

# ESQUEMA NACIONAL DE SEGURIDAD

| | |
|---|---|
| Clasificación de la información | DIFUSIÓN ILIMITADA |
| Ámbito de difusión | Usuarios con acceso al sistema de información |
| Propietario | Responsable de seguridad técnico |

## Contenido

1. INTRODUCCIÓN ..... 4
2. PRINCIPIOS Y DIRECTRICES ..... 6
2.1. PREVENCIÓN ..... 6
2.2. DETECCIÓN ..... 7
2.3. RESPUESTA ..... 7
2.4. RECUPERACIÓN ..... 8
3. ALCANCE ..... 8
4. MISIÓN ..... 9
5. ORGANIZACIÓN DE LA SEGURIDAD ..... 9
5.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN ..... 9
5.1.1. CONSTITUCIÓN ..... 9
5.1.2. FUNCIONES Y RESPONSABILIDADES ..... 9
6. 6. ROLES Y RESPONSABILIDADES ..... 11
7. PROCEDIMIENTOS DE DESIGNACIÓN Y RENOVACION ..... 14
8. DATOS DE CARÁCTER PERSONAL ..... 14
9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, REVISIÓN Y MEJORAS ..... 15
10. TERCERAS PARTES ..... 16
11. OBLIGACIONES DEL PERSONAL ..... 16

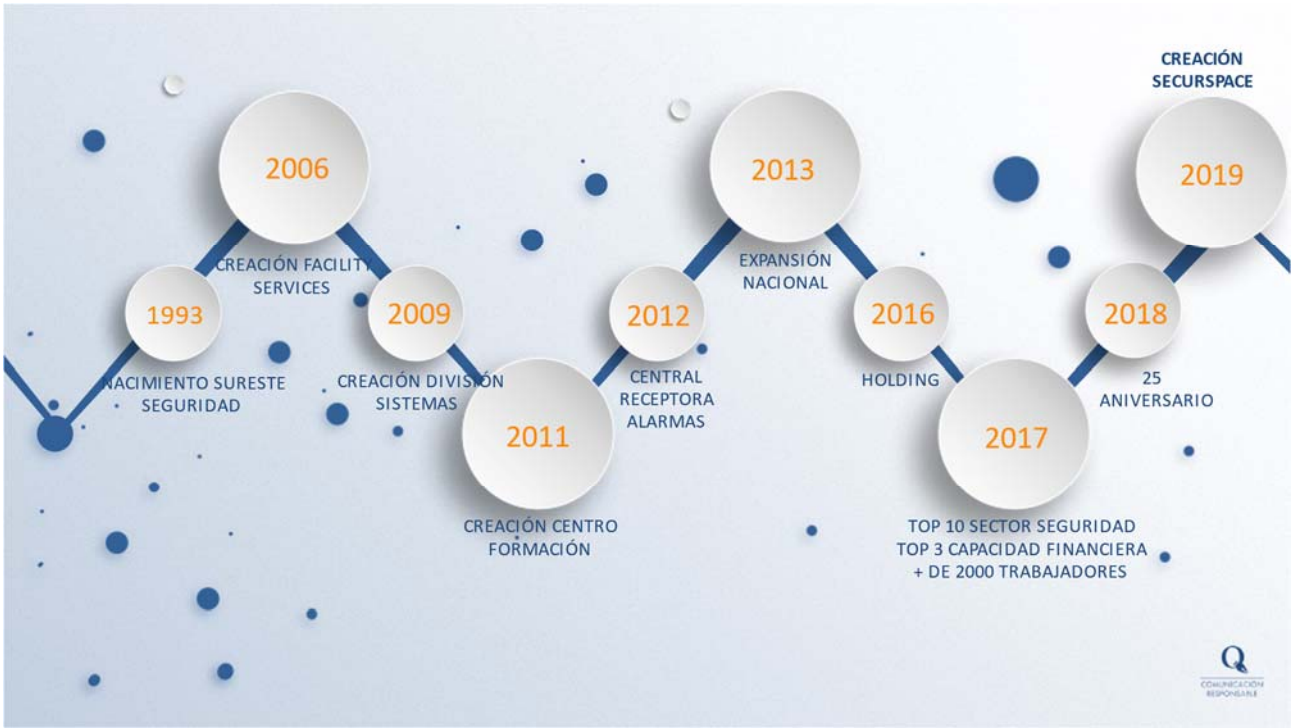
## 1. INTRODUCCIÓN

Presentación:

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.

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

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.

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.

## 2. PRINCIPIOS Y DIRECTRICES

### *2.1. 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.

### *2.2. 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.

### *2.3. 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

### *2.4. 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.

## 3. 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.

## 4. 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.

## 5. 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, ...)

### *5.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN*

#### *5.1.1. 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.

#### *5.1.2. 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.

## 6. 6. ROLES Y RESPONSABILIDADES

### 6.1 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<br>Monitorización y configuración de medidas de Seguridad |

### 6.2. 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.

## 7. 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.

## 8. 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.

## 9. 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) ñ) 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

## 10. 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.

## 11. 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