# MARCO ORGANIZATIVO

## POLÍTICA DE SEGURIDAD

COPIA CONTROLADA Nº:

| Rev. | Fecha | Motivo del Cambio |
|---|---|---|
| 0 | 02.07.21 | Primer ejemplar |
| 1 | 15.12.23 | Adecuación RD 311/2022 |
| 2 | 03.01.24 | Actualización Marco Normativo |
| 3 | 03.06.24 | Adaptación a ISO 27001:2022 |
| | | |
| | | |
| | | |



| ELABORADO POR:<br>Responsable de Seguridad | REVISADO POR:<br>Responsable del Sistema | APROBADO POR:<br>Gerente |
|---|---|---|
| FIRMADO<br><br>FECHA: 03.06.24 | FIRMADO<br><br>FECHA: 03.06.24 | FIRMADO<br><br>FECHA: 03.06.24 |

# MARCO ORGANIZATIVO

POLÍTICA DE SEGURIDAD

## Contenido

## 1 APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 03 de junio de 2024 por la TECON Soluciones Informáticas, S.L.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

## 2 INTRODUCCIÓN

TECON Soluciones Informáticas, 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 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 los departamentos 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.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC 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.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 1 del ENS.

### 2.1 PREVENCIÓN

Los departamentos deben 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 los departamentos deben implementar 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, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

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

### 2.2 DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

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

### 2.3 RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

### 2.4 RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes 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 de información que soportan los procesos de Comercialización, consultoría, instalación y mantenimiento de hardware; software a medida; sistemas cloud, sistemas informáticos e infraestructuras de telecomunicaciones"**

## 4 MISIÓN Y OBJETIVOS

TECON unifica las perspectivas legal y tecnológica para ofrecer a sus usuarios una solución integral a sus necesidades de Administración electrónica. Ofrece sus servicios de Comercialización, consultoría, instalación y mantenimiento de hardware; software a medida; sistemas cloud, sistemas informáticos e infraestructuras de telecomunicaciones a la administración pública.

Estas cuestiones se materializan con las aportaciones de un amplio equipo de personas formadas, certificadas y en permanente actualización de conocimientos, así como en métodos y prácticas.

La excelencia en la ejecución, la fidelidad en el marco de relaciones y la empatía hacia el cliente y entre compañeros actúan como valores y principios básicos que rigen nuestra actuación.

En el ámbito concreto del Esquema Nacional de Seguridad, el sistema de la información pretende lograr alcanzar **los siguientes objetivos:**

- Cumplir con las necesidades y expectativas de las partes interesadas involucradas dentro del alcance del sistema protegiendo la información interna y relacionada con la prestación de los servicios, considerando las dimensiones de:
  - Confidencialidad para asegurar que la información solo sea accedida por aquellos que cuenten con la autorización respectiva. Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
  - Integridad para preservar la veracidad y completitud de la información y los métodos de procesamiento. Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
  - Disponibilidad para asegurar que los usuarios autorizados tienen acceso a la información y los procesos, sistemas y redes que la soportan, cuando se requiera. La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.
  - Trazabilidad: Para asegurar que queda constancia fehaciente del uso del servicio y del acceso a los datos, es decir, que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. Toda acción desarrollada en el sistema o sobre la información, puede ser

imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.

- Autenticidad: Para asegurar que quien accede al servicio es realmente quien se cree y garantizar la fuente de la que proceden los datos. Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a duda.

- Demostrar liderazgo por parte de la Presidencia, dotando de recursos al sistema y asegurando que la política y los objetivos de seguridad que se establezcan sean compatibles con la estrategia de la organización.

- Gestionar la implementación del sistema de información de manera que proporcione ventajas competitivas en relación con otros agentes del sector, aprovechando la inercia que puede otorgar la gestión adecuada de la seguridad.

- Apostar por la **mejora continua**, y la implementación de medidas de seguridad eficaces y eficientes.

- Establecer anualmente objetivos, relacionados con ámbitos específicos de seguridad alineados con el ENS.

- Cumplir con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales de seguridad, alineando dichos requisitos con la privacidad y la seguridad de la información.

- Sensibilizar y concienciar de manera estable y permanente a todo el personal de la organización en cuanto a la seguridad de la información.

- Fomentar y mantener el buen nombre de la organización en relación con los servicios desarrollados, saber y respuesta activa (reactiva y proactiva) ante incidentes de seguridad, mantenimiento la imagen y reputación.

## 5 PRINCIPIOS

La política de seguridad de la información de TECON se desarrolla de acuerdo con los siguientes principios:

- **Principio de confidencialidad:** se deberá garantizar que la información sea accesible únicamente para aquellas personas expresamente autorizadas para ello.

- **Principio de integridad:** se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.

- **Principio de disponibilidad:** se garantizará la prestación continua de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada.

- **Principio de gestión del riesgo:** Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.

- **Principio de mejora continua:** se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados para aumentar la capacidad de adaptación a la constante evolución del entorno.

- **Principio de proporcionalidad en coste:** la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.

- **Principio de cumplimiento normativo:** todos los sistemas de información se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquella relacionada con la intimidad y la protección de datos de carácter personal y con la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.

- **Principio de prevención:** Los departamentos deben 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 los departamentos deben implementar 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, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben: 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.

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

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

- **Principio de respuesta:** Los departamentos deben: establecer mecanismos para responder eficazmente a los incidentes de seguridad; designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos; establecer protocolos para el

intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

- **Principio de recuperación:** Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

## 6 MARCO NORMATIVO

- Norma UNE ISO/IEC 27001:2022
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad. (ITS) de Conformidad con el ENS y la de Auditoría del ENS.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Ley 3/2012, sobre el teletrabajo.
- Guías CCN-STIC (800).

## 7 ORGANIZACIÓN DE LA SEGURIDAD.

### 7.1 COMPROMISO DE LA DIRECCIÓN

Dirección de TECON, aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

La Dirección de la entidad se compromete a:

- La revisión, aprobación y verificación de cumplimiento de las Políticas de Seguridad de la Información contenidas en este sistema.
- Mantener habilidades y calificaciones apropiadas en seguridad de la información a través de la educación profesional continua.
- La promoción activa de una cultura de seguridad.
- Asegurar la información de roles y responsabilidades en seguridad de la información a todo el personal antes de del acceso a la información de la organización
- Facilitar la divulgación de las políticas a todos los empleados.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- Habilitar canal confidencial de denuncias de violaciones de las políticas o procedimientos de seguridad de la información

## 7.2 COMITÉS: FUNCIONES Y RESPONSABILIDADES

Los Comités, que se constituirán como órganos colegiados, de conformidad con lo señalado en la Ley 40/2015, estarán formados por los miembros de todas las partes implicadas.

En este sentido y con las funciones atribuidas en materia de Seguridad de la Información y seguridad física se crea el Comité de Seguridad del TECON Soluciones Informáticas, S.L.

.
El Comité de Seguridad estará formado por:

- Responsable de la Información
- Responsable de los Servicios
- Responsable de Seguridad
- Responsable del Sistema
- Responsable del sistema de gestión

Las funciones para cada uno de los roles se establecen en el siguiente punto.

Las funciones del Comité de Seguridad son las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:

- Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando 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 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.
- Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con el Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

Asimismo, podrán ser delegadas otras funciones por otro órgano de la entidad con competencias en la materia. Las funciones atribuidas al Comité por otro órgano no podrán ser delegadas si bien podrán ser revocadas en cualquier momento.

El Comité se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

### 7.3 ROLES: FUNCIONES Y RESPONSABLIDADES.

Los roles, funciones y responsabilidades de Dirección, los miembros del Comité de seguridad y el personal sin funciones específicas en el SGSI se establecen a continuación:

**Dirección**

La Dirección es la máxima responsable de la gestión de la TECON. Sus funciones relacionadas con el Sistema de gestión de seguridad de la información son las siguientes:

- Establece la Política General del SGSI de TECON
- Aprueba la Declaración de Aplicabilidad a partir del establecimiento de los objetivos de control y controles derivados del análisis de los riesgos.
- Convocatoria para realizar las revisiones del Sistema.
- Asegura que se proporcionen los recursos necesarios, adecuados y su disponibilidad para el mantenimiento del Sistema de gestión de seguridad de la información.
- Asegura el establecimiento, mantenimiento y desarrollo de sistemas de comunicación dentro de la organización a fin de alcanzar un adecuado nivel de eficacia del Sistema de gestión de seguridad de la información.
- Realiza las revisiones periódicas del Sistema de gestión de seguridad de la información de TECON
- Aprueba el Manual del sistema de gestión de la seguridad de la información, las Políticas, Procedimientos y sus sucesivas revisiones.
- Aprueba el Programa de Auditorías Internas y el Plan de Formación Anual, entre otros documentos del sistema.
- En general acepta, firmando, la documentación de TECON

**Responsable de la información:**

- Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de la información constituye asimismo una actividad indelegable. (ART 10)
- La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos. (art. 43).

**Responsable de servicio:**

- Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS. (art. 10).

- Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios.
- Potestad de establecer los requisitos del servicio en materia de seguridad.

**Responsable de la seguridad:**

- Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. (art. 10)
- 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.
- Suscribir la Declaración de Aplicabilidad, responsabilizándose de las medidas de seguridad en ella reflejadas.
- Monitorizar el estado de seguridad del sistema, proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoria implementados en el sistema.

**Responsable del Sistema:**

- Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
- 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.

**Responsable de la Gestión del SGSI**

La Dirección de la TECON elige un responsable de la Gestión del SGSI, y le confiere la autoridad y responsabilidad suficiente para:

- Elaborar el Manual, las políticas, los procedimientos y demás documentación relacionados con la gestión del sistema.
- Difunde toda la documentación de la gestión del SGSI.
- Asegurar que el Sistema de gestión de seguridad de la información se encuentra establecido, implantado y mantenido.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

- Estudiar y analizar las reclamaciones de los clientes, no conformidades y auditorías que se produzcan referentes a la gestión del SGSI.
- Establecer las acciones correctivas y preventivas que estime oportunas, así como su seguimiento y análisis.
- Informar al Responsable de la Seguridad del funcionamiento del Sistema de gestión de seguridad de la información, para que ésta pueda llevar a cabo la revisión del mismo.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas TECON, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Revisar regularmente la implantación del Sistema de gestión de seguridad de la información.
- Elaborar el programa de auditorías internas y el plan de formación.
- Promover la toma de conciencia del personal en el cumplimiento de los requisitos del SGSI.
- Controlar la documentación y custodia del archivo general del Sistema de gestión de seguridad de la información.
- Implantar las medidas de seguridad física necesarias para el mantenimiento de la seguridad del SGSI.
- El Responsable del Sistema puede proponer la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

**Personal sin funciones específicas en el SGSI:**

- El personal de TECON sin funciones específicas en el SGSI de TECON deberá seguir las instrucciones establecidas en los diferentes documentos del SGSI donde se establezcan pautas de comportamiento y obligaciones para el cumplimiento del SGSI.

## 8 ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en niveles, según el ámbito de aplicación y el nivel de detalle técnico. Dichos niveles de desarrollo son los siguientes:

a) Políticas de seguridad de la información, constituido por el presente documento y el manual de seguridad.

b) Normativas de obligado cumplimiento, asociados a diferentes ámbitos normativos, por ejemplo, la normativa de seguridad para empleados.

c) Procedimientos operativos, documentos que describen explícitamente y paso a paso como realizar una cierta actividad, por ejemplo, gestión de incidentes, o copias de seguridad.

d) Instrucciones o procedimientos técnicos, propios del área de sistemas, especifican, por ejemplo, los distintos tratamientos asociados a tipologías de incidente.

## 9 DATOS DE CARÁCTER PERSONAL

En relación con el tratamiento de los datos personales, este se hará ajustándose a la regulación vigente, acogiéndose de manera especial al cumplimiento del RGPD y la LOPDGDD.

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

## 11 OBLIGACIONES DEL PERSONAL

Todos los miembros de TECON Soluciones Informáticas, S.L., incluidos en el alcance, 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.

## 12 TERCERAS PARTES

Cuando TECON Soluciones Informáticas, S.L. preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando TECON Soluciones Informáticas, S.L. utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña 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.

Los licitantes tienen la obligación de que las soluciones o servicios prestados sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y en este caso posean las correspondientes Declaraciones de Conformidad, según lo señalado en la citada Instrucción Técnica de Seguridad.

**DOCUMENTOS RELACIONADOS**

| | |
|---|---|
| CS | Comité de seguridad |