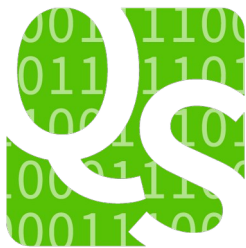


 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 1 de 12
--	--------------------------------------	--

# **SGSI.01-04 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ENS**



**quersystem**

## ÍNDICE

1.	Aprobación y Entrada en Vigor.....	3
2.	Introducción.....	3
2.1.	Prevencción.....	4
2.2.	Detección.....	4
2.3.	Respuesta.....	4
2.4.	Recuperación.....	4
3.	Alcance.....	5
4.	Misión.....	5
5.	Marco Normativo.....	6
6.	Organización de la Seguridad.....	7
6.1.	Comité de seguridad de la información.....	7
6.2.	Responsable de la Información.....	8
6.3.	Responsable del Servicio.....	8
6.4.	Responsable de Seguridad.....	8
6.5.	Responsable del sistema.....	9
7.	Procedimiento de Designación.....	10
8.	Revisión de la Política de Seguridad de la Información.....	10
9.	Datos de Carácter Personal.....	10
10.	Gestión de Riesgos.....	11
11.	Desarrollo de la Política Seguridad de la Información del Personal.....	11
12.	Obligaciones del Personal.....	12
13.	Terceras Partes.....	12

## CONTROL DE VERSIONES

Revisión	Fecha	Motivo del Cambio
1.0	16/01/2020	Primera emisión

 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 3 de 12
--	--------------------------------------	--

## 1. Aprobación y Entrada en Vigor

Esta Política de Seguridad de la Información es efectiva desde su entrada en vigor y hasta que sea reemplazada por una nueva Política.

## 2. Introducción

QUER SYSTEM depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con 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 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.

QUER SYSTEM debe 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.

QUER SYSTEM debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 4 de 12
--	--------------------------------------	--

## 2.1. Prevención

QUER SYSTEM 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 implementará 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se debe:

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

## 2.2. Detección

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

## 2.3. Respuesta

QUER SYSTEM:

- Establecerá mecanismos para responder eficazmente a los incidentes de seguridad.
- Designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecerá 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, QUER SYSTEM dispondrá de planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 5 de 12
--	--------------------------------------	--

### **3. Alcance**

Esta política se aplica a todos los sistemas TIC de QUER SYSTEM y a todos los miembros de este, que dan soporte a las actividades de prestación de los siguientes servicios en el área de la tecnología de la información y las comunicaciones:

- Servicios Cloud de pago por uso en la nube.
- Servicio de consultoría IT e implantación de proyectos tecnológicos.
- Servicio de Comunicaciones Unificadas
- Sincronización de ficheros
- Servicio avanzado de monitorización interna y externa
- Servicio de Virtualización de escritorios

### **4. Misión**

QUER SYSTEM es una organización experta en consultoría y servicios TIC, especializada en la implantación de proyectos tecnológicos que aportan a las empresas de forma integrada soluciones para la gestión empresarial.

Somos especialistas en la confección a medida de soluciones tecnológicas 360° mediante la integración de productos de los principales desarrolladores.

Nuestros servicios son totalmente personalizados, creando protocolos a medida para garantizar una excelente calidad de servicio y una óptima gestión de los clientes y recursos.

Nuestra misión es ayudar al desarrollo de personas y entidades a través de las mejores soluciones del mercado y el amplio conocimiento y experiencia sobre ellas.

 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 6 de 12
--	--------------------------------------	--

## 5. Marco Normativo

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

- **Real Decreto 3/2010**, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** (ENS) en el ámbito de la administración electrónica.
- **Real Decreto 951/2015**, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- **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**).
- **Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de **Datos Personales y garantía de los derechos digitales**.
- **Real Decreto Legislativo 1/1996**, de 12 de abril, por el que se aprueba el Texto Refundido de la **Ley de Propiedad Intelectual**.
- Ley de Propiedad Industrial.
- **Ley 34/2002**, de 11 de julio, de **Servicios de la Sociedad de la Información** y de comercio electrónico.

 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 7 de 12
--	--------------------------------------	--

## 6. Organización de la Seguridad

La implantación de la Política de Seguridad en QUER SYSTEM requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol específico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

- a) El Comité de Seguridad de la Información
- b) Responsable del Servicio
- c) Responsable de la Información
- d) Responsable de Seguridad de la Información
- e) Responsable de Sistemas

En los siguientes apartados se especifican las funciones atribuidas a uno de estos roles.

### 6.1. Comité de seguridad de la información

El Comité de Seguridad de la Información coordina la seguridad de la información en QUER SYSTEM. Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
  - Principales incidencias en la Seguridad de la Información.
  - Elaboración y actualización de planes de continuidad.
  - Cumplimiento y difusión de las Políticas de Seguridad.

El Secretario del Comité de Seguridad TIC será el Responsable de Seguridad y tendrá como funciones:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 8 de 12
--	--------------------------------------	--

## 6.2. Responsable de la Información

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.
- Determina los niveles de seguridad de la información.

## 6.3. Responsable del Servicio

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad de la información.

## 6.4. Responsable de Seguridad

Responsable de la definición, coordinación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de QUER SYSTEM.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
  - La estrategia de seguridad de la información definida por el Comité de Seguridad.
  - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de QUER SYSTEM y normativa de desarrollo.
- Supervisar los incidentes de seguridad producidos en QUER SYSTEM.
- Difundir en QUER SYSTEM las normas y procedimientos contenidos en la Política de Seguridad de la Información y normativa de desarrollo, así como las funciones y obligaciones en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables en materia de protección de datos personales y de seguridad de la información.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de QUER SYSTEM.



 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 9 de 12
--	--------------------------------------	--

## 6.5. Responsable del sistema

Es responsable de asegurar la ejecución de medidas para asegurar los activos y servicios de los sistemas de información, que soportan la actividad de QUER SYSTEM, de acuerdo a los objetivos de la organización.

Las funciones del Responsable de Sistemas de la Información son las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de QUER SYSTEM, conforme a la estrategia de seguridad definida.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en QUER SYSTEM.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- El Responsable del Sistema puede acordar 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.

 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 10 de 12
--	--------------------------------------	---

## 7. Procedimiento de Designación

Se designan las siguientes responsabilidades:

- **Responsable del Servicio:** Alguien de la alta dirección, normalmente el Director General.
- **Responsable de la Información:** Alguien de la alta dirección, normalmente el Director General.
- **Responsable de Seguridad:** Alguien de la Dirección Ejecutiva que entienda que hace cada departamento y como los departamentos se coordinan entre sí para alcanzar los objetivos marcados por la Dirección.
- **Responsable del Sistema:** Alguien de operaciones, Responsable del desarrollo, operación y mantenimiento el Sistema de Información.

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

El Responsable de Seguridad de la Información será nombrado por el Director General a propuesta del Comité de Seguridad TIC.

## 8. Revisión de la Política de Seguridad de la Información

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

## 9. Datos de Carácter Personal

QUER SYSTEM trata datos de carácter personal.

En aplicación del principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos, las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

Se aplicará, asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 11 de 12
--	--------------------------------------	---

## **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.

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

## **11. Desarrollo de la Política Seguridad de la Información del Personal**

Esta política de seguridad de la Información complementa las políticas de seguridad de QUER SYSTEM en materia de protección de datos de carácter personal.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. 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.

 <b>quersystem</b>	<b>POLITICA DE SEGURIDAD ENS</b>	Versión: 1 Código: SGSI.01-04 Fecha: 16/01/2020 Página: 12 de 12
--	--------------------------------------	---

## **12. Obligaciones del Personal**

Todos y cada uno de los usuarios de los sistemas de información de QUER SYSTEM son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros de QUER SYSTEM 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 disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de QUER SYSTEM recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros de QUER SYSTEM, 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.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

## **13. Terceras Partes**

Cuando QUER SYSTEM preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando QUER SYSTEM utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.