SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SGSI_POL_001

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Contenido

Elaboró:	Govertis	**Revisó**:		**Aprobó**:	Junta de Gobierno
Cargo:	Consultor	**Cargo:**		**Cargo:**	Junta de Gobierno
Fecha:	04/07/2019	**Fecha:**		**Fecha:**	16/12/2019

1 Objetivo

El objeto de la presente Política de Seguridad de la Información es determinar el alcance y estructura del sistema de gestión de seguridad (SGSI) implantado en el Colegio de Ingenieros de Caminos, Canales y Puertos, en base a las directrices determinadas por las normativas de referencia en la materia, en especial el Esquema Nacional de Seguridad.

La Política de Seguridad de la Información es un instrumento, previsto en el Reglamento de Cumplimiento Normativo, para el cumplimiento normativo en la materia de seguridad de la información y complementario de la protección de datos de carácter personal.

2 Alcance

La Política de Seguridad de la Información afectará a la información y datos personales tratados por medios electrónicos y en soporte en papel que el Colegio, incluyendo todos sus centros directivos (Sede Central y Demarcaciones), gestiona en el desarrollo de sus funciones y en el ámbito de sus competencias.

El alcance del Sistema de Gestión de Seguridad de la Información, en adelante SGSI, del Colegio de Ingenieros de Caminos, Canales y Puertos es el siguiente:

"Sistema de Información para la adecuada gestión de la Corporación en su conjunto y para la prestación de los servicios necesarios para la ordenación de la actividad profesional de los colegiados".

3 Misión y objetivos

El Colegio de Ingenieros de Caminos, Canales y Puertos, tiene definido en sus estatutos su naturaleza (artículo 1), sus fines (artículo 2) y las funciones que asume el colegio (artículo 3).

En el ámbito concreto de la seguridad, el SGSI corporativo pretende lograr alcanzar los siguientes objetivos:

- Cumplir con las necesidades y expectativas de las partes interesadas involucradas dentro del alcance del SGSI 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 dirección, dotando de recursos al SGSI 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 SGSI 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 la norma del 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 corporativa.
- 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.

4 Principios

La política de seguridad de la información del Colegio de Ingenieros de Caminos, Canales y Puertos 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. El análisis y gestión de riesgos son parte esencial del proceso de protección de datos y de seguridad de la información del Colegio, de forma que permita el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo el Colegio tendrá en cuenta los riesgos que se derivan para los derechos de las personas con respecto al tratamiento de sus datos personales. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.
- 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: el Colegio establecerá medidas de protección, detección y recuperación de forma que resulten proporcionales a los potenciales riesgos y a la criticidad y valor de la información, de los tratamientos de datos personales y de los servicios afectados.

- 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: Las áreas de dirección de Sede Central y Demarcaciones del Colegio 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, en dichas áreas se 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, el Colegio debe:
    - autorizar los sistemas antes de entrar en operación;
    - evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria;
    - y 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: El Colegio debe: establecer mecanismos para responder eficazmente a los incidentes de seguridad; designar punto de contacto para las comunicaciones con respecto a incidentes detectados en las distintas áreas del Colegio; 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, el Colegio debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.
- Responsabilidad proactiva: el Colegio y su estructura serán responsables del cumplimiento de los principios anteriormente señalados y adoptarán las medidas técnicas y organizativas que permitan estar en condiciones de demostrar dicho cumplimiento.
- Alcance estratégico: la protección de datos y la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles orgánicos y directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del Colegio para conformar un todo coherente y eficaz.

Responsabilidad diferenciada: en los sistemas de información responsabilidad del Colegio se observará el principio de responsabilidad diferenciada de forma que se delimiten las diferentes responsabilidades y roles.

Los principios anteriores se concretan en un conjunto de medidas particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios de la PSI y que inspiran las actuaciones del Colegio en dicha materia. Se establecen los siguientes:

a) Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el RGPD, la LOPDyGDD y el Esquema Nacional de Seguridad.

b) Gestión de activos de información: Los activos de información del Colegio se encontrarán inventariados y categorizados y estarán asociados a un responsable.

c) Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las tecnologías de la información y de las comunicaciones. La información que se transmita a través de redes de

comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

El Colegio dispondrá de un Procedimiento para la gestión de brechas de seguridad, por el que se rige la gestión de brechas de seguridad relativas a la protección de datos personales de los que el Colegio sea responsable del tratamiento

i) Gestión de la continuidad: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información y de protección de datos de carácter personal.

5 Marco normativo

De conformidad con la disposición adicional primera y el artículo 77.1 LOPDYGDD las medidas de seguridad del Esquema Nacional de Seguridad son aplicables a los tratamientos de datos personales cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público. El Esquema Nacional de Seguridad se

rige por el 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.

Por extensión, y por coherencia del sistema de seguridad de la información de toda la Corporación, las medidas del Esquema de Seguridad de la Información serán aplicable por el Colegio a todos los tratamientos de información.

La presente política se rige por la siguiente legislación y normativa de referencia:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDYGDD).
- 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 (RGPD)
- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, respecto del patrimonio documental generado en el ejercicio de funciones públicas.
- 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.
- Guías CCN-STIC (800).
- UNE/ISO-IEC 27.001:2013: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

6 Roles y funciones, organización de la seguridad

El Colegio de Ingenieros de Caminos, Canales y Puertos dispone de un Comité de Seguridad de la Información formado por diferentes roles, para atender las necesidades de seguridad tanto técnicas como organizativas, permitiendo de esta forma una mejor distribución de la información y toma de decisiones.

Estos recursos, comienzan por la designación de la seguridad como función diferenciada mediante los siguientes miembros y funciones:

- Responsable de la información que determinará los requisitos de la información tratada.

- Responsable del servicio que determinará los requisitos de los servicios prestados.
- Responsable del Tratamiento (Protección de Datos): que determina los fines y medios del tratamiento.
- Responsable de Seguridad (CISO) que determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Delegado de Protección de Datos: que informará, asesorará, y supervisará sobre el cumplimiento en materia de protección de datos de carácter personal incluidos los aspectos de seguridad (integridad, confidencialidad y disponibilidad) y violación de datos personales asesorando sobre la necesidad o no de notificación a la autoridad de control y, en su caso a los propios interesados y comunicando en su caso el incidente a la autoridad de control de protección de datos en virtud de su rol de punto de contacto previsto en el RGPD y la LOPDGDD. Su nombramiento lo debe realizar el responsable de tratamiento de manera diferenciada al resto de miembros de Comité de Seguridad ya que sus cometidos no se ciñen únicamente a aspectos de seguridad. Para evitar el conflicto de intereses, debe tener voz, pero no voto en las decisiones y deliberaciones del Comité de Seguridad.
- Responsable del Sistema (CIO) supervisará la infraestructura de los sistemas de información dentro de la organización y es responsable de establecer los estándares de información para facilitar el control de la gestión de todos los recursos corporativos.
- Administrador de la Seguridad del Sistema que implementará y velará por la correcta implementación de las decisiones para satisfacer los requisitos establecidos por el CISO y el CIO.

El documento para su designación y renovación, así como las funciones concretas de cada uno de los roles aquí definidos y los mecanismos de coordinación y resolución de conflictos, vienen definidos en el documento del SGSI "*SGSI_POL_001_A1 Roles y responsabilidades*".

Debido a la capacidad y el tamaño del Colegio de Ingenieros de Caminos, Canales y Puertos, se ha considerado que las responsabilidades identificadas en esta política se implementen en dos roles tal y como indica la guía *CCN-STIC-801 del ESQUEMA NACIONAL DE SEGURIDAD: RESPONSABILIDADES Y FUNCIONES* en su Anexo B. *Estructuras posibles de implementación* para "Estructura mínima. A saber, son:

Gobierno y Supervisión: una figura integrando las siguientes funciones:

- Responsable del Tratamiento
- Responsable de la Información.

• Responsable del Servicio. • Responsable de la Seguridad (Formado por el Comité de Seguridad)
• Delegado de Protección de Datos (DPD)
Operación: una figura, reportando a Dirección, e integrando las siguientes funciones: • Responsable del Sistema. • Administrador de Seguridad.

7 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.

8 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 LOPDYGDD.

El tratamiento de datos de carácter personal se rige por el Manual de Privacidad del Colegio, y siempre se tendrán en cuenta los siguientes principios:

a) Licitud, lealtad y transparencia: los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.

b) Legitimación en el tratamiento de datos personales: solo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD.

c) Limitación de la finalidad: los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
d) Minimización de datos: los datos de carácter personal serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
e) Limitación del plazo de conservación: los datos de carácter personal personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines que justificaron su tratamiento.
f) Integridad y confidencialidad: los datos de carácter personal serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto incluso después de haber concluido aquél.
g) Responsabilidad proactiva: el Colegio y su estructura serán responsables del cumplimiento de los principios anteriormente señalados y adoptarán las medidas técnicas y organizativas que permitan estar en condiciones de demostrar dicho cumplimiento.
h) Atención de los derechos de los afectados: se adoptarán medidas en la organización que garanticen el adecuado ejercicio por los afectados, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos de carácter personal.

9 Obligaciones del personal

Toda la estructura y personal del Colegio prestarán su colaboración en las actuaciones de implementación de la Política de Seguridad de la Información, aprobada por la Junta de Gobierno.

Todas las personas que presten servicio en el Colegio tienen la obligación de conocer y cumplir lo previsto en la presente Política así como en las normas y procedimientos que la desarrollen, aplicando los principios de seguridad en el desempeño de su cometido. El significado y alcance del uso seguro del sistema se concretará y plasmará en la Normativa de Seguridad.

Todo el personal que presta servicio en el Colegio tiene asimismo el deber de colaborar en la mejora de los principios y requisitos en materia de protección de datos y

seguridad de la información evitando y aminorando los riesgos a los que se encuentra expuesta la información y los datos personales de los que es responsable o encargado el Colegio. A tal efecto, comunicarán a los integrantes de la estructura organizativa de la PSI cualquier propuesta o sugerencia que ayude a preservar la confidencialidad, la integridad y la disponibilidad de la información.

Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema informático estará identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

10 Profesionalidad. Concienciación y formación.

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

El Colegio desarrollará actividades formativas específicas orientadas a la concienciación y formación del personal que presta sus servicios en el Colegio para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios.

El Colegio dispondrá los medios necesarios para que todas las personas con acceso a la información sean informadas acerca de sus deberes y obligaciones en materia de seguridad de la información y protección de datos así como de los riesgos existentes en el tratamiento de la información.

La Política de seguridad de la Información y su desarrollo normativo se difundirá entre el personal del Colegio, estando disponible de manera permanente en el portal del empleado.

El delegado de protección de datos supervisará las acciones de concienciación y formación del personal que participa en las operaciones de tratamiento con datos personales, a fin de garantizar el cumplimiento de la Política de Seguridad de la Información.

11 Gobierno del modelo

11.1. Titularidad

La aprobación de esta Política de Seguridad de la Información, así como del documento de Roles y Responsabilidades, corresponde a la Junta de Gobierno del Colegio. El Responsable de la Información propondrá a la Junta de Gobierno la modificación de la Política.

Corresponderá al Responsable de la Información, a propuesta del Comité de Seguridad de la Información, la adopción de los procedimientos, guías e instrucciones técnicas y la aprobación de las medidas de seguridad necesarios para el desarrollo de la presente Política.

11.2. Interpretación

Corresponde a la Secretaría General la interpretación de este documento.

11.3. Validez y revisión

Este modelo entrará en vigor desde la fecha de su aprobación y publicación.

La presente PSI se someterá a un proceso de revisión, al menos anual, a fin de adaptarse a las circunstancias técnicas u organizativas y evitar su obsolescencia.

11. 4. Publicidad

La presente Política se publicará en la web del Colegio, en el apartado de Transparencia.

12 Documentos relacionados

- SGSI_POL_001_A1 Roles y responsabilidades
- CCN-STIC-801 del ESQUEMA NACIONAL DE SEGURIDAD: RESPONSABILIDADES Y FUNCIONES