POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esquema Nacional de Seguridad

Categoría Básica

Colegio Oficial
Arquitectos
Sevilla

Versión actual	1.0
Fecha de aprobación	3/05/2024
Aprobado por	Responsable de la Información
Revisado por	Responsable del Sistema
Elaborado por	Responsable de la Seguridad

CONTROL DE CAMBIOS		
Versión	Descripción del cambio	Fecha
1.0	Generación del borrador del documento	26/04/2024

Índice de contenidos

1. Introducción **4**
2. Objeto **4**
3. Alcance **5**
3. Responsabilidades **5**
4. Políticas generales **6**
4.1. Medidas disciplinarias 9
4.2. Revisión de la Política de Seguridad 10

1. Introducción

El Colegio Oficial de Arquitectos de Sevilla es la organización profesional integrada por los arquitectos de la provincia de Sevilla como corporación de Derecho Público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines.

El Colegio Oficial de Arquitectos de Sevilla cuenta con más de 2530 colegiados, y tiene una gran presencia en la provincia y un gran prestigio nacional e internacional, basado en su capacidad de integración en la sociedad y los servicios que presta a arquitectos y usuarios.

Junto con el resto de Colegios andaluces, constituye el Consejo Andaluz de Colegios de Arquitectos, ente que representa a la profesión a nivel autonómico, y a nivel nacional forma parte del Consejo Superior de Colegios de Arquitectos de España.

Desde el punto de vista de los primeros, el Colegio vela por la ética, formación y ordenación del libre ejercicio de la profesión de arquitecto, representa sus intereses y difunde sus proyectos, en los más modernos campos de actuación de la profesión, ofreciendo alternativas avanzadas de tecnología, información e intercambio, compatibles con el resto de los Colegios en Andalucía y España, y con otras Asociaciones, Instituciones o Fundaciones de Arquitectos de todo el mundo. Para ello utiliza todos los Sistemas, Redes y Bases de Datos de mayor eficiencia, interdependencia y acceso global.

El Colegio ejerce también una importante labor cultural, social y corporativa en la provincia, mediando en conflictos en defensa de los derechos de los ciudadanos o entre los propios arquitectos, ejerciendo la opinión profesional en todos los temas de su competencia, favoreciendo la proyección de la arquitectura, el urbanismo y el medio ambiente en la sociedad. En su labor de divulgación promueve actos culturales, conferencias y exposiciones que muestran, de forma local e itinerante, la mejor arquitectura del momento.

2. Objeto

El objeto del presente documento es la definición de la Política de Seguridad de la información del Colegio Oficial de Arquitectos de Sevilla (CoaSevilla), dentro del alcance señalado en el Esquema Nacional de Seguridad y el Reglamento General Europeo de Protección de Datos, cumpliendo con todas sus especificaciones que son de aplicación.

La presente Política se ha definido atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de la empresa que resultan de la aplicación de las previsiones contempladas en los Anexos I y II del Real

Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

El objetivo de la presente Política de Seguridad de la información es establecer los principios básicos y requisitos mínimos de seguridad necesarios para proteger la información, así como la tecnología utilizada para su procesamiento, así como garantizar la calidad de la información y la prestación continuada de los servicios.

Para ello, define directrices de implantación de medidas organizativas, técnicas y legales, desde la concepción del sistema y en todo su ciclo de vida hasta su desconexión y destrucción, y define los responsables de su desarrollo, implantación y gestión.

La implantación de dichas medidas se realizará de forma preventiva garantizando la preservación de la información, y el cumplimento de las leyes en vigor que afecten a su uso y tratamiento.

3. Alcance

La política de seguridad de la información será de aplicación y de obligado cumplimiento para todos los empleados y usuarios que, de manera permanente o eventual, trabajen con información o sistemas de información de carácter general propiedad de la CoaSevilla.

Esta normativa ha sido elaborada por el Responsable de Seguridad, revisada por el Responsable del Sistema y aprobada por el Responsable de la Información atendiendo a las recomendaciones del Responsable de Seguridad.

Cualquier modificación posterior entrará en vigor al día siguiente de su aprobación y publicación por parte del Responsable de la Información. En este caso, la versión anterior quedará anulada por la última versión de esta normativa.

3. Responsabilidades

Será responsabilidad del Responsable de la Información, poner en marcha las medidas definidas en esta normativa. El Responsable de Seguridad evaluará regularmente las medidas implantadas y posibles mejoras.

4. Políticas generales

CoaSevilla, tiene entre sus fines y objetivos, principales, ordenar el ejercicio de la profesión en su ámbito, representar y defender los intereses de los arquitectos, contribuir a su formación, velar por la observancia de la deontología profesional y por el adecuado nivel de calidad del ejercicio profesional, y realizar las prestaciones de interés general en relación con la arquitectura, el urbanismo y el medio ambiente, que considere oportunas o se les encomiende por ley.

Asume su compromiso con la seguridad de la información, comprometiéndose a adecuada gestión de esta, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la a la seguridad de la información utilizada. Por todo lo anteriormente expuesto, la Dirección establece los siguientes objetivos de seguridad de la información:

- Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.

- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones

- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.

- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Para poder lograr estos objetivos es necesario:

- Mejorar continuamente nuestro sistema de seguridad de la información

- Cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribimos además de los compromisos adquiridos con los clientes, así como la actualización continua de los mismos. El marco legal y regulatorio en el que desarrollamos nuestras actividades es:

    - 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
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- LEY 40/2015, de 1 de octubre, Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- Identificar las amenazas potenciales, así como el impacto en las operaciones del negocio que dichas amenazas, en caso de materializarse, puedan causar.

- Preservar los intereses de sus principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.

- Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.

- Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.

- Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.

- Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.

- Estructurar nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:

La gestión de nuestro sistema se encomienda al Responsable de la Información y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente Política de Seguridad de la Información.

Los roles o funciones de seguridad definidos en CoaSevilla son:

Función	**Deberes y responsabilidades**
Responsable de la Información	- Tomar las decisiones relativas a la información tratada
Responsable de los Servicios	- Coordinar la implantación del sistema - Mejorar el sistema de forma continua
Responsable de la Seguridad	- Determinar la idoneidad de las medidas técnicas - Proporcionar la mejor tecnología para el servicio
Responsable del Sistema	- Coordinar la implantación del sistema - Mejorar el sistema de forma continua

Esta definición se completa en los perfiles de puesto y en los documentos del sistema.

El procedimiento para su designación y renovación será la ratificación en el comité de seguridad.

El comité para la gestión y coordinación de la 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 este comité. Los miembros del comité de seguridad de la información son:

- Responsable de la Información.
- Responsable de los Servicios.
- Responsable de la Seguridad.
- Responsable del Sistema.

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de CoaSevilla.

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

4.1. Medidas disciplinarias

En caso de no cumplirse las políticas y procedimientos de seguridad de la empresa, estos sistemas podrán ser igualmente utilizados para hacer efectivas las medidas establecidas en el art. 20.3 del Estatuto de los Trabajadores sobre control empresarial. Por lo que ponemos en su conocimiento que, con independencia de las finalidades principales de la recogida de datos, aquellos datos que se obtengan a través de los citados sistemas y que, en atención a ello, obren en poder de la sede de CoaSevilla podrán ser utilizados en sede disciplinaria laboral, sirviendo la presente cláusula informativa como efectiva comunicación al efecto.

4.2. Revisión de la Política de Seguridad

Periodicidad:

La presente Política de Seguridad será revisada al menos anualmente. La frecuencia de revisión podrá ser modificada en función de los siguientes factores:

- Cambios en el entorno: nuevos riesgos, nuevas tecnologías, cambios regulatorios, etc.
- Evaluación de la eficacia de la política: si la política ha sido efectiva en la protección de la información y los sistemas.
- Cambios en la organización: cambios en la estructura, procesos o tecnologías de la organización.

Documentación:

La revisión de la Política de Seguridad será documentada, incluyendo los cambios realizados y las razones de los mismos. La documentación será archivada y estará disponible para su consulta por las partes interesadas.

Responsabilidades:

El responsable de la seguridad de la información será responsable de coordinar la revisión de la Política de Seguridad. Los responsables de los diferentes departamentos serán responsables de proporcionar información y apoyo al proceso de revisión.

La Dirección
Fecha: 3/05/2024