Anotec engineering

PO.SGSI_01

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Marzo 2025

Elaborado por

INNOVASUR

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 31 de marzo 2025 por el comité de dirección.

Esta Política de Seguridad de la Información (en adelante, Política de Seguridad) entrará en vigor el día posterior a la fecha anteriormente indicada y hasta que sea reemplazada por una nueva política.

2. OBJETO

ANOTEC ENGINEERING, (en adelante ANOTEC) considera la información un activo esencial para el cumplimiento adecuado de sus funciones. Buena parte de la información contenida en los sistemas de información de las entidades públicas y privadas y los servicios que prestan constituyen activos nacionales estratégicos. La información y los servicios prestados están sometidos a amenazas y riesgos provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.

En su empeño por garantizar que los servicios disponibles a través de medios electrónicos a los usuarios se presten en unas condiciones de seguridad máxima, ANOTEC desarrolla y aprueba esta Política de Seguridad de la Información, aplicando las medidas mínimas de seguridad exigidas por en la norma UNE-EN ISO/IEC 27001 en lo referente a:

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. Mejora continua del proceso de seguridad.

Las diferentes áreas deben cerciorarse de que la seguridad de la información es una parte vital de los servicios prestados por ANOTEC, y ha de custodiar dicha información en todo su ciclo de vida (recogida, transporte, tratamiento, almacenamiento y destrucción). Las áreas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, garantizando así la continuidad en la prestación de los servicios con una calidad y seguridad adecuada.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

Esta Política de Seguridad asegura un compromiso manifiesto de la alta dirección para la difusión, consolidación y cumplimiento de la presente Política.

3. ALCANCE

La presente Política de Seguridad tiene aplicación a todas las áreas, servicios, empleados internos y externos de ANOTEC, cualquiera que sea su clasificación jerárquica. Igualmente, aplica a todos los sistemas de la información e infraestructuras de comunicación utilizadas para la realización de las funciones propias de ANOTEC.

Con esta política de seguridad de la información, la organización muestra su compromiso por establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de acuerdo a los principios recogidos en el artículo 5 del Real Decreto 311/2022 y la norma UNE-EN ISO/IEC 27001. Esto es:

- Entender la seguridad como un proceso integral.
- Gestionar la seguridad basándonos en los riesgos.
- Monitorizar y vigilar contínuamente los eventos de seguridad para garantizar la prevención, detección, respuesta y conservación. .
- Establecer defensas
- Evaluar el estado de la seguridad periódicamente
- Realizar una diferenciación clara de las responsabilidades

4. MISIÓN Y OBJETIVOS

ANOTEC, en el empeño por cumplir los intereses, funciones y competencias encomendadas, pone a disposición de los usuarios los servicios y actividades necesarias para satisfacer las aspiraciones e intereses de la empresa y sus usuarios. Para potenciar su misión, ANOTEC hace uso de las tecnologías apropiadas y pone en valor la relación electrónica con los usuarios, creando la confianza necesaria basada en un sistema de seguridad de la información integral y que alcanza a toda la organización.

Estos sistemas pretenden 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. Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

1. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos personales y a la prestación de servicios a través de medios electrónicos.

2. Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con rapidez a los incidentes.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

3. Proteger los recursos de información de la entidad y la tecnología utilizada para su procesamiento frente a amenazas, internas o externas, deliberadas o accidentales.

4. Proporcionar confianza a los usuarios protegiendo su información durante todo su ciclo de vida.

5. Facilitar la mejora continua de los procesos de seguridad, procedimientos, productos y servicios.

6. Garantizar la continuidad de la entidad estableciendo proyectos de contingencia en los servicios críticos y manteniendo en todo momento la seguridad.

7. Concienciar, formar y motivar al personal sobre la importancia de la seguridad en el entorno del trabajo.

5. MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades y competencias de ANOTEC y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está regulada, principalmente, por la siguiente legislación:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- 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, RGPD). 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, RGPD).

También forman parte del marco normativo las restantes normas estatales y autonómicas que pudieran afectar a la prestación del servicio de ANOTEC, a la seguridad de la información y los servicios que ésta maneja, así como a la protección de datos de carácter personal.

El mantenimiento de todo este marco normativo será responsabilidad del Responsable de Seguridad de la Información de ANOTEC, o la persona que esta delegue, y se mantendrá de forma Anexa en los medios y/o soportes que determine el Comité de Seguridad. También se incluirán las instrucciones técnicas de seguridad de obligado cumplimiento. Así mismo, el Responsable de la Seguridad asegurará que se han identificados las guías de seguridad del CCN que serán de aplicación para mejorar el cumplimiento de lo establecido en esta norma de referencia.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

De manera explícita, se atenderá a lo descrito en la Norma ISO 27001-Sistema de Gestión de la seguridad de la Información, que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002. La aplicación de la norma UNE-EN ISO/IEC 27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

6. ORGANIZACIÓN DE SEGURIDAD

La organización de la Seguridad de la Información en ANOTEC queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades.

La responsabilidad de la seguridad recae, en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad y de facilitar los recursos adecuados para alcanzar los objetivos propuestos. En este sentido, la Dirección de ANOTEC será la encargada de establecer:

- Que la Política de seguridad es adecuada con el propósito de la organización.
- Que se establece el compromiso de la organización respecto del cumplimiento de los requisitos legales.
- Que considera la seguridad como un proceso en el que debe ser aplicado por defecto y por diseño e incluirse en el inicio del desarrollo de los proyectos, aplicando las convenientes medidas de seguridad y aplicando los principios de mejora continua.

Para gestionar y coordinar proactivamente la seguridad de la información se constituye como órgano de gestión el **COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.**

A fin de gestionar y coordinar la seguridad de la información, ANOTEC, ha establecido los siguientes órganos:

Órganos colegiados:

- Comité de Seguridad

Órganos unipersonales:

- Responsable de la Información
- Director de Tecnología (CTO)
- Responsable de Seguridad
- Responsable del SGSI
- Secretario del comité

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

6.1 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El comité de seguridad de la información es el órgano colegido encargado de velar por la seguridad de la información.

NOMBRAMIENTO

Los miembros de este Comité serán nombrados por la dirección de la entidad, contemplando medidas transitorias con objeto de garantizar el cumplimiento de la seguridad. Además, las futuras resoluciones de nombramientos de responsables de áreas o cambios en la distribución de funciones de área deberán contemplar expresamente el nombramiento como miembro en este comité de seguridad de la información.

Los miembros del Comité, así como los roles de seguridad serán revisados cada tres años o con ocasión de vacante.

FUNCIONES DEL COMITE

Sus funciones son las siguientes:

- Responsabilidades derivadas del tratamiento de datos personales.
- Atender las inquietudes de la entidad y de las diferentes áreas.
- Informar regularmente del estado de la seguridad de la información a la dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de ANOTEC en lo que respecta a la 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 el propio Comité de Seguridad antes de su aprobación final la dirección.
- Aprobar la normativa de seguridad de la información.
- Evaluar los riesgos de manera periódica para establecer las adecuadas medidas de seguridad necesarias atendiendo a los resultados.
- 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 ANOTEC 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 auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la organización en materia de seguridad.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- 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.
- 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.
- Establecer medidas adecuadas para la formación, información y concienciación de todo el personal en materia de seguridad de la información y protección de datos de carácter personal.
- 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.
- En caso de ocurrencia de incidentes de seguridad de la información, aprobará el Plan de Mejora de la Seguridad.

El Comité de Seguridad de la Información no tiene por qué ser un comité técnico, pero recabará regularmente del personal técnico propio o externo la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

Resolución de conflictos:

El Comité de Seguridad de la Información, se encargará de la resolución de los conflictos y/o diferencias de opiniones que pudieran surgir entre los roles de seguridad. En caso de que el Comité no tuviera capacidad o autoridad para la resolución de determinados conflictos, lo elevará a la dirección para su resolución.

ORGANIZACIÓN DEL COMITÉ:

El comité estará constituido, al menos, por los siguientes cargos:

a. RESPONSABLE DE LA INFORMACIÓN

Determinará los requisitos de la información tratada.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. Asesorará y tendrá potestad para determinar técnicamente los requisitos de la información y de los servicios en materia de seguridad. Tendrá la potestad, igualmente, de determinar los niveles de seguridad de la información.

Así mismo informará sobre el estado de la seguridad en el área de los sistemas de la información y comunicación. Podrá convocar las reuniones, remitir información y comunicados a los miembros de la comisión.

b. DIRECTOR DE LA TECNOLOGÍA (CTO)

Determinará los requisitos de los servicios prestados.

Será la persona responsable, directamente o bien por delegación, de la explotación de las distintas áreas de la entidad estableciendo requisitos, fines y medios para la realización de dichas tareas. Determinará los requisitos de seguridad de los servicios prestados. Esto incluye la responsabilidad de determinar los niveles de seguridad de los servicios y para ello, podrá recabar asesoramiento del responsable de seguridad y del responsable del sistema.

Incluirá las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control. Tendrá, además, la misión de valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios, teniendo en consideración la repercusión en la capacidad de ANOTEC 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 usuarios.

Además, tendrán la obligación de vigilar el cumplimiento de las normas de seguridad dentro de su área e informar al **Responsable de la Información** del cumplimiento de la normativa de seguridad aprobada por el Comité de Seguridad.

c. RESPONSABLE DE LA SEGURIDAD

Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

Es la persona designada por la dirección que determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

Las dos funciones esenciales del Responsable de la Seguridad son:

a. 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 esta Política de Seguridad de la Información de la organización.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

b. Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Si el sistema de información, dado su complejidad, distribución, separación física o número de usuarios así lo requiriera, ANOTEC podrá designar **Responsables de Seguridad Delegados**, en los que se podrá delegar funciones, pero nunca responsabilidades. Estos Responsables de Seguridad Delegados tendrán dependencia directa del Responsable de Seguridad.

Entre las funciones que se le atribuyen al Responsable de Seguridad, se encuentran las siguientes:

- Coordinará y controlará las medidas definidas en el Registro de Actividades del Tratamiento y en general se encargará del cumplimiento de las medidas de seguridad que detalla el informe de evaluación de impacto en la protección de datos.
- Reportará directamente al Comité de Seguridad de la Información.
- Podrá actuar, en caso que así se determinara, como Secretario del Comité de Seguridad de la Información.
- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y realizará la categorización del Sistema.
- Realizará el Análisis de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas y del resultado del Análisis de Riesgos.
- Facilitará a la dirección información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por la norma.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información, para su aprobación por parte de la dirección.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
- Elaborará los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Analizará y propondrá salvaguardas que prevengan incidentes similares en caso de que estos se hubieran producido.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

- Elaborará los Planes de Continuidad de Sistemas que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
- Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

El responsable de la seguridad deberá ser distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades.

En el caso de externalización del servicio de responsable de seguridad, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado.

d. RESPONSABLE DEL SISTEMA

Se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad. Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados. Sus funciones, de manera concreta, son las siguientes:

a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.

b. Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

c. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

d. 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 con el Responsable de la Seguridad antes de ser ejecutada.

e. Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.

f. Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.

g. Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.

h. Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

i. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

j. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.

k. La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

l. La aplicación de los Procedimientos Operativos de Seguridad (POS).

m. Asegurar que los controles de seguridad establecidos son adecuadamente observados.

n. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

o. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

p. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

q. Informar al Responsable de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

r. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

En caso de ausencia de esta figura, las funciones del Responsable del Sistema las asumirá el Responsable de Seguridad en consonancia con las indicaciones del Director de Tecnología (CTO)

e. SECRETARIO/A DEL COMITÉ

Levantará actas de las reuniones del Comité de Seguridad de la Información. Dicho rol será asumido por el Responsable de Seguridad.

7. GESTIÓN Y ESTRUCTURA DE LA DOCUMENTACIÓN

Se deberá comunicar la información documentada relativa a los controles de seguridad al personal que trabaja en la entidad (empleados y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos de la norma.

La información documentada será clasificada en: pública o publicable, interna, confidencial y secreta, dando el uso adecuado de acuerdo a dicha clasificación y según el criterio que se establezca en la normativa de clasificación de la información.

Un procedimiento definirá los criterios de etiquetado de los documentos que formen parte del Sistema de información.

Así, la documentación que compone dicho sistema se distribuye de la siguiente manera.

1. Política de Seguridad de la Información (PO). Conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

2. Normativa (NR). Marco regulatorio que contiene las conductas permitidas o prohibidas, así como también define el alcance, conceptos básicos, marco, responsabilidades y objetivos de una determinada medida o conjunto de medidas.

3. Procedimiento (PR). Protocolos que definen y detallan procesos y mecanismos, o fases que desarrollan las diferentes acciones para la consecución de un determinado resultado.

4. Registros (RG). Se trata de herramientas y tablas que recopilan datos e indicadores con los que monitorizar el cumplimiento de un control o evaluar la eficacia del mismo.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

Este mismo orden determina la jerarquía y prelación de estos documentos.

Anotec mantedrá un registro en el que se recopilarán todos los documentos que forman parte del catálogo del sistema objeto de esta política. El Responsable del SGSI será el encargado de mantener y actualizar la documentación del sistema.

8. CONCIENCIACIÓN

ANOTEC establecerá los mecanismos necesarios, atendiendo a las propuestas del Comité de Seguridad, para que todo el personal disponga de la información, formación y concienciación apropiada para gestionar de acuerdo a esta Política de Seguridad y su normativa interna derivada la información, tanto en materia de privacidad como de seguridad.

El Comité establecerá mecanismos adecuados de difusión de la información y registrará todas las acciones formativas que se dispongan en este sentido.

9. GESTIÓN DEL RIESGO

ANOTEC realizará periódicamente y cada vez que los sistemas de la información sufran una alteración significativa un Análisis de Riesgos, siguiendo las directrices de la norma en su punto 6.1.2, de modo que se puedan anticipar los riesgos existentes. Este Análisis de Riesgos y sus conclusiones han de ser analizadas por el Comité de Seguridad y establecer las salvaguardas adecuadas para que el nivel de riesgo sea aceptable.

Para que esto se plasme el Comité desarrollará un procedimiento de Análisis de Riesgos y Evaluación de Impacto Potencial que ha de establecer claramente los valores de riesgo aceptables, los criterios de aceptación de riesgo residual, la periodicidad del análisis y cuándo se realizará de modo excepcional.

El análisis de riesgos que realice ANOTEC atenderá igualmente y de manera concreta a aquellos que se deriven del tratamiento de los datos personales en el desempeño de sus funciones.

10. PROTECCIÓN DE DATOS PERSONALES

ANOTEC únicamente recogerá datos personales 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 técnicas y organizativas pertinentes para el cumplimiento de la legislación en materia de protección de datos.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com

11. TERCERAS PARTES

Cuando ANOTEC preste servicios a otras entidades o maneje información de otras entidades, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad.

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

Cuando algún aspecto de esta Política de Seguridad 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.

12. APROBACIÓN Y REVISIÓN DE ESTA POLÍTICA DE SEGURIDAD

La presente política de seguridad ha de ser un documento que refleje fielmente el compromiso de ANOTEC con la seguridad de la información. Por lo tanto, esta política podrá ser modificada a propuesta del Comité de Seguridad para adaptarse a cambios en el entorno legislativo, técnico u organizativo. Tanto la aprobación inicial de esta política como la revisión futura de la misma, se realizará por la dirección de la entidad tras propuesta del comité de seguridad de la información. Esta política se revisará, al menos, con una periodicidad anual por el comité de seguridad o cuando las circunstancias así lo requieran.

Anotec Engineering, SLU · Plaza Escultor Domingo Sánchez Mesa, 1 - oficina 5 · 18600 Motril (Granada) · España · tel. (+34) 958 620 631
Inscrito en el Registro Mercantil de Gramada Tomo 1509 Libro 0 Folio 217 Hoja GR-44140 CIF: ESB-19538271
www.anotecengineering.com