A.T. Medtra©

Política de Seguridad

Política de Seguridad

Fecha

21 de febrero de 2022

Versión documento

Versión	Fecha	Motivo del Cambio
1.0	21/02/2022	Creación de SGSI conforme al ENS

Contenido

1. POLÍTICA DE SEGURIDAD

La Política de Seguridad de A.T. MEDTRA nace de la preocupación por parte de la Dirección de garantizar la plena satisfacción de las partes interesadas, de la gestión del servicio ofrecido a los clientes, así como la gestión de la seguridad de sus sistemas de información.

La Dirección de la organización enfoca la Seguridad de la Información, como un sistema para prestar servicios que satisfagan las necesidades del cliente, teniendo en cuenta los requisitos de la actividad de la organización, así como los requisitos legales, reglamentarios o contractuales. Todos los procesos internos y externos quedan adscritos y afectos a la presente política o cuantas políticas transversales se desarrollen para dar cumplimiento a la misma.

La Política de Seguridad tiene por objeto proteger los activos de información del sistema de información de la organización, así como los activos de información de nuestros clientes con los que exista un acuerdo contractual, ante cualquier amenaza, sea interna o externa, deliberada o accidental. Se busca garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con urgencia a los incidentes para recuperarse lo antes posible y minimizar el impacto.

La Seguridad de la Información está implícita en cada uno de los puntos de esta política, e integrada en los procesos de negocio como herramienta clave para conseguir los objetivos de negocio de la organización. Esta política queda alineada plenamente con los objetivos de negocio e integrada en la estrategia de la organización.

A.T. MEDTRA tiene implantado, y mejora continuamente, un Sistema de Gestión de la Seguridad de la Información acorde con al Esquema Nacional de Seguridad.

La Política de Seguridad tiene vigencia desde la aprobación por la Dirección y mientras no se apruebe una posterior, se mantendrá vigente. La Política es comunicada y puesta a disposición de todos los afectados, tanto internos como externos.

Toda violación de la presente política o aquellas que la desarrollen, de las normas y procedimientos, será considerado por el procedimiento disciplinario, incluyéndose proveedores y colaboradores externos que serán tramitados por su procedimiento oportuno.

2. ALCANCE

La Política de Seguridad es de aplicación sobre todo el personal de la organización, incluyendo sus contratistas y el personal contratado temporalmente; afecta a cualquier tipo de información, tanto la que sea propiedad de la organización como la que procede de clientes, con independencia del soportes o medio en el que se encuentre, tipología o categoría; y aplica a cualquier activo de información propiedad de la organización que afecte al sistema.

3. COMPROMISOS DE LA DIRECCIÓN

El Director General de AT MEDTRA está comprometido con el desarrollo e implementación del Sistema de Gestión de la Seguridad de la Información y con la mejora continua de su eficacia.

El Director General es el Responsable del Comité de Seguridad, y el resto de los responsables y trabajadores de la organización están comprometidos con la seguridad, además de por sus cargos, por formar parte del Comité de Seguridad, y ser así parte activa del mismo.

El Director General:

- Comunica a la organización la importancia de satisfacer tanto los requisitos del cliente como los de seguridad, del servicio, los legales, reglamentarios, y las obligaciones contractuales.
- Establece y comunica el alcance del SGSI.
- Define y comunica la Política de Seguridad, normas y procedimientos.
- Comunica la Política de Seguridad y la importancia de cumplir con ella a clientes y a proveedores (contrato de confidencialidad).
- Asegura el establecimiento y la comunicación de los objetivos de seguridad de la Información.
- Lleva a cabo las revisiones por la Dirección anuales.
- Dirige las revisiones del SGSI.
- Vela por que se realicen las auditorías internas del SGSI, anualmente.
- Asegura que se revisan los resultados de las auditorías para identificar oportunidades de mejora.
- Asegura la provisión y disponibilidad de recursos.
- Asegura que se gestionan y se evalúan los riesgos de seguridad de la información, a intervalos planificados.
- Define el enfoque a tomar para la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos.
- Aprueba los niveles de riesgo aceptables para la organización.
- Establece roles y responsabilidades en materia de seguridad.
- Determina las cuestiones externas e internas que son pertinentes para el propósito de la organización y su dirección estratégica.

El compromiso de la Dirección está reflejado en la presente política.

4. OBJETIVOS

Los objetivos del Sistema de Gestión de la Seguridad de la Información (SGSI) de la organización son:

- Mantener una gestión adecuada del SGSI de acuerdo con los estándares de seguridad y las buenas prácticas del sector, llevando a cabo todo esto de manera que se aseguren ventajas competitivas para la organización.

- Proteger la información interna 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 dudas.
- Establecer anualmente objetivos específicos en relación a la Seguridad de la Información, que garanticen la mejora continua del SGSI, siendo estos consistentes con los presentes objetivos.
- Desarrollar un proceso de análisis del riesgo y, de acuerdo a su resultado, implementar las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos.
- Establecer los medios necesarios para garantizar la continuidad del negocio de la organización.
- Cumplir con los requisitos del negocio, las obligaciones legales y las obligaciones contractuales de seguridad.
- Asegurar que los activos de la organización solo sean utilizados por usuarios autorizados en el ejercicio de sus funciones, sus perfiles definidos o según asignaciones extraordinarias.
- Establecer y difundir los roles y responsabilidades relacionados con la Seguridad de la Información.
- Sensibilizar y concienciar de manera estable y permanente a todo el personal de la organización en cuanto a la seguridad de la información.
- Fomentar y mantener el buen nombre de la organización en relación a los servicios desarrollados, saber y respuesta activa (reactiva y proactiva) ante incidentes de seguridad, mantenimiento la imagen y reputación.
- Reflejar en la Declaración de Aplicabilidad del ENS las medidas de seguridad y dimensiones definidos en el Esquema Nacional de Seguridad.
- Sancionar cualquier violación a esta política, así como a cualquier política o procedimiento del SGSI.

5. LEGISLACIÓN APLICABLE Y REQUISITOS CONTRACTUALES

Se identifican las siguientes obligaciones legales aplicables a la organización en relación a la seguridad de la información:

- **Esquema Nacional de Seguridad**:
  - Real Decreto 3/2010 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
  - 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.
  - 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.
  - Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
  - Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
  - 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.
  - Aplicabilidad: alcance del SGSI.
- **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 (RGPD)**.
- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**.
  - Aplicabilidad: tratamiento de datos de carácter personal propios tanto de A.T.MEDTRA, como de empresas externas (encargados de tratamiento, destinatarios).
- **Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE)**
  - Aplicabilidad: actividades comerciales en internet de la organización.
- **Ley Orgánica 10/1195, de 23 de noviembre, del Código penal**.
  - Aplicabilidad: actividad de la empresa.
- **Copyright – Derecho de autor**. **Real decreto 1/1196 Derechos de autor y propiedad intelectual. Ley 17/2001 Derechos de marcas nombres comerciales.**
  - Aplicabilidad: licencias software, nombres comerciales.

Además, se consideran los requisitos contractuales establecidos en contratos de clientes o proveedores que requieren de requisitos específicos en materia de seguridad.

6. ESTRUCTURA DE SEGURIDAD

En PR-Estructura de Seguridad se establecen los roles de seguridad, defiendo para cada uno, los deberes y responsabilidades de su cargo, así como el procedimiento para su designación y renovación.

Además, en el mencionado documento se establece la estructura del Comité de Seguridad para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

Los roles y responsabilidades en relación al SGSI son comunicados a las nuevas incorporaciones y recordados periódicamente a todo el personal de la organización.

7. DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA

La documentación generada dentro del SGSI es controlada y aprobada por el Comité de Seguridad.

Esta documentación se encuentra localizada en un directorio de acceso restringido (**\\Servidor2\ENS-Comite)** para los miembros del Comité, únicamente haciéndose públicos los documentos que se consideran que debe ser conocidos por todos a través de **\\Servidor2\ENS.**

En *PR- Control de Documentación* se establece la gestión que se realiza de la documentación del SIG, especificando la categorización establecida.

8. PRINCIPIOS DE SEGURIDAD

El SGSI se encuentra enmarcado por los siguientes principios de seguridad:

- Seguridad por defecto.
- Seguridad basada en el liderazgo y en la organización.
- Organización de la Seguridad
- Seguridad basada en procedimientos
- Seguridad gestionada en base al riesgo
- Seguridad considerando incidentes
- Continuidad de los servicios
- Seguridad considerando la gestión de recursos
- Seguridad de áreas y entorno
- Seguridad como requisito legal

8.1 SEGURIDAD POR DEFECTO

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La seguridad del sistema contempla los aspectos

de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

Las funciones de operación, administración y registro de actividad son las mínimas necesarias, y se asegura que sólo son accesibles por las personas, o desde localizaciones o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso.

El uso del sistema es sencillo y seguro, de forma que una utilización insegura requiere de un acto consciente por parte del usuario.

Para mantener el proceso de seguridad integral, se realiza una organización de la información en carpetas de acceso restringido, conforme a los principios de protección frente a pérdidas, accesos indebidos, divulgación o uso indebido, deterioro de la información o pérdida de disponibilidad. Cada usuario únicamente accede a la información que requiere para llevar a cabo su actividad.

Se conoce en todo momento el estado de seguridad del sistema o de sus componentes, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les puedan afectar.

8.2 SEGURIDAD BASADA EN EL LIDERAZGO Y EN LA ORGANIZACIÓN

La seguridad compromete a todos los miembros de la organización, en base a sus diferentes roles, considerando diferentes responsabilidades.

La Dirección es quien lidera la organización y promueve la cultura de seguridad, asignando los roles requeridos y potenciando la transversalidad de la seguridad en cada proceso desarrollado o servicio a terceros.

La seguridad del sistema es revisada de conformidad a los requisitos, la política y los procedimientos aprobados por la Dirección. Las revisiones son por parte de la Dirección y por revisiones internas o auditorias del sistema. Específicamente la organización y el sistema se pueden someter a procesos de certificación externos, conforme a lo establecido por el Esquema Nacional de Seguridad y cualquier otro estándar de seguridad que le pudiera interesar.

8.3 ORGANIZACIÓN DE LA SEGURIDAD

Se establece una estructura organizativa en la organización, donde se establecen roles específicos, pero siempre considerando el principio de separación de funciones. Se designan a las personas que ocupan los roles, por periodos anuales, siendo estos renovados automáticamente mientras que la Dirección no establezca una nueva persona para ocupar el cargo.

8.4 SEGURIDAD BASADA EN PROCEDIMIENTOS

La seguridad del sistema se documenta mediante procedimientos de operación que son puestos a disposición de los usuarios implicados en el mismo. Los cambios son gestionados, las capacidades del sistema son medidas y controladas y los entornos están separados. Se desarrollan procedimientos de protección del sistema, incluyendo procedimientos de copias y restauración.

Se documentan los acuerdos con proveedores y colaboradores que forman parte del sistema. La cadena de suministro es controlada con relación a los requisitos de seguridad, la prestación de servicios o los cambios de suministradores.

Las redes son gestionadas, incluyendo cuando sea necesario, el cifrado o el control de comunicaciones.

8.5 SEGURIDAD GESTIONADA EN BASE AL RIESGO

La gestión de riesgos es parte esencial del proceso de seguridad, manteniéndose permanentemente actualizado, bajo el liderazgo de la Dirección.

La gestión de riesgos se realiza por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema de información y la organización, basándose en la metodología detallada y documentada en *PR-Análisis y Gestión de Riesgos,* permitiendo la repetición de la medición y análisis.

8.6 SEGURIDAD CONSIDERANDO INCIDENTES

El proceso de gestión de incidentes, incluye la detección y notificación de los incidentes de seguridad, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas, especialmente cuando afecta a terceros, y el registro de las actuaciones ejecutadas.

Los incidentes de seguridad permiten la recopilación de evidencias, de manera que se pueda identificar y documentar la recogida, la adquisición y la preservación de la información.

8.7 CONTINUIDAD DE LOS SERVICIOS

La continuidad forma parte del sistema de gestión, conforme a las necesidades de la organización y los controles establecidos. La organización considera el análisis de impacto y las consecuencias de la información que el mismo muestre.

8.8 SEGURIDAD CONSIDERANDO LA GESTIÓN DE RECURSOS

Todo el personal relacionado con el sistema y con la información, es formado e informado de sus deberes y obligaciones en materia de seguridad, siendo controladas y supervisadas sus acciones.

Cada usuario que accede a la información del sistema está identificado de forma única, de modo que se conoce, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

La responsabilidad es exigible mediante un procedimiento disciplinario, que al igual que las pautas de seguridad, conoce previamente el usuario. Este procedimiento está alineado con la normativa laboral.

El usuario con acceso concedido al sistema, pueda o no desarrollar acciones, está sometido a secreto y reserva, aun cuando finalice su relación con la organización. Ningún usuario accede al sistema sin estar previamente informado de este extremo.

8.9 SEGURIDAD DE ÁREAS Y ENTORNO

La organización previene los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Las áreas pueden ser de control propio o derivadas al propio prestador afectado.

8.10 SEGURIDAD COMO REQUISITO LEGAL

La Dirección establece como requerimiento de seguridad, el pleno cumplimiento de las obligaciones legales y contractuales, ligadas a la información. Los requisitos son identificados y organizados para su correcta gestión.

Para tener éxito en la Política de Seguridad enunciada, esta Dirección solicita la adhesión y participación de todos a todos los niveles, tanto en sus actuaciones individuales como cuando forman parte de grupos de trabajo, con el fin de establecer y mantener al día un Sistema de Gestión de Seguridad de la Información que asegure la satisfacción de nuestros clientes y la consecución de los Objetivos de Negocio.

9. DATOS DE CARÁCTER PERSONAL

A.T. MEDTRA trata datos de carácter personal de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD). La organización está cumpliendo con todas las disposiciones del GDPR para el tratamiento de los datos personales de su responsabilidad, y manifiestamente con los principios descritos en el artículo 5 del GDPR,

por los cuales son tratados de manera lícita, leal y transparente en relación con el interesado y adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

La organización garantiza que implementa políticas técnicas y organizativas apropiadas para garantizar las medidas de seguridad que establece el artículo 32 GDPR con el fin de proteger los derechos y libertades de los interesados.

Isidoro Fernández Muñoz
Director General de A.T. MEDTRA, S.L.

72110010L ISIDORO FERNANDEZ (R: B39305156)

Firmado digitalmente por 72110010L ISIDORO FERNANDEZ (R: B39305156)
Fecha: 2022.08.17 08:20:18 +02'00'

Datos de Contacto

A.T. MEDTRA, S.L.
Parque Científico y Tecnológico
Edificio 3000
C/ Isabel Torres 11 B
39011 Santander
Cantabria
España

Servicio Online de Lunes a Viernes de 08:30 de la mañana a 18:30 de la tarde
Teléfono: 942 23 51 41
Fax: 942 24 12 05

Correo electrónico:
atmedtra@atmedtra.es
Web:
www.atmedtra.es