Política de Seguridad de la Información

Comité de Seguridad

Fecha de aprobación: 15 dic 2022

Clasificación: USO PÚBLICO

1. OBJETO

Recopilar las Políticas de Seguridad de la Información de **ADA SISTEMAS**, que proporcionarán orientación para la gestión y el apoyo a la seguridad de la información, de acuerdo con los requisitos comerciales de la entidad, con las leyes y regulaciones aplicables, además de establecer el alcance del Sistema de Gestión de la Seguridad de la Información (SGSI).

2. ALCANCE

Este procedimiento se aplicará a todo el personal de **ADA SISTEMAS** involucrado en el desarrollo, implementación y mantenimiento del Sistema de Gestión de la Seguridad de la Información.

3. REFERENCIAS

Apartados de la Norma UNE-ISO/IEC 27001:2014:

- 5.2 Política
- A.5.1.1 Políticas para la seguridad de la información
- A.5.1.2 Revisión de las Políticas para la Seguridad de la Información

4. DESARROLLO

4.1. Directrices de Gestión de la Seguridad de la Información

Esta política gestiona la seguridad de la información de **ADA SISTEMAS** desde el más alto nivel de gestión de la organización, estableciendo un marco para controlar la implementación del Sistema de Gestión de la Seguridad de la Información, la aprobación de la política de seguridad, la distribución de esta a empleados, proveedores, clientes, y en última instancia para todos los interesados, ya sean internos o externos a la organización.

La Política de Seguridad de la Información está definida y aprobada por la DIRECCION de **ADA SISTEMAS** y ha tenido en cuenta las características del negocio, los requisitos contractuales firmados con los clientes, así como la legislación más relevante que afecta al Sistema de Gestión de la Seguridad de la Información de **ADA SISTEMAS**.

4.2. Política de Seguridad de la Información Corporativa

En **ADA SISTEMAS**, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, por lo que existe un compromiso expreso de protegerla como parte de una estrategia orientada a la continuidad del negocio, la gestión de riesgos y la consolidación de una cultura de seguridad, basándonos para ello, en los tres pilares fundamentales de la seguridad de la información:

- **Confidencialidad**: es la garantía de acceso a la información de los usuarios que se encuentran autorizados para tal fin.
- **Integridad**: es la preservación de la información completa y exacta.
- **Disponibilidad**: es la garantía de que el usuario accede a la información que necesita en ese preciso momento.

Los citados pilares garantizan la seguridad de la información en las áreas de seguridad física, lógica e institucional.

Entendiendo la confidencialidad, integridad y disponibilidad de la información como un marco de referencia, y alineando estos con los requisitos de negocio, **ADA SISTEMAS** establece los siguientes objetivos de Seguridad:

- Asegurar que los activos de información reciban un nivel adecuado de protección.
- Clasificar la información para indicar su sensibilidad y criticidad.
- Definir los niveles de protección y las medidas especiales de tratamiento según su clasificación.

Para la consecución de dichos objetivos **ADA SISTEMAS** atenderá a los siguientes requisitos de Seguridad de la Información:

- La seguridad en la Gestión de los Recursos Humanos, antes durante y al finalizar el empleo.
- La gestión adecuada de los activos que implique la clasificación de la información y la manipulación de los soportes
- El establecimiento de un robusto control de acceso lógico a sus sistemas y aplicaciones, gestionando los permisos y los privilegios de los usuarios.
- La protección de las instalaciones y del entorno físico, mediante el diseño de áreas de trabajo seguras y la seguridad de los equipos.
- La garantía de la seguridad en las operaciones mediante la protección contra el software malicioso, la realización de copias de seguridad, el establecimiento de registros y su supervisión. el control del software en explotación. la gestión de las vulnerabilidades técnicas y la elección de técnicas - adecuadas para la auditoria de los Sistemas.
- La seguridad de las comunicaciones, protegiendo las redes y el intercambio de Información.
- El aseguramiento de la seguridad en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.
- La realización de un desarrollo seguro de software, separando los entornos de desarrollo y producción, y realizando las pruebas funcionales de aceptación adecuadas
- El control de las relaciones con los proveedores, exigiendo de forma contractual el cumplimiento de las medidas de seguridad pertinentes y unos niveles aceptables en la prestación de sus servicios.
- La eficacia en la gestión de los Incidentes de seguridad, estableciendo los canales adecuados para su notificación, respuesta y aprendizaje oportuno.
- La realización de un plan de continuidad de negocio que proteja la disponibilidad de los servicios durante una crisis o desastre.
- La Identificación y cumplimiento de la normativa aplicable poniendo especial interés en la propiedad intelectual y en la protección de los datos de carácter personal.
- La revisión de los presentes requerimientos de la seguridad de la información para garantizar el cumplimiento y eficacia de estos.

La Dirección de **ADA SISTEMAS**, mediante la presente política de Seguridad, se compromete a gestionar la seguridad de la información, para cumplir los objetivos de seguridad marcados, realizando planes de tratamiento del riesgo que hayan sido resultado del correspondiente análisis al que se verán sometidos los sistemas de la información de la organización.

Para ello, la Dirección de **ADA SISTEMAS** ha nombrado un Comité de Seguridad**,** cuya función principal será determinar los requisitos de seguridad asociados a los servicios y medir los objetivos de seguridad con métricas predeterminadas que ofrezcan resultados objetivos y comparables, y que permitan determinar su eficacia para poder así, identificar las posibles mejoras.

4.3. Seguridad de los Recursos Humanos

Los objetivos de controlar la seguridad del personal son:

- Reducir los riesgos de error humano, puesta en marcha de irregularidades, uso indebido de instalaciones y recursos, y manejo no autorizado de la información.
- Explicar las responsabilidades de seguridad en la etapa de reclutamiento del personal e incluirlas en los acuerdos a firmar y verificar su cumplimiento durante el desempeño de las tareas del empleado.
- Asegúrese de que los usuarios estén al tanto de las amenazas y preocupaciones de seguridad de la información y estén capacitados para apoyar la Política de Seguridad de la Información de la organización en el curso de sus tareas normales.
- Establecer compromisos de confidencialidad con todo el personal y usuarios fuera de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de las debilidades de seguridad existentes, así como los incidentes, con el fin de minimizar sus efectos y prevenir su reincidencia.

Esta Política se aplica a todo el personal de **ADA SISTEMAS** y el personal externo que realiza tareas dentro de la empresa.

RRHH incluirá funciones de seguridad de la información en las descripciones de los trabajos de los empleados, informará a todo el personal que contrate sus obligaciones con respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

El Responsable de Gestión de la Seguridad (RGS) (CISO), es responsable de monitorear, documentar y analizar los incidentes de seguridad reportados, así como de comunicarlos al Comité de Seguridad de la Información y a los propietarios de información.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Gestión de la Seguridad (RGS) (CISO) maneje informes de incidentes y anomalías del sistema. El Comité también estará al tanto, supervisará la

investigación, supervisará la evolución de la información y promoverá la resolución de incidentes de seguridad de la información.

El Responsable de Gestión de la Seguridad (RGS) (CISO) participará en la preparación del Compromiso de Confidencialidad que firmará los empleados y terceros que desempeñen funciones en **ADA SISTEMAS**, en el asesoramiento sobre las sanciones que se aplicarán por incumplimiento de esta Política y en el tratamiento de incidentes de seguridad de la información.

Todo el personal de **ADA SISTEMAS** es responsable de informar sobre las debilidades e incidentes de seguridad de la información que se detectan oportunamente.

4.4. Seguridad Física y Ambiental

Los objetivos de esta política son:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de **ADA SISTEMAS**.
- Proteger el equipo de procesamiento de información crítico de **ADA SISTEMAS**, colocándolo en áreas protegidas y protegido por un perímetro de seguridad definido, con las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección de la misma en su traslado y permanecer fuera de las áreas protegidas, por mantenimiento u otros motivos.
- Controlar los factores ambientales que podrían perjudicar el buen funcionamiento del equipo de cómputo que alberga la información de **ADA SISTEMAS**.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus tareas habituales.
- Proporcionar protección proporcional a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de **ADA SISTEMAS**: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

El Responsable de Gestión de la Seguridad (RGS) (CISO), junto con los Titulares de la Información, según proceda, definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal de **ADA SISTEMAS** a las áreas restringidas bajo su responsabilidad. Los Propietarios de Información autorizarán formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de **ADA SISTEMAS** cuando lo consideren apropiado.

Todo el personal de **ADA SISTEMAS** es responsable del cumplimiento de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas.

4.5. Control de Acceso a los Sistemas de Información

El control del acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de **ADA SISTEMAS** y otras redes públicas o privadas.
- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.

4.6. Desarrollo y Mantenimiento del Sistema

La seguridad en el desarrollo y mantenimiento de sistemas tiene como objetivo:

- Garantizar la inclusión de controles de seguridad y validación de datos en el desarrollo de sistemas informáticos.
- Definir y documentar los estándares y procedimientos que se aplicarán durante el ciclo de vida de la aplicación y en la infraestructura base en la que se admiten.
- Definir métodos para proteger la información crítica o sensible.

Esta Política se aplica a todos los sistemas informáticos, tanto de desarrollo propio o de terceros, como a todos los Sistemas Operativos y/o Software que integren cualquiera de los entornos administrados por **ADA SISTEMAS**.

El Responsable de Gestión de la Seguridad (RGS) (CISO) junto con el propietario de la Información definirá los controles a implementar en sistemas desarrollados internamente o por terceros, sobre la base de una evaluación previa del riesgo.

El Responsable de Gestión de la Seguridad (RGS) (CISO) junto con el Propietario de la Información, definirá en función de la criticidad de la información, los requisitos de protección por métodos criptográficos. A continuación, el CISO definirá, junto con el CTO, los métodos de cifrado que se utilizarán.

4.7 Gestión de Incidentes

Los objetivos principales de la Gestión de incidentes son los de:

- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo.
- Reducir los posibles riesgos e impactos que pueda causar el incidente.
- Velar por la integridad de los sistemas en el caso de un incidente de seguridad
- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma; y poner en práctica un plan de comunicación empresarial adecuado.
- Promover la eficiencia empresarial.

4.8. Gestión de la Continuidad del Negocio

La seguridad en la administración de la continuidad de las actividades de **ADA SISTEMAS** tiene como objetivos:

- Minimizar los efectos de posibles interrupciones de las actividades normales de **ADA SISTEMAS** (ya sean resultado de desastres naturales, accidentes, fallas de equipos, acciones deliberadas u otros hechos) y proteger los procesos críticos a través de una combinación de controles preventivos y acciones de recuperación.
- Analizar las consecuencias de la interrupción del servicio y tomar las medidas adecuadas para prevenir hechos similares en el futuro.
- Maximizar la efectividad de las operaciones de contingencia de **ADA SISTEMAS** con el establecimiento de planes que incluyan al menos los siguientes pasos:

  1. **Notificación/Activación**: Consistente en la detección y determinación de daños y activación del plan.
  2. **Reanudar**: Consistente en la restauración temporal de las operaciones y la recuperación de los daños causados al sistema original.
  3. **Recuperación**: Consistente en la restauración de las capacidades del proceso del sistema a condiciones normales de funcionamiento.

- Garantizar la coordinación con el personal de **ADA SISTEMAS** y los contactos externos que participarán en estrategias de planificación de contingencias. Asigne funciones para cada actividad definida.

El Responsable de Gestión de la Seguridad (RGS) [CISO] participará activamente en la definición, documentación, pruebas y actualización de planes de contingencia. Los Propietarios de Información y el Responsable de Gestión de la Seguridad (RGS) [CISO]realizarán las siguientes funciones:

- Identificar las amenazas que puedan causar interrupciones en los procesos o actividades de **ADA SISTEMAS**.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global para abordar la continuidad de las actividades de **ADA SISTEMAS**.
- Preparar los planes de contingencia necesarios para asegurar la continuidad de las actividades de **ADA SISTEMAS**.

4.9. Revisión de la Políticas de Seguridad de la Información

Cada responsable de Departamento garantizará la correcta implementación y cumplimiento de las reglas y procedimientos establecidos de seguridad de la información, dentro de su área de responsabilidad.

El Responsable de Gestión de la Seguridad (RGS) (CISO) llevará a cabo revisiones periódicas de todas las áreas de **ADA SISTEMAS** con el fin de garantizar el cumplimiento de las políticas, reglas y procedimientos de seguridad de la información. Las áreas a revisar incluyen:

- Sistemas de información.
- Proveedores del sistema.
- Propietarios de información.
- Usuarios.

Los Propietarios de Información apoyarán la revisión periódica del cumplimiento de las políticas, estándares, procedimientos y otros requisitos de seguridad de la información aplicables.

Así mismo, las Políticas de la Seguridad de la Información se revisarán al menos de forma anual o cuando por incidentes, o cambios en el sistema se estime oportuno. Los resultados de las revisiones serán siempre supervisados por el Responsable de Gestión de la Seguridad (RGS) (CISO).

Los resultados de las revisiones se incluirán en el informe anual de la Revisión del Sistema por la Dirección.

4.10 Incumplimiento de las Políticas

El incumplimiento de políticas, normas y procedimientos de **ADA SISTEMAS** en materia de seguridad de la información se considera un delito grave o muy grave, dando lugar a la aplicación de sanciones de acuerdo con la legislación vigente, sin perjuicio de cualquier otra responsabilidad derivada de las mismas. Se considera falta:

- **"Grave"** aquel incumplimiento de políticas, normas y procedimientos de **ADA SISTEMAS** en materia de seguridad de la información que afecte a las obligaciones y responsabilidades del personal.
- **"Muy grave"** aquel incumplimiento de políticas, normas y procedimientos de **ADA SISTEMAS** en materia de seguridad de la información que afecte a las obligaciones y responsabilidades del personal y, que además de eso, comporte un agravio para la organización o las personas que forman parte de ella, ya sea por temas de secreto profesional, pérdidas económicas o daños morales o reputación de **ADA SISTEMAS** o de las personas que forman parte de **ADA SISTEMAS**.

Estos incumplimientos también se recogen en el procedimiento sobre uso adecuado de sistemas de información

5. RESPONSABILIDADES

Las responsabilidades definidas por la metodología y actividades descritas en el procedimiento son las siguientes:

Roles	Responsabilidades
Dirección	• Definir y aprobar la Política de Seguridad • Nombrar al Comité de Seguridad
Responsable RRHH	• Informar a todo el personal que contrate sus obligaciones con respecto al cumplimiento de la Política de Seguridad de la Información • Gestionar los Compromisos de Confidencialidad con el personal • Coordinar las tareas de capacitación de los usuarios con respecto a esta Política.
Responsable de Gestión de la Seguridad (RGS) (CISO)	• Monitorear, documentar y analizar los incidentes de seguridad reportados • Comunicar al Comité de Seguridad de la Información y a los propietarios de información los incidentes de seguridad. • Participar en la preparación del Compromiso de Confidencialidad que firmará los empleados y terceros que desempeñen funciones en **ADA SISTEMAS**,

	• Definir las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación • Verificar el cumplimiento de las disposiciones de seguridad física y medioambiental. • Definir los controles a implementar en sistemas desarrollados internamente o por terceros, sobre la base de una evaluación previa del riesgo. • Definir en función de la criticidad de la información, los requisitos de protección por métodos criptográficos • definir, junto con el CTO, los métodos de cifrado que se utilizarán • Participar activamente en la definición, documentación, pruebas y actualización de planes de contingencia • Llevar a cabo revisiones periódicas de todas las áreas de **ADA SISTEMAS** con el fin de garantizar el cumplimiento de las políticas, reglas y procedimientos de seguridad de la información. • Supervisar los resultados de las revisiones de las Políticas
Responsable de Área / Departamento / Proyecto (Afectados)	• Definir los niveles de acceso físico del personal de **ADA SISTEMAS** a las áreas restringidas bajo su responsabilidad • Garantizar la correcta implementación y cumplimiento de las reglas y procedimientos establecidos de seguridad de la información
Comité de Seguridad	• Implementar los medios y canales necesarios para que el Responsable de Gestión de la Seguridad (RGS) (CISO) maneje informes de incidentes y anomalías del sistema • Supervisar la investigación, supervisar la evolución de la información y promoverá la resolución de incidentes de seguridad de la información. •
Propietarios de Información	• Autorizar el trabajo fuera del sitio con información sobre su negocio a los empleados de ADA SISTEMAS cuando lo consideren apropiado.

	• Definir los controles a implementar en sistemas desarrollados internamente o por terceros, sobre la base de una evaluación previa del riesgo. • Definir en función de la criticidad de la información, los requisitos de protección por métodos criptográficos • Revisar periódica del cumplimiento de las políticas, estándares, procedimientos y otros requisitos de seguridad de la información aplicables.
Todo el personal	• Informar sobre las debilidades e incidentes de seguridad de la información que se detectan oportunamente. • Cumplir de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas.