POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código	SGSI-03
Documento	Política de Seguridad de la Información
Versión	1.0
Fecha de la versión	29/01/2025
Nivel de confidencialidad	Pública
Aprobado por	Dirección
Firma y fecha de la aprobación	

© CYBERTIX SIMULATION TECHNOLOGIES SL – Confidencial.

Información del documento	
Entidad	FIT LEARNING Systems S.L.
Objeto	Exponer la Política de Seguridad de la Información de la Entidad, entendida como conjunto de principios básicos y líneas de actuación a los que la organización se compromete.
Ámbito de aplicación	Todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen información que se encuentre dentro del alcance del Sistema de Gestión de la Seguridad de la Información.
Usuarios	Todas las personas con acceso a la información dentro del alcance, independientemente de si el individuo es empleado o no de la Entidad (aplica también a contratistas, clientes o cualquier tercero que tenga acceso a la información).
Documentos relacionados	• Alcance del SGSI. • Lista de requisitos del SGSI.
Propietario del documento	Responsable de la Seguridad de la Información.
Validez y actualización	El propietario del documento es el responsable de verificar, y si es necesario, actualizar, el documento por lo menos una vez al año. Asimismo, el propietario del documento es competente para interpretar las dudas que puedan surgir en su aplicación y verificar su efectividad. Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios: • La cantidad de personal, interno y externo, que cumplen una función en el SGSI pero que no están familiarizados con esta política. • La existencia de responsabilidades ambiguas o ineficacia en la implementación y mantenimiento del SGSI. • El incumplimiento del SGSI en relación a la normativa, obligaciones contractuales y demás documentos internos de la organización.

Anexos	
Código	Descripción
SGSI-03.01	Designación de responsables en la seguridad de la información
SGSI-03.02	Cartel de política de seguridad de la información

ÍNDICE

1. Introducción

La información es un activo que, al igual que otros activos importantes, es esencial para las actividades de la organización y, por consiguiente, necesita ser debidamente protegida. La información puede ser almacenada de muchas formas, incluyendo: formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato material (por ejemplo, papel), así como la información intangible que forma parte del conocimiento del personal.

Toda la información guardada y procesada por la organización está expuesta a ataques, errores, riesgos naturales (por ejemplo, inundaciones o incendios) y está expuesta a vulnerabilidades inherentes a su uso.

Por tanto, este activo debe ser adecuadamente protegido, mediante controles y medidas de seguridad frente a las distintas amenazas que puedan afectarle, independientemente de los soportes en la que se encuentre (papel o soporte digital), medios de transmisión, sistemas, equipos o personas que intervengan en su recogida, registro, tratamiento o supresión.

La Seguridad de la Información es la protección de este activo con la finalidad de asegurar que la información no está accesible a aquellas personas o entidades no autorizadas, que dicha información es veraz y no ha sido objeto de manipulaciones no autorizadas y que está disponible cuando se necesita.

La Seguridad de la Información es un proceso que requiere de medios técnicos y humanos, en la que es fundamental la máxima implicación y colaboración de todo el personal de la organización.

La Dirección es consciente del valor de la información y está profundamente comprometida con la política descrita en el presente documento.

2. Términos y definiciones

- **Confidencialidad**: es la propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
- **Integridad**: es la propiedad de la información por la cual solo es modificada por personas o entidades autorizadas y de una forma permitida, de manera que dicha información sea veraz y completa.
- **Disponibilidad**: es la propiedad de la información de ser accesible y estar lista para su uso a demanda de una entidad autorizada.
- **Sistema de información:** es el conjunto de aplicaciones, servicios, activos de tecnologías de la información y otros componentes que se utilizan para manejar la información.
- **Seguridad de la información**: es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión de la Seguridad de la Información (SGSI)**: conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son gestionados de manera colectiva por una organización. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar sus objetivos de negocio.
- **Riesgo:** estimación del nivel de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

3. Principios fundamentales de esta Política

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, en su transmisión, transporte, almacenamiento y hasta su borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

- **Principio de confidencialidad:** la información y los sistemas de información deberán ser accesibles únicamente para aquellas personas, órganos, entidades y/o procesos expresamente autorizados para ello. A esto se suma la obligación de secreto profesional de todo el personal que tenga acceso a la información.

- **Principio de integridad:** se deberá garantizar el mantenimiento de la integridad de la información, así como de los procesos de tratamiento de la misma, estableciéndose mecanismos para asegurar que los procesos de creación, recepción, tratamiento, almacenamiento y distribución de la información contribuyan a preservar que sea veraz y completa.
- **Principio de disponibilidad y continuidad:** se deberá garantizar un nivel de disponibilidad en los sistemas de información y se dotará de medidas necesarias para asegurar la continuidad de los servicios y su recuperación ante posibles contingencias graves.
- **Principio de gestión del riesgo:** se deberá habilitar un proceso metódico, sistemático y continuo de análisis, evaluación y tratamiento de los riesgos para la seguridad de la información como mecanismo básico sobre el que debe girar la gestión de la seguridad de la información.
- **Principio de proporcionalidad en costes:** la implantación de los controles y medidas de seguridad que mitiguen los riesgos de seguridad de la información deberá realizarse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará de que los recursos para el SGSI estén disponibles.
- **Principio de concienciación y formación:** se desarrollarán iniciativas que permitan al personal involucrado en el SGSI conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De la misma forma, se fomentará la formación específica en seguridad TIC de todas aquellas personas que gestionan y administran los sistemas de información y los dispositivos de red y telecomunicaciones.
- **Principio de prevención:** se desarrollarán planes y actuaciones específicas orientadas a prevenir la ocurrencia de incidentes relacionados con la seguridad de la información.
- **Principio de detección y respuesta:** se debe monitorizar la operación del sistema continuamente para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, respondiendo eficazmente, a través de los mecanismos establecidos, a los incidentes de seguridad que ocurran.
- **Principio de mejora continua:** se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad de la información planificados anualmente y el grado de eficacia de los controles y medidas de seguridad implantadas, con el fin de adecuarlos a la evolución de los riesgos y el entorno tecnológico cambiante.
- **Principio de la seguridad de la información en el ciclo de vida de los sistemas:** las especificaciones de seguridad de la información se incluirán en todas las fases del ciclo de vida de los sistemas y servicios, a través de los correspondientes procedimientos de control.

4. Objetivos y medición

Los objetivos generales para el SGSI son los siguientes:

- Gestionar los riesgos que existen para la seguridad de la información de una forma sistemática, completa y contrastada.
- Aumentar confianza de los clientes y otras partes interesadas, en cuanto a la seguridad de la información que nos depositan, y a la que tenemos (o podríamos) tener acceso.
- Cumplir con las obligaciones contractuales contraídas con los clientes, tantos externos como internos.
- Cumplir con los SLA (acuerdos de nivel de servicio) que hemos establecido.
- Cumplir con las disposiciones y requisitos marcados por la normativa de protección de datos personales y el resto de las leyes aplicables a la organización.
- Asegurar la mejora continua del SGSI para responder a los cambios futuros.

El Director General es el responsable de revisar estos objetivos generales y establecer nuevos.

Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por el Responsable de la Seguridad de la Información y son aprobados por el Director General.

5. Requisitos de seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información y la protección de datos personales, como también con las obligaciones contractuales.

En el documento ***Lista de requisitos del SGSI*** se detallan los requisitos legales, normativos, contractuales y de otra índole aplicables al SGSI.

6. Roles, funciones y responsabilidades

La Dirección asigna y comunica las responsabilidades, autoridades y roles en lo referente a la seguridad de la información. También se asegurará de que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados.

A continuación, se describen los roles que existen en la organización y sus responsabilidades.

6.1. Dirección

La Dirección está comprometida con la política descrita en este documento y el consciente del alto valor de la información y del grave impacto económico y de imagen que puede producir un incidente de seguridad.

La Dirección asume las siguientes responsabilidades:

- Demostrar liderazgo y compromiso con respecto al SGSI.
- Asegurar que se establece la política y los objetivos de seguridad de la información y que son compatibles con la dirección estratégica de la organización.
- Aprobar y comunicar la Política de Seguridad de la Organización, así como las normas de uso de los sistemas y la importancia de su cumplimiento a todo el personal, interno y externo, a los clientes y a los proveedores.
- Reunirse al menos una vez al año, y cuando cualquier evento o solitud extraordinaria lo demande, para ser informado sobre el SGSI y actualizar la estrategia, en su caso, en materia de seguridad de la información.
- Asegurar que estén disponibles los recursos necesarios para el funcionamiento y cumplimiento del SGSI.
- Fomentar una cultura de seguridad de la información.
- Apoyar la mejora continua en los procesos de seguridad de la información.
- Definir el enfoque del análisis y evaluación de riesgos de seguridad de la información y los criterios para asumir los riesgos, así como asegurar la evaluación continua de ellos con al menos una periodicidad anual.
- Aprobar la documentación correspondiente del SGSI.
- Determinar las medidas disciplinarias o de cualquier otro tipo, que puedan aplicarse a los responsables de brechas de seguridad.
- Aprobar planes de formación y proyectos para mejorar la seguridad de la información.
- Asegurar que se realizan auditorías internas de seguridad de la información y que se revisan los resultados para identificar oportunidades de mejora.

6.2. Responsable de la Seguridad de la Información

La persona con el cargo de Responsable de la Seguridad de la Información asumirá las siguientes funciones:

- Supervisar el cumplimiento de la presente política, de sus normas, procedimientos derivados y la apropiada configuración de seguridad de los sistemas de información.
- Realizar, en colaboración con el Administrador de la Seguridad, los preceptivos análisis y evaluación de riesgos, así como de seleccionar los controles y medidas de seguridad apropiadas que deben implantarse. Analizará también los riesgos residuales calculados en el análisis.
- Establecer los controles y las medidas de seguridad para cumplir los requisitos de seguridad de la información establecidos por la Dirección.

- Verificar que los controles y medidas de seguridad son adecuados para proteger la información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Realizar la coordinación y seguimiento de la implantación y operación del SGSI, así como informar de su desempeño.
- Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada periodo.
- Definir qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.
- Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones a presentar a la Dirección para que adopte, en su caso, las medidas correctoras adecuadas.
- Elaborar la Declaración de Aplicabilidad.
- Realizar el control documental del sistema, gestionando los mecanismos de acceso a la misma.
- Convocar y dirigir el Comité de Seguridad de la Información, elaborando las pertinentes Actas de Reunión.
- Responsabilizarse de la ejecución de las decisiones de la Dirección en relación al SGSI.
- Proponer a la Dirección la documentación que tenga que aprobar.

Asimismo, también realizará o supervisará la realización de actividades más técnicas, como:

- La implementación, gestión y mantenimiento de los controles y medidas de seguridad aplicables a los sistemas de información, dispositivos de red y telecomunicaciones.
- La gestión, configuración y actualización del hardware y software correspondiente.
- La aplicación de los procedimientos operativos de seguridad.
- Aplicar los cambios de configuración a los sistemas de información y dispositivos.
- La gestión de las autorizaciones concedidas a los usuarios y los privilegios otorgados.
- Comprobar que los controles de seguridad establecidos se cumplen estrictamente, así como los procedimientos aprobados.
- Las instalaciones y actualizaciones de software y hardware para garantizar que la seguridad no se ve comprometida.
- Monitorizar la seguridad del sistema a través de las herramientas establecidas para la gestión de eventos de seguridad y los mecanismos de auditoría interna implementados en el sistema.
- Informar a los responsables correspondientes de cualquier anomalía o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad de la información, desde su detección hasta su resolución.

6.3. Coordinador de Protección de Datos

El Coordinador de Protección de Datos desempeñará las siguientes funciones:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD.
- Cooperar con la autoridad de control.

- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

6.4. Usuarios

Cualquier persona que acceda a la información gestionada por la organización será considerada un usuario.

Los usuarios son responsables de su conducta cuando accedan a información o utilicen los sistemas de información de la organización. El usuario es responsable de todas las acciones realizadas con sus identificadores o credenciales personales.

Por tanto, los usuarios tienen la obligación de:

- Conocer y cumplir la Política de Seguridad de la Información, las normas, procedimientos e instrucciones correspondientes.
- Proteger y custodiar la información de la organización, evitando la revelación, transmisión o comunicación al exterior, borrado, mal uso o destrucción (accidental o no autorizada) de la misma, independientemente del soporte en el que se encuentre o los medios por los que ha sido accedida o conocida.

6.5. Comité de Seguridad de la Información

El Comité de Seguridad de la Información siempre ha de estar compuesto por los siguientes cargos:

- Responsable de la Seguridad de la Información
- Responsable del Sistema

Además, si se requiere la presencia por alguna circunstancia especial se incorporarán:

- Director General
- Coordinador de Protección de Datos
- Director Financiero

Sus funciones son las siguientes:

- Atender las inquietudes de la Dirección y de sistemas.
- Promover la mejora continua del SGSI.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
- Revisar las políticas, normas y procedimientos del SGSI, al menos anualmente.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación del personal, desde el punto de vista de seguridad de la información.
- Priorizar las actuaciones en materia de seguridad de la información cuando los recursos sean limitados.
- Resolver conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización.
- 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.
- Promover la realización de auditorías del SGSI y técnicas.
- Se debe reunir cada 2 meses para revisión de los diferentes controles y actividades relacionadas.

7. Evaluación de riesgos y controles

Para la organización es primordial conocer los riesgos a que está expuesta la información y elaborar una estrategia para gestionarlos adecuadamente, ya que únicamente conociendo el estado de la seguridad de la información podrán tomarse decisiones adecuadas para mitigarlos a un umbral aceptable.

La entidad debe determinar los niveles de riesgo a partir a los cuáles tomará acciones de tratamiento sobre los mismos. Un riesgo se considera aceptable cuando implantar más controles de seguridad se estima que consumiría más recursos que el posible impacto asociado.

Una vez llevado a cabo el proceso de evaluación de riesgos, la Dirección será responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo, que normalmente implicarán la implantación de controles y medidas de seguridad.

8. Seguridad de la información en nuevos proyectos

El gerente de cada proyecto que se inicie en la organización, afectado por el alcance del SGSI, y de acuerdo con el Responsable de la Seguridad de la Información, debe incluir las reglas y requisitos correspondientes sobre la seguridad de la información relacionada con el proyecto en cuestión.

9. Comunicación de la política

El Responsable de la Seguridad de la Información debe asegurarse de que todo el personal, interno y externo, estén familiarizados con esta política, así como las empresas que accedan, gestionen o traten información de la organización.

El conjunto de políticas, normas y procedimientos complementarios a esta Política de Seguridad de la Información deberán ser también comunicados a las personas, empresas e instituciones implicadas en cada caso.

Se definirán periódicamente programas de concienciación y formación al personal y se le entregará o pondrá a disposición de ellos la información que les corresponda en función de su puesto.

10. Gestión de registros guardados en base a este documento

Código	Nombre	Ubicación	Responsable del archivo	Controles para la protección del registro	Tiempo de retención
					3 años

11. Control de versiones

Versión	Fecha	Autor	Descripción de la modificación
1.0	03/06/2025	ESM	Versión inicial del documento