	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.01 ANEXO I	VERSIÓN 1.0
		FECHA 31/03/2025	PÁGINA 1 de 10

INTRODUCCIÓN

La Dirección de ESTUDIOS RAFER considera la información y los sistemas que la soportan activos estratégicos que deben protegerse para:

- Salvaguardar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- Garantizar el cumplimiento normativo y contractual, especialmente lo establecido por el Real Decreto 311/2022 (ENS Nivel Medio) y la Norma ISO/IEC 27001:2022.
- Asegurar la continuidad del negocio y la resiliencia operativa frente a incidentes.
- Contribuir a la confianza de clientes, personal y otras partes interesadas.

Para ello, ESTUDIOS RAFER implanta y mantiene un Sistema de Gestión de la Seguridad de la Información (SGSI) que se fundamenta en los siguientes principios:


- **Mejora continua:** aplicar el ciclo PDCA y revisar periódicamente la eficacia del SGSI.
- **Gestión de riesgos:** identificar, analizar, valorar y tratar los riesgos de forma sistemática, dejando evidencia en el Plan de Seguridad del Sistema de Información (PSI).
- **Cumplimiento legal:** observar todas las obligaciones legales, reglamentarias y contractuales aplicables.
- **Responsabilidad y rendición de cuentas:** asignar funciones y responsabilidades claras, verificando su cumplimiento mediante auditorías internas y externas.
- **Concienciación y formación:** asegurar que todo el personal y terceras partes comprendan y asuman sus obligaciones en materia de seguridad.
- **Seguridad por diseño y por defecto:** integrar controles de seguridad desde el inicio del ciclo de vida de los sistemas.

Directrices corporativas derivadas de estos principios:

- Proteger los activos de información contra accesos no autorizados y pérdida de confidencialidad, integridad o disponibilidad.
- Disponer de planes de continuidad de negocio y recuperación ante desastres probados al

Este procedimiento es propiedad de ESTUDIOS RAFER

Nivel de seguridad del documento: Uso público. No está permitida su reproducción, distribución o comunicación fuera del destinatario salvo autorización.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.01 ANEXO I	VERSIÓN 1.0
		FECHA 31/03/2025	PÁGINA 2 de 10

menos una vez al año.

- Gestionar adecuadamente todas las incidencias de seguridad, notificando al CCN-CERT los incidentes significativos y aprendiendo de éstos.
- Mantener los recursos humanos y tecnológicos actualizados y alineados con las mejores prácticas del sector.
- Fomentar la cultura de seguridad y respeto a la privacidad en todas las actividades de la organización.

ALCANCE

La presente Política aplica a la actividad de **«Impartición de actividades de formación ocupacional»** que ESTUDIOS RAFER desarrolla en sus instalaciones de Lugo y a los sistemas, redes, procesos, personal y terceros que intervienen en dicha actividad. Incluye:

- Centros de trabajo, aulas y oficinas donde se trate información.
 - Infraestructuras tecnológicas (servidores, estaciones de trabajo, redes, equipos portátiles y dispositivos móviles).
 - Plataformas de formación on-line y sistemas de gestión académica y administrativa.
 - Servicios alojados in-house o en la nube cuya administración dependa de ESTUDIOS RAFER.
 - Personal interno, colaboradores y proveedores con acceso a la información o a los sistemas.
- Quedan excluidos aquellos sistemas no relacionados con la actividad descrita que se encuentren expresamente fuera del inventario de activos.


MISIÓN Y PRINCIPIOS

Misión: Ser un proveedor estratégico que impulse la excelencia en la formación ocupacional, garantizando la seguridad y privacidad de la información de nuestros clientes, alumnado y personal.

Para cumplir la misión, ESTUDIOS RAFER adopta los siguientes principios rectores:

Este procedimiento es propiedad de ESTUDIOS RAFER

Nivel de seguridad del documento: Uso público. No está permitida su reproducción, distribución o comunicación fuera del destinatario salvo autorización.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.01 ANEXO I	VERSIÓN 1.0
		FECHA 31/03/2025	PÁGINA 3 de 10

1. **Confidencialidad:** evitar la divulgación no autorizada de la información.
2. **Integridad:** salvaguardar la exactitud y completitud de la información y los métodos de procesamiento.
3. **Disponibilidad:** asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando lo requieran.
4. **Autenticidad y trazabilidad:** garantizar la correcta identificación de las partes y el no repudio de las transacciones.
5. **Proporcionalidad y adecuación:** aplicar controles de acuerdo con la categorización ENS «nivel medio».


MARCO NORMATIVO

Esta Política se alinea, entre otras, con las siguientes normas y reglamentos:

- Real Decreto 311/2022, de 3 de mayo, Esquema Nacional de Seguridad (ENS).
- Guías CCN-STIC, especialmente las series 400, 600 y 800
- ISO/IEC 27001:2022 e ISO/IEC 27002:2022.
- Ley Orgánica 3/2018 y Reglamento (UE) 2016/679 (RGPD)
- Real Decreto-ley 12/2018 y Reglamento de Desarrollo sobre seguridad de las redes y sistemas de información. Ley 11/2022, General de Telecomunicaciones.
- Reglamento (UE) 910/2014 (eIDAS)
- Reglamento (UE) 2019/881 (Cybersecurity Act).
- Legislación laboral, de propiedad intelectual y cualquier otra aplicable a la actividad.

Este procedimiento es propiedad de ESTUDIOS RAFER

Nivel de seguridad del documento: Uso público. No está permitida su reproducción, distribución o comunicación fuera del destinatario salvo autorización.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.01 ANEXO I	VERSIÓN 1.0
		FECHA 31/03/2025	PÁGINA 4 de 10

ROLES: FUNCIONES Y RESPONSABILIDADES

El **Comité de Seguridad de la información** estará formado por:

- Ramón Martínez Gómez Gerente
- Yago López López: Responsable TIC.
- María Sánchez: Responsable de RRHH.
- Gema Graña: Responsable de Formación.

Dentro de la infraestructura de seguridad de la información de la empresa y del propio comité estas personas han sido designadas como:


- Ramón Martínez Gómez Gerente y Responsable de Sistema
- Yago López López: Responsable de Seguridad y Secretario del Comité.
- María Sánchez: Responsable de Información.
- Gema Graña: Responsable de Servicio.

RESPONSABLE DE INFORMACIÓN

- Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.
- Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
- Aprobación de los niveles de seguridad de la información.
- Proteger los activos.
- Cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos.

Este procedimiento es propiedad de ESTUDIOS RAFER

Nivel de seguridad del documento: Uso público. No está permitida su reproducción, distribución o comunicación fuera del destinatario salvo autorización.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.01 ANEXO I	VERSIÓN 1.0
		FECHA 31/03/2025	PÁGINA 5 de 10

RESPONSABLE DEL SERVICIO


- Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.
- Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
- Aprobación de los niveles de seguridad de los servicios.
- Proteger los activos.
- Cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos

RESPONSABLE DE SEGURIDAD

- Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Convoca las reuniones del Comité de Seguridad de la Información.
- Junto con el Responsable de Sistema, vela por el cumplimiento del ENS, especialmente en términos de actualización de controles y categorización de activo.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Este procedimiento es propiedad de ESTUDIOS RAFER


Nivel de seguridad del documento: Uso público. No está permitida su reproducción, distribución o comunicación fuera del destinatario salvo autorización.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.01 ANEXO I	VERSIÓN 1.0
		FECHA 31/03/2025	PÁGINA 6 de 10

- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y de su Reglamento de Desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT (Computer Security Incident Response Team – Equipo de Respuesta ante Emergencias Informáticas) de referencia (CCN-Cert, INCIBE..).
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa

Este procedimiento es propiedad de ESTUDIOS RAFER

Nivel de seguridad del documento: Uso público. No está permitida su reproducción, distribución o comunicación fuera del destinatario salvo autorización.


	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.01 ANEXO I	VERSIÓN 1.0
		FECHA 31/03/2025	PÁGINA 7 de 10

RESPONSABLE DEL SISTEMA

- Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
- Desarrollar, operar y mantener del Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Junto con el Responsable de Seguridad, vela por el cumplimiento del ENS, especialmente en términos de actualización de controles y categorización de activo.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba de este.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.

Este procedimiento es propiedad de ESTUDIOS RAFER

Nivel de seguridad del documento: Uso público. No está permitida su reproducción, distribución o comunicación fuera del destinatario salvo autorización.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.01 ANEXO I	VERSIÓN 1.0
		FECHA 31/03/2025	PÁGINA 8 de 10

- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- 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 el responsable de seguridad, antes de ser ejecutada.

DATOS DE CARACTER PERSONAL

ESTUDIOS RAFER, trata los datos de carácter personal, por lo que mantiene un “registro de actividades de tratamiento”, al que tendrán acceso sólo las personas autorizadas, en el que se recogen los datos afectados y los responsables del tratamiento. Todos los sistemas de información de ESTUDIOS RAFER se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado registro.

OBLIGACIONES DEL PERSONAL


Todos los trabajadores de ESTUDIOS RAFER, tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de ESTUDIOS RAFER, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC dentro del alcance recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o, si, por el contrario se trata de un cambio de puesto de trabajo o de

Este procedimiento es propiedad de ESTUDIOS RAFER

Nivel de seguridad del documento: Uso público. No está permitida su reproducción, distribución o comunicación fuera del destinatario salvo autorización.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.01 ANEXO I	VERSIÓN 1.0
		FECHA 31/03/2025	PÁGINA 9 de 10

responsabilidades en el mismo.

TERCERAS PARTES

Las terceras partes relacionadas con ESTUDIOS RAFER, dentro del alcance, firman con la empresa un acuerdo que protege la información intercambiada.

Cuando ESTUDIOS RAFER, utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte, quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.


Cuando algún aspecto de la Política 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.

La Dirección de ESTUDIOS RAFER, ejerciendo su liderazgo, se compromete al SGSI y a asignar los recursos humanos, técnicos y financieros necesarios para cumplir con los requisitos establecidos en el Sistema de Gestión, y conseguir los objetivos fijados.

La presente política es conocida y suscrita por todo el personal de ESTUDIOS RAFER contemplado en el alcance, de acuerdo con las exigencias de la Dirección. Esta política ha sido aprobada por el Comité de Seguridad de ESTUDIOS RAFER y se revisará anualmente, o siempre que se produzcan cambios significativos en la organización, los servicios, la normativa o los resultados de las auditorías, asegurando su continua adecuación a las dimensiones de seguridad requeridas.

Este procedimiento es propiedad de ESTUDIOS RAFER

Nivel de seguridad del documento: Uso público. No está permitida su reproducción, distribución o comunicación fuera del destinatario salvo autorización.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO SGSI.01 ANEXO I	VERSIÓN 1.0
		FECHA 31/03/2025	PÁGINA 10 de 10

Cada persona trabajadora de la empresa es responsable de cumplir esta Política y sus procedimientos según aplique a su puesto de trabajo, así como de conocer y cumplir con las obligaciones específicas de las normas y disposiciones legales de aplicación a la empresa, de manera que se garantice la Confidencialidad, Integridad, Trazabilidad, Autenticidad y Disponibilidad de la información.

El compromiso de ESTUDIOS RAFER con la seguridad de la información es continuo, buscando la mejora constante de las medidas implementadas para garantizar el cumplimiento de esta política, requisitos, medidas y disposiciones legales de aplicación a la empresa.



Dirección de ESTUDIOS RAFER

31/03/2025

Este procedimiento es propiedad de ESTUDIOS RAFER

Nivel de seguridad del documento: Uso público. No está permitida su reproducción, distribución o comunicación fuera del destinatario salvo autorización.