POLÍTICA SGSI	CODIGO : SGSI-05-01 REV/ED:0 *26/12/2023* Uso Interno

CUADRO DE REVISIONES		
Fecha	**Rev.**	**Modificación**
26/12/2023	0	Aprobación de la Versión inicial

OBJETIVO

Ofimática, reconociendo las implicaciones en materia de seguridad de la información relacionadas con su actividad y sus grupos de interés, ha desarrollado la presente declaración con el fin de establecer su Política de Seguridad de la Información. El objetivo primordial de esta política es asegurar la adecuada protección de los activos de información y mantener la continuidad de los servicios proporcionados. Ofimática ha implementado las medidas de seguridad necesarias para garantizar un nivel de riesgo aceptable, así como la capacidad de prevención, detección, respuesta y recuperación frente a posibles incidentes de seguridad. Asimismo, Ofimática reconoce la importancia de monitorear los niveles de prestación de los servicios, analizar las vulnerabilidades reportadas y establecer una respuesta efectiva frente a los incidentes que puedan surgir.

Ofimática se compromete a cumplir con las especificaciones funcionales de sus servicios, asegurando la integridad de la información sin interrupciones o modificaciones no autorizadas. Además, se garantiza que personas no autorizadas no tengan acceso a la información. Conscientes de la importancia de proteger los datos almacenados o transmitidos, Ofimática ha implementado sistemas de información y redes con la capacidad necesaria para resistir de manera confiable accidentes, acciones ilícitas, o malintencionadas. Estas medidas de seguridad garantizan el acceso, autenticidad, confidencialidad, disponibilidad, trazabilidad y conservación de los datos, así como la continuidad de los servicios utilizados en entornos electrónicos.

Ofimática asume la responsabilidad de garantizar la seguridad de las Tecnologías de las Información y Comunicación (TIC) como parte integral en todas las fases del ciclo de vida de los sistemas de información. Esto implica desde la concepción hasta el retiro del servicio, incluyendo la toma de decisiones en el desarrollo o adquisición, así como las actividades operativas. En la planificación y en las solicitudes de propuestas de proyectos se identifican y consideran los requisitos de seguridad y las necesidades de financiamiento asociadas a cada etapa.

Con el objetivo de cumplir los principios establecidos en esta Política de Seguridad de la Información y garantizar el nivel de seguridad requerido por Ofimática, el Comité de Seguridad de la Información elabora anualmente un informe detallando las medidas de seguridad aprobadas, en concordancia con el principio de gestión de riesgos. Estas medidas deben implementarse en el ejercicio económico siguiente a su aprobación debido a su carácter necesario. Asimismo, el informe incluye aquellas medidas que se consideran deseables para fortalecer la estrategia de seguridad diseñada por el Comité.

ÁMBITO DE APLICACIÓN

Conforme a la Política de Seguridad de la Información y las normativas correspondientes. Se establecen medidas de seguridad que deben ser aplicadas. Según lo dispuesto en dichas normativas, a todos los sistemas servicios y recursos TIC de Ofimática que respalden los procesos organizacionales y afecten a los diferentes activos de información asociados a ellos.

Los recursos TIC de la organización tienen como finalidad brindar soporte a los procesos de negocio de Ofimática, así como a las tareas de gestión necesarias para el correcto funcionamiento de la organización. Estos recursos engloban sistemas centrales y departamentales, estaciones de trabajo, ordenadores, impresoras, periféricos y otros dispositivos de salida, redes internas y externas, servicio de almacenamiento que sean propiedad de Ofimática.

La presente Política de Seguridad de la información se aplica además de a las personas usuarias internas de Ofimática, a toda persona, institución, entidad o servicio interno o externo que haga uso de los recursos TIC de la organización, y que se conecte de forma directa o indirecta a los susodichos recursos, con especial atención a aquellos que se prestan a través de internet. Ofimática considera una persona usuaria a todo sujeto que realice una de las acciones descritas.

PRINCIPIOS BASICOS DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de seguridad de la información, así como su correspondiente normativa, se fundamenta en principios básicos de protección cuyo objetivo es asegurar que Ofimática tenga la capacidad para lograr sus objetivos gracias al correcto uso de sistemas de información.

Estos principios básicos son considerados en todo momento para la toma de decisiones vinculadas a la seguridad de la información. A continuación, se expone la definición de cada uno de ellos:

a) Seguridad Integral.

La seguridad es entendida como un proceso integral que abarca todos los elementos humanos, técnicos, materiales y organizativos que tienen influencia en el sistema. En consecuencia, resulta preciso garantizar que cada uno de los individuos participantes estén en conocimiento de la actual Política de Seguridad y que desempeñen sus funciones de manera acorde a la misma. Asimismo, es necesario que los implicados en el proceso de seguridad actúen de manera coordinada durante la implementación y control de

las medidas de seguridad. Dicha coordinación debe estar presente en toda iniciativa y acción realizada por Ofimática.

b) Gestión de riesgos.

Analizar y gestionar los riesgos resulta una pieza clave para el proceso de seguridad de la información. Consecuentemente, se persigue mantener los niveles de riesgo en unos límites mínimos que sean asumibles gracias a la implementación de medidas de seguridad que sean adecuadas y estén actualizadas de manera continua. El objetivo de esta labor es garantizar que existe una proporcionalidad entre la naturaleza de los datos de Ofimática y los procesos de tratamiento, así como entre los riesgos y medidas de seguridad que se adopten.

c) Prevención y recuperación ante desastres.

Esta seguridad de los sistemas engloba las necesidades de prevención, detección y recuperación frente a las amenazas que puedan materializarse o que puedan tener un impacto relevante sobre los datos gestionados por los sistemas de información o en los servicios que presta Ofimática. Por ello, son adoptadas las siguientes medidas:

- Medidas de prevención, como la disuasión y la reducción de exposición, entre otras.
- Medias de detección en conjunto a las medias de reacción, con el propósito de garantizar que la respuesta ante incidentes de seguridad sea optima.
- Medidas de recuperación que permitan la restauración de la información y los servicios.

El sistema debe preservar los datos e información en soporte electrónico, al igual que la disponibilidad de los servicios durante todo el ciclo de vida de la información digital.

d) Líneas de defesa

Es esencial que el sistema cuente con una estrategia integral de protección que incorpore múltiples niveles de seguridad. Estos niveles deben ser diseñados de tal manera que, en caso de un incidente inevitable, se pueda proporcionar una respuesta oportuna y efectiva. Esto ayudara a disminuir la probabilidad de comprometer la integridad total del sistema y minimizar el impacto final.

Para lograr esto, es fundamental establecer una serie de barreras defensivas que abarquen medidas organizativas, físicas y lógicas.

e) Reevaluación periódica.

Ofimática revisa y actualiza de forma periódica las medidas de seguridad implementadas para asegurar su efectividad frente a los riesgos cambiantes y los sistemas de protección.

La seguridad que se deriva de estos principios fundamentales también cumple con los requisitos establecidos en el artículo 32.1b) de Reglamento General de Protección de Datos. Según dicho articulo el objetivo de la seguridad es garantizar la capacidad de mantener de manera continua la confidencialidad, integridad, disponibilidad y resiliencia de los servicios y sistemas de tratamiento de datos.

LIDERAZGO Y COMPROMISO

La dirección de Ofimática demuestra su liderazgo y compromiso con los principios fundamentales de seguridad de la información al implementar el Sistema de Gestión de Seguridad de la Información (SGSI) y asumir las siguientes responsabilidades:

- Asegurarse que la política de Seguridad de la Información y la Normativa de Seguridad de la Información, así como sus objetivos, estén establecidos y sean coherentes con la dirección estratégica de la organización.
- Comunicar la importancia de una gestión efectiva del sistema y el cumplimiento de los requisitos establecidos.
- Garantizar la disponibilidad de los recursos necesarios para el correcto funcionamiento del SGSI.
- Apoyar otras funciones de gestión relevantes para fortalecer su liderazgo en sus respectivas áreas de responsabilidad.
- Liderar y ofrecer apoyo a las personas que contribuyen al funcionamiento del SGSI.
- Asegurar que el SGSI alcance los resultados previstos.
- Promover la mejora continua en términos de seguridad de la información.

POLÍTICA DE GESTIÓN Y OBJETIVOS

La dirección de Ofimática es consciente de la necesidad de garantizar el cumplimiento de los niveles fijados de confidencialidad, integridad, disponibilidad, trazabilidad y autenticación de sus activos de información, para impulsar las labores de la organización y alcanzar los objetivos estratégicos de manera efectiva. Además de demostrar la capacidad de ofrecer soluciones y servicios de manera coherente, así como gestionar eficientemente los servicios prestados a sus clientes.

Con el propósito de lograrlo, Ofimática ha desarrollado e implementado el SGSI, que ofrece un marco de referencia solido para el seguro tratamiento de los activos de la organización, al tiempo que garantiza la satisfacción y confianza de todas las partes interesadas al adoptar una metodología eficiente para la prestación de servicios.

Ofimática asume los siguientes compromisos en relación con la gestión de la seguridad de la información:

- Expresar el firme compromiso de la Dirección hacia el SGSI y la gestión de la seguridad de la información, tanto para los activos propios como para los de sus empresas clientes.
- Garantizar la plena integración de los requisitos del SGSI en los procesos operativos de la organización.
- Establecer metas de seguridad de la información que sean coherentes con el contexto y la dirección estratégica de la empresa.
- Definir, elaborar e implementar los mecanismos de control necesarios, promoviendo un enfoque basado en procesos y una perspectiva orientada a los riesgos, para cumplir constantemente con los niveles de riesgo asumidos por la organización.
- Promover una cultura de gestión integral de los sistemas de información tanto a nivel interno, involucrando a todo el personal, como externo, en las interacciones con empresas clientes, personas usuarias y empresas proveedoras.
- Fomentar el compromiso, brindar apoyo y liderar al personal para contribuir a la eficacia del SGSI, garantizando la disponibilidad de los recursos necesarios y respaldando a sus otros roles directivos relevantes en la implantación del sistema de gestión a sus respectivas áreas de responsabilidad.
- Mantener la confianza y la satisfacción de las partes interesadas en todo momento.
- Cumplir con la legislación y las regulaciones vigentes, así como las normas y especificaciones que sean aplicables a los servicios ofrecidos por Ofimática priorizando siempre la satisfacción de las empresas clientes.
- Encarar la gestión de la seguridad de la información como un proceso de mejora continua y constante.

Con el fin de asegurar su compromiso, y considerando que el propósito de la seguridad de la información es garantizar la continuidad de los negocios y minimizar el riesgo de daños al prevenir incidentes de seguridad, así como reducir su posible impacto cuando sea inevitable, Ofimática establece los siguientes

objetivos estratégicos en relación con la seguridad de la información, acorde al contexto y la dirección estratégica de la empresa:

- Fomentar una cultura organizacional arraigada en la seguridad, donde la protección de la información sea una prioridad y esté integrada en todos los niveles de gestión.
- Salvaguardar la confidencialidad, disponibilidad e integridad de los datos de la organización para asegurar el cumplimiento de su estrategia empresarial, así como de los requisitos contractuales y legales vigentes.
- Realizar un exhaustivo análisis y una gestión enfocada en la evaluación de riesgos, con el objetivo de anticiparse y mitigar posibles incidentes.
- Optimizar las inversiones de seguridad, asegurando que estén alineadas con los objetivos empresariales y maximizando su impacto.
- Aprovechar de forma eficiente y efectiva el conocimiento y la infraestructura de seguridad disponibles para fortalecer las defensas de Ofimática.
- Proteger los recursos de información y las tecnologías utilizadas por Ofimática de amenazas tanto internas como externas, independientemente de su intencionalidad o causalidad.
- Monitorizar y generar informes sobre los procesos para garantizar el cumplimiento de los objetivos establecidos.

Ofimática establece los siguientes objetivos específicos en materia de seguridad la información, alineados con los objetivos empresariales y estratégicos.

a. Salvaguarda de los activos de información

Es fundamental contar con una sólida protección de todos los recursos del sistema. La gestión de riesgo es un pilar clave en materia de seguridad de la información y se considera una actividad esencial según los estándares vigentes. Por lo tanto, Ofimática basa gran parte de sus esfuerzos en proteger la información, los activos y el negocio mediante una evaluación y priorización exhaustiva de los riesgos de seguridad. Estos resultados juegan un papel crucial en la toma de decisiones.

b. Controles de acceso lógico: autenticación

Un sistema de información debe ser utilizado únicamente por usuarios autorizados, y se deben implementar medidas para detectar y bloquear a aquellos que no cuenten con autorización. La autenticación robusta protege al sistema contra el riesgo de suplantación de identidad.

c. Salvaguarda de la confidencialidad

Dentro del ámbito de la seguridad de la información, la confidencialidad se refiere a la protección de los datos e información intercambiados entre un emisor y uno o mas destinatarios, asegurando que permanezcan a salvo de accesos no autorizados.

d. Preservación de la integridad

La garantía de la integridad de los datos implica resguardar la información contra modificaciones o manipulaciones no autorizadas. Por lo tanto, se fundamenta en la implementación de medidas de seguridad para mitigar los riesgos de manipulación, evitando el acceso y la alteración no autorizada de la información. Es esencial tener en cuenta los riesgos que pueden afectar la integridad de la información, especialmente en situaciones en las que se accede a datos provenientes de redes no confiables, como las redes públicas o internet.

e. Disponibilidad

La disponibilidad se refiere al funcionamiento continuo e ininterrumpido de los sistemas de información. Ofimática garantiza la disponibilidad de sus sistemas de información y establece procedimientos documentados para asegurar la continuidad del negocio en situación adversas. Estas medidas están diseñadas para minimizar el impacto de interrupciones y asegurar que los sistemas estén constantemente disponibles para su uso.

f. Auditoría de actividades de seguridad

Ofimática tiene como objetivo la supervisión y el registro constante de posibles incidentes y actividades sospechosas, con el propósito de prevenir eventos indeseados. Se lleva a cabo una auditoria exhaustiva de las actividades de seguridad para mantener un control efectivo y garantizar la integridad del sistema.

ORGANIZACIÓN DE LA SEGURIDAD

Con el objetivo de garantizar la correcta ejecución de todas las fases del ciclo de vida de protección de la información y asignar de manera adecuada las responsabilidades correspondientes, Ofimática establece una estructura que promueve la implementación coherente de la presente política de seguridad de la información. Dicha estructura capacita de forma efectiva para adaptarse a los frecuentes cambios tecnológicos y organizativos.

En consecuencia, Ofimática establece el siguiente Comité y Roles generales relacionados con la supervisión y gestión de la seguridad la información:

- Comité de Seguridad de la Información
- Responsable de Seguridad de la Información.

La definición y explicación de estos roles y sus responsabilidades se encuentra detalla en el documento titulado "**SGSI-05-02 Roles y responsabilidades**".

DATOS DE CARÁCTER PERSONAL

Ofimática llevaba a cabo tratamientos de datos personales y mantiene un Registro de Actividades de Tratamiento que registra dichos tratamientos y los responsables correspondientes.

Cada uno de los sistemas de información de la organización cumple con los niveles de seguridad exigidos por la normativa, en consonancia con la naturaleza y finalidad de los datos personales. Las medidas implementadas en virtud de esta política de seguridad de la información, junto con los análisis de riesgos y las evaluaciones de impacto llevadas a cabo para cumplir con los requisitos del Reglamento General de Protección de Datos, se coordinan con el Comité de Seguridad de la Información y el Responsable de Seguridad.

OBLIGACIONES DE LOS USUARIOS

Es responsabilidad de todo el personal de Ofimática conocer y cumplir con la Política de Seguridad de la Información y la Normativa de Seguridad derivada de ella. Recae en el Comité de Seguridad de la Información la tarea de garantizar que dichas políticas sean comunicadas a todos los involucrados, disponiendo de los medios necesarios para ello.

Resulta necesario que todo el personal comprenda la importancia de colaborar en la protección de los sistemas de información. Cada persona desempeña un papel fundamental en el mantenimiento y mejora de la seguridad de Ofimática.

Siguiendo esta premisa, se establece un programa de sensibilización continua con el objetivo de conciencias a todos los miembros de Ofimática, especialmente a aquellos que se han unido recientemente.

Aquel personal con responsabilidad en el uso, operación o gestión de los sistemas TIC reciben formación en el uso seguro de dichos sistemas, según sea necesario para llevar a cabo sus tareas. Dicha formación es de carácter obligatorio previo a asumir cualquier responsabilidad, ya sea en la primera asignación laboral o en caso de cambio de posición o responsabilidades dentro de la empresa.

RESPONSABILIDADES DE LOS USUARIOS EN CASO DE INCUMPLIMIENTO

El Comité de Seguridad de la Información posee la capacidad para evaluar si el personal de Ofimática esta incumpliendo algunas de las obligaciones dispuestas por la Política de Seguridad de la Información, así como en su normativa e instrucciones derivadas.

De detectarse alguna falta, se implementan medidas preventivas y correctivas con el propósito de preservar y salvaguardar las redes y los sistemas de información. Estas acciones se llevan a cabo sin perjuicio de las posibles repercusiones disciplinarias que sean proporcionales al incumplimiento.

Una vez se constate un incumplimiento de la presente política, el Comité de Seguridad de la Información, mediante los canales establecidos, procede a iniciar las acciones disciplinarias pertinentes. El proceso que seguir y las sanciones aplicables se encuentran en consonancia con la legislación vigente relativa al régimen disciplinario del personal al servicio de Ofimática.

RELACIÓN CON TERCERAS PARTES

En caso de que Ofimática preste servicios a otros organismos o maneje información proveniente de ellos, el responsable de esta relación se encargará de comunicar la Política de Seguridad de la Información, así como las directrices y pautas en materia de seguridad derivadas de ella. Asimismo, se concretan canales de comunicación y coordinación eficaces entre los correspondientes Comités de Seguridad de la Información, con el fin de asegurar una efectiva colaboración en temática de seguridad. De manera complementaria, se implementan procedimientos de actuación para responder de manera oportuna eficiente ante los incidentes de seguridad, permitiendo una rápida reacción en caso de que se produzcan eventos que pongan en peligro la seguridad de la información.

En caso de que Ofimática utilice servicios de terceros o comparta información con ellos, el responsable de dicha relación se encarga de comunicar la Política de Seguridad de la Información, así como las directrices y pautas en materia de seguridad aplicables a dichos servicios o información. Estos terceros están sujetos a las obligaciones y medidas de seguridad establecidas en dichas instrucciones y normativa, pudiendo implementar sus propios procedimientos operativos para dar respuestas a las exigencias resultantes de la relación. Además, se establecen procedimientos específicos para prevenir, detectar, informar y resolver incidentes de seguridad. Se busca asegurar que el personal de las terceras partes sea plenamente consciente de las políticas de seguridad, al menos al nivel que se establece en la presente política de seguridad de la información.

Concretamente, las terceras partes tienen la obligación de garantizar el cumplimiento de políticas de seguridad que se basen en estándares auditables, y están sujetos a controles y revisiones llevadas a cabos por terceros acreditados para verificar el cumplimiento de dichas políticas. Además, se asegura, mediante auditorias o certificados de destrucción la eliminación, que al finalizar el contrato el tercero proceda a cancelar y eliminar de manera adecuada los datos correspondientes a Ofimática.

Si una tercera parte no puede cumplir con algún aspecto de la política de seguridad, se requiere un informe al Responsable de Seguridad de la Información respectivo, en el que se identifiquen los riesgos implicados y se propongan medidas para abordarlos. Dicho informe debe ser sometido a aprobación del Comité de Seguridad de la Información de Ofimática antes de dar continuidad a la relación o servicio correspondiente.

MARCO NORMATIVO

- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- Real Decreto 1720/2007, de 21 de diciembre, porque se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (LPI), regularizando, aclarando y armonizando las disposiciones vigentes en la materia.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE).
- Todas aquellas normas de carácter general o interno, que resulten de aplicación a Ofimática en el marco de esta Política de Seguridad.
- Estatuto de los trabajadores.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

REVISIONES, APROBACIÓN Y ENTRADA EN VIGOR

CUADRO DE REVISIONES		
26/12/2023	0	Propuesta versión inicial por el Comité de Seguridad de la Información

El texto de la presente Política de Seguridad de la Información fue aprobado por Dirección:

Firma y fecha.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva política.

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en la presente Política de Seguridad de la Información.