POLÍTICA UNIFICADA DE SEGURIDAD DE LA INFORMACIÓN (PGSI) DEL GRUPO SERVINFORM, S.A.

Texto aprobado por la Dirección (Ignacio Rufo Rodríguez, Consejero Delegado)
Revisado: Comité de Seguridad de la Información
Fecha: 11 de diciembre de 2023
Versión 4.0

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

1.- INTRODUCCIÓN

Este documento expone la Política de Seguridad de las directrices y principios establecidos por SERVINFORM, S.A., DIAGONAL COMPANY SERVICES & SOLUTIONS, S.L., ARTEOS DIGITAL, S.L., BETAN, S.A., SVFM PT, UNIPESSOAL LDA, HISPAPOST, S.A., SELLING INSURANCE COMPANY, S.L. y SVF FINANCE, S.L. -en adelante para este documento como GRUPO SERVINFORM-, resultando la misma como el conjunto de los principios básicos y líneas de actuación a los que la organización se compromete bajo el Esquema Nacional de Seguridad (ENS) según el Real Decreto 311/2022 y la norma UNE-EN ISO/IEC 27001:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad.

GRUPO SERVINFORM, constituida por empresas con presencia tanto en España como en otros países, es una de las principales compañías del mundo por ingresos en su sector para soluciones de Business Process Outsourcing (BPO), Transformación Tecnológica (TD), Atención al Cliente (ATC) con Centro de Atención al Cliente (CAC) y Atención al Usuario (CAU), Gestión de activos, Servicios Industriales de Billing, Distribución postal y del E-Commerce.

El propósito y misión del GRUPO SERVINFORM en materia de "Gestión de la Seguridad" es contar con una organización comprometida y flexible que permita responder tanto a las necesidades de nuestros clientes como a aquellos requisitos aplicables no especificados, superando las expectativas de los mismos.

GRUPO SERVINFORM ratifica su firme compromiso con la Excelencia y la mejora continua en la prestación de sus servicios encaminados a satisfacer las necesidades de externalización de procesos de negocio, transformación tecnológica, atención al cliente, gestión de activos, servicios industriales de billing y distribución postal capaces de dar respuesta, con calidad, eficacia, fiabilidad e integrando la prevención en su actividad laboral diaria, a las necesidades y expectativas de sus grupos de interés.

GRUPO SERVINFORM, consciente de los compromisos que contrae con sus clientes, empleados y demás partes interesadas considera la Calidad, la Seguridad y Salud en el Trabajo, la Conciliación de la vida personal y laboral, la Seguridad de la Información y la Responsabilidad Social, factores prioritarios para el desarrollo de su actividad.

Para alcanzar sus objetivos, esta labor se desarrolla por medio de la implementación y mantenimiento de un Sistema de Gestión de la Seguridad de la información (SGSI) adaptado al Esquema Nacional de Seguridad (ENS) y desarrollado por el R.D. 311/2022 y bajo la norma internacional UNE-EN ISO/IEC 27001:2022

Dicho Sistema ha sido implementado con el compromiso de todo el personal y es responsabilidad de la Dirección General del GRUPO SERVINFORM, velar por su estricto cumplimiento, dotándolo de todos los recursos necesarios para llevarlo a cabo pudiendo, en cualquier momento, tomar las acciones correctivas necesarias para conseguirlo.

Es parte de nuestra estrategia, a partir de ahora, la seguridad integral como un elemento crítico y fundamental. Este reto se multiplica en exigencia e importancia si lo aplicamos a un entorno tan específico y crítico como el nuestro, donde el tratamiento y la gestión segura de la información, se imponen como una necesidad para competir y mejorar en el futuro.

Asimismo, la legislación actual es clara en lo referente a la seguridad de la información, disponiéndose de un marco legal muy concreto que requiere de un cumplimiento exigente por parte de todos y todas, pero que ayuda a adoptar las medidas de seguridad apropiadas en los Sistemas de la Información.

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la empresa. Dicha información, puede existir en diversas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en proyecciones o en forma oral en las conversaciones.

Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento con el fin de garantizar la calidad de la información, la continuidad del negocio, minimizar el riesgo, permitir maximizar el retorno de las inversiones y las oportunidades de negocio, dar cumplimiento de los objetivos de seguridad definidos y asegurar así la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los sistemas de información y por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables.

La seguridad de la información es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y en el que es fundamental la máxima colaboración e implicación de todo el personal de la empresa.

La finalidad del ENS en conjunto con la norma ISO es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Tiene como objetivo establecer la política de seguridad en la utilización de medios electrónicos a través de principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Se crean así las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas (controles) de seguridad para garantizar la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos. El ENS es de aplicación a las Administraciones Públicas españolas (Administración General del Estado, Comunidades Autónomas, Entidades Locales) y a aquellas organizaciones privadas que les proveen servicios o soluciones tecnológicas.

Esto permite dar cumplimiento a un Real Decreto Español y disponer de un Sistema de Gestión de Seguridad de la Infomación que permita asegurar las dimensiones de los sistemas de información, sus servicios y su información.

La política de seguridad se ha establecido de acuerdo con los principios básicos señalados en el capítulo II del R.D. 311/2022 (artículo 12) y del Anexo A de la norma ISO (control 5.1) y se ha desarrollado aplicando los siguientes requisitos mínimos: Organización e implantación del proceso de seguridad, análisis y gestión de los riesgos, gestión de personal, profesionalidad, autorización y control de los accesos, protección de las instalaciones, adquisición de productos de seguridad y contratación de servicios de seguridad, mínimo privilegio, integridad y actualización del sistema, protección de la información almacenada y en tránsito, prevención ante otros sistemas de información interconectados, registro de la actividad y detección de código dañino, incidentes de seguridad, continuidad de la actividad y mejora continua del proceso de seguridad.

La Dirección del GRUPO SERVINFORM, consciente de la importancia de la seguridad y del valor de la información en el ámbito laboral, asume y dispone los siguientes compromisos con respecto al Sistema de Gestión de Seguridad de la Información (SGSI):

- Asegurar que se establecen objetivos de seguridad, siempre alineados con la estrategia de la empresa.
- Asegurar que los requisitos de seguridad se integran en los procesos de la organización.
- Asegurar los recursos necesarios para el sistema de gestión de seguridad.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del sistema de gestión de seguridad.
- Asegurar que el sistema de gestión de seguridad consigue los resultados previstos.
- Dirigir y apoyar a las personas, para contribuir a la eficacia del sistema de gestión de seguridad.
- Promover la mejora continua del sistema de gestión.
- Y apoyar los roles pertinentes para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

Para ello, la Dirección asegurará que todo el personal del GRUPO SERVINFORM, cumple con las políticas, normativas, procedimientos e instrucciones relativas a la seguridad, quedando profundamente comprometida con la política descrita en este documento.

2.- DEFINICIONES

- **Sistema de Información**: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- **Riesgo**: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- **Gestión de riesgos**: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
- **Sistema de Gestión de Seguridad de la Información (I):** Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.
- **Disponibilidad**: Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
- **Integridad**: La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- **Confidencialidad**: La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- **Autenticidad (relativo al ENS)**: Se debe asegurar la identidad u origen de la información.
- **Trazabilidad (relativo al ENS)**: Se debe asegurar para ciertos datos quién hizo qué y en qué momento.

3.- ALCANCE

Los sistemas de información que soportan los mecanismos de seguridad de la información de los procesos de negocio y activos de información empleados en el desarrollo, gestión y prestación, mantenimiento, mejora y continuidad relacionados con la prestación de los servicios de:

- **Business Process Outsourcing (BPO)** para servicios de subcontratación o externalización de procesos de negocio de Gestión documental, Atención Presencial de Clientes, Back Office (sectoriales), Procesos globales de Gestión de Proveedores, Gestión Hipotecaria, Procesos Legales y Carga de Tarifas (turismo).
- **Transformación Tecnológica (TD)** para Customer Communications Management (CCM), Robotización de Procesos (RPA) extendida con componentes de AI/IDP (Artificial Intelligence/Intelligent Document Processing), Know Your Costumer (KYC) y biometría, Firma Electrónica, Onboarding Digital y Fraude, Videoidentificación, Desarrollo de Soluciones de Negocio, Project Management Office (PMO) y Consultoría TIC.

- **Atención al Cliente (ATC)** con Centro de Atención al Cliente (CAC) y Atención al Usuario (CAU) para servicios de Recobros, Atención a negocios y empresas, Información al cliente, Banca telefónica, Asistencia nivel I y II, Cita previa, Gestión de averías, Gestión de incidencias, Consultoría, Reversión y Verificación contable, Centro de Ventas Omnicanal (Venta cruzada, Venta directa, Upselling, Televenta, Concertación de citas y Encuestas) y los servicios integrales de Relación con Clientes.
- **Gestión de activos** para servicios de Gestión Non-Performing Loans (NPLs), Conversión y Admisión de Real Estate Owned (REOs) y Gestión Patrimonial.
- **Servicios Industriales de Billing** (Impresión digital alta capacidad, Ensobrado Inteligente, Manipulado, Acondicionamiento postal y Procesos electrónicos de confirmación y certificación), Marketing Directo , Marketing Electoral, Book on Demand (Impresión digital de libros y Plataforma de gestión) y Packaging (Diseño estructural, Diseño gráfico, Colorimetría, Impresión offset convencional y UV, Contracolados, Acabados y Manipulado).
- **Distribución postal y del E-Commerce** (última milla para envíos postales diarios nacionales).

De acuerdo con la categorización del sistema vigente Y relacionados con la prestación de los Servicios del GRUPO SERVINFORM en todas las ubicaciones donde la organización desarrolla su actividad.

Esta Política, así como del resto de las mismas y de cualquier procedimiento o documentación incluida dentro del repositorio de documentación del SGSI son de obligado cumplimiento sin excepciones y según la declaración de aplicabilidad (SoA) y el catálogo de servicios de la compañía y atañen a todo el personal de la organización, incluyendo a todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentren estas y de si el individuo es empleado o no de la organización. Por lo tanto, también se aplica a los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas del GRUPO SERVINFORM.

Las visitas y personal externo que accedan a las instalaciones no están exentas del cumplimiento de las obligaciones indicadas en la documentación del SGSI, y el personal interno observará y velará por su cumplimiento.

La organización desestima la aplicación de la presente Política de Seguridad sobre aquellos sistemas de información no reflejados en este apartado.

4.- PRINCIPIOS

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

- **Principio de seguridad como un proceso integral**: la seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información.
- **Principio de confidencialidad**: los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.
- **Principio de integridad y calidad**: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.
- **Principio de disponibilidad y continuidad**: se garantizará un nivel de disponibilidad en los sistemas de información y se dotarán los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.
- **Principio de gestión del riesgo**: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.
- **Principio de proporcionalidad en coste**: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.
- **Principio de concienciación y formación**: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad informática de todas aquellas personas que gestionen y administren Sistemas de Información y Telecomunicaciones.
- **Principio de prevención**: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad informática.
- **Principio de la existencia de líneas de defensa**: desarrollando una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizando el impacto final sobre el mismo articulando diferentes líneas de defensa constituidas por medidas de naturaleza organizativa, física y lógica.
- **Principio de detección y respuesta**: los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente, a través de los mecanismos establecidos al efecto, a los incidentes de seguridad.
- **Principio de conservación**: el sistema de información garantizará la conservación de los datos e información en soporte electrónico.
- **Principio de vigilancia y mejora continua**: se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad planificados anualmente y el grado de eficacia de los controles de seguridad informática implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico para la prestación de los servicios a la Administración Pública.

- **Principio de seguridad TIC en el ciclo de vida de los sistemas de información**: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- **Principio de función diferenciada**: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

5.- MARCO JURÍDICO DE LA POLÍTICA DE SEGURIDAD

La presente Política de Seguridad de la Información se elabora en cumplimiento de la exigencia de la norma UNE-EN ISO/IEC 27001:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad y del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, dicho real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales y será también de aplicación a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

El SGSI del GRUPO SERVINFORM, es un sistema de información que trata datos personales y le será de aplicación lo dispuesto en el 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) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el R.D. 311/2022.

Y en general, otras normas que en la actualidad o en el futuro, de carácter general o interno, resulten de aplicación al GRUPO SERVINFORM en el marco de esta Política de Seguridad.

6.- DIRECTRICES Y OBJETIVOS

GRUPO SERVINFORM tiene como objetivo concienciar a todos los miembros de la organización acerca de la necesidad de garantizar la Seguridad, y de convertir esta necesidad en una tarea colectiva, en la cual debe implicarse todo el personal de las mismas.

Las directrices generales y objetivos que se establecen son los siguientes:

- Implantar en la Organización un Sistema de Gestión de la Seguridad de la Información (SGSI).
- Establecer unos procedimientos sistemáticos que aseguren la exactitud y calidad de los datos de carácter personal.
- Asignar los Responsables que velen por el cumplimiento de la Norma.
- Garantizar a los interesados el ejercicio de sus derechos de acceso, rectificación, cancelación, oposición, portabilidad, limitación del tratamiento y a no ser objeto de decisiones automatizadas, de forma acorde con los requisitos y especificaciones establecidas en la normativa y legislación vigente aplicable.
- Informar a todos los empleados sobre la existencia de los distintos documentos incluidos en el SGSI.
- Formar a todos los empleados que acceden a los datos en las directrices y procedimientos del SGSI.
- Velar por el cumplimiento de la legislación vigente y del SGSI.

La Dirección se compromete a revisar periódicamente el contenido del SGSI, para garantizar su adecuación a las necesidades de la organización y de los cambios legales que pudieran ocurrir.

7.- APLICACIÓN DE LAS MEDIDAS

La adaptación al ENS implica que el GRUPO SERVINFORM y su personal deben aplicar las medidas mínimas de seguridad exigidas por el propio ENS y la UNE-EN ISO/IEC 27001, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes unidades de gestión del GRUPO SERVINFORM deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y los costes asociados deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Las unidades de gestión del GRUPO SERVINFORM deben estar preparadas para prevenir, detectar, reaccionar y la conservación de incidentes, de acuerdo con el Artículo 8 del ENS y de los controles del Anexo A de la norma UNE-EN ISO/IEC 27002:2022 5.24 Planificación y

preparación de la gestión de incidentes de seguridad de la información, 5.25 Evaluación y decisión sobre eventos de seguridad de la información, 5.26 Respuesta a los incidentes de seguridad de la información, 5.27 Aprender de los incidentes de seguridad de la información, 5.28 Recogida de pruebas y 5.30 Preparación de las TIC para la continuidad de la actividad

7.1.- PREVENCIÓN

El GRUPO SERVINFORM debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad determinadas por el ENS y la UNE-EN ISO/IEC 27001, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, la organización debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

7.2.- DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS y la norma UNE-EN ISO/IEC 27001:2022.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

7.3.- RESPUESTA

El GRUPO SERVINFORM debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con la(s) empresa(s).

- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los equipos de Respuesta a Emergencias (CERT) reconocidos a nivel nacional como CCN-CERT, INCIBE y otros equivalentes.

7.4.- CONSERVACIÓN

Para restaurar la disponibilidad de los servicios, se deberán desarrollar planes de contingencia de los sistemas TIC que incluyan actividades de recuperación de la información que contribuyan a la continuidad del servicio, todo ello sin merma de los restantes principios básicos y requisitos mínimos establecidos, garantizando la conservación de los datos e información en soporte electrónico.

8.- ORGANIZACIÓN DE LA SEGURIDAD

GRUPO SERVINFORM de acuerdo con la Política de Seguridad y a las necesidades de la organización, ha definido y asignado los roles y responsabilidades, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación. También detalla la estructura y composición del comité para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

9.- DATOS DE CARÁCTER PERSONAL

La Dirección del GRUPO SERVINFORM, consciente de la importancia de garantizar la seguridad de los sistemas de información con datos de carácter personal y en cumplimiento del RGPD (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), y de la Ley 3/2018 de Protección de Datos y Garantía de los Derechos Digitales, mantiene implementado un sistema integrado de gestión eficaz y adecuado, con el fin de garantizar los niveles de seguridad exigidos por la legislación vigente en materia de Protección de Datos de Carácter Personal.

GRUPO SERVINFORM promueve el concepto de Seguridad de la Información y de los Datos Personales, y el Principio de Responsabilidad Proactiva, estableciéndose responsabilidades para garantizar la seguridad, integridad, confidencialidad, disponibilidad y calidad de los procedimientos, tratamientos, manipulación, comunicaciones, consultas, interconexiones o transferencias de datos de carácter personal.

GRUPO SERVINFORM, en el tratamiento de datos personales cumplirá los principios relativos al tratamiento recogidos en la normativa de Protección de Datos:

- **Principio de licitud, lealtad y transparencia**: los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado.
- **Principio limitación de la finalidad**: los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
- **Principio de minimización de datos**: los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Principio de exactitud**: los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
- **Principio de limitación del plazo de conservación**: los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.
- **Principio de integridad y confidencialidad**: los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.
- **Principio de proactividad:** SERVINFORM en cumplimiento de dicho principio adoptará las medidas técnicas y organizativas necesarias que se estimen oportunas no sólo para garantizar la aplicación efectiva del sistema de gestión de Protección de Datos implantado sino también para poder demostrarlo.

10.- GESTIÓN DE RIESGOS/AMENAZAS

GRUPO SERVINFORM realizará los análisis de riesgos y amenazas que considere necesarios para contribuir a la seguridad de las actividades, medios y personas de la compañía. La metodología, periodicidad y otras características de dichos análisis se adaptarán a las necesidades específicas de cada uno de ellos y conservando las correspondientes evidencias de los mismos dentro del SGSI según los procedimientos del mismo.

11.- DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política se desarrolla para dar cumplimiento a las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso y apoyada por otros documentos específicos que detallan aspectos con una mayor profundidad.

Los documentos del SGSI aprobados y en su última versión vigente, se encontrarán a disposición de todos los miembros de la organización y otras partes interesadas que necesiten y justifiquen conocerlos, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Concretamente, esta Política de Seguridad, estará accesible públicamente.

La documentación relativa a la Seguridad estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- **Primer nivel**: Política de Seguridad de la Información del ENS y la norma UNE-EN ISO/IEC 27001:2022. Documento de obligado cumplimiento por todo el personal, interno y externo de la Organización, recogido en el presente documento y aprobado por el Consejero Delegado de SERVINFORM.

  En un nivel inferior, la política de seguridad debe ser apoyada por otras normas o procedimientos sobre temas específicos que obligan aún más la aplicación de los controles de seguridad y se estructuran normalmente para tratar las necesidades de determinados grupos dentro de una organización o para cubrir ciertos temas.

- **Segundo nivel**: Normativas y procedimientos de seguridad específicos. De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente, desarrollados por SERVINFORM en el marco de su SGSI en los que se han incluido los aspectos específicos del ENS para cumplir con los requisitos mínimos de seguridad que marca su artículo 12 y del Anexo A de la norma UNE-EN ISO/IEC 27001:2022 según su Declaración de Aplicabilidad (SoA) de acuerdo a la categorización vigente del sistema.

  La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Responsable de Seguridad bajo la supervisión del Comité de Seguridad.

- **Tercer nivel**: Procedimientos e Instrucciones Técnicas (IT) de seguridad. Estos son documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.
  La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable del Sistema de Información correspondiente, bajo la supervisión del Responsable de Seguridad. En caso de que los procedimientos afectaran a varios sistemas de información será responsabilidad del Responsable de Seguridad el aprobarlos.

- **Cuarto nivel**: Informes, registros y evidencias electrónicas. Todos ellos, recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

  La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito.

Otra documentación: Adicionalmente, se puede disponer, de procedimientos de apoyo que incluyen el modo específico en que se deben acometer las directrices generales indicadas en las políticas y por parte de los responsables designados. Se podrán seguir en todo momento los procedimientos, normas, instrucciones técnicas y recomendaciones STIC, así como las guías CCN-STIC de las series 400, 500 y 600, series NIST (del Computer Security Resource

Center) y CIS (Center for Internet Security) y cualquier otra documentación adicional como referencia para los mismos.

Además, se seguirán las directrices indicadas por la Agencia de Protección de Datos Española (AEPD) y aquellos otros que regulen su cumplimiento, especialmente con el registro de Actividades de Tratamiento de Datos para el GRUPO SERVINFORM.

12.- APLICACIÓN DE LA POLITICA DE SEGURIDAD SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD

GRUPO SERVINFORM para el correcto desempeño de sus funciones de negocio se basa y ayuda del tratamiento de diferentes tipos de activos, bienes, datos, información, etc. sustentados por los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyendo estos, uno de los activos principales del GRUPO SERVINFORM de tal manera que el daño o pérdida de los mismos, inciden en la realización de sus servicios y pueden poner en peligro la continuidad de la organización.

Para que esto no suceda, esta Política de Seguridad tiene como objetivos principales:

- Proteger, mediante controles/medidas, los activos frente a amenazas que puedan derivar en incidentes de seguridad.
- Paliar los efectos de los incidentes de seguridad.
- Establecer un sistema de clasificación de la información y los datos con el fin de proteger los activos críticos de información.
- Definir las responsabilidades en materia de seguridad generando la estructura organizativa correspondiente.
- Elaborar un conjunto de reglas, estándares y procedimientos aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- Especificar los efectos que conlleva el incumplimiento de la Política de Seguridad en el ámbito laboral.
- Evaluar los riesgos que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- Verificar el funcionamiento de las medidas/controles de seguridad mediante revisiones de seguridad internas realizadas por expertos independientes.
- Formar a los usuarios en la gestión de la seguridad y en tecnologías de la información y las comunicaciones.
- Controlar el tráfico de información y de datos a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- Observar y cumplir la legislación en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecten a los activos de la organización.

- Proteger el capital intelectual de la organización para que no se divulgue ni se utilice ilícitamente.
- Reducir las posibilidades de indisponibilidad a través del uso adecuado de los activos de la organización.
- Defender los activos ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- Controlar el funcionamiento de las medidas de seguridad averiguando el número de incidencias, su naturaleza y efectos.

La Dirección del GRUPO SERVINFORM asume la responsabilidad de apoyar y promover el establecimiento de las medidas organizativas, técnicas de control necesarias para el cumplimiento de la presente Política de Seguridad, así como, de proveer aquellos recursos que sean necesarios para resolver con la mayor rapidez y eficacia posible, las no conformidades e incidentes de seguridad de la información que pudiesen surgir, y la puesta en funcionamiento de las medidas necesarias para que estas no vuelvan a ocurrir.

Esta Política será mantenida, actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos de la organización. A este efecto se revisará de forma planificada o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

13.- OBLIGACIONES DE LAS PERSONAS DEL GRUPO SERVINFORM

Todos los miembros del GRUPO SERVINFOM tienen la obligación de conocer y cumplir esta Política de Seguridad y la documentación de seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados, teniendo en cuenta siempre las disponibilidades presupuestarias y de recursos dispuestos por el GRUPO SERVINFORM.

Todos los empleados de la organización están sujetos a funciones y obligaciones.

Todo el personal de la entidad que disponga de acceso a los datos de carácter personal y/o acceda a información gestionada por el GRUPO SERVINFORM debe cumplir con las siguientes obligaciones:

- No se permite la difusión de datos de carácter personal ni confidenciales pertenecientes a la entidad quedando obligados a guardar secreto de la información, terminada incluso la relación laboral.
- El usuario se responsabilizará de notificar toda incidencia según el procedimiento de gestión de incidencias. No notificar una incidencia será considerada una omisión del deber del trabajador.

- El usuario se responsabilizará de todos los accesos que se realicen bajo sus identificadores y/o credenciales, por tanto, no deberá revelar nunca sus claves de acceso.
- El usuario se responsabilizará siempre que abandone el puesto de trabajo a cerrar su sesión o bloquear el equipo con contraseña.
- No se podrán instalar aplicaciones no corporativas en los sistemas de la entidad sin el consentimiento del Responsable del Servicio.
- No se permite la copia de datos de carácter personal, en soportes, sin la autorización expresa del delegado de protección de datos.
- El usuario se responsabilizará de guardar copias de todos los correos que incluyan anexos con datos personales vinculados a la organización.

Todos los trabajadores del GRUPO SERVINFORM atenderán al menos una vez al año, a una acción de concienciación en materia de seguridad TIC. Se establecerá un programa de acciones para la formación y capacitación continua, para atender a todos los miembros de la organización relacionados con la ciberseguridad en su área correspondiente, en particular a los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias y de recursos en el GRUPO SERVINFORM.

En su caso, si además se requiere formación específica en otras cuestiones relacionadas con la seguridad, las personas la recibirán mediante el correspondiente plan de formación, en la medida en que la necesiten para realizar su trabajo.

14.- TERCERAS PARTES

Cuando el GRUPO SERVINFORM preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad. Para ello, se establecerán canales para información y coordinación de los respectivos Comités de Seguridad del ENS y en su caso de otras normas y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el GRUPO SERVINFORM utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la documentación del SGSI necesaria que implique a dichos servicios o información. Dicha tercera parte quedará sujeta a todas las obligaciones establecidas en la mencionada documentación. Con ello, el proveedor deberá garantizar que su personal está adecuadamente formado en materia de seguridad, al menos al mismo nivel que la organización y de acuerdo con los requerimientos que sean necesarios.

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 los que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados con anterioridad al inicio del proyecto.

15.- APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR

El Consejero Delegado (CEO) del GRUPO SERVINFORM es el responsable de aprobar la política de seguridad.

En Madrid, a 11 de diciembre de 2023

Por Ignacio Rufo Rodríguez,

CEO y Consejero Delegado