POLÍTICA DE SEGURIDAD DEL GRUPO SERVINFORM, S.A.

Texto aprobado por la Dirección (Ignacio Rufo Rodríguez, Consejero Delegado)
Revisado: Comité de Seguridad de la Información
Fecha: 23 de noviembre de 2020
Versión 3.9

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

1.- INTRODUCCIÓN

La presente Política de Seguridad de la Información se elabora en cumplimiento de la exigencia del Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), en el ámbito de la Administración Electrónica, que en su artículo 11 establece la obligación a las Administraciones Públicas y a los proveedores de servicios de las Administraciones públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.

Esta Política de Seguridad sigue también las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional (CCN), centro adscrito al Centro Nacional de Inteligencia (CNI).

Dará cumplimiento también a la Política de Seguridad del Sistema de Gestión de la Seguridad de la Información de acuerdo a los requisitos de la norma UNE-EN ISO/IEC 27001:2017 para garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el cumplimiento de los objetivos fijados alineada junto al ENS.

Ley 40/2015, de Régimen Jurídico del Sector Público establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados y recoge el Esquema Nacional de Seguridad en su artículo 156.

Mientras que la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones Públicas el relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

La finalidad del ENS 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.

La finalidad de la UNE-EN ISO/IEC 27001:2017 es fijar el marco de actuación necesario para proteger los recursos de información frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar la seguridad de la información, preservando su confidencialidad, integridad y disponibilidad. Además, asegurará el cumplimiento de los objetivos mediante el proceso de mejora continua y de una manera apropiada mediante PHVA (Planificar, Hacer, Verificar, Hacer) con el compromiso adquirido por la Dirección.

Siendo ambas finalidades similares en cuanto a su naturaleza y finalidades a cumplir por el GRUPO SERVINFORM, S.A. (en adelante SERVINFORM), es necesario disponer de una integración muy clara, pues ambas herramientas son complementarias y constituyen un binomio perfecto para la ciberseguridad.

A través de la Guía CCN-STIC-825 se establecen los aspectos comunes y diferenciadores entre la ISO/IEC 27001 y ENS pudiendo abordar, dentro de un mismo alcance para los sistemas de información, la certificación integrada de ambos referenciales. Esto permite dar cumplimiento a un Real Decreto Español y disponer de un Sistema de Gestión de Seguridad de reconocimiento internacional ISO que permita entre ambos, asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los sistemas de información, sus servicios y su información.

La presente Política de Seguridad, se establece de acuerdo con los principios básicos de seguridad aplicando los requisitos mínimos de 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, Seguridad por defecto, Integridad y actualización del sistema, Protección de la información almacenada y en tránsito, Prevención ante otros sistemas de información interconectados, Registro de actividad, Incidentes de seguridad, Continuidad de la actividad y Mejora continua del proceso de seguridad.

La adaptación al ENS implica que SERVINFORM y su personal deben aplicar las medidas mínimas de seguridad exigidas por el propio ENS, 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 de 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 de SERVINFORM deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

1.1.- Prevención

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, 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.

1.2.- 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 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 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.

1.3.- Respuesta

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 SERVINFORM.
- 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, CNPIC y otros equivalentes.

1.4.- Recuperación

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.

2. 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:

- Recepción, Almacenamiento, Tratamiento, Impresión, Acabado de documentos de clientes y su comunicación y transmisión por cualquier método electrónico (SMS, Email, etc.)
- Desarrollo de Servicios y Aplicaciones, Digitalización y Automatización de Negocio, Gestión de Redes Sociales, Centralita Virtual VoIP Omnicanal, Mobiliario y Tecnología para Punto de Venta e IOT y Desarrollo de algoritmos de Machine Learning e Inteligencia Artificial.
- Prestación de los servicios de Centro de Atención Telefónica (recepción, ventas, emisión, c2c, etc.), Gestión de Peticiones, Soporte Técnico, Backoffice a usuarios y Gestiones Administrativas.
- Gestión de recobro y recuperación de deuda tanto a nivel nacional como internacional.

En general esta política se aplica a todos los sistemas TIC de SERVINFORM y a todos los miembros de la organización, sin excepciones, de acuerdo con la declaración de aplicabilidad (SOA) y el catálogo de servicios vigente a la fecha de emisión del certificado para todos los centros principales y auxiliares dependientes de los mismos donde se realizan las actividades del Grupo SERVINFORM siendo estos los que se relacionan a continuación:

- Madrid, Avda. de los Premios Nobel, 37, 28850 – Torrejón de Ardoz (Madrid).
- Sevilla, Polígono Industrial PISA, Cl. Manufactura, 1, 5, 7, 9 y 11 y Cl. Artesanía 22-26, 41927 – Mairena del Aljarafe (Sevilla).
- Valencia, Polígono Industrial del Mediterráneo, Cl. Fila 8, 46550 – Albuixech (Valencia).
- Bilbao, Polígono Industrial Leguizamón, Cl. Gorbeia, 1, 48450 – Etxebarri (Bizkaia).
- Barcelona, Cl. de Roselló y Porcel, 21, 08016 – Barcelona.

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

3.- MISIÓN

SERVINFORM, empresa líder de servicios integrales, ofrece a sus clientes el mejor servicio con Alta Calidad en la Gestión de Servicios TI, Seguridad para el personal y respeto al Medio Ambiente, en conocimiento de su contexto.

El propósito de SERVINFORM en materia de "Calidad", "Gestión de la Seguridad de la Información" y "Calidad en la Gestión de Servicios TI" 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.

En lo que respecta al Medio Ambiente, SERVINFORM se compromete a protegerlo, racionalizando el consumo de los recursos y de la energía así como a prevenir la posible contaminación de suelos, atmósfera y aguas, de manera que las actividades sean ejecutadas y gestionadas de una manera eficiente y sostenible.

En cuanto a prevención de riesgos laborales, SERVINFORM es consciente de que la salud y seguridad del personal contribuye a la ejecución de nuestra actividad empresarial, y se compromete a proporcionar unas condiciones de trabajo seguras y saludables garantizando la prevención de los daños y deterioros de la salud, por lo que preserva y desarrolla los recursos humanos y enfoca sus esfuerzos a la eliminación o reducción de los riesgos más relevantes, así como a proporcionar los recursos necesarios para implementar oportunidades de mejora.

La Dirección de SERVINFORM, ha adquirido el compromiso de integrar la igualdad de oportunidades entre mujeres y hombres en la organización como principio básico y transversal, ello queda plasmado en el Plan de igualdad.

Para alcanzar los objetivos, esta gestión se desarrolla por medio de la implementación y mantenimiento de un Sistema de Gestión integrado de Calidad ISO/EC 9001:2015, Medio ambiente ISO/IEC 14001:2015, Gestión del Servicio (TI) ISO/IEC 20000-1:2011, Sistemas de Gestión de la Seguridad de la Información ISO/IEC 27001:2017 y Seguridad y Salud en el Trabajo ISO/IEC ISO 45001:2018 respectivamente entre otros.

Dicho Sistema es desarrollado con el compromiso de todo el personal y es responsabilidad del Consejero Delegado de SERVINFORM, velar por su estricto cumplimiento, dotando de los recursos necesarios para llevarlo a cabo pudiendo, en cualquier momento, tomar las acciones correctivas necesarias para conseguirlo.

SERVINFORM es consciente de que la información manejada de sus clientes en aquellos sistemas empleados para poder prestar los servicios y todas las actividades necesarias relacionadas en el presente alcance, se ha convertido en uno de los principales activos de nuestra organización, y es por ello por lo que cuidarla y protegerla se convierte en un objetivo absolutamente prioritario.

Es parte de nuestra estrategia, a partir de ahora, la seguridad de la información 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, pero que ayuda a adoptar las medidas de seguridad apropiadas en los sistemas de la información.

4.- MARCO NORMATIVO

SERVINFORM se encuentra sujeto a la siguiente normativa en los servicios prestados a sus clientes:

De ámbito internacional:

- ISO/IEC 27001
- ISO/IEC 9001
- ISO/IEC 14001
- ISO/IEC 45001
- ISO/IEC 20000-1
- CMMIDEV-3

De ámbito Europeo:

- Reglamento Europeo de Protección de Datos 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.
- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013.

De ámbito Estatal:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Ley 40/2015 recoge el Esquema Nacional de Seguridad (ENS) en sus artículos 46.3 y 156.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- BOE Núm. 28. Resolución de 15 de noviembre de 2011 donde se establecen los contenidos mínimos de los planes de seguridad del operador y planes de protección específicos conforme a lo dispuesto en el Real Decreto 704/2011.

- Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley Orgánica 10/1995, de 23 de noviembre, Código Penal.
- Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, del Código penal.
- Real Decreto 1514/2007, de 16 de noviembre, por el que se aprueba el Plan General de Contabilidad.
- Acuerdo de entendimiento entre la Agencia Estatal de Administración Tributaria y la Asociación Business Software Alliance para la prevención del fraude fiscal.

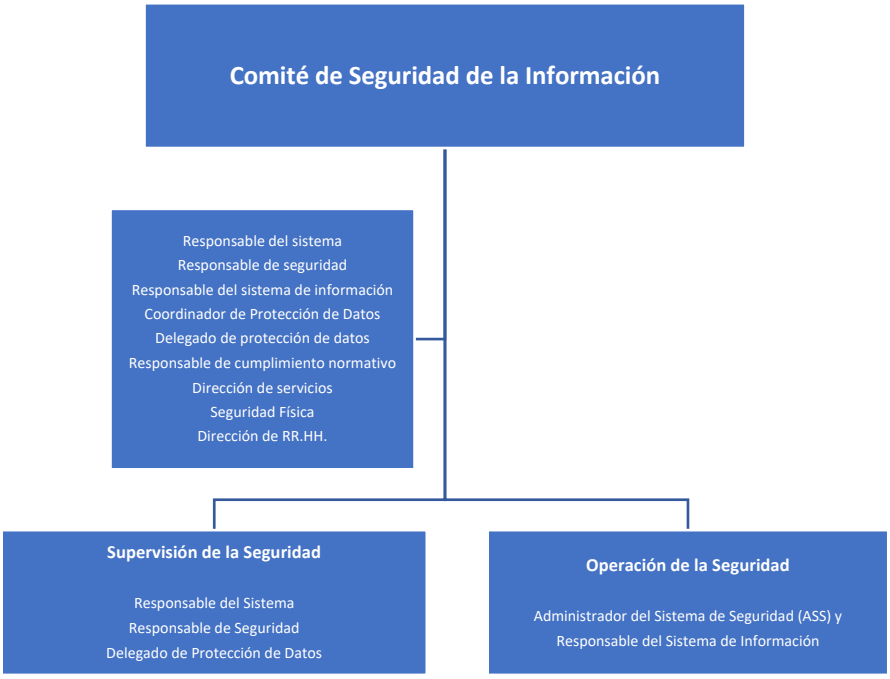
De ámbito interno:

- Estatutos de SERVINFORM, así como sus normativas de desarrollo relacionadas con los objetivos del mismo.
- Código ético de SERVINFORM.

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

5.- ORGANIZACIÓN DE LA SEGURIDAD

En los sistemas de información se diferenciará la persona responsable de la información, del servicio y de la seguridad. Siguiendo uno de los principios básicos del ENS sobre la seguridad como función diferenciada se han establecido en SERVINFORM, los roles y responsabilidades diferenciadas que se describen a continuación.



5.1.- Responsable de la información y del servicio (Comité)

El órgano responsable de la seguridad de la información y del servicio será el **Comité de Seguridad de la Información** que determinará los requisitos de la información tratada en materia de seguridad y sobre la base del establecimiento previo de los niveles de seguridad en cada dimensión de los sistemas. Además, como responsable del servicio determinará los requisitos de los servicios prestados y sus niveles de seguridad. Este rol será asumido por el Presidente del Comité.

5.2.- Responsable del sistema (CSO)

La persona líder del proceso de Seguridad de los Sistemas de Información y Servicios del Proceso Gestión de Sistemas de Información de SERVINFORM, es la responsable del sistema conforme a los requisitos del Esquema Nacional de Seguridad y la Norma de Gestión ISO/IEC 27001 (Responsable del Sistema de Gestión de los Sistemas de Información) y determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Entre las tareas principales del responsable del sistema se encuentran:

- Recibir los informes de auditoría y adoptar las medidas correctoras adecuadas con las conclusiones aportadas por el responsable de seguridad.
- En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas. (Esta decisión debe ser acordada con los

responsables de la información afectada, del servicio afectado y el responsable de la seguridad, antes de ser ejecutada).
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

5.3.- Responsable de seguridad (CISO)

La persona líder del Proceso de Gestión de Seguridad de la Información de SERVINFORM es el Responsable de Seguridad conforme a los requisitos del Esquema Nacional de Seguridad y determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Entre las tareas principales del responsable de seguridad se encuentran:

- Coordinar y controlar las medidas de seguridad, aplicables y definidas en los procedimientos de aplicación.
- Controlar directamente los mecanismos que permiten el registro de accesos no permitiendo la desactivación ni la manipulación de los mismos.
- Revisar al menos una vez al mes la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados.
- Proponer decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Realizar propuestas sobre la adquisición de productos y contratación de servicios relacionados con la seguridad.
- Dar cumplimiento a los requisitos mínimos de seguridad aplicables a la categoría media del sistema según el ENS y sin perjuicio del cumplimiento de lo requerido por lo dispuesto en el Reglamento General de Protección de Datos de Carácter Personal.
- Formalizar, aprobar formalmente y firmar el cumplimiento de las medidas de seguridad del Anexo II del ENS, incluidas las compensatorias y su justificación, en un documento que se denominará Declaración de aplicabilidad (SOA).
- Analizar los informes de auditoría del ENS y presentar las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.
- Mantener la seguridad de la información gestionada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la presente Política de Seguridad de la Información.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

5.4.- Delegado de Protección de Datos (DPO)

El DPO puede ser una persona física o un órgano colegiado, cuyas funciones se señalan en el artículo 39 del Reglamento (UE) 679/2016, así como los artículos 36 y 37 de la Ley Orgánica 3/2018, y se ocupa de la aplicación de la legislación

sobre privacidad y protección de datos en la entidad en la que desarrolla sus funciones.

El delegado de protección de datos tendrá como mínimo 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 presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, 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.
- 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, y realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Para ello deberá ser capaz de:

- Recabar información para determinar las actividades de tratamiento, analizar y comprobar la conformidad de las actividades de tratamiento, e informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- Recabar información para supervisar el registro de las operaciones de tratamiento.
- Asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.
- Asesorar sobre:
    - Si se debe llevar a cabo o no una evaluación de impacto de la protección de datos
    - Qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos.
    - Si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa.
    - Qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos de intereses de los afectados.

    - Si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y
    - Si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes al Reglamento.
- Priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.
- Asesorar al responsable del tratamiento sobre: qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos, qué áreas deben someterse a auditoría de protección de datos interna o externa, qué actividades de formación internas proporcionar al personal o a los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

El DPO deberá reunir conocimientos y la práctica en materia de protección de datos. Se han identificado, en consecuencia, aquellos conocimientos, habilidades o destrezas necesarias que tiene que saber o poseer el Delegado de Protección de Datos para llevar a cabo una de las funciones propias de su puesto.

Estas funciones genéricas del DPO se pueden concretar en tareas de asesoramiento y supervisión, entre otras, en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditoría de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgos de los tratamientos realizados.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.

- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

5.5.- Administrador del Sistema de Seguridad (ASS) y Responsable de los sistemas de información

El Administrador del Sistema de Seguridad (ASS) y como Responsable de los Sistemas de Información, dentro de sus áreas de actuación, tendrán asignadas las siguientes funciones:

- Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Elaborar procedimientos técnicos de seguridad de los sistemas de información.
- Elaborar planes de continuidad de los sistemas de información.
- Colaborar para la realización del análisis de riesgos de los sistemas de información de los que es responsable.
- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- Informar al Responsable de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

5.6.- Comité de Seguridad de la Información

El Comité de Seguridad de la Información es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité.

Tiene como objetivo prioritario realizar una evaluación continua del estado de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información implantado en la organización, derivado este del cumplimiento del Esquema Nacional de Seguridad, la Norma de Gestión ISO/IEC 27001 y de la protección de datos de carácter personal según normativa vigente.

De acuerdo con ello, las responsabilidades del Comité de Seguridad de la Información serán, entre otras, las que se definirán ampliamente en el ACTA DE CONSTITUCIÓN DEL COMITÉ, coordinar la seguridad de la información a nivel de organización para, entre otros aspectos, racionalizar la implantación de las diferentes medidas de seguridad requeridas por el sistema y evitar disfunciones que permitan fallas de seguridad al dejar al sistema con puntos débiles donde pudieran ocurrir accidentes o se pudieran perpetrar ataques.

Los miembros del comité de seguridad de la información son:

- Responsable del sistema
- Responsable de seguridad
- Administrador del Sistema de Seguridad (ASS) y Responsable del sistema de información
- Coordinador de Protección de Datos
- Delegado de protección de datos
- Responsable de cumplimiento normativo
- Dirección de servicios
- Seguridad Física
- Dirección de RR.HH.

Estos miembros son designados por el Comité de Dirección, único órgano que puede nombrarlos, renovarlos y cesarlos.

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de ésta.

5.7.- Comité de Dirección

El Comité de Dirección, tendrá las siguientes responsabilidades específicas en el ámbito del ENS:

- Liderar el sistema.
- Proporcionar los recursos necesarios para el sistema.
- Mejorar continuamente nuestro sistema de seguridad de la información.

- Coordinar, nombrar y resolver conflictos del Comité de Seguridad.
- Tomar las acciones correctivas necesarias para conseguir los objetivos.

5.8.- Coordinación, nombramiento y resolución de conflictos

La coordinación se lleva a cabo en el seno del Comité de Dirección. Podrá delegar en el Comité de Seguridad de la Información.

Los nombramientos, ceses, etc. correrán a cargo exclusivo del Comité de Dirección exclusivamente.

La resolución de conflictos, se delegará en el Comité de Seguridad de la Información, quien deberá resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización en materia de Seguridad, elevando únicamente aquellos casos en los que no tenga suficiente autoridad para decidir al Comité de Dirección. La resolución de estos conflictos será tratada mediante la correspondiente convocatoria sobre los puntos del día a tratar y quedará formalizada una vez tratada la misma con su resolución o elevación al Comité de Dirección en su caso, mediante la correspondiente Acta de la sesión.

6.- DATOS DE CARÁCTER PERSONAL

La Dirección de 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.

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.

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.

Es objetivo de esta Dirección concienciar a todos los miembros de la empresa acerca de la necesidad de garantizar la Seguridad de la Información y de los Datos Personales, y de convertir esta necesidad en una tarea colectiva, en la cual debe implicarse todo el personal de la empresa.

Las directrices generales que se establecen son las siguientes:

- Implantar en la Organización una Norma de Seguridad, plasmada en el Documento de Seguridad.
- 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 la Norma de Seguridad.
- Formar a todos los empleados que acceden a los datos en las directrices y procedimientos de la Norma.
- Velar por el cumplimiento de la legislación vigente y de la Norma de Seguridad.

El Documento de Seguridad ha sido elaborado de forma que se trabaje sobre la prevención de los defectos, más que sobre su corrección.

La eficacia y aplicación de la normativa de seguridad es responsabilidad directa de la Dirección. En su nombre y representación, se ha nombrado un Delegado de Protección de Datos, quien supervisará la implantación, desarrollo, seguimiento y mantenimiento de la misma, evaluando su adecuación y correcta aplicación. El Delegado de Protección de Datos posee la suficiente autoridad para intervenir en la empresa, en la medida que se estime conveniente, y para desempeñar un papel activo en la implantación del

Documento de Seguridad, así como del resto de documentos del sistema, identificando problemas, verificando su eficacia y coordinando las actividades que puedan verse afectadas. La Dirección se compromete a revisar periódicamente el contenido de la Política de Seguridad, para garantizar su adecuación a las necesidades de la organización y de la legislación vigente.

7.- GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política de Seguridad realizarán un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurran cambios en la infraestructura sobre la cual se realice el tratamiento.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados.

8.- DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política se desarrolla por medio del Documento de Seguridad que afronte aspectos específicos. La Normativa de Seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Para dar cumplimiento a la misma, se han tenido en cuenta los requisitos mínimos del Art. 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, para articular la gestión continuada de la seguridad de acuerdo con los principios básicos indicados a continuación y aprobada por el Consejero Delegado de la Organización:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos.

h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

Los anteriores principios básicos, quedan reflejados en la documentación relativa a la Seguridad de la Información que 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.
- Segundo nivel: Normativas y Procedimientos de Seguridad.
- Tercer nivel: Procedimientos e Instrucciones Técnicas de Seguridad.
- Cuarto nivel: Informes, registros y evidencias electrónicas.

La Política se encuentra aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

La normativa de seguridad estará disponible en la intranet de SERVINFORM y esta Política de Seguridad estará accesible públicamente en la web de la organización.

8.1.- Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, de la Organización, recogido en el presente documento y aprobado mediante el Consejero Delegado de la Organización.

8.2.- Segundo Nivel: Normativas y Procedimientos de Seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente, desarrollados por SERVINFORM en el marco de su Sistema de Gestión en los que se han incluido los aspectos específicos del ENS para cumplir con los requisitos mínimos de seguridad que marca su artículo 11, tal y como indica CCN-STIC 825 ENS y la Certificación que establece el marco de seguridad ISO/IEC 27001:2017, apartado 5.1.

Para facilitar la trazabilidad entre las medidas de seguridad requeridas por el ENS y su implantación en SERVINFORM en el marco del SGSI, en la Declaración de Aplicabilidad del ENS se ha procedido a mapear las medidas de seguridad aplicables del Anexo II con los controles del Anexo A de ISO 27001. Realizado de acuerdo con la Guía de Seguridad (CCN-STIC 825) Esquema Nacional de Seguridad – Certificaciones 27001.

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

8.3.- Tercer Nivel: Procedimientos Técnicos de Seguridad

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.

8.4.- Cuarto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que 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.

8.5.- Otra documentación

Se podrá 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).

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 SERVINFORM.

9.- APLICACIÓN DE LA POLÍTICA DE SEGURIDAD SOBRE EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Debido a que es necesario dar cumplimiento a un Real Decreto Español y disponer de un Sistema de Gestión de Seguridad de reconocimiento internacional ISO que permita entre ambos, asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los sistemas de información, sus servicios y su información, todo ello bajo un proceso de mejora continua e integrados de manera sistemática los procesos de mejora del SGSI dentro de los procesos normales de revisión, en SERVINFORM se definen de forma específica los siguientes principios en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) para proteger la información interna relacionada con la prestación de los servicios, considerando las dimensiones de:

- **Confidencialidad**: la información tratada por SERVINFORM será conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.
- **Integridad**: la información tratada por SERVINFORM será completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.
- **Disponibilidad**: la información tratada por SERVINFORM estará accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.
- **Autenticidad**: que permita verificar y garantizar que el origen de la información a la que se accede o modifica es correcto. Se han establecidos los procedimientos e implementado los sistemas buscando que los accesos a la información no puedan generar dudas en este sentido, pudiendo conocer y contrastar al autor de toda información.
- **Trazabilidad**: de los accesos y modificaciones de la información que permita conocer quién, cuándo y cómo se ha realizado. Para ello se han implantado los sistemas y registros adecuados para la realización de los análisis y detección de accesos no autorizados tanto a nivel informático como físico de manera que toda acción quede registro del autor.
- **Legalidad**: SERVINFORM garantizará el cumplimiento de toda legislación o requisito contractual que sea de aplicación. Y en concreto, la normativa en vigor relacionada con el tratamiento de datos de carácter personal.

SERVINFORM para el correcto desempeño de sus funciones de negocio se basa y ayuda del tratamiento de diferentes tipos de datos e información, sustentados por los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyendo estos, uno de los activos principales de 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, se ha diseñado una Política de Seguridad de la Información cuyos fines principales son:

- 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 de la información 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 auditorías de seguridad internas realizadas por auditores 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 afecte a los activos de SERVINFORM.
- 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 de 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 de la Información. 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.

De igual forma, para gestionar los riesgos que afronta SERVINFORM se establece un procedimiento de evaluación de riesgos formalmente definido.

Por su parte, todas las políticas y procedimientos incluidos en el SGSI como en el ENS, serán revisados, aprobados e impulsados por la Dirección de SERVINFORM.

10.- OBLIGACIONES DEL PERSONAL

Todos los miembros de SERVINFORM tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados, teniendo en cuenta siempre las disponibilidades presupuestarias de SERVINFORM.

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

Todo el personal de la entidad que disponga de acceso a los datos de carácter personal debe cumplir con las siguientes obligaciones:

- No se permite la difusión de datos de carácter personal ni confidencial perteneciente a la entidad. Estando obligado a guardar secreto de la información incluso terminada 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 su identificador y contraseña, por tanto, no deberá revelar la contraseña.
- El usuario se responsabilizará siempre que abandone el puesto de trabajo de cerrar su sesión o bloquear el equipo con contraseña.
- No se podrán instalar aplicaciones en los sistemas de la entidad sin el consentimiento del Responsable de Seguridad.
- 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 entidad

Todos los trabajadores de SERVINFORM bajo el alcance del ENS atenderán a una acción de concienciación en materia de seguridad TIC, al menos, una vez de forma anual. Se establecerá un programa de acciones para la concienciación continua, para atender a todos los miembros de SERVINFORM relacionados con la ciberseguridad en su área correspondiente, en particular a los de nueva incorporación, teniendo en cuenta

siempre las disponibilidades presupuestarias de SERVINFORM. Se realizará una acción de concienciación al menos de forma anual y de manera continuada para el personal de nueva incorporación.

En su caso, si se requiere formación específica para el manejo seguro de los sistemas, las personas con responsabilidad en la operación o administración de sistemas TIC la recibirán en la medida en que la necesiten para realizar su trabajo.

11.- TERCERAS PARTES

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

Cuando SERVINFORM utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que implique a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa. Con ello, el proveedor deberá garantizar que su personal está adecuadamente formado en materia de seguridad de acuerdo con los requerimientos de SERVINFORM.

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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

ANEXO I. GLOSARIO DE ABREVIATURAS.

- **AEPD:** Agencia de Protección de Datos Española.
- **C2C:** Cliente a Cliente.
- **CCN:** Centro Criptológico Nacional.
- **CERT:** Equipo de Respuesta ante Emergencias Informáticas.
- **CIS:** Centro de la Seguridad de Internet.
- **CMMIDEV:** Integración de sistemas modelos de madurez de capacidades para el desarrollo de software.
- **CNI:** Centro Nacional del Inteligencia.
- **CNPIC:** Centro Nacional de Protección de Infraestructuras y Ciberseguridad.
- **DPO:** Delegado de Protección de Datos.
- **ENISA:** Agencia de la Unión Europea para la Ciberseguridad.
- **ENS:** Esquema Nacional de Seguridad.
- **FSC:** Consejo de Administración Forestal.
- **IEC:** Comisión Electrotécnica Internacional.
- **INCIBE:** Instituto Nacional de Ciberseguridad.
- **ISO:** Organización Internacional de Normalización o Estandarización.
- **IOT:** Internet de las cosas.
- **NIST:** Instituto Nacional de Estándares y Tecnología.
- **PEFC:** Programa para el Reconocimiento de Certificación Forestal.
- **RGPD:** Reglamento General de Protección de Datos.
- **RR.HH.:** Recursos Humanos.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **SMS:** Servicio de Mensajes Cortos.
- **SOA:** Declaración de Aplicabilidad.
- **STIC:** Servicio de las Tecnologías de la Información y las Comunicaciones.
- **TIC:** Tecnologías de la Información y las Comunicaciones.
- **UE:** Unión Europea.
- **UNE:** Asociación Española de Normalización.
- **VoIP:** Voz IP.

ANEXO II. REFERENCIAS.

- Reglamento Europeo de Protección de Datos 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. https://www.boe.es/doue/2016/119/L00001-00088.pdf

- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013. https://www.boe.es/doue/2019/151/L00015-00069.pdf

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. https://www.boe.es/buscar/pdf/2010/BOE-A-2010-1330-consolidado.pdf

- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. https://www.boe.es/boe/dias/2015/11/04/pdfs/BOE-A-2015-11881.pdf

- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad. https://www.boe.es/boe/dias/2016/11/02/pdfs/BOE-A-2016-10108.pdf

- Ley 40/2015 recoge el Esquema Nacional de Seguridad (ENS) en sus artículos 46.3 y 156. https://www.boe.es/boe/dias/2015/11/04/pdfs/BOE-A-2015-11881.pdf

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

- Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico. https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf

- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf

- BOE Núm. 28. Resolución de 15 de noviembre de 2011 donde se establecen los contenidos mínimos de los planes de seguridad del operador y planes de protección específicos conforme a lo dispuesto en el Real Decreto 704/2011. https://www.boe.es/boe/dias/2011/11/23/pdfs/BOE-A-2011-18439.pdf

- Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social. https://www.boe.es/buscar/pdf/2015/BOE-A-2015-11724-consolidado.pdf

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público. https://www.boe.es/buscar/pdf/2017/BOE-A-2017-12902-consolidado.pdf

- Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales. https://www.boe.es/buscar/pdf/1995/BOE-A-1995-24292-consolidado.pdf

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. https://www.boe.es/buscar/pdf/2014/BOE-A-2014-4950-consolidado.pdf

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual. https://www.boe.es/buscar/pdf/1996/BOE-A-1996-8930-consolidado.pdf

- Ley Orgánica 10/1995, de 23 de noviembre, Código Penal. https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf

- Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. https://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf

- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, del Código penal. https://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3439.pdf

- Real Decreto 1514/2007, de 16 de noviembre, por el que se aprueba el Plan General de Contabilidad. https://www.boe.es/buscar/pdf/2007/BOE-A-2007-19884-consolidado.pdf