seresco

Política de Seguridad

23/03/2021

Índice de contenido

1. Misión

Seresco, S.A. es una empresa de servicios tecnológicos especializada en la provisión de servicios de:

- ***Infraestructuras, Sistemas y Seguridad a terceros***
- ***Gestión, administración, desarrollo, soporte y mantenimiento de nómina***
- ***Consultoría y Desarrollo de Software***
- ***Cartografía y Catastro***
- ***Transformación Digital***

Seresco Atlântico, Unipessoal, Lda es una empresa de servicios tecnológicos especializada en la provisión de servicios de:

- ***Gestión, administración, soporte y mantenimiento de nómina***

La Dirección de Seresco (entendido como Seresco S.A y Seresco Atlântico, Unipessoal, Lda) en el marco de su Plan Estratégico y acorde a su Misión - *aportar soluciones mediante el uso de la tecnología de forma eficiente y segura* - ha considerado necesario incluir una declaración única y extensible a toda la entidad, en relación a la gestión de la seguridad.

A través del Sistema de Gestión de Seguridad de la Información, la Dirección de Seresco adquiere el compromiso firme de:

- **Mantener el pleno cumplimiento legal y normativo,** alineando los procesos y los servicios, a la normativa vigente en cada momento, y que afecta de manera indirecta o directa, al perfil de cliente (administración pública o sector privado), a la información implicada (*pública, restringida o secreta*) o en general a la seguridad de la información y/o servicio.
- **Sensibilizar y concienciar** de manera estable y permanente al usuario de la organización.
- **Fomentar y mantener una buena reputación de la organización,** en relación a la seguridad de los servicios prestados.
- **Disponer de respuestas a los incidentes de seguridad**, mediante acciones preventivas y cuando fuera preciso acciones de respuesta y recuperación, adecuadas y detalladas.
- **Asegurar que los activos de la organización, sólo sean utilizados por usuarios autorizados** en el ejercicio de sus funciones, según perfiles definidos o según asignaciones extraordinarias.
- **Tratar los datos personales de manera lícita, leal, transparente, con fines determinados y explícitos, legítimos sin ser usados para fines posteriores incompatibles**. Los datos personales tratados serán adecuados, pertinentes y limitados, exactos y actualizados. Serán tratados durante el tiempo necesario garantizándose la seguridad de los mismos.
- **Considerar la seguridad desde el diseño y por defecto** incluyendo a la Oficina de Protección de Datos siempre en la etapa más temprana del diseño y desarrollo de sistemas de información.
- **Proteger la información** interna y la relacionada con la prestación de los servicios a clientes, considerando las dimensiones de:

- **Confidencialidad:** Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
- **Integridad:** Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
- **Disponibilidad:** La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.

La organización podrá considerar otras dimensiones relacionadas con la seguridad, derivadas de requerimientos legales (o en su caso, de requerimientos de negocio), considerándose:

- **Trazabilidad:** Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.
- **Autenticidad:** Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a dudas.

La organización mantendrá las tres primeras dimensiones de seguridad y las dos añadidas, cuando sea preciso.

- **Entender la seguridad como un proceso integral,** constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La seguridad del sistema contemplará los aspectos de **prevención, detección y corrección**, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

1.1. Prevención

Se 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 Seresco implementará las medidas de seguridad pertinentes. Para garantizar el cumplimiento de la política, se 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

Seresco establecerá controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuará en consecuencia. Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

1.3. Respuesta

Seresco establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente con las partes interesadas.

1.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, Seresco desarrolla planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.

2. Alcance

La política de seguridad de la información, será de aplicación **a toda la información** del sistema con independencia del soporte o medio en el que se encuentre, tipología o categoría, **a todo el personal** de Seresco y también a terceros colaboradores, que accedan al sistema y/o presten servicios a la organización, así como **a cualquier activo** de información propiedad de la organización, o en régimen de uso y que afecte al sistema, considerándose en cualquier momento del ciclo de vida del sistema de seguridad.

Asimismo, la presente política, afecta a los datos personales gestionados y tratados por la organización.

Esta política estará accesible a todos los miembros de la organización, mediante su publicación en la intranet.

2.1. Alcance del sistema ENS

Específicamente en Seresco S.A se aplicarán las **medidas de seguridad de categoría media** recogidas en el Esquema Nacional de Seguridad al sistema de información que da soporte a los servicios del área de I***nfraestructuras, Sistemas y Servicios, agrupados en:***

- Consultoría de Sistemas, Servicios, Compliance y Seguridad
- Infraestructura como servicio
- Service Desk
- Operación y Administración de Sistemas, Infraestructuras y Seguridad

3. Marco normativo

Seresco, S.A. se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- El convenio colectivo aplicable, correspondiente a “Oficinas y Despachos”.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- RD-ley 13/2012 de 30 de marzo, ley de cookies.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- ISO/IEC 27001
- ISO/IEC 20000-1

Seresco Atlântico, Unipessoal Lda se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

- DL n.º 7/2004, de 07 de Janeiro (comércio electrónico no mercado interno e tratamento de dados pessoais);
- Lei n.º 41/2004, de 18 de agosto (protecção de dados pessoais e privacidade nas telecomunicações);
- Lei n.º 58/2019 de 8 de agosto (assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679);
- Lei n.º 102/2009, de 10 de Setembro (Regime jurídico da promoção da segurança e saúde no trabalho);
- Decreto-Lei n.º 110/2018 de 10 de dezembro (Código da Propriedade Industrial);

4. Organización de seguridad

4.1. Comité de Seguridad: funciones y responsabilidades

El Comité de Seguridad está formado por los Directores de áreas, el Responsable de Seguridad, el Responsable de Sistemas, el Responsable del Sistema de Gestión Integrado, Responsables de los sistemas ISO 20000-1 e ISO 27001 y Responsable de la Oficina de Protección de Datos.

El Comité tendrá las siguientes funciones:

1. Desarrollar la estrategia de seguridad de la información, definiendo planes de seguridad y realizando un seguimiento de ejecución.
2. Coordinar servicios y funciones relacionados con la seguridad.
3. Asesorar en materia de Seguridad de la Información a la empresa y a los diferentes responsables.
4. Resolver los conflictos de responsabilidad relacionados con seguridad.
5. Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
6. Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación (Privacy by Design).
7. Aprobar el nivel de riesgo aceptable.
8. Realizar un seguimiento de la gestión de los incidentes de seguridad.
9. Revisar y aprobar regularmente la Política de Seguridad de la Información.
10. Aprobar la normativa de Seguridad de la Información.
    Otras atribuciones según matriz de responsabilidades.

4.2. Roles unipersonales: Funciones y Responsabilidades

Los diferentes roles junto con sus respectivas funciones y responsabilidades están reflejados en la matriz de roles y responsabilidades de Seresco y en el procedimiento de Roles y Responsabilidades.

4.3. Procedimientos de designación de personas

El Responsable de Seguridad de la Información será nombrado por el Comité de Seguridad.

5. Gestión de riesgos

Todos los sistemas afectados por esta Política estarán sujetos a un análisis periódico de riesgos con el objetivo de evaluar las amenazas a las que puedan estar expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

El Responsable de Seguridad es el encargado de que se realice el análisis de riesgos y una vez identificadas las carencias y debilidades deberá tomar las medidas necesarias para minimizarlas hasta niveles aceptables.

El proceso de gestión de riesgos comprende las siguientes fases:

- Identificación de activos.
- Análisis de riesgos.
- Selección de medidas de seguridad a aplicar, que deberán de ser proporcionales a los riesgos y estar justificadas.

Para la realización del análisis de riesgos se utiliza la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información del Ministerio de Administraciones Públicas).

Como resultado del análisis de riesgos realizado se elabora un Plan de Seguridad que una vez puesto en marcha determinará el Riesgo residual del activo, asumido por la Dirección.

6. Desarrollo de la Política de Seguridad

Esta Política se desarrolla por medio de Normativa de Seguridad que afronta aspectos específicos. La normativa de Seguridad está 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.

Otras Políticas que complementan esta Política de Seguridad, accesibles a través del portal del Sistema de Gestión integrado (https://sgi.seresco.es) son:

- PCO-00 Políticas de uso aceptable de los activos TIC
- PCO-10 Política de metadatos
- PCO-12 Política de privacidad y protección de datos
- PCO-14 Política de Teletrabajo y Trabajo en Movilidad

7. Concienciación y formación

Seresco desarrollará actividades específicas en materia de formación y concienciación en Seguridad de la Información, así como sensibilización de los riesgos a los que están expuestos los Sistemas de Información, cuyos destinatarios deben ser todas las personas con responsabilidades en materia de Seguridad.

Las personas con responsabilidad en el uso, operación o administración de sistemas deberán recibir formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

Desde Seresco se dispondrá de los medios necesarios para publicar, difundir y facilitar el conocimiento de esta política de seguridad, así como de sus documentos de desarrollo.

8. Obligaciones del personal

Todos los empleados de Seresco 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 disponer los medios necesarios para que la información llegue a los afectados.

9. Seguridad con terceras partes

Seresco desarrollará los servicios a terceros conforme a la presente política y cuando se trate de Administraciones Públicas, les hará participes de la presente, y de cuantos procesos y procedimientos afecten a la seguridad de la información y /o servicio.

Seresco gestionará el acceso y tratamiento por parte de terceros, con acceso a datos personales.

Cuando se establezca una cadena de suministro en la gestión o administración de soluciones a terceros, se mantendrá la presente política aplicable a todos los eslabones presentes.

10. Proceso de revisión de la política de seguridad

La Política de Seguridad de la Información será revisada por el Comité de Seguridad a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por Comité de Seguridad.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

11. Aprobación de la Dirección

La Dirección de Seresco asume el compromiso de proveer todos los recursos y medios para la implementación del Plan de Seguridad de la Información y Privacidad, de las Políticas, Procedimientos, Instrucciones y Normas desarrolladas al efecto y de velar por su cumplimiento.

La Dirección demuestra su compromiso, mediante la revisión y aprobación de las Políticas y otras normas que desarrollan el sistema, revisando los riesgos y aprobando el riesgo residual, considerando el informe de evaluación de impacto, participando en el Comité de Seguridad, promoviendo la cultura de seguridad y especialmente, dotando de asignación efectiva a esta política mediante recursos y medios.

A tales efectos aprueba y publica esta política para su correcta difusión.

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

En Oviedo, a 23 de marzo de 2021.

11388250F MANUEL ANGEL BUSTO (R: A33011826)

Firmado digitalmente por 11388250F MANUEL ANGEL BUSTO (R: A33011826)
Fecha: 2021.03.23 11:53:27 +01'00'

Manuel Angel Busto Riesgo
Director General