SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD Y PRIVACIDAD

Acuerdo de la Dirección de OPTIMISSA por el que se acuerda la "Política de Seguridad y Privacidad de OPTIMISSA de conformidad con el Esquema Nacional de Seguridad, ISO 27001.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 156.2 dispone la creación, a través de reglamento, del Esquema Nacional de Seguridad.

En cumplimiento y desarrollo de la misma, se aprobó el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica. Esta norma tiene por objeto el establecimiento de los principios básicos y requisitos mínimos de una política de seguridad en la utilización de medios electrónicos, que permita la adecuada protección de la información.

Es de aplicación a las administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos que se gestionen en el ejercicio de sus competencias.

Con la misma se pretende proporcionar las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de una serie de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos de manera que permita a los usuarios el ejercer sus derechos y a OPTIMISSA cumplir sus deberes a través de estos medios electrónicos.

El citado Real Decreto establece en su artículo 11 que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente.

Esta política de seguridad se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

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.

En cumplimiento de lo dispuesto en el Esquema Nacional de Seguridad, la Dirección de OPTIMISSA, ha acordado la aprobación del documento que figura a continuación en todos y cada uno de los puntos contemplados en el mismo.

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 09 de mayo del 2023 por la Dirección de OPTIMISSA.

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

2. VIGENCIA Y ACEPTACIÓN DE LA POLÍTICA DE SEGURIDAD

Esta política estará vigente desde la fecha de su firma.

El aseguramiento de que todas las personas que influyen en la seguridad conocen la política y los objetivos planteados, se conseguirá gracias a su difusión, por parte del Responsable de Seguridad, a todos los niveles de la organización que corresponda, así como por medio de la distribución de los documentos que aplican a cada nivel en los distintos puestos de trabajo.

En el momento de la incorporación de un empleado (interno o externo) a la entidad, éste aceptará la política de seguridad de la organización comprometiéndose a su cumplimiento.
La presente política será examinada, mínimo anualmente, en las revisiones del Sistema por la Dirección, para asegurar su continua adecuación y eficacia. Se tendrán en cuenta cambios significativos en el marco legal y de negocio, resultados de auditorías, así como análisis de riesgos y sugerencias de mejora.

En este sentido, se establecerán objetivos documentales y cuantificables que serán elaborados y revisados periódicamente por parte de Dirección.

3. INTRODUCCIÓN

La Política de Seguridad de la Información se elabora en cumplimiento de las siguientes exigencias legales:

• Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

• Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril del 2016 (RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD).

Para que los servicios ofrecidos por OPTIMISSA se presten con eficacia, en términos de nivel de servicio, seguridad, disponibilidad y alcance, la Dirección de la empresa apuesta por una gestión basada en un cumplimiento estricto de cualquier requisito legal que le afecte, en la creación de valor para sus clientes y en la implantación de una serie de buenas prácticas, articuladas a través de modelos de referencia, como son las Normas ISO y el ENS y tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad, o trazabilidad de la información tratada o los servicios prestados.

Por este motivo, OPTIMISSA ha decidido desarrollar su Política de Seguridad de la Información, que fija sus Objetivos de Seguridad alineados con las necesidades de negocio, el reconocimiento del valor añadido de los sistemas a proteger y una compresión de los riesgos asociados a estos sistemas y expresados en los siguientes términos:

- Cumplimiento con los requerimientos de negocio.
- Protección de los activos afectados de las amenazas internas, externas, accidentales o deliberadas, accesos no autorizados, etc.
- Se analizarán los riesgos de seguridad de la información de todos los servicios prestados por la organización, incluidos en el alcance del sistema y se establecerán los controles asociados necesarios para mitigar los riesgos identificados. Estos controles de seguridad se desarrollarán de acuerdo a las directrices recogidas en la Normativa de Seguridad de la Información y en el ENS

- Mantenimiento del riesgo al que está sometida la información por debajo del nivel exigido por OPTIMISSA.
- Optimización de los costes y garantía de la seguridad en la prestación de servicios incluidos en el alcance, por parte de OPTIMISSA asegurando la confidencialidad de la información y manteniendo la integridad y la disponibilidad de la misma.
- Cumplimiento de los requerimientos legislativos y regulatorios.
- Elaboración, mantenimiento y prueba de Planes de Continuidad de Negocio.
- Establecer un Plan de formación y concienciación en materia de seguridad de la información que ayude al personal implicado a conocer y cumplir esta política, y a prevenir los riesgos identificados o potenciales.
- Gestión de todo tipo de incidentes de seguridad.
- Implantación de un sistema de mejora continúa basado en un control permanente de la gestión y en la estrategia de gestión de riesgos adoptada por la empresa.

La Política de Seguridad se desarrolla mediante documentos específicos (Procedimientos…), que determinan, dentro de su ámbito, la forma en que esta política debe ser aplicada a los distintos activos y procesos de OPTIMISSA incluidos dentro del Alcance del SGSI, para que, alcanzando sus objetivos particulares, contribuyan al cumplimiento de la misión y objetivos de la empresa.

Por todo ello, la Dirección de OPTIMISSA declara explícitamente su conocimiento y aprobación de la política desarrollada en este ámbito, de forma que todo el personal afectado (interno o externo) debe conocerla y aplicarla como parte de las tareas propias de su función en la empresa.

GRUPO ALTEN dota de los recursos necesarios para la aplicación efectiva de esta política, y para su buen desarrollo, tanto en las actividades de implantación como en el posterior mantenimiento de todo el Sistema de Gestión de la Seguridad de la Información.

La presente política es conocida por todo el personal de OPTIMISSA contemplado en el alcance, de acuerdo a las exigencias de la Dirección.

3.1 Prevención

OPTIMISSA 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 los departamentos deben implementar las medidas mínimas de seguridad determinadas por el
ENS y LOPD, 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, los departamentos deben:

- 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.

3.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua 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, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya prestablecido como normales.

3.3 Respuesta

OPTIMISSA debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar 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. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

3.4 Recuperación

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

4. ALCANCE

OPTIMISSA aplica su SGSI basado en **ISO 27001** sobre su Sistema de Gestión de Seguridad de la Información, que comprende "El SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN QUE DA SOPORTE A LOS SERVICIOS DE CONSULTORÍA, TECNOLOGÍAS DE LA INFORMACIÓN Y SERVICIOS DE INGENIERÍA, A LOS PROCESOS DE GESTIÓN DE LA ACTIVIDAD COMERCIAL, LA GESTIÓN DE LAS OFERTAS PARA PROYECTOS DEL ÁREA DE LA ADMINISTRACIÓN PÚBLICA, ASÍ COMO DE LA SEGURIDAD DE LA INFORMACIÓN DE AQUELLOS PROYECTOS EN LOS CUALES SE EXIJA POR PARTE DEL CLIENTE REQUISITOS DE SEGURIDAD SOBRE SU GESTIÓN; SEGÚN LA DECLARACIÓN DE APLICABILIDAD VIGENTE", que aplica a sus sedes de Madrid, Lisboa, Optimissa y Alten Delivery Center Spain.

OPTIMISSA aplica el **Esquema Nacional de Seguridad** sobre el sistema de información que dan soporte a los Servicios de Implantaciones Tecnológicas, Desarrollo de software, Administración de Infraestructura, Soporte a Aplicaciones, incluido soporte a NEDAES. Según la Declaración de Conformidad vigente, de categoría ALTA.

5. MISIÓN

Corresponde a OPTIMISSA, en el marco de los fines y funciones que legal y estatutariamente le han sido conferidos, la puesta en marcha y ejecución de, entre otras, las siguientes actuaciones:

(i) Velar por la satisfacción de los intereses generales relacionados con el cliente.
(ii) La representación exclusiva de esta profesión en el ámbito de su competencia.
(iii) La defensa de los derechos e intereses profesionales de los trabajadores.
(vii) La provisión de servicios que aporten elementos para el éxito de nuestros grupos de interés, propiciando, al mismo tiempo, el desarrollo permanente de la organización y de las personas vinculadas y relacionadas con ella.

6. MARCO NORMATIVO

La definición de un sistema idóneo de gestión de la seguridad de la información como el de OPTIMISSA ha de pasar por la consideración de, al menos, las siguientes disposiciones normativas:

- Reglamento (UE) 2016/679 del Parlamento Europeo, de 27 de abril de 2016, por el que se aprueba el Reglamento General de Protección de Datos.

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- 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.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

También se incluyen en el marco normativo las guías del ENS, en su versión más actualizada y conforme al RD 311/2022.

Así como las siguientes disposiciones normativas de Portugal:

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)
- Decreto-Lei n.º 7/2004 - Serviços da sociedade de informação, em especial do comércio electrónico (Transpõe a directiva 2000/31/CE).
- Lei n.º 51/2011 - Altera a Lei das Comunicações Electrónicas, que estabelece o regime jurídico aplicável às redes e serviços conexos e define as competências da Autoridade Reguladora Nacional neste domínio, transpondo as Directivas n.os 2002/19/CE, 2002/20/CE, 2002/21/CE, 2002/22/CE e 2009/140/CE.
- Lei n.º 58/2019 - Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados
- Lei n.º 46/2012 - Transpõe a Diretiva n.º 2009/136/CE, na parte que altera a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, procedendo à primeira alteração à Lei n.º 41/2004, de 18 de agosto, e à segunda alteração ao Decreto -Lei n.º 7/2004, de 7 de janeiro.

7. ORGANIZACIÓN DE LA SEGURIDAD

Todo personal de OPTIMISSA involucrado en los procesos incluidos en el alcance, será responsable de la implementación de esta Política de Seguridad de la Información, dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha política por parte de su equipo de trabajo.

7.1 Comité: funciones y responsabilidades

El **Comité de Calidad y Seguridad de la Información** de OPTIMISSA, asume las siguientes funciones principales:

- **Implantación y actualización continúa del SGSI** del área. Este Comité se encargará, en último término, de asegurar el correcto desarrollo e implantación del SGSI dentro del alcance, definiendo las acciones oportunas para conseguir este propósito.
- Puesta en marcha de los planes definidos en el **Procedimiento de Revisión y Mejora Continua**.
- Asegurar que los **objetivos de seguridad de la información** están identificados, son acordes a los requisitos de la entidad y están integrados en los procesos críticos.
- Creación de un foro donde se discutan y coordinen los aspectos estratégicos afectados dentro del alcance del SGSI a nivel corporativo y tanto a nivel de negocio, organizativo, técnico y de Gestión de Personas.
- Análisis y resolución de reclamaciones y no conformidades detectadas dentro del alcance del SGSI y propuesta / validación del plan de trabajo / acciones correctivas asociadas.

Suministro / dotación de los recursos internos y externos necesarios para el adecuado funcionamiento del SGSI.

7.2 Roles: funciones y responsabilidades

A continuación, se exponen más en detalle, los roles y responsabilidades a tener en cuenta como parte de la aplicación de la Política de Seguridad dentro del ámbito del SGSI implantado en OPTIMISSA:

- La **Dirección de** OPTIMISSA es el órgano encargado de aprobar la política y de autorizar sus modificaciones.
- El **Responsable de Gestión de la Seguridad (RGS)** es la persona que se va a encargar de coordinar todas las actuaciones en materia de seguridad dentro del alcance del SGSI.

  El Responsable de Gestión de la Seguridad (RGS) es el encargado de centralizar la dirección de las actividades del SGSI en la organización. En ese ámbito, tendrá las siguientes funciones:

  - Convocar periódicamente al Comité de Calidad y Seguridad de la Información coordinando las actuaciones del mismo y elaborando las pertinentes presentaciones o informes para el seguimiento del proyecto para tratar los temas que conciernen a las actividades del SGSI de la organización.
  - Levantar actas de estas reuniones (las actas se tratan como registros auditables del sistema).
  - Reportar al Comité de Dirección, elaborando las pertinentes presentaciones o informes cuando sea necesario.
  - Definición y aplicación del ciclo PDCA, a través de la realización y supervisión de tareas, propias y asignadas al Comité.
  - Realización del Análisis de Riesgos anual y elaboración/presentación a la Dirección y/o Comité del informe correspondiente.
  - Elaboración y presentación de los Informes de Revisión y Mejora anuales.
  - Proponer a la Dirección los objetivos genéricos anuales de mejora sobre el sistema.
  - Actualización anual de los documentos (normativas, políticas, procedimientos, manuales…) y registros que forman la base del Sistema, prestando mucha atención a que no existan discrepancias entre la documentación y la situación actual en la organización.
  - Definición de los indicadores que forman el Cuadro de Mando en cada ciclo de mejora, estableciendo objetivos particulares para cada uno de ello.

- Coordinación con Asesoría Jurídica para la revisión periódica de la legislación aplicable en materia de seguridad de la información y cumplimientos con los requisitos en materia de protección de datos.
- Aseguramiento del ejercicio de los derechos sobre los interesados.
- Coordinación con TI para la elaboración y cierre de Informes de Incidentes de Seguridad, tomando para ello, las medidas que sean precisas.
- Gestión de los Registros de Control junto con los responsables de las áreas incluidas en el alcance.
- Coordinar las actuaciones de la Auditoría interna anual, que se debe llevar a cabo previamente a la externa, comprobando principalmente el cumplimiento de objetivos marcados sobre los indicadores del cuadro de mando, y las actuaciones recogidas en los planes anuales de Acción y Tratamiento de Riesgos.
- Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Coordinación con TI para la revisión de las altas de nuevos aplicativos, en cuanto a los requisitos de seguridad se refiere, dando el consentimiento para su puesta en producción, después de realizar y analizar los resultados de la pertinente auditoria de seguridad sobre los mismos (siguiendo los procedimientos establecidos dentro del sistema).

- Los **Responsables y Usuarios de la Información**

  Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente y las tareas derivadas de procedimientos, normas e instrucciones.

  Con carácter general, las responsabilidades de seguridad de información corporativo se reparten de la siguiente manera:

  - **Responsable de la información:** Determina y define los requisitos de la información tratada.
  - **Usuario de la Información**: cualquier persona que accede a la información contenida en el activo. Es responsabilidad suya acceder a la misma en base a su necesidad de conocimiento y de acuerdo con las políticas y procedimientos definidos.

- El **Responsable del Servicio** será la persona encargada de trasladar y definir los requisitos de seguridad a los proyectos y/o servicio dentro del alcance. Esta definición deberá estar alineada con los requisitos que defina el responsable de seguridad y responsable de sistemas. Los requisitos de seguridad deberán estar alineados con los requisitos del proyecto.

- El **Responsable del Sistema** tiene las siguientes funciones:
  - Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
  - Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
  - Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

- **Recursos Humanos** o los responsables del área en el caso de los empleados externos, cumplirá la función de notificar a todo el personal que ingresa sus obligaciones respecto

del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella se deriven.

- El **Responsable del Área Legal - DPO** tendrá las siguientes funciones:
  - verificará el cumplimiento de la presente política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con sus empleados y con terceros.
  - Verificar el cumplimiento con los requisitos en materia de protección de datos.
  - Asegurar el ejercicio de los derechos en materia de protección de datos sobre los interesados.

Quien sea propuesto por el Comité de Calidad y Seguridad de la Información, será responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta política y por las normas, procedimientos y prácticas que de ella surjan.

7.3 Procedimiento de Designación

La Dirección de OPTIMISSA nombra:

- Al Responsable de Gestión de la Seguridad.
- A los Responsables de la Información.

Los nombramientos se revisarán cada 2 años o cuando el puesto quede vacante.

7.4 Política de Seguridad de la Información

Será misión del Comité de Calidad y Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el mismo comité y difundida para que la conozcan todas las partes afectadas.

Esta política será revisada con una periodicidad máxima anual, y sus cambios deberán ser aprobados por la Dirección de la empresa.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar 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 ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Calidad y Seguridad de la Información establecer una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Calidad y Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis y Gestión de riesgos.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa al resto de procedimientos, procesos e instrucciones técnicas aprobadas por la Dirección.

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla en la intranet, en la herramienta interna Inside y en la página web de la empresa, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

10. OBLIGACIONES DEL PERSONAL

Todos los empleados de OPTIMISSA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Calidad y Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados. Igualmente, será de obligado cumplimiento todos los procedimientos e instrucciones técnicas que engloban el sistema de gestión de la seguridad de la información.

A todos los empleados de OPTIMISSA se les informará adecuadamente sobre concienciación en materia de seguridad. Se establecerá un programa de concienciación continua para atender a todos los empleados de OPTIMISSA, en particular a los de nueva incorporación.

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

11. TERCERAS PARTES

Cuando OPTIMISSA preste servicios o maneje información de terceros, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando OPTIMISSA utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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.

12. VIOLACIÓN DE LA POLÍTICA DE SEGURIDAD

El incumplimiento de la Política y Normativa de Seguridad por parte de un empleado (interno o externo) podrá dar lugar, en el ámbito laboral, a responsabilidades de acuerdo a lo establecido en el Estatuto de los Trabajadores y para el caso de vinculación civil o mercantil con OPTIMISSA a aquellas responsabilidades que se deriven de la naturaleza de dicha vinculación.

13. CRITERIO DE CLASIFICACIÓN DE LA DOCUMENTACIÓN

La clasificación, etiquetado y protección de la información se hará según lo establecido en el procedimiento PO-SI-06 Procedimiento de Clasificación, Etiquetado y Protección de la Información, el cual establece los niveles de clasificación de la información en *Pública, Interna y Confidencial.*

14. DATOS DE CARÁCTER PERSONAL

OPTIMISSA trata datos de carácter personal. El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables

correspondientes. Todos los sistemas de información de OPTIMISSA se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

15. RESPONSABLE DEL TRATAMIENTO DEL DATO

En cumplimiento de lo establecido en el Reglamento General de Protección de Datos (en adelante "RGPD"), le informamos de que los datos recabados referentes a su persona y que han sido facilitados por Ud. son incorporados a un fichero cuyo responsable es ALTEN SOLUCIONES PRODUCTOS AUDITORIA E INGENIERÍA, S.A.U. De conformidad con el artículo 13 del RGDP, a continuación, se le proporciona la información referente al tratamiento de sus datos personales:

Titular	OPTIMISSA SERVICIOS GENERALES, SL
C.I.F	B64850290
Dirección	Calle Vía de los Poblados 3, edificio 5 planta 2, 28033 Madrid
Contacto	A/A Delegado de protección de datos
e-mail	gestiondedatos@alten.es
Teléfono	917910000

16. POLÍTICA DE PRIVACIDAD PARA CANDIDATOS Y PARA CONTACTOS

OPTIMISSA establece Políticas de privacidad para contactos y para candidatos, así como información legal pertinente a sus partes interesadas. Todas ellas están publicadas en su página web para su consulta. Puede consultarse en los siguientes enlaces

https://www.alten.es/informacion-legal/

https://www.alten.es/politica-privacidad-contacto/

https://www.alten.es/politica-privacidad-candidato/