ANEXO I POLITICAS

ANEXO I.I. POLITICA GENERAL DEL SISTEMA DE GESTIÓN

SOLUTIA INNOVAWORLD TECHNOLOGIES, S.L. tiene como objetivo dar soluciones en el ámbito empresarial, desarrollando actividades de venta, instalación, mantenimiento de hardware, desarrollo de aplicaciones software y outsourcing personal especializado en informática, mediante un equipo profesional comprometido con un Sistema de Gestión interno como garantía de un servicio de calidad hacia el cliente y de respeto al medio ambiente.

La base para cumplir la misión de SOLUTIA es ofrecer servicios y productos orientados a las necesidades del cliente conservando el medio ambiente. Los procesos están enfocados a su satisfacción, y se miden mediante la evaluación de los indicadores de los procesos.

Por todo ello nuestra Organización y nuestra política se centra en:

- Ofrecer productos y servicios con calidad y respeto y protección al medio ambiente orientados a las necesidades de los clientes.
- Optimizar los procesos para que estén enfocados a la satisfacción de nuestros clientes, así como otras partes interesadas, y a la conservación del medio ambiente.
- Evaluar y medir los indicadores de los procesos, como herramienta de seguimiento y mejora del funcionamiento del Sistema de Gestión.
- Revisar, actualizar, evaluar y cumplir con los requisitos solicitados de acuerdo a la legislación aplicable, las obligaciones legales y normativas de carácter ambiental que afecten a la organización, así como otros requisitos que la organización suscriba.
- Tener un compromiso de mejora continua y prevención de la contaminación impulsado desde el liderazgo y compromiso de la Dirección.
- Impulsar que el personal tenga una actitud de integración y colaboración.
- Detectar las incidencias que surjan de nuestros procesos, analizarlas y proponer las acciones correctivas o preventivas mejor consensuadas, que permitan la consecución de los objetivos de calidad y la minimización de los aspectos ambientales
- Formar para que los miembros estén concienciados y sensibilizados con los objetivos y metas de la organización. Además, esta política se comunica a todos los empleados y contratistas y se pone a disposición de todos los clientes.
- Aplicar todos los medios técnicos y económicos disponibles en la preservación del medio ambiente, estableciendo adecuados mecanismos de control para fomentar la reutilización, reciclado y adecuada gestión de los residuos generados y promoviendo la racionalización energética a través de los programas de eficiencia en el consumo.
- Controlar los recursos humanos para contar con un personal formado y motivado.

- Mejorar continuamente nuestro sistema de gestión y crecer como organización

Esta política es la base para conseguir los objetivos y metas de la empresa, con estrategias que mejoren la eficiencia, la rentabilidad y los procesos en base a la importancia de la Calidad y el Respeto al Medio Ambiente en el correcto desarrollo de sus actividades.

Sevilla, 15 de febrero de 2021

Director General

ANEXO I.II. POLITICA DE PRESUPUESTOS Y CONTABILIDAD DE LOS SERVICIOS

El proceso de presupuestos y contabilidad debe ser la base para evaluar y controlar los costes asociados a la prestación de los servicios.

Con objeto de ofrecer un servicio de calidad, cumpliendo con los requisitos, acuerdos de nivel de servicio suscritos y realizando un uso eficiente de los recursos la Dirección de **SOLUTIA** ha establecido el procedimiento PRESUPUESTO Y CONTABILIDAD DE SERVICIOS basándose en las siguientes premisas:

- Aportar previsiones sobre los costes en los que se incurrirá durante el desarrollo de los servicios.
- Establecer la referencia para poder contrastar y controlar si los costes reales se ajustan a los previstos.
- Evitar incertidumbres y reducir los riesgos de incurrir en sobre costes no previstos.
- Valorar las repercusiones que puedan poseer los cambios sobre los costes de los servicios y sus márgenes de beneficios.

ANEXO I.III. POLITICA DE CONFIGURACIÓN

Con objeto de garantizar el cumplimiento de los acuerdos a nivel de servicio suscritos y optimizar las posibles actuaciones a realizar en los sistemas de los clientes (cambios, gestión de incidentes, etc.), **SOLUTIA** ha de poseer información sobre los equipos y componentes incluidos en el alcance de los servicios contratados, disponiendo, al menos, referencias de su número de serie, marca y modelo.

Para ello, el proceso de gestión de la configuración, en cumplimiento de lo establecido en esta política, debe:

- Proporcionar información exacta sobre las características de los elementos de configuración al resto de procesos del Sistema de Gestión.
- Asegurar que la información registrada de los elementos de configuración se mantiene actualizada.

- Controlar los cambios que se produzcan sobre los activos, manteniendo sus historiales al día.

ANEXO I. IV. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

En SOLUTIA INNOVAWORLD TECHNOLOGIES, S.L. (en adelante SOLUTIA), conscientes de que la información manejada es un recurso con gran valor, se ha establecido un Sistema de Gestión de acuerdo con los requisitos establecidos en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, y la norma UNE-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.

El objetivo de la Política de Seguridad es fijar el marco de actuación necesario para proteger los recursos de información frente a amenazas, internas o externas, deliberadas o accidentales que puedan afectar a los sistemas de información necesarios para la prestación de los servicios, a información de nuestros clientes gestionada por SOLUTIA o la información propia considerada como confidencial.

Para ello deberán identificarse aquellos riesgos que puedan afectar los elementos que constituyen los sistemas que dan soporte a la actividad de SOLUTIA y puedan afectar a la confidencialidad, integridad y disponibilidad de los sistemas o la información antes reseñada. Para cada uno de los riesgos identificados deberá determinarse la probabilidad de que se manifieste la amenaza, el nivel de vulnerabilidad de la organización frente a ésta y el impacto que tendría su materialización. Adicionalmente, el Comité de Dirección se compromete a establecer medidas que traten de reducir el nivel de riesgos de aquellos elementos del Sistema que se sitúen por encima del aceptable.

La eficacia y aplicación del Sistema de Gestión es responsabilidad directa del Comité de Dirección, la cual es responsable de la aprobación, difusión y cumplimiento de la presente Política de Seguridad. En su nombre y representación se ha elegido un Responsable del Sistema de Gestión, que posee la suficiente autoridad para desempeñar un papel activo en el Sistema de Gestión, supervisando su implantación, desarrollo y mantenimiento.

Esta Política será de obligado cumplimiento para todo el personal participante en la prestación de los servicios ofrecidos por la entidad y todo aquel que pueda acceder a los recursos de información relacionados con éstos.

Toda persona cuya actividad pueda, directa o indirectamente, verse afectada por los requisitos del Sistema de Gestión, está obligada al cumplimiento estricto de la Política de Seguridad.

MARCO NORMATIVO

El Sistema de Gestión de la Seguridad de la Información implantado en Solutia debe dar respuesta a los requisitos establecidos al respecto en la legislación vigente aplicable a la actividad de la entidad y que tiene como referentes principales:

REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

R.D. 951/2015, de 23 de octubre, de modificación del R.D. 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Así mismo, SOLUTIA dará cumplimiento a los requisitos en materia de seguridad que puedan trasladarles los clientes de sus servicios.

En el Listado de Documentos Externos (01.02) del Sistema de Gestión se incluye una relación pormenorizada de la legislación, normativa y otros requisitos en la materia, a los que SOLUTIA debe dar respuesta. Dicho listado se actualiza de forma regular, analizándose los requisitos derivados de la normativa y compromisos suscritos, evaluándose su cumplimiento de forma periódica.

ORGANIZACIÓN DE SEGURIDAD

La implantación de la Política de Seguridad en SOLUTIA requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad
b) Responsable de la Información
c) Responsable del Servicio
d) Responsable de Seguridad
e) Responsable del Sistema de Información

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles:

Comité de Seguridad

El Comité de Seguridad coordina la seguridad de la información. Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas.

Las funciones del Comité de Seguridad son las siguientes:

- Revisión y aprobación de la Política de Seguridad y de las responsabilidades principales.
- Definir e impulsar la estrategia y la planificación de la seguridad proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad.
- Supervisión y seguimiento de aspectos tales como:
    - Principales incidencias en la Seguridad de la Información.
    - Elaboración y actualización de planes de continuidad.
    - Cumplimiento y difusión de las Políticas de Seguridad.

El Secretario del Comité de Seguridad será el Responsable de Seguridad y tendrá como funciones:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Responsable de la Información

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.
- Determina los niveles de seguridad de la información.

Responsable del Servicio

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad de la información.

Responsable de Seguridad

Responsable de la definición, coordinación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos.

Las funciones del Responsable de Seguridad son las siguientes:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
    - La estrategia de seguridad de la información definida por el Comité de Seguridad.
    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información.
- Supervisar los incidentes de seguridad producidos.
- Difundir las normas y procedimientos contenidos en la Política de Seguridad de la Información así como las funciones y obligaciones en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables en materia de protección de datos personales y de seguridad de la información.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas.

Responsable del Sistema de Información

Es responsable de asegurar la ejecución de medidas para asegurar los activos y servicios de los sistemas de información, que soportan la actividad, de acuerdo a los objetivos de la organización.

Las funciones del Responsable de Sistemas de la Información son las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos, conforme a la estrategia de seguridad definida.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.

- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. 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.

PROCEDIMIENTO DE DESIGNACIÓN

Se designan las siguientes responsabilidades:

- Responsable de la Información: Alguien de la alta dirección, normalmente el Director General.
- Responsable del Servicio: Alguien de la alta dirección, normalmente el Director General.
- Responsable de Seguridad: Alguien de la Dirección Ejecutiva que entienda que hace cada departamento y como los departamentos se coordinan entre sí para alcanzar los objetivos marcados por la Dirección.
- Responsable del Sistema: Alguien de operaciones, Responsable de la operación y mantenimiento del Sistema de Información.

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

El Responsable de Seguridad será nombrado por el Director General a propuesta del Comité de Seguridad.

REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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 esta. La Política será aprobada por el Director General y difundida para que la conozcan todas las partes afectadas.

DATOS DE CARÁCTER PERSONAL

En aplicación del principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos, las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

Se aplicará, asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

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 Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad 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.

OBLIGACIONES DEL PERSONAL

Todos y cada uno de los usuarios de los sistemas de información son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros de SOLUTIA tienen la obligación de conocer y cumplir esta política de seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de SOLUTIA recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos, 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.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

TERCERAS PARTES

Cuando SOLUTIA preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando SOLUTIA 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 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.

Sevilla, 17 de enero de 2022
Director General

ANEXO I.V. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

Ante la contratación de cualquier servicio a un tercero, el responsable del área destinataria de los servicios, junto con el Responsable del Sistema de Gestión de la Seguridad de la Información, deberá analizar analizar si existe necesidad de que el tercero acceda a información sensible o a sistemas que puedan gestionarla.

En aquellos casos en los que proceda deberá identificar los posibles riesgos a los que puedan estar expuestos dicha información o sistemas durante la prestación del servicio. Para ello, entre otras cuestiones, deberán tenerse en cuenta aspectos como:

- La criticidad de la información afectada.
- El modo en que deberá acceder a la información o los sistemas de información.
- Los medios a utilizar y el tratamiento que realizará el tercero de dicha información.
- Requisitos legales (p.e. LOPD) y requisitos de seguridad de la propia organización que resulten de aplicación.
- Posibles repercusiones sobre los intereses de otras partes implicadas

Como resultado deberá determinar:

- Las medidas de control que deberá aplicar el tercero durante la prestación del servicio a fin de asegurar un tratamiento adecuado de la información.
- El modo, y bajo qué condiciones, el tercero podrá subcontratar el servicio a una cuarta parte.
- Medidas de seguridad adicionales que se deban aplicar internamente durante la prestación del servicio.
- Mecanismos de control que deberán aplicarse sobre el tercero para asegurar el cumplimiento de los términos de los acuerdos que se suscriban.

ANEXO I.VI. POLÍTICA DE CAMBIOS

Con objeto de evitar interrupciones no planificadas o la degradación de los servicios, es esencial gestionar cuidadosamente los cambios.

Los cambios requieren de una planificación meticulosa con objeto de asegurar su éxito y, de una forma racional, identificar y evitar cualquier impacto negativo sobre los servicios.

Deberán someterse, por tanto, al proceso de gestión de cambios, requiriendo la aprobación del Jefe del Proyecto correspondiente:

- El diseño de nuevos servicios o la modificación del objetivo o alcance de los servicios incluidos en el catálogo de servicios de la entidad.
- Las modificaciones de las sistemáticas o las tecnologías empleadas para la presentación de los servicios actuales.
- Los cambios que puedan realizarse tanto en las infraestructuras de clientes gestionadas por **SOLUTIA** como en las propias necesarias para la prestación de los servicios.

Una vez que el cambio haya sido planificado y aprobado por primera vez, pudiendo catalogarse a partir de ese momento como conocido o estándar, podrá considerarse como preaprobado las siguientes veces que deba implementarse.

En el caso de aquellos cambios de emergencias, que deban efectuarse para restablecer los servicios o evitar una caída inminente, podrá procederse sin contar con una planificación previa ni el visto bueno de la Dirección.

ANEXO I.VII. POLITICA DE ENTREGA

Dentro de los servicios prestados por **SOLUTIA** deben considerarse como entrega el suministro e instalación de equipos y componentes informáticos.

Con objeto de garantizar que estos servicios se presten de forma adecuada y en concordancia con los acuerdos de nivel suscritos **SOLUTIA** ha establecido una Política de Entregas basada en los siguientes principios:

- Planificación y supervisión de las entregas, asegurando su puesta en producción dentro de los plazos acordados con los clientes o marcados por los acuerdos de nivel se servicio aplicables.
- Asegurar el correcto funcionamiento de los sistemas, realizando las pruebas pertinentes sobre el contenido exacto considerado en la entrega, antes de su liberación y posterior puesta en servicio.

HISTORICO DE CAMBIOS

EDICIÓN	MOTIVO DEL CAMBIO	FECHA
00	Edición inicial.	30/06/15
01	Adecuación a la versión UNE ISO/ IEC 27001:2014. Inclusión de la política de seguridad de la información en las relaciones con los proveedores.	30/06/2016
02	Se incluye referencias al desarrollo de software en la política general del sistema de gestión.	15/02/2021
03	Modificación del ANEXO I. IV. POLITICA DE SEGURIDAD DE LA INFORMACIÓN para adecuarlo al ENS	17/01/2021