TUYÚ TECHNOLOGY

Talento
Compromiso
Resultados.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (ENS)

Marzo, 2022

ÍNDICE

TABLA DE REVISIONES		
REVISIÓN	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACIÓN**
01	04/03/2022	Redacción inicial del documento

ELABORADO Y REVISADO: Responsable de Seguridad	
FECHA:	28/02/2022
FIRMA: **Ramón García**	

APROBADO: Director General	
FECHA:	04/03/2022
FIRMA: **Cesar Álvarez**	

1. Aprobación y entrada en vigor

Documento revisado y aprobado el día 04 de marzo de 2022 por el Comité de Seguridad. En adelante, nos referiremos al Sistema de Seguridad de la Información del **ENS,** cuándo utilicemos el término **SGSI** (Sistema de Gestión de la Seguridad de la Información) dada su integración en el sistema de gestión integrado.

Siguiendo las recomendaciones de la GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-402), y en función de nuestro alcance, los comités del Sistema ENS y del SGSI se podrán realizar al mismo tiempo dada la integración y equivalencia de estos en **TUYÚ Technology**. De la misma manera la persona Responsable de Seguridad del SGSI, será también la Responsable de Seguridad ENS.

Esta Política de Seguridad de la Información es efectiva desde la fecha de su aprobación por el Comité de Seguridad, hasta que sea reemplazada por una nueva Política

2. Introducción.

TUYÚ Technology depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, 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.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos y Reglamento Europeo de Protección de Datos, 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.

TUYÚ Technology debe cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del servicio, desde su concepción hasta su retirada, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

TUYÚ Technology debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad y a la Ley Orgánica de Protección de Datos.

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

3. Principios y directrices

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son los marcados en el artículo 4 del RD 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, de manera que las amenazas existentes no se materialicen o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

3.1. Prevención

TUYÚ Technology 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 implementarán las medidas mínimas de seguridad determinadas por el ENS, el RGPD y la LOPDGDD, 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **TUYÚ Technology** 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.

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

TUYÚ Technology:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos.
- Establece protocolos de intercambio de información relacionada con incidentes con clientes y proveedores.

3.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, **TUYÚ Technology** ha desarrollado planes de contingencia de los sistemas TIC como parte de su plan de continuidad del servicio y actividades de recuperación.

4. Alcance

La Política de Seguridad se aplica a toda la empresa y a sus activos de información:

- A todos los departamentos, tanto a su personal directivo como a empleados y empleadas.
- A los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la organización.
- A bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.

- A la información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.
- A la información cedida dentro de un marco legal establecido, que será considerada como propia a efectos exclusivos de su protección.
- A todos los sistemas utilizados para administrar y gestionar la información, sean propios o alquilados o licenciados por la misma.

En general, al sistema de gestión de seguridad de la información que da soporte a las actividades del negocio de:

Gestión de proyectos de tecnologías de la información y prestación de servicios informáticos. Servicios de monitorización, operación, asistencia técnica y administración de aplicaciones, sistemas físicos y virtuales prestados para el desarrollo de proyectos internos y externos de ámbito nacional e internacional, en base a la declaración de aplicabilidad vigente.

5. Categoría del Sistema

5.1. Fundamentos para la determinación de la categoría del sistema

La determinación de la categoría del sistema de **TUYÚ Technology** se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar los objetivos.
b) Proteger los activos a nuestro cargo.
c) Cumplir nuestras obligaciones diarias de servicio.
d) Respetar la legalidad vigente.
e) Respetar los derechos de las personas.

La determinación de la categoría del sistema se realizará de acuerdo con lo establecido en el RD 951/2015 de 23 de octubre, y se aplicará a todos los sistemas empleados para la prestación de los servicios incluidos en el alcance.

5.2. Dimensiones de la seguridad

A fin de poder determinar el impacto que tendría sobre **TUYÚ Technology** un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad, que serán identificadas por sus correspondientes iniciales en mayúsculas:

a) Autenticidad [A].
b) Confidencialidad [C].
c) Disponibilidad [D].
d) Integridad [I].
e) Trazabilidad [T].

5.3. Determinación del nivel requerido en una dimensión de seguridad

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) **Nivel BAJO**. Se utiliza cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un **perjuicio limitado** sobre las funciones de **TUYÚ Technology**, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1. La reducción de forma apreciable de la capacidad de **TUYÚ Technology** para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.
2. El sufrimiento de un daño menor por los activos de **TUYÚ Technology**.
3. El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4. Causar un perjuicio menor a algún individuo, que aun siendo molesto pueda ser fácilmente reparable.
5. Otros de naturaleza análoga.

b) **Nivel MEDIO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un **perjuicio grave** sobre las funciones de **TUYÚ Technology**, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

1. La reducción significativa la capacidad de **TUYÚ Technology** para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.
2. El sufrimiento de un daño significativo por los activos de **TUYÚ Technology**.
3. El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4. Causar un perjuicio significativo a algún individuo, de difícil reparación.
5. Otros de naturaleza análoga.

c) **Nivel ALTO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un **perjuicio muy grave** sobre las funciones de **TUYÚ Technology**, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

1. La anulación de la capacidad de **TUYÚ Technology** para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
2. El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de **TUYÚ Technology**.
3. El incumplimiento grave de alguna ley o regulación.
4. Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5. Otros de naturaleza análoga.

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

5.4. Determinación de la categoría del sistema

Con carácter general se definen tres categorías en el ENS: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.
c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

La determinación de la categoría del sistema sobre la base de lo indicado no implicará que se altere, por este hecho, el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo.

Teniendo en cuenta lo establecido en los apartados 5.3 y 5.4 la categoría del sistema de **TUYÚ Technology** es **MEDIA**, quedando establecida la sistemática para su determinación en el documento **IT1 IT-P4 ANÁLISIS DE RIESGOS.**

6. Declaración de la política de seguridad

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de **TUYÚ Technology**.

- En **TUYÚ Technology** se reconoce expresamente la importancia de la información, así como la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad del negocio, o al menos suponer daños muy importantes, si se produjera una pérdida total e irreversible de determinados datos.
- **TUYÚ Technology** implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad, del RGPD y de la LOPDGDD, y cumple con todos los requisitos legales aplicables.
- La información y los servicios están protegidos contra pérdidas de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Los controles serán proporcionales a la criticidad de los activos a proteger y a su clasificación.
- La responsabilidad de la seguridad de la información involucrada en la prestación de los servicios incluidos en el alcance del ENS es de la Dirección General, que pondrá los medios adecuados, sin perjuicio de que los empleados y empleadas o usuarios y usuarias asuman su parte de responsabilidad respecto a los medios que utiliza, según lo indicado en las normativas y en los procedimientos complementarios. En el punto 8 “Organización de la Seguridad” de este mismo documento se describen las funciones y responsabilidades del Comité de Seguridad, que gestionará la seguridad de la información, y de sus miembros.
- Quienes desempeñen la función de Seguridad de la Información y otras de administración relacionadas, serán quienes administren la seguridad.
- Se ha identificado a las personas responsables de la información, que deberán promover el establecimiento de los controles y medidas destinadas a proteger los datos que la integran, especialmente los de carácter personal o críticos.
- Se establecerá dentro de la normativa un sistema de clasificación de la información, con diferentes niveles.
- Se establecerán los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y, en general, de cualquier activo de **TUYÚ Technology.**
- Los aspectos específicos más relacionados con la información sobre datos personales están regulados por el conjunto de normas recogidas en este documento de seguridad y en la normativa interna o de otra índole a la que pueda remitir o que se cite.
- Quienes no cumplan lo determinado en estas normas y en los procedimientos complementarios podrán ser sancionados de acuerdo con la legislación laboral, o bien con sanciones personalizadas si

están vinculados a **TUYÚ Technology** bajo contratos no laborales, de acuerdo con las cláusulas que figuren en dichos contratos en este último caso.

- Deberán realizarse periódicamente evaluaciones de riesgos y, en función de las debilidades, determinar si es necesario elaborar planes de implantación o reforzamiento de controles.
- Se fomentará la difusión de información y formación en seguridad a empleados, empleadas, colaboradores y colaboradoras, previniendo la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar su posible existencia lo antes posible, y en caso de que existieren, procurándose una difusión muy restringida de las indagaciones.
- El personal de **TUYÚ Technology** deberá conocer las normas, reglas, estándares y procedimientos relacionados con su puesto de trabajo, así como sus funciones y obligaciones, además de la separación de funciones y la revisión independiente de los registros, cuando sea necesario, de quién ha hecho qué, cuándo y desde dónde.
- Las incidencias de seguridad serán comunicadas y tratadas apropiadamente.

7. Marco normativo

Con carácter general será objeto de análisis las disposiciones incluidas en el BOE 173 relativo al Código de Derecho de la Ciberseguridad. Las leyes aplicables a **TUYÚ Technology** en materia de Seguridad de la Información son:

1) **Ley 3/2018**, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales de 13 de diciembre, tiene por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/67 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, garantizando el derecho fundamental de las personas físicas a la protección de datos, amparado por el artículo 18.4 de la Constitución y garantizar los derechos digitales de la ciudadanía, conforme al mandato establecido en el artículo 18.4 de la Constitución.
2) **Ley 34/2002**, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. La presente ley tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
3) **Ley 39/2015,** de 1 de octubre del Procedimiento Administrativo Común de las Administraciones Públicas, tiene por objeto regular los requisitos de validez y eficacia de los actos administrativos, el procedimiento administrativo común a todas las Administraciones Públicas, incluyendo el sancionador y el de reclamación de responsabilidad de las Administraciones Públicas, así como los principios a los que se ha de ajustar el ejercicio de la iniciativa legislativa y la potestad reglamentaria.
4) **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público. La presente Ley establece y regula las bases del régimen jurídico de las Administraciones Públicas, los principios del sistema de responsabilidad de las Administraciones Públicas y de la potestad sancionadora, así como la organización y funcionamiento de la Administración General del Estado y de su sector público institucional para el desarrollo de sus actividades
5) **Ley 56/2007**, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información Ley 59/2003, de 19 de diciembre, de firma electrónica. Tiene como objetivo fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas. Además, esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación. Las disposiciones contenidas en esta ley no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten.

6) **Ley Orgánica 1/2015**, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal de Delitos Informáticos.
7) **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. Tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones
8) **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, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
9) **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.
10) **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 (RGPD), en vigor desde el 24 de mayo de 2016 pero no será aplicable hasta el 25 de mayo de 2018.

TUYÚ Technology cumple con la legislación citada y con todos sus requisitos.

8. Organización de la seguridad

La implantación de la Política de Seguridad en **TUYÚ Technology** 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 el documento **IT8 P4 ASIGNACIÓN RESPONSABILIDADES SGSI**, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información (SGSI)
b) Responsable de la Información
c) Responsable del Servicio
d) Responsable de Seguridad de la Información
e) Responsable de Sistemas
f) Personal Técnico
g) Personal

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

8.1. Comité SGSI: Funciones y responsabilidades

El Comité SGSI coordina la seguridad de la información en **TUYÚ Technology**. Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas.

Las funciones del Comité SGSI son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información 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 de la Información.
- 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.

La Secretaría del Comité SGSI será asumida por la persona Responsable de Seguridad y tendrá como funciones:

- Convocar las reuniones del Comité SGSI.
- 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.

8.2. Roles: Funciones y responsabilidades

8.2.1. 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.
- Proporcionar la información necesaria para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de la persona Responsable del Sistema.
- En relación con el análisis de riesgos, aceptar los riesgos residuales de las informaciones manejadas que sean de su competencia.

8.2.2. 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
- En el ámbito de cada servicio, proporcionar la información necesaria para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de la persona Responsable del Sistema.

8.2.3. Responsable de Seguridad de la Información

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

Las funciones de la persona Responsable de Seguridad de la Información son las siguientes:

- Dirigir las reuniones del Comité SGSI, informando, proponiendo y coordinando sus actividades y decisiones.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de **TUYÚ Technology**.

- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
  - La estrategia de seguridad de la información definida por el Comité SGSI.
  - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de **TUYÚ Technology** y normativa de desarrollo.
- Supervisar los incidentes de seguridad producidos en **TUYÚ Technology**.
- Difundir en **TUYÚ Technology** las normas y procedimientos contenidos en la Política de Seguridad de la Información y normativa de desarrollo, 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 de **TUYÚ Technology**.

Perfil: La persona Responsable de Seguridad de la Información, hará de intermediaria entre la organización y los recursos bajo el alcance del sistema. Ha de ocupar un cargo relevante en la organización y conocer bien el funcionamiento de los servicios y departamentos implicados en el sistema, ya que deberá tomar decisiones que pueden afectar al funcionamiento de esta.

Al ser intermediaria con los distintos procesos del sistema debe poseer un perfil de gestión de recursos, tanto técnicos como humanos, para la coordinación de todas las personas responsables de cada proceso de sistema.

La persona designada para ocupar este cargo debe poseer una experiencia mínima de 3 años.

8.2.4. Responsable de Sistemas

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

Las funciones de la persona Responsable de Sistemas de 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 las personas Responsables Técnicas Informáticas encargadas de personificar una gestión de la seguridad de los activos de **TUYÚ Technology**, 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 en **TUYÚ Technology**.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- La persona Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si se le ha informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con las personas responsables de la información afectada, del servicio afectado y la persona Responsable de la Seguridad, antes de ser ejecutada.

8.2.5. Personal Técnico

El Personal Técnico tiene las siguientes responsabilidades:

- Desarrollo del código efectivo de las aplicaciones que le sean asignadas, basándose en los requerimientos previos del analista, o del arquitecto de software.
- Realizar una codificación libre de errores, efectuando las pruebas necesarias para tal efecto.
- Realizar una correcta gestión de versiones en el desarrollo.
- Mantener el código organizado en repositorios que permitan realizar una correcta trazabilidad sobre todos los cambios que se realizan.
- Documentar, tanto en el propio código, insertando comentarios que faciliten su compresión, como en la documentación del proyecto, detallando los procesos, algoritmos y funciones empleados en la solución de cada uno de los desarrollos.
- Realizar su desarrollo aplicando prácticas seguras de codificación desde el punto de vista de la seguridad de la información (Desarrollo Seguro).
- Informar en todo momento del estado y situación de cada uno de los proyectos en los que está involucrado.
- Mantener el código actualizado y funcional, en base de los nuevos requerimientos que le sean solicitados.

Perfil: En función del puesto requerido para cubrir las necesidades del servicio (técnicos/as de sistemas, programadores/as, analistas programadores/as, analistas orgánicos/as, analistas funcionales, etc.).

8.2.6. Personal

Las **funciones** y **obligaciones** atribuidas al personal de **TUYÚ Technology**, son las siguientes:

- Acceder únicamente a los datos que necesite para el ejercicio de sus funciones.
- Todos los datos de carácter personal que con motivo del desempeño de los trabajos que les sean encomendados conozcan los usuarios y usuarias, son confidenciales y habrán de guardar estricta reserva al respecto, no divulgándolos más allá de lo estrictamente necesario para realizar su trabajo.
- Cualquier incidencia acaecida habrá de ser comunicada de acuerdo con lo indicado en el Procedimiento de Gestión de peticiones, incidencias y problemas.
- El deber de no sacar fuera del ámbito de TUYÚ Technology ninguna clase de datos sin autorización expresa de la persona Responsable del Sistema de Gestión.
- El deber de no dejar su pantalla de acceso a los Sistemas e información activa cuando por cualquier causa deje su puesto de trabajo desatendido.
- La obligación de disponer de clave de acceso a los ordenadores y modificarla cuando así se establezca.
- El cumplimiento estricto de las normas, políticas y procedimientos de seguridad contenidos en este Documento de Seguridad que les afecten.
- Queda expresamente prohibido destruir, alterar o dañar de cualquier otra forma los datos, programas o documentos electrónicos.
- Queda expresamente prohibido intentar borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
- Ejecución de los servicios del alcance.

9. Procedimiento de Designación

Se designan las siguientes responsabilidades:

- **Responsable del Servicio**: Alguien de la alta dirección, normalmente el Director General.
- **Responsable de la Información**: Alguien de la alta dirección, normalmente el Director General.

- **Responsable de Seguridad**: Alguien de la Dirección que entienda qué hace cada departamento y cómo los departamentos se coordinan entre sí para alcanzar los objetivos marcados por la Dirección. Normalmente el Director de Operaciones
- **Responsable de Sistemas**: Alguien de operaciones, Responsable del desarrollo, operación y mantenimiento de los Sistema de Información. Normalmente el Director de Operaciones.

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

Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité SGSI y prevalecerá en todo caso el criterio de la Dirección General.

Las personas Responsables de Seguridad de la Información y de Sistemas serán(n) nombrada(s) por el Director General a propuesta del Comité SGSI.

10. Revisión de la Política de Seguridad de Información

Será misión del Comité SGSI 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 Director General y difundida para que la conozcan todas las partes afectadas.

11. Datos de carácter personal

TUYÚ Technology trata 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.

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

13. Desarrollo de la Política de Seguridad de la información del personal

Esta política de seguridad de la Información complementa las políticas de seguridad de **TUYÚ Technology** en materia de

- Protección de datos de carácter personal, conforme al RGPD y la LOPDGDD

- Política del Sistema de Gestión, conforme a las normas ISO 9001- 14001 -27001- ISO 20000-1.
- Política de Vigilancia y Cumplimiento Normativo.

Esta Política se desarrollará por medio de normativa 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.

La normativa de seguridad estará disponible tanto en la Intranet como Web Corporativa y accesible para personal externo e interno.

14. Documentación del sistema

Con objeto de garantizar la seguridad de la información, **TUYÚ Technology** establece políticas de clasificación y etiquetado de información en términos de relevancia frente a requisitos legales, valor, sensibilidad y criticidad ante revelación y modificación no autorizada.

La persona Responsable de Seguridad establece las pautas de clasificación y etiquetado y vigila su cumplimiento de forma periódica. En caso de detectar alguna desviación debe gestionarlo de acuerdo con el Procedimiento de No Conformidades, Acciones Correctivas y de Mejora. Asimismo, la persona Responsable de Seguridad debe comunicar y sensibilizar al personal involucrado sobre la importancia del tratamiento de la información de acuerdo con la categoría establecida.

14.1. Clasificación y Tratamiento

a) Confidencial: Información especialmente sensible para **TUYÚ Technology.**

Su acceso está restringido únicamente a la Dirección y a aquel personal que necesite conocerla para desempeñar sus funciones.

Se incluye la información que contenga Datos de Carácter Personal. Esta información debe etiquetarse adecuadamente con la marca de agua “CONFIDENCIAL”

Se deben implementar todos los controles necesarios para limitar el acceso a la misma únicamente a aquel personal que necesite conocerla.

Para los Datos de Carácter Personal, se deben cumplir también las medidas de seguridad indicadas en el Documento de Gestión del Sistema de Privacidad

b) **Interna:** Información propia de **TUYÚ Technology**, accesible para todos sus empleados y empleadas.

Por ejemplo, la Política de Seguridad de la compañía, el directorio de personal u otra información accesible en la intranet corporativa.

Esta información debe etiquetarse adecuadamente con la marca de agua “INTERNO”, y estar accesible para todo el personal. No debe difundirse a terceros salvo autorización expresa de la Dirección de la empresa.

c) **Pública**: Cualquier material de la empresa sin restricciones de difusión. Por ejemplo, información publicada en la página web o materiales comerciales.

Esta información no está sujeta a ningún tipo de tratamiento especial.

15. Obligaciones del personal

Todos los miembros de **TUYÚ Technology** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité SGSI disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **TUYÚ Technology** recibirán concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **TUYÚ Technology**, 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.

16. Terceras partes

Cuando **TUYÚ Technology** 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 **TUYÚ Technology** 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 de la persona 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.

Firma de Aprobación:

Fdo.: César M. Álvarez González

Director General