ATENZIA tiene como misión liderar la definición del concepto "Bienestar" ofreciendo los mejores servicios asistenciales a las personas que requieren apoyo, técnico y humano, para mantener una vida independiente y activa. Para ello:

- Contribuimos al bienestar (físico, mental y social) de las personas usuarias mediante la aplicación de un modelo de atención centrado en la persona, predictivo, preventivo, integral y ubicuo, capaz de evolucionar para adaptarse a las necesidades cambiantes de los individuos.
- Aplicamos programas de prevención, seguimiento e intervención sociosanitaria y apoyo psicosocial para mejorar la calidad de vida de las personas, proporcionando tranquilidad y seguridad a las personas usuarias y a su entorno
- Nos comprometemos con los más vulnerables extendiendo nuestro modelo de atención a problemáticas particulares como la violencia de género, la soledad, el abuso de mayores, etc.

Nuestros compromisos en seguridad de la información son:

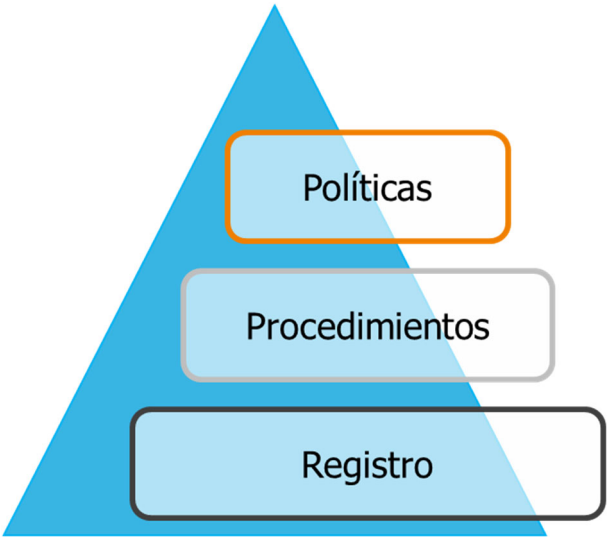
- Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Para poder lograr estos objetivos es necesario:

- Mejorar continuamente nuestro sistema de seguridad de la información.
- Cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribamos además de los compromisos adquiridos con los clientes, así como la actualización continúa de los mismos. El marco legal y regulatorio en el que desarrollamos nuestras actividades es:
  - ✓ 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.

- ✓ Ley Orgánica 3/2018, de 5/12, de protección de datos personales y garantía de los derechos digitales (LOPDGDD).
- ✓ Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- ✓ Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual.
- ✓ Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.
- Preservar los intereses de sus principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.
- Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.
- Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Garantizar la continuidad de las Operaciones mediante un Plan de Continuidad ante situaciones de catástrofe, contingencias en suministro eléctrico, caídas de un CPD, fallos en telecomunicaciones, ….
- Estructurar nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:



La gestión de nuestro sistema se encomienda al Responsable de Gestión y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente Política Integrada de Sistemas de Gestión.

Los roles o funciones de seguridad definidos son:

Función	Deberes y responsabilidades
Responsable de la información	❑ Tomar las decisiones relativas a la información tratada.
Responsable de los servicios	❑ Coordinar la implantación del sistema. ❑ Mejorar el sistema de forma continua.
Responsable de la seguridad	❑ Determinar la idoneidad de las medidas técnicas. ❑ Proporcionar la mejor tecnología para el servicio.
Responsable del sistema	❑ Coordinar la implantación del sistema. ❑ Garantizar la Continuidad de las operaciones. ❑ Mejorar el sistema de forma continua.

Dirección	❑ Proporcionar los recursos necesarios para el sistema. ❑ Liderar el sistema.

Esta definición se completa en los perfiles de puesto y en los documentos del sistema.
El procedimiento para su designación y renovación será la ratificación en el comité de seguridad.

El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité. Los miembros del comité de seguridad de la información son:

- ✓ ***Responsable de la información.***
- ✓ ***Responsable de los servicios.***
- ✓ ***Responsable de la seguridad.***
- ✓ ***Responsable del sistema.***
- ✓ ***Dirección Empresa.***

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

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento. Las decisiones son tomadas por mayoría, y en el caso de empate decide el Responsable de Seguridad.

La documentación referida a la seguridad del sistema se encuentra estructurada en carpetas dentro del OneDrive de la compañía, dividido en subcarpetas nombradas por puntos de norma y marcos de operación, las cuales recogen los distintos procedimientos, registros y evidencias, con acceso restringido para el personal de la compañía, no pudiendo acceder personal externo no autorizado.

La documentación de seguridad se estructura en:

- Política de Seguridad.
- Normativa de seguridad: documentos que describen el uso de equipos, servicios e instalaciones. Describen lo que se considera uso indebido, la responsabilidad del personal con respecto al cumplimiento o violación de la normativa, derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

- Documentos específicos: documentación de seguridad desarrollada según las guías CCN-STIC que resulten de aplicación.
- Procedimientos de seguridad: documentos que detallan cómo operar los elementos del sistema.

Esta política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

Marisa Picornell Elizalde
Adjunta al Consejo de Administración
Fecha: 9/04/2024