Política de Seguridad de la Información

La Dirección del Grupo Mercantil Ayesa**,** en adelante **AYESA,** es consciente y tiene asumido que uno de los objetivos más importantes de la compañía es la protección de los activos de información de cualquier amenaza, ya sea interna o externa, deliberada o accidental, que suponga un riesgo para la confidencialidad, integridad o disponibilidad de la información.

AYESA considera que la planificación, la implantación de controles, la supervisión y la mejora continua de la seguridad de la información son procesos de gestión esenciales para asegurar la competitividad y la sostenibilidad del negocio, considerando la seguridad por defecto una prioridad en la gestión.

Es por ello por lo que la Dirección asume esta responsabilidad y se compromete a:

1. Implantar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información para las actividades que se establecen en el PR-8004: Gestión de la Seguridad de la Información.
2. Contribuir desde la gestión de la seguridad de la información a cumplir con la misión y objetivos establecidos por **AYESA**.
3. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.
4. Adoptar las medidas de seguridad adecuadas para el tratamiento de los datos de carácter personal, siguiendo las directrices del Reglamento Europeo de Protección de Datos y manteniendo la suficiente diligencia para cumplir con el principio de responsabilidad proactiva y el principio de accountability.
5. Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
6. Proteger los recursos de información de **AYESA** y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
7. Concienciar y formar a las personas de **AYESA** y a sus colaboradores en Seguridad de la Información.
8. Evaluar y tratar los riesgos y amenazas a los que están expuestos la información, los servicios y sistemas de **AYESA**.
9. Facilitar los recursos humanos y materiales necesarios para llevarlos a cabo. En particular asegura que se definen y comunican las funciones y responsabilidades del Sistema Gestión de la Seguridad en la Información, manteniendo actualizado el documento DO-8002 "Estructura Organizativa de Seguridad de la Información".
10. Asegurar que, para cualquier adquisición de productos, tanto software como hardware, se tengan en cuenta requisitos de seguridad.

11. Implementar las medidas necesarias para el registro de la actividad y el análisis de los mismos en busca de patrones anormales y la puesta en marcha de las acciones adecuadas para su tratamiento.

El Sistema de Gestión de la Seguridad de la Información de **AYESA** se basa en los siguientes principios y directrices:

- **Prevención**: **AYESA** debe prevenir, y evitar, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, la Dirección deben implementar las medidas mínimas de seguridad determinadas por el Esquema Nacional de Seguridad regulado mediante Real Decreto 3/2010, de 8 de enero, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Para ello la Dirección de **AYESA** debe:
  - Autorizar los sistemas o los servicios antes de entrar en operación.
  - Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
  - Solicitar la revisión periódica del cumplimiento del ENS y de los requisitos de la Norma UNE-ISO/IEC 27001 por parte de terceros.
- **Detección**: La Dirección de **AYESA** debe asegurar que se monitoriza la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia. De igual manera, debe establecer los mecanismos adecuados para asegurar que cualquier incidente de seguridad sea comunicado al Responsable de Seguridad.
- **Respuesta:** La Dirección de **AYESA** debe establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- **Recuperación**: Para garantizar la disponibilidad de los servicios críticos, l Dirección de **AYESA** debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

El marco normativo de las actividades de **AYESA** en el este ámbito es:

a) 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.
b) RD 251/2015 de 23 de octubre por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
c) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD)
d) Ley 9/2017, de 8 de noviembre, de contratos del sector público
e) Norma UNE-ISO/IEC 27001:2014

Para llevar a cabo esta política **AYESA** se han establecido sistemáticas de trabajo documentadas en procedimientos, instrucciones, documentos y plantillas que están a disposición de todas las personas de **AYESA** en la intranet y que son de obligado cumplimiento para todo **AYESA**, así como para terceras partes suministren bienes o servicios a **AYESA**.

Esta Política de Gestión de la Seguridad de la Información está a disposición de las partes interesadas que pudieran solicitarla.

LA DIRECCIÓN DE SERVICIOS GENERALES
En Sevilla, a 21 de enero de 2020