El Grupo EYSA es una compañía española con vocación internacional y gran experiencia. Apoyándonos en la tecnología e innovadores modelos de gestión, ayudamos a conectar ciudades y ciudadanos dentro del proceso de transformación de las Smart Cities. Proporcionamos soluciones integrales y actuamos conforme a nuestra visión de lo que deben ser las ciudades del siglo XXI, basadas en un enfoque innovador y fieles a valores de sostenibilidad.

Nuestra **MISIÓN** se centra en colaborar en el desarrollo de la ciudad del futuro, apoyándonos en la tecnología.

Nuestra **VISIÓN** es liderar los servicios de movilidad para conectar ciudades y ciudadanos.

El Grupo EYSA define la presente Política de Seguridad de la Información, de carácter obligatorio para empleados y empresas colaboradoras, teniendo como objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con rapidez frente a los incidentes que puedan ocurrir.

Como empresa proveedora de servicios en desarrollo de software y consultoría para la Administración Pública, asumimos nuestro compromiso con la seguridad de la información y la gestión del servicio. Nos comprometemos a una adecuada gestión de la misma para ofrecer a todos nuestros grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

Por todo lo anteriormente expuesto, la Dirección establece los siguientes **objetivos** de seguridad de la información y gestión del servicio:

- 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.
- Apostamos firmemente por el uso de las tecnologías más innovadoras e implementamos en nuestros servicios los últimos avances en el sector.
- Apostar por el **desarrollo tecnológico propio**, que nos permite ofrecer a nuestros clientes servicios y soluciones específicas, adaptadas a sus necesidades en cada momento y cada situación.
- Poner nuestra profesionalidad y capacidad de innovación al servicio de las ciudades y sus ciudadanos.
- Prestar en servicio excelente mediante la Inmediatez en la respuesta y en la resolución de incidentes.

Para poder lograr estos objetivos es necesario:

- **Mejorar continuamente** nuestro sistema de seguridad de la información y gestión del servicio.
- **Cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribimos** 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 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.
- ISO/IEC 20000 de Calidad de Servicios.
- ISO/IEC 27001:2022 de Seguridad de la Información.

Debemos **identificar las amenazas potenciales**, así como el **impacto en las operaciones de negocio** que dichas amenazas, caso de materializarse, puedan causar.

Tenemos la **obligación** de:

- Salvaguardar los intereses de nuestras 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, y 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 las buenas prácticas exigidas a los sistemas.

- 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.
- 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 Seguridad y el sistema estará disponible en nuestro sistema de información, en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos conforme nuestro procedimiento en vigor de gestión de los accesos.

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

Cualquier violación de la presente Política de Seguridad de la Información y gestión del Servicio puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con lo establecido en la normativa interna y la normativa legal de aplicación.

Es responsabilidad de todos los empleados del Grupo notificar al Responsable de Seguridad de la Información de la Sociedad y/o al Delegado de Protección de Datos cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

Los **roles o funciones de seguridad** definidos en EYSA 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 - Mejorar el sistema de forma continua
Responsable del SGSI	- Implantación, desarrollo y mantenimiento del SGSI.
Dirección	- Proporcionar los recursos necesarios para el sistema - Liderar el sistema

La descripción se completa en los **perfiles de puesto** y en los **documentos del sistema**.

El procedimiento para su designación y renovación será ratificado 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.
- Responsable del Sistema de Gestión de Seguridad de la información.
- Dirección Empresa (socios-administradores).

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

El comité de seguridad es un órgano ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de nuestra empresa.

Nuestra **política se desarrolla** aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad: a través del procedimiento EYSA-MG 001 Manual de Gestión.
- Análisis y gestión de los riesgos: a través del procedimiento ENS04.
- Gestión de personal: a través del procedimiento EYSA - PG 003 Recursos.
- Profesionalidad: a través del procedimiento EYSA - PG 003 Recursos.
- Autorización y control de los accesos: a través de la política de 01. Política de Control de Acceso Lógico.
- Protección de las instalaciones: a través del procedimiento ENS 03 Medidas de protección.
- Adquisición de productos: a través del procedimiento ENS 01 Marco Operacional.
- Seguridad por defecto: a través de los procedimientos de bastionado de servidores y de procedimiento de configuración de los ordenadores para usuarios.
- Integridad y actualización del sistema: a través de los procedimientos de bastionado de servidores y de procedimiento de configuración de los ordenadores para usuarios.
- Protección de la información almacenada y en tránsito: a través de la política de clasificación y Política de uso medios tecnológicos sociales.
- Prevención ante otros sistemas de información interconectados mediante el procedimiento ENS 03 Medidas de protección.
- Registro de actividad: a través del procedimiento ENS 02 Marco operacional.

- Incidentes de seguridad: a través del documento 04. Política de Gestión de Incidentes de Seguridad.
- Continuidad de la actividad: a través del plan de continuidad del negocio.
- Mejora continua del proceso de seguridad: a través del procedimiento EYSA PG 001 Mejora.

Esta política es efectiva desde el momento de su publicación y se revisa como mínimo una vez al año. El objetivo de las revisiones periódicas es adecuarla a los cambios en el contexto de la Organización, con atención a las cuestiones externas e internas, analizándose las incidencias acaecidas de seguridad de la información y las No Conformidades encontradas en el SGSI. Todo ello armonizado con los resultados de los diferentes procesos de apreciación del riesgo. Al revisar la Política también se revisará todas las Normas y demás documentos que la desarrollan, siguiendo un proceso de actualización periódica sujeto a los cambios relevantes que pudieran acontecer: crecimiento de la empresa, cambios organizacionales, cambios en la infraestructura y desarrollo de nuevos servicios, entre otros.

11810626B JAVIER DELGADO (R: A28385458)

Firmado digitalmente por 11810626B JAVIER DELGADO (R: A28385458)
Fecha: 2025.03.20 19:22:49 +01'00'

D. JAVIER DELGADO DELGADO
Consejero Delegado
Grupo EYSA