USO INTERNO

MS-02

DECLARACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DATOS SOBRE LA PRESENTE EDICIÓN

	Elaborado	Aprobado
Nombre	Antonio Martínez	Jesús Sánchez
Cargo	Responsable SGSI	Director Ejecutivo
Firma		
Fecha	21.01.2019	21.01.2019

Nº de Versión	Fecha	RESUMEN DE CAMBIOS / COMENTARIOS
1.0	03.12.2008	Creación del documento.
2.0	11.12.2009	Modificación política para 2009-2010
2.1	15.01.2011	Modificación política 2011. Se eliminan los objetivos
2.2	07.02.2012	Revisión anual
2.3	16.01.2013	Revisión anual
2.4	22.12.2014	Revisión anual
2.5	07.01.2015	Revisión anual. Inclusión de puntos adicionales debido a la actualización al estándar ISO 27001:2013.
2.6	11.01.2016	Revisión anual
2.7	10.01.2017	Revisión anual. Actualización e inclusión de objetivos alto nivel.
2.8	15.12.2017	Revisión anual, sin cambios.
2.9	21.01.2019	Revisión anual, sin cambios.
3.0	15.12.2019	Revisión anual, inclusión de requisitos de privacidad
4.0	01.10.2020	Adaptación al ENS y aprobación
4.1	02.11.2020	Cambios en listado regulacion

CONSIDERACIONES DE SEGURIDAD

La presente documentación es propiedad de Áudea, Seguridad de la Información S.L. y tiene el carácter de confidencial. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro. Asimismo tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito de Áudea, Seguridad de la Información S.L. (en adelante Áudea), titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguida conforme dicte la ley.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Misión: Convertirnos en el mejor partner para nuestros clientes en la gestión de la ciberseguridad, seguridad de la información, riesgos, resiliencia y el cumplimiento normativo, usando nuestro portafolio de servicios y productos adaptados continuamente a un contexto cambiante.

Alcance: Esta política es de aplicación a las actividades, información, servicios, activos, recursos, sistemas de información, y terceras partes involucradas en la prestación de servicios de la organización.

La Dirección de Áudea quiere dar a conocer, a través de este documento, a sus trabajadores, clientes, proveedores y otras partes interesadas su convencimiento de que la gestión de la Seguridad de la Información y la privacidad es un factor clave para el correcto desarrollo de la organización.

Desde la creación de la compañía, se estableció como propuesta de valor la seguridad de la información y la protección de la información privada, en todas y cada una de las actividades de la organización, más si cabe como una demostración a todas las partes interesadas de una apuesta real en este ámbito. Este elemento de valor ha permitido desde entonces diferenciarnos de la competencia, garantizando además de la privacidad, confidencialidad, integridad y disponibilidad, el correcto funcionamiento de los sistemas y servicios, y el cumplimiento de cualquier requisito legal, normativo o contractual en relación con la seguridad de la información.

Es especialmente relevante una efectiva gestión de un Sistema de Gestión de Seguridad de la Información, basado en ISO/IEC 27001, por la sensibilidad de la información tratada de nuestros clientes, y empleados, entre otros.

Objetivos: Esta Política de Seguridad de la Información muestra el compromiso de la Dirección, y tiene como objetivos de alto nivel:

- Asegurar el cumplimiento de la legislación, reglamentación y normativas aplicables, así como todos aquellos requisitos que la organización considere oportunos llevar a cabo para mantener un Sistema de Gestión de Seguridad de la Información, que le permita conseguir una mejora continua de su actuación.
- Cumplir con las necesidades y expectativas de las partes interesadas involucradas dentro del alcance del SGSI, preservando la Privacidad, Disponibilidad, Integridad, Confidencialidad, Trazabilidad y Autenticidad de la información.
- Demostrar liderazgo por parte de la dirección asegurando que la política de Seguridad de la Información, y los objetivos de seguridad se establecen y son compatibles con la dirección estratégica de la organización.
- Asignar las funciones y responsabilidades necesarias en el ámbito de la seguridad y privacidad, y proporcionar el soporte necesario.
- Apostar por la “mejora continua”, como mecanismo primordial de la evolución y adaptación de la organización.
- Implementar medidas de seguridad y privacidad eficaces y eficientes
- Establecer y revisar periódicamente el nivel de seguridad (apetito del riesgo) basándose en la evaluación de riesgos.
- Formar, concienciar y motivar al personal sobre la importancia de cumplir los requisitos del SGSI.
- Tener en cuenta la seguridad de la información y privacidad en proveedores y subcontratistas.

Marco Normativo: Esta política es la base en la que se sustenta el cumplimiento sobre cualquier requerimiento legal o regulatorio en materia de seguridad de la información, donde estacan:

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
- Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley 40/2015, de 02 de octubre, Régimen del Sector Publico (deroga Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos).
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- 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
- RD 03/2010, de 08 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- RD 951/2015, de 23 de octubre, de modificación del RD 03/2010, de 08 de enero, por el que se regula el esquema Nacional de Seguridad en el ámbito de la administración electrónica"
- Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.
- Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad (Documento BOE-A-2016-10109).
- Instrucción Técnica de Seguridad (ITS) de informe del Estado de la Seguridad (Documento BOE-A-2016-10108).
- Instrucción Técnica de Seguridad (ITS) de Auditoria de la Seguridad (Documento BOE-A-2018-4573).
- Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.

Organización de la seguridad: La seguridad de la información se sustenta en los siguientes roles:

- Comité de Seguridad de la Información (Comité Dirección): Formado por el CEO y todos los responsables de áreas de la organización:
  - Es el máximo responsable (accountable) en materia de seguridad de la información
  - Aprueba esta política y la revisa, al menos, una vez al año
- El Responsable de Seguridad de la Información: Designado por el Comité de SI.
  - Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
  - Independiente del Responsable del Sistema
- Responsable del Sistema, con una responsabilidad compartida entre la Dirección de Operaciones (proporciona los requisitos) e inmediata en los distintos terceros que gestionan, operan y custodian los sistemas de información que opera la organización
  - Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
- Responsable del Servicio:
  - Determina los requisitos (de seguridad) de los servicios prestados, éstos recaen en cada responsable de área.
  - Incluye las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
  - Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y otros requisitos.
- Responsable de la Información:
  - Determina los requisitos (de seguridad) de la información tratada, éstos recaen en cada responsable de área.
  - Valorará las consecuencias de un impacto negativo sobre la seguridad de la información atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y otros requisitos.

Madrid, 26 de Octubre de 2020 Jesús Sánchez Echeverría