POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

AP Interactive Solutions, empresa especializada en la provisión de soluciones de infraestructura cloud, ciberseguridad y desarrollo de software. La organización ofrece servicio de computación en la nube, servidores dedicados, almacenamiento, colocation en data center, servicios gestionados, protección DDoS y consultoría en ciberseguridad. AP Interactive se compromete a garantizar la seguridad de la información y la continuidad del negocio basado en los principios de confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad cumpliendo con los requisitos de las normas ISO 27001 y del Esquema Nacional de Seguridad.

En este marco, AP Interactive ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022 y el Esquema Nacional de Seguridad (ENS), fundamentado en los siguientes pilares:

1. Confidencialidad: Garantizar que la información sea accesible únicamente para aquellos autorizados a tener acceso.
2. Integridad: Salvaguardar la exactitud y completitud de la información y métodos de procesamiento.
3. Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información cuando se necesite.
4. Autenticidad: Garantizar la identidad de los usuarios y el origen de la información.
5. Trazabilidad: Asegurar el rastro de las acciones realizadas sobre la información.

Para ello, la Dirección asume su compromiso con la seguridad de la información y establece los siguientes principios:

- Liderazgo y compromiso: La Dirección lidera y apoya el SGSI, proporcionando los recursos necesarios para su operación y mejora.
- Gestión de riesgos: Identificar, evaluar y tratar los riesgos de seguridad de la información, reduciendo al máximo los impactos potenciales sobre la confidencialidad, integridad y disponibilidad de los activos, especialmente en entornos de trabajo remoto y desarrollo distribuido.
- Mejora continua: Establecer objetivos de seguridad y evaluar el desempeño del SGSI para asegurar su idoneidad, adecuación y eficacia continua.
- Cumplimiento legal y contractual: Cumplir con los requisitos legales, reglamentarios y contractuales aplicables, incluyendo el Reglamento General de Protección de Datos (RGPD), la LOPDGDD y los requisitos del Esquema Nacional de Seguridad (ENS).
- Seguridad desde el diseño: Implementar medidas de seguridad desde las etapas iniciales de todos los proyectos en la infraestructura tecnológica.
- Formación y concienciación: Motivar y formar a todo el personal en materia de seguridad de la información para garantizar que conocen sus responsabilidades y actúan conforme a las políticas establecidas.
- Continuidad del negocio: Asegurar la capacidad de la organización para continuar la prestación de servicios esenciales y recuperar las operaciones en caso de interrupción.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento.

Esta política se revisa periódicamente para garantizar su adecuación al contexto de la organización y está documentada, comunicada y disponible para todas las partes interesadas.

Aprobado el 17 de febrero del 2026. Versión 01

Firmado por Dirección