

## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

TELECOMUNICACIONES PUBLICAS ANDALUZAS, S.L, es una empresa dedicada a instalación y mantenimiento: de cámaras, centralitas de telefonía ip, antenas, redes de cableado estructurado, instalaciones de enlaces de banda ancha wimax. Realización de proyectos de instalaciones ict, electricidad, apertura, cableado estructurado. Sus instalaciones están ubicadas en P.I. Santa Ana, Fase 5ª Parcela E-9. 41590, La Roda de Andalucía (Sevilla).

La Gerencia de TELECOMUNICACIONES PUBLICAS ANDALUZAS, S.L reconoce que la información es un recurso que tiene valor para nuestra organización y por tanto debe ser protegida. Esta información puede presentarse de diversas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o medios electrónicos, representada en imágenes, o expuesta en una conversación. La Seguridad de la Información protege a ésta de una amplia gama de amenazas, a fin de garantizar la continuidad comercial, minimizar el daño y maximizar la productividad de la empresa.

Así por tanto podemos definir la Seguridad de la Información como un conjunto de medidas, controles, procedimientos y acciones destinados a cumplir con los tres aspectos básicos esenciales para prestar un buen servicio, el cumplimiento de la legalidad vigente y la imagen de la propia entidad:

- a.- **Confidencialidad:** la información debe ser conocida exclusivamente por las personas autorizadas, en el momento y forma prevista.
- b.- **Integridad:** asegurando que la información y sus métodos de proceso son exactos y completos;
- c.- **Disponibilidad:** la información debe estar accesible y ser utilizable por los usuarios autorizados en todo momento, debiendo estar garantizada su propia persistencia ante cualquier eventualidad.

La Seguridad de la Información se logra implementando un conjunto adecuado de controles, que abarcan políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software.

Por todo ello, la política de seguridad de la organización se fundamenta en los siguientes principios:

- Para una eficiente y correcta gestión de los riesgos a que están expuestos todos los procesos de nuestra organización, se deben cubrir todos los procesos involucrados en: identificar, evaluar y calificar los riesgos, tomando acciones para mitigar o anticiparlos, monitorear y revisar su progreso.
- Proteger los recursos de información de la organización, 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
- Promover el compromiso con la Seguridad de la Información, facilitando la participación y valorando todos los aportes innovadores del personal.
- Cumplir con todos los requisitos impuestos por nuestros clientes así como todos aquellos de tipo legal y otros requisitos aplicables en el campo de seguridad de la información que nos fueran requeridos.

## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Mejorar continuamente la eficacia del Sistema de Gestión de Seguridad de la Información utilizando para esto la mejora continua que proporciona la implementación de la Norma UNE ISO/IEC 27001:2007, con el objeto de aumentar nuestra competitividad en el mercado local, a través de la utilización de herramientas de control de procesos, auditorías, análisis de riesgos, capacitaciones y la concientización del uso de las herramientas.
- Cumplimentado todo el desarrollo de nuestra empresa, bajo los requisitos legales o reglamentarios y de las obligaciones de seguridad contractuales.
- Establecer anualmente objetivos con relación a la Seguridad de la Información.
- Desarrollar un proceso de análisis del riesgo y de acuerdo a su resultado, implementar las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos por la organización.
- Establecer los objetivos de control y los controles correspondientes, en virtud de las necesidades que en materia de riesgos surjan del proceso de Análisis de riesgos manejado.
- Concienciar y formar en materia de seguridad de la información a todo el personal.
- Facilitar los medios necesarios para garantizar la continuidad del negocio de la empresa.
- Sancionar cualquier violación a esta política y a cualquier política o procedimiento del SGSI.
- Todo empleado es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas.
- Todo empleado es responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y de las políticas y procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información.
- El Responsable de Seguridad de la Información es responsable directo sobre el mantenimiento de esta política, por brindar consejo y guía para su implementación, e investigar toda violación reportada por el personal.

Para la aplicación efectiva de estos principios es absolutamente necesario el apoyo a los mismos por parte, tanto del equipo directivo como de toda la plantilla, así como de proveedores y clientes

En la Roda de Andalucía a 30-11-10