



Nuestra **POLÍTICA DE GESTIÓN INTEGRADA de Calidad, Ambiental y Seguridad de la Información** establece:

El COMPROMISO de proporcionar y mantener los máximos niveles de calidad del servicio, generando el menor impacto ambiental posible. Con unos VALORES que nos caracterizan como organización:

La Filosofía de AirON se sustenta en la convicción de que el conocimiento, la ciencia y la tecnología deben estar al servicio del ser humano y de su desarrollo, contribuyendo a generar procesos y espacios de vida y trabajo más saludables, creativos y, por tanto -creemos firmemente en ello-, más eficientes y eficaces.

Nuestro valor diferencial es que buscamos y ofrecemos valor de uso, soluciones y servicios diseñados e implementados en base a las posibilidades, potencialidades y concreciones estructurales, generando valor compartido y una nueva cultura sostenible.

El PROPÓSITO es ser una organización orientada a la gestión por procesos y análisis de riesgos, para asegurar el control y mejora de éstos, la integración de nuestro personal en su desarrollo y el cumplimiento del compromiso de calidad, protección del medio ambiente, la eficiencia energética y la prevención de la contaminación, a fin de buscar la máxima satisfacción de nuestros clientes. Así como ser un referente para los sectores y actividades;

El Sistema de Gestión según los requisitos de las normas ISO 9001:2015 & ISO 14001:2015, es aplicable para el alcance:
Prestación de servicios de puesta a disposición de profesionales en el sector de tecnologías de la información

El Sistema de Gestión según los requisitos de las normas ISO 27001:2014, es aplicable para el alcance:

Sistemas de Información que dan soporte a los procesos de:

- Servicio de consultoría de recursos humanos en IT
- Mantenimiento it de recursos internos
- Soporte it, control y resolución de incidencias, de cliente

Según la declaración de aplicabilidad vigente.

El Sistema de Gestión según los requisitos de las normas ISO/IEC 20000-1:2018, es aplicable para el alcance:

Sistema de Gestión de Servicios para el soporte (control y resolución de incidencias) sobre TI, internos y externos, de acuerdo con el catálogo de servicios vigente.

Así como en nuestro entorno social. Todo fundamento en el desarrollo de las personas, como elemento indispensable para lograr la MEJORA CONTINUA de nuestros procesos, el sentido de pertenencia la organización y su realización personal.

Conscientes de la necesidad de contar con Sistemas Normalizados de reconocimiento internacional, la organización ha alineado su Sistema de Gestión a las normas ISO 9001:2015 de Gestión de Calidad, ISO 14001:2015 de Gestión Ambiental, ISO 27001:2017 de Gestión de la Seguridad de la Información e ISO/IEC 20000-1:2018 de Gestión del Servicio de Tecnología de la Información.

Por ello, la Dirección se compromete a liderar y mantener un Sistema de Gestión Integrado en la organización basado en la mejora continua y en las siguientes directrices:

- El serio compromiso de conocer las necesidades y expectativas de nuestros clientes y partes interesadas, para lograr su satisfacción, y de mejora continua, estableciendo y verificando el cumplimiento de los objetivos estratégicos.
- El compromiso del cumplimiento de la legislación y reglamentación aplicable, así como de los requisitos que se suscriban.
- El compromiso por la conservación ambiental, intentando desarrollar una gestión acorde a la protección del medio ambiente dentro de nuestras posibilidades como empresa.
- Garantizar en todo momento el cumplimiento de los acuerdos de nivel de servicio fijados a través de una eficaz gestión de los servicios. Dicha gestión de servicios es un pilar estratégico fundamental de la empresa.
- Asegurar la seguridad de la información propia y de nuestros clientes. Nuestra actividad implica el tratamiento de información variada como forma de ejecutar procesos básicos propios de su actividad. Sabiendo que los sistemas de información, aplicaciones, infraestructuras de comunicaciones, archivos y bases de datos, constituyen un activo importante de la empresa, la dirección prioriza la confidencialidad, integridad y disponibilidad de la información a la hora de definir y delimitar los objetivos y responsabilidades para las diversas actuaciones técnicas y organizativas y vigila el cumplimiento del marco legal, de las directivas y políticas específicas y de los procedimientos definidos.
- El compromiso por la revisión continua de las competencias y mejora continua, a fin de garantizar la calidad de los servicios y su capacidad de afrontar los retos crecientes que nos plantean nuestros clientes.
- Establecer colaboraciones estratégicas para crear interacciones de mejora de la calidad y valor añadido.

Todo nuestro personal acepta el compromiso de mejorar la calidad de los servicios, de los procesos auxiliares de la empresa y desarrollar una conducta medioambiental responsable, dentro de los diferentes puestos de trabajo.

La Dirección.
Rev.04, en Madrid a 15 de enero de 2020.



POLITICA DE DESARROLLO SEGURO.

Decálogo de directrices mínimas.

1. Partir siempre de un **modelo de permisos mínimos**, es mejor ir escalando privilegios por demanda de acuerdo a los perfiles establecidos en las etapas de diseño.
2. Si se utiliza un lenguaje que no sea compilado, asegurarse de **limpiar el código que se pone en producción**, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido.
3. **Nunca confiar en los datos que ingresan a la aplicación**, todo debe ser verificado para garantizar que lo que está ingresando a los sistemas es lo esperado y además evitar inyecciones de código.
4. **Hacer un seguimiento de las tecnologías utilizadas para el desarrollo**. Estas van evolucionando y cualquier mejora que se haga puede dejar obsoleta o inseguras versiones anteriores.
5. **Todos los accesos que se hagan a los sistemas deben ser validados**.
6. Para intercambiar información sensible **utilizar protocolos para cifrar las comunicaciones**, y en el caso de almacenamiento **la información confidencial debería estar cifrada utilizando algoritmos fuertes y claves robustas**.
7. Cualquier funcionalidad, campo, botón o menú **nuevo debe agregarse de acuerdo a los requerimientos de diseño**. De esta forma se evita tener porciones de código que resultan siendo innecesarias.
8. **La información almacenada en dispositivos móviles debería ser la mínima**, y más si se trata de contraseñas o datos de sesión. Este tipo de dispositivos son los más propensos a ser que se pierdan y por lo tanto su información puede ser expuestas más fácilmente.
9. **Cualquier cambio que se haga debería quedar documentado**, esto facilitará modificaciones futuras.
10. **Poner más cuidado en los puntos más vulnerables**, no hay que olvidar que el nivel máximo de seguridad viene dado por el punto más débil.

*La Dirección.
Rev.01, en Madrid a marzo de 2019.*