

POLÍTICA INTEGRADA

Aire Networks es un operador mayorista de servicios de telecomunicaciones con licencia de operador nacional otorgada por la Comisión Nacional del Mercado de la Competencia en España que ofrece servicios de conectividad, voz, audiovisual, alojamiento y seguridad a operadores, empresas y organismos públicos.

Desde el ámbito de la prestación de servicios profesionales de telecomunicaciones, se propone la búsqueda de la excelencia en todos y cada uno de los procedimientos que se ejecutan, con el fin de mejorar la experiencia y satisfacción del cliente. Por ello, se decide implantar un Sistema de Gestión de Calidad basado en la norma ISO 9001, en su edición en vigor.

Además, consciente de la problemática ambiental actual, se considera fundamental el respeto al medio ambiente en todas las actividades desarrolladas, de forma que se compromete a realizar una gestión ambiental de acuerdo a la actual norma ISO 14001 que permita minimizar los aspectos ambientales perjudiciales, fomentar la protección del medio ambiente y la prevención de la contaminación.

Para el correcto desempeño de las funciones de negocio y poder disponer de la información cuando sea necesaria, que dicha información sea íntegra y que se preserve la confidencialidad de la misma, se decide implantar un Sistema de Gestión de Seguridad de la Información basado en la vigente norma ISO 27001. Para ello se basa y ayuda del tratamiento de diferentes tipos de datos e información, sustentados por los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyendo éstos, uno de los activos principales de Aire Networks, de tal manera que el daño o pérdida de los mismos inciden en la realización de sus servicios y pueden poner en peligro la continuidad de la organización.

Así mismo, Aire Networks mediante esta Política establece el marco para el desarrollo, implantación, revisión y mejora de los Planes de Continuidad de acuerdo con lo establecido en la ISO 22301. Dichos planes pretenden:

- Dar una respuesta adecuada y oportuna ante la materialización de un riesgo de seguridad o medio ambiente de características catastróficas, que provoquen un escenario de falta de disponibilidad de alguno de los componentes básicos de la actividad del Grupo: personas, edificios y oficinas, tecnología, información y proveedores.
- Aminorar la repercusión de las posibles catástrofes sobre las actividades de negocio, garantizando que se preservan los datos y funciones esenciales o, de no ser posible, que tales datos o funciones se recuperen, oportuna y progresivamente, hasta la vuelta a la normalidad.

Por lo tanto, para poder garantizar una calidad óptima de todos los servicios, respetando el medio ambiente, con las medidas de seguridad de la información adecuadas, y estableciendo los planes de continuidad pertinentes, se considera la gestión de la calidad, del medio ambiente, continuidad del negocio y de la seguridad de la información como requisitos imprescindibles, estableciendo los siguientes principios en su gestión:

- Obtener la **satisfacción** de los clientes, profesionales y de las demás partes interesadas, comprometiéndose en la **mejora continua** de los servicios y en una adecuada actitud y aptitud en la



atención a los organismos a los que se prestan servicios para controlar y **reducir el número de incidencias** a través de tres vertientes: FORMACIÓN, ATENCIÓN y RESOLUCIÓN de incidencias.

- Cumplir con todos los **requisitos legales y otros requerimientos** que Aire Networks suscriba relativos a la **calidad de los servicios** y a los **impactos asociados a los aspectos ambientales**.
- Mantener y mejorar continuamente la eficacia en la gestión de Aire Networks **añadido la calidad** de los servicios prestados y la **minimización de la contaminación**, mediante el establecimiento y revisión de **objetivos**, indicadores, realización de auditorías, **mejorando el desempeño ambiental** y concluyendo en la toma de decisiones.
- Impulsar la **comunicación, formación, sensibilización y motivación** de los profesionales, colaboradores y proveedores en los asuntos relacionados con la calidad y el medio ambiente.
- Mejorar los procesos internos teniendo en cuenta la seguridad de la información y la continuidad del negocio, así como, la **prevención de la contaminación** y la **preservación de los recursos naturales**, que se pueda producir como consecuencia de las actividades y los servicios desarrollados.
- Minimizar el **impacto ambiental** de las actividades realizadas, mediante un **uso eficiente de la energía** y la **conservación de los recursos**, la **reducción de residuos** y la prevención de la contaminación.
- **Proteger**, mediante controles/medidas, **los activos** frente a amenazas que puedan derivar en incidentes de seguridad.
- **Paliar** los efectos de **los incidentes** de seguridad.
- **Establecer** un sistema de **clasificación de la información** y los datos con el fin de proteger los activos críticos de información.
- **Definir las responsabilidades** en materia de seguridad de la información y continuidad del negocio generando la estructura organizativa correspondiente.
- **Elaborar** un conjunto de **reglas, estándares y procedimientos** aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- **Especificar** los efectos que conlleva el **incumplimiento** de la Política de Seguridad en el ámbito laboral.
- **Evaluar los riesgos** que afectan a los activos los procesos críticos con el objeto de adoptar las medidas/controles de seguridad oportunos y los planes de continuidad adecuados en caso de que se produzca un desastre.
- **Verificar** el funcionamiento de **las medidas/controles de seguridad/Planes de continuidad** mediante auditorías de seguridad internas realizadas por auditores independientes.
- **Formar a los usuarios en la gestión de la seguridad** y en tecnologías de la información y las comunicaciones, así como en la continuidad del negocio.
- **Controlar el tráfico de información y de datos** a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.



- **Observar y cumplir la legislación** en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecte a los activos de Aire Networks.
- **Proteger el capital intelectual de la organización** para que no se divulgue ni se utilice ilícitamente.
- **Reducir** las posibilidades de **indisponibilidad** a través del uso adecuado de los activos de la organización.
- **Defender los activos** ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- **Controlar el funcionamiento de las medidas de seguridad** averiguando el número de incidencias, su naturales y efectos.
- **Proteger al personal** tanto en su operativa normal como en una situación de emergencia.
- Gestionar los riesgos clave para la continuidad de los procesos considerados críticos por Aire Networks.
- **Minimizar el impacto** que pudiera derivarse de cualquier situación de emergencia sobre los procesos, servicios o activos identificados como críticos.
- **Retornar al estado de normalidad** lo antes posible una vez mitigadas las consecuencias del incidente producido.
- **Garantizar que tanto el Plan de Continuidad como los Planes de Contingencia** ante desastres se desarrollan e implementan de forma adecuada, actualizándolos cuando se considere necesario tras las revisiones periódicas y cada vez que se produzca un cambio significativo que pueda afectar a los mismos dentro de un proceso de mejora continua de los mismos.

Todo el equipo de Aire Networks es responsable de cumplir y hacer cumplir esta Política Integrada.

CEO

Elche, 19 de Julio de 2023

