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.

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 esta, se decide implantar un Sistema de Gestión de Seguridad de la Información basado en la vigente **norma ISO 27001, ISO 27017, e ISO 27018**. Incorporar a los sistemas de Aire Networks las medidas de seguridad establecidas en las mismas, que garantizan la dimensiones de; **integridad, confidencialidad y disponibilidad** en los sistemas de información. Adicionalmente la ISO 27018 implantada, aporta la capacidad de poder garantizar una mejor protección de los datos personales que se tratan en los productos y servicios ofrecidos como proveedor tipo Cloud.

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 estos inciden en la realización de sus servicios y pueden poner en peligro la continuidad de la organización.

En particular, para la prestación de servicios del producto comercial OASIX (Co-location e IaaS) y el servicio transversal GECO, Aire Networks está relacionada a través de los medios electrónicos, entre otros, con los ciudadanos, empleados, clientes y proveedores y con otros prestadores de servicios de telecomunicaciones. Estos servicios deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la **disponibilidad, integridad, o** confidencialidad de la información tratada o de los servicios prestados y todo ello, con la finalidad de garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes de seguridad que se produzcan.

Con el avance de las nuevas tecnologías en los últimos años, como es el caso del almacenamiento en la nube, que proporciona a las organizaciones múltiples beneficios relacionados con la rapidez y facilidad de acceso a la información desde cualquier punto. Este modelo de gestión proporcionado por Aire Networks tiene como contrapartida la preocupación sobre la protección de datos y la privacidad de estos en cuanto a la información de identificación personal (PII). Con el fin de disponer de procesos que den cobertura a los servicios en la nube, desde Aire Networks se implanta la **normativa ISO 27018 Protección Información Personal en Nube**.

Así, los sistemas de Aire Networks necesarios para la prestación de los citados servicios deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la **confidencialidad, integridad, y disponibilidad**, uso previsto y valor de la información y los servicios, estando preparados para prevenir, detectar, reaccionar y recuperarse de incidentes. Para defenderse de estas amenazas, se requiere una estrategia que permita adaptarse a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que, sin perjuicio de las medidas ya adoptadas, tanto Aire Networks como su personal deban aplicar las medidas mínimas de seguridad exigidas por las ISO de la familia 270xx, así como realizar un seguimiento continuo de los niveles de prestación de los servicios, seguir y analizar las

vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes que se produzcan para garantizar la continuidad de los servicios prestados.

Es por ello por lo que, las distintas áreas y departamentos de Aire Networks deben tomar conciencia de que la seguridad en los sistemas de información es una parte integral de cada etapa del ciclo de vida de cada uno de los Sistemas de Información existentes en Aire Networks, desde su concepción hasta su retirada de servicio, pasando por las fases de desarrollo o adquisición y las actividades de explotación. Asimismo, se tendrá en cuenta que los requisitos de seguridad y las necesidades de financiación de estos, deben ser identificados e incluidos en la planificación y en la solicitud de ofertas. Estableciendo los siguientes principios en su gestión:

- Asegurar los recursos necesarios para que, el Sistema de Gestión esté disponible.
- **Observar y cumplir** con todos los **requisitos legales y otros requerimientos** que Aire Networks suscriba relativos a **la seguridad de la información**, **protección de datos** y regulación aplicable al **sector de las telecomunicaciones**. Aire Networks dispone de procedimientos internos en los que se analiza el marco legal y regulatorio en el que se desarrollarán las actividades.

- **Proteger**, mediante controles/medidas, **los activos** frente a amenazas que puedan derivar en incidentes de seguridad. A estos efectos, la seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el Sistema.

- **Paliar** los efectos de **los incidentes** de seguridad. A estos efectos, Aire Networks basa su procedimiento de incidencias en la prevención, reacción y recuperación.
- **Establecer** un sistema de **clasificación de la información** y los datos con el fin de proteger los activos críticos de información. Y, además, definir las directrices para la estructuración de la documentación del sistema, su gestión y acceso.
- **Definir las responsabilidades** en materia de seguridad de la información 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 esta Política y del resto de Políticas de seguridad de la información en el ámbito laboral.
- **Evaluar los riesgos** que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos, siendo la gestión de riesgos uno de los principios básicos del sistema de gestión integrado. Asimismo, disponer de una estrategia de protección constituida por múltiples capas de seguridad. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.
- **Verificar** el funcionamiento de **las medidas/controles de seguridad** mediante auditorías de seguridad internas realizadas por auditores independientes. Las medidas de seguridad **se reevaluarán y actualizarán** periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.
- **Formar a los usuarios en la gestión de la seguridad** y en tecnologías de la información y las comunicaciones.

- **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.
- **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 naturaleza y efectos
- **Disminuir los riesgos de información privilegiada autorizada.**
- **Asegurar el aislamiento de clientes de servicios de múltiples tenencias y en la nube (incluida la virtualización).**
- **Asegurar la protección y confidencialidad de los activos del cliente.**

Raúl Aledo Coy

CEO

Elche, 23 de Septiembre 2024