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 el vigente **Esquema Nacional de Seguridad (ENS)**. De esta forma se añaden los controles y requisitos del ENS para el mejor cumplimiento relacionados con los servicios que se puedan ofrecer a administraciones públicas.

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 sus servicios del producto comercial OASIX (Co-location e IaaS), 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, trazabilidad, autenticidad 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.

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, trazabilidad, autenticidad, 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 el **Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, en adelante también ENS),** 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.

Por lo tanto, para poder garantizar una calidad óptima de todos los servicios, respetando el medio ambiente y con las medidas de seguridad de la información adecuadas (en cumplimiento además, de lo previsto en el artículo 6, en cuanto a la seguridad integral y al artículo 12, en lo que a la política de seguridad se refiere, del

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad), se considera la gestión de la calidad, del medio ambiente y de la seguridad de la información como requisitos imprescindibles, estableciendo los siguientes principios en su gestión:

1. Aprobación y entrada en vigor

Texto aprobado por el Responsable de Seguridad del Sistema de Gestión de Seguridad de la Información (SGSI) de AIRE NETWORKS en sesión de 17/07/24. Y que se ratifica por el CEO de la compañía con la firma del presente documento.

La presente Política de Seguridad de la Información será revisada como mínimo una vez al año de modo que se garantice su adaptación a las nuevas circunstancias, técnicas u organizativas, que pudieran surgir.

Esta Política es efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

2. Prevención, detección, reacción y respuesta

Los Departamentos de Aire Networks deben estar preparados para prevenir, detectar, reaccionar y recuperarse frente a incidentes, de acuerdo con el Artículo 8 del ENS.

2.1. Prevención

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa a distintos niveles. Por tanto, se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. Respuesta

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- Ponerse en contacto con las Fuerzas y Cuerpos de Seguridad según los procedimientos específicos previstos.
- Establecer comunicación con los cuerpos de emergencias y protección civil.
- **Paliar** los efectos de **los incidentes** de seguridad. A estos efectos, Aire Networks basa su procedimiento de incidencias en la prevención, reacción y recuperación.

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. Alcance

3.1. Ámbito subjetivo:

La presente Política es de aplicación a todos los miembros de la plantilla Aire Networks, y en particular a aquellos que utilicen, operen y administren los sistemas de información y comunicaciones definidos en el Alcance del Sistema de Gestión.

De acuerdo con lo anterior, todo el personal de la Aire Networks tiene la obligación de conocer y cumplir la misma.

Asimismo, será de aplicación, en los términos y condiciones previstos en el apartado 12, a aquellos terceros en los que concurra alguno de estos supuestos:

(i) Terceros organismos para los que Aire Networks preste servicios o de los que maneje información.

(ii) Terceros prestadores de servicios a Aire Networks o a los que se les ceda información.

3.2. Ámbito objetivo:

Esta Política se aplica a todos los sistemas de Aire Networks necesarios para la prestación de los servicios de conectividad, alquiler de alojamiento en centro de datos, telefonía fija y móvil, servicios del producto comercial OASIX (Co-location e IaaS) y el servicio transversal GECO relacionados con las funciones que le son atribuidas por la legislación vigente, y con la Misión corporativa declarada en la presente Política.

Específicamente se aplica a los departamentos que dan soporte a su cadena de valor, al ejercicio de derechos y cumplimiento de deberes por medios electrónicos, y a la interacción por medios electrónicos con los clientes, proveedores y resto de partes interesadas comprendidas en el MN-I-01 Manual Integrado.

4. Marco normativo

Aire Networks, en su condición de operador mayorista de telecomunicaciones, se rige por lo dispuesto en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones en su disposición adicional decimosexta y las disposiciones transitorias séptima, novena y duodécima, y la ley 11/2022 General de Telecomunicaciones.

Adicionalmente, y específicamente en cuanto inciden o pueden incidir en la materia objeto de la presente Política, le son de aplicación las siguientes:

- Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio.
- Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 54/2003, de 12 de diciembre, de reforma del marco normativo de la prevención de riesgos laborales.
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
- Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre.
- Ley 21/2014, de 4 de noviembre, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- REGLAMENTO (UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

En todo caso, lo anterior se entenderá sin carácter exhaustivo y sin perjuicio de lo regulado en cualquier otra normativa que resulte de aplicación.

5. Organización de la Seguridad de la Información

La Dirección de Aire Networks, en el ejercicio de las funciones de dirección y gestión ordinaria de la entidad y de sus servicios, es la máxima responsable del impulso y cumplimiento de lo previsto en la presente política y demás normas, guías y procedimientos de Calidad, Medio Ambiente y Seguridad que, en el desarrollo de la misma, se aprueben.

Para la organización, gestión, y coordinación de la Calidad, Medio Ambiente y Seguridad de la información dentro de Aire Networks se dispone de la siguiente estructura con las funciones y responsabilidades que, asimismo, a continuación, se detallan:

- Comité de Normativas ISO
- CEO
- Responsable de Seguridad
- Responsable de Calidad
- Responsable de Medio Ambiente
- Responsable de Documentación
- Responsable de la Información
- Responsable del Servicio
- Responsable del Sistema
- Administrador de la Seguridad del Sistema

En caso de conflicto entre los distintos órganos que tienen encomendadas competencias en materia de seguridad de la información éstos serán resueltos por el superior funcional y, en última instancia, por el CEO.

Particularmente, el CEO de Aire Networks es competente para:

- La creación del Comité de Normativas ISO
- El nombramiento del Responsable de Seguridad y su sustituto.
- El nombramiento de los Responsables de la Información.
- El nombramiento de los Responsables del Servicio.
- El nombramiento del Responsable del Sistema.
- El nombramiento de los Administradores de Seguridad del Sistema.

En otras palabras, los Responsables de la Información, los Responsables del Servicio, el Responsable del Sistema y los Administradores de Seguridad serán nombrados por el CEO, como Alta Dirección en el sistema de gestión, ya sea directamente o a través del Comité de Normativas ISO siempre que el CEO forme parte del mismo.

Se entenderá renovados los cargos de forma anual desde su nombramiento a no ser que los órganos competentes indicados en este apartado realicen un nuevo nombramiento. En ese caso se asumirá como válido el último nombramiento y no se procederá a la renovación de los cargos nombrados previamente, puesto que cesaran en su cargo relativo al ENS y al sistema de gestión integrado.

Finalmente se establece que a las reuniones del Comité de Normativas ISO, asistirán normalmente: el Responsable de Seguridad, el Responsable de Calidad, el Responsable de Medio Ambiente y el Responsable de Documentación, en caso de ser requerida de información técnica serán citados: los Responsables de la Información, los Responsables del Servicio, el Responsable del Sistema y los Administradores de Seguridad.

5.1. COMITÉ DE NORMATIVAS ISO

5.1.1. CREACIÓN Y COMPOSICIÓN DEL COMITÉ:

Se ha procedido a crear un Comité de Seguridad de la Información bajo la denominación de "Comité de Normativas ISO" compuesto por el representante de la Alta Dirección y por cada uno de los responsables que constan en la presente política.

A requerimiento del Comité se podrá convocar a alguna de sus reuniones a cualquier otra persona cuya participación se estime conveniente en el marco del ENS.

Asimismo, por el Presidente del Comité de Normativas ISO de la Información se podrá acordar la constitución de cuantos grupos de trabajo se estimen necesarios para el desarrollo de las funciones encomendadas.

5.1.2. RESPONSABILIDADES Y FUNCIONES DEL COMITÉ:

El Comité de Seguridad de la Información coordina la seguridad de la información en el ámbito de gestión de Comité de Normativas ISO, siendo sus principales funciones las siguientes:

- Establecer y aprobar anualmente los objetivos de calidad, medio ambiente y seguridad de la información.
- Aprobar y revisar la Política de Seguridad de la Información (ISO 27001, ISO 27018 y Esquema Nacional de Seguridad).
- Revisar la documentación del Sistema de Gestión Integral.
- Evaluar los aspectos ambientales asociados a la actividad de la organización.
- Revisar el Programa Anual de Calidad, Medio Ambiente y Seguridad de la Información.
- Identificar las necesidades de formación y planificar las acciones formativas.
- Revisar los informes finales de las auditorías realizadas.
- Comprobar el seguimiento y control de las acciones correctivas y propuestas de mejoras.
- Aprobar los aspectos ambientales, así como los aspectos medioambientales significativos.
- Revisar y aprobar, en coordinación con los responsables de los sistemas de gestión, los cambios que les puedan afectar para garantizar los recursos suficientes y la correcta gestión de los cambios aplicados.
- Aprobar el Plan de Auditorías Internas anual y definir la cualificación de los auditores internos.
- Contratar los auditores de una tercera parte para la realización de la auditoría externa.
- Definir y aprobar los indicadores del Sistema de Gestión Integral.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

5.1.3. FUNCIONAMIENTO DEL COMITÉ:

El Comité se reunirá con carácter ordinario una vez al año y con carácter extraordinario cuando lo decida su Presidente o cuando:

a) Aparezcan incidencias de seguridad graves que afecten a cualquier área del ámbito de gestión de Aire Networks.
b) Surjan nuevas necesidades de seguridad que requieran de la participación de los componentes del Comité.

El Secretario del Comité de Normativas ISO tiene las siguientes funciones:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

5.2. ROLES: FUNCIONES Y RESPONSABILIDADES

5.2.1. CEO

La misión del CEO se basa en demostrar liderazgo y compromiso con respecto al Sistema de Gestión Integral (Sistema de Gestión de Calidad, Sistema de Gestión Ambiental, el Sistema de Gestión de Seguridad de la Información y Esquema Nacional de Seguridad).

Sus funciones y responsabilidades son las siguientes:

- Asumir la responsabilidad y obligación de rendir cuentas con relación a la eficacia del Sistema de Gestión Integral.
- Asegurar el establecimiento de la Política y de los objetivos de calidad, medio ambiente y seguridad de la información (ISO 27001, ISO 27018 y Esquema Nacional de Seguridad), y que éstos sean compatibles con el contexto y la dirección estratégica de la organización.
- Asegurar la integración de los requisitos del Sistema de Gestión Integral dentro de los procesos de negocio de la organización.
- Promover el uso del enfoque a procesos y el pensamiento basado en riesgos.
- Asegurar los recursos necesarios para el Sistema de Gestión Integral de la Información esté disponibles.
- Comunicar la importancia de una gestión de calidad, medioambiental y de seguridad de la información eficaz y de conformidad con los requisitos del Sistema de Gestión Integral.
- Asegurar que el Sistema de Gestión Integral logre los resultados previstos.
- Comprometer, dirigir y apoyar a las personas, para contribuir a la eficacia del Sistema de Gestión Integral.
- Promover la mejora continua.
- Apoyar otros roles pertinentes de la dirección, para demostrar su liderazgo en la forma en la que aplique a sus áreas de responsabilidad.
- Determinar, comprender y cumplir regularmente los requisitos del cliente y los legales y reglamentarios aplicables.
- Determinar y considerar los riesgos y oportunidades que pueden afectar a la conformidad de los productos y servicios y la capacidad de aumentar la satisfacción del cliente.
- Mantener el enfoque en el aumento de la satisfacción del cliente.

5.2.2. RESPONSABLE DE SEGURIDAD

El Responsable de Seguridad se encargará de gestionar el Sistema de Gestión Integral.

Sus funciones y responsabilidades son las siguientes:

- Definir, actualizar y difundir la política, los procedimientos y los formatos del SGI.
- Proponer los objetivos del SGI.
- Definir el modelo de clasificación y la gestión de activos de la información de la compañía.
- Evaluar los recursos necesarios para la Seguridad de la Información.
- Realizar y mantener actualizado el análisis de riesgos de seguridad de la información con base en lo establecido en el SGI.
- Definir y ejecutar el plan de tratamiento de los riesgos de seguridad de la información.
- Proponer e implantar los controles definidos para la mitigación del riesgo.
- Formular los planes de gestión de riesgos y supervisar su implantación.
- Informar de los resultados sobre indicadores medibles.
- Proponer mejoras en el sistema de Seguridad de la Información.
- Planificar y controlar la implementación de las medidas de mejora o acciones correctivas y su efectividad.
- Verificar la aplicación de las medidas de seguridad necesarias para la protección de la información SGI.
- Promover la formación y concienciación en materia de seguridad de la información.
- Elaborar una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
- Facilitar al Responsable de Información y al Responsable de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Elaborar, junto al “Responsable de Sistemas”, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Normativas ISO.

- Elaborar los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Normativas ISO.
- Validar los Planes de Continuidad de Sistemas que elabore el "Responsable de Sistemas", que deberán ser aprobados por el Comité de Normativas ISO y probados periódicamente por el Responsable de Sistemas.
- Aprobar las directrices propuestas por el Responsable de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
- Evaluar y proponer salvaguardas que prevengan incidentes similares en el futuro.
- Evaluar los riesgos de las actividades subcontratadas.
- Evaluar a los proveedores en relación con la Seguridad de la Información.
- Realizar las revisiones de seguridad del SGI.
- Asegurar el cumplimiento de la Ley de Protección de Datos y Garantía de los Derechos Digitales y su Reglamento Europeo.

5.2.3. RESPONSABLE DE LA INFORMACIÓN

El Responsable de la Información es la persona que tiene la potestad de establecer los requisitos de la información en materia de seguridad, es decir, de determinar los niveles de seguridad de la información, teniendo la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

Será Responsable de la Información el superior jerárquico del Departamento responsable de la gestión de la información. Cuando una información dependa de varios Departamentos podrá asumir la condición de Responsable de la Información el Comité de Normativas ISO.

Sus funciones son:

- Clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).
- La aprobación de los niveles de seguridad se realizará a propuesta del Responsable de Seguridad de la Información oído el Responsable del Sistema.
- Validar los preceptivos análisis de riesgos y, junto a los Responsables de los Servicios y contando con la participación y asesoramiento del Responsable de Seguridad de la Información y del Responsable del Sistema, seleccionar las salvaguardas a implantar.
- Aceptar, junto con los Responsables de los Servicios, los riesgos residuales calculados en el análisis de riesgos, y realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

5.2.4. RESPONSABLE DEL SERVICIO

El Responsable del Servicio es la persona que tiene la potestad de establecer los requisitos del servicio en materia de seguridad, es decir, de determinar los niveles de seguridad de los servicios, teniendo la responsabilidad última del uso que se haga de un determinado servicio y, por tanto, de su protección.

Será Responsable del Servicio el superior jerárquico del Departamento responsable de la prestación del servicio. Cuando un servicio dependa de varios Departamentos podrá asumir la condición de Responsable del Servicio el Comité de Normativas ISO.

Sus principales funciones son:

- Determinar los niveles de seguridad del servicio en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

- La aprobación de los niveles de seguridad se realizará a propuesta del Responsable de Seguridad de la Información oído el Responsable del Sistema.
- Validar los preceptivos análisis de riesgos y, junto a los Responsables de la Información y contando con la participación y asesoramiento del Responsable de Seguridad de la Información y del Responsable del Sistema, seleccionar las salvaguardas a implantar.
- Aceptar, junto con los Responsables de la Información, los riesgos residuales calculados en el análisis de riesgos, y realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

5.2.5. RESPONSABLE DEL SISTEMA

Es la persona responsable de:

- Desarrollar, operar y mantener el Sistema (entendiendo como tal el conjunto de sistemas de información de Aire Networks) durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Acordar la suspensión del manejo de una cierta Información o la prestación de un cierto Servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y el Responsable de la Seguridad de la Información, antes de ser ejecutada
- Elaborar los procedimientos operativos de seguridad de la información.
- Colaborar juntamente con el Responsable de Seguridad de la Información en el diseño de planes de mejora de la seguridad.
- Elaborar el Plan de Continuidad del Sistema.
- Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema.
- Investigar los incidentes de seguridad que afecten al sistema y comunicarlos al Responsable de Seguridad de la Información.
- Reportar al Responsable de Seguridad de la Información: (a) De las actuaciones en materia de seguridad, en particular, lo relativo a decisiones de arquitectura de sistema. (b) Resumen consolidado de incidentes de seguridad. (c) De la eficacia de las medidas de protección que se deben implantar.
- Designar responsables del Sistema Delegados. Cuando en atención a la complejidad, distribución, separación física o número de usuarios de los sistemas de información, sea necesario personal adicional para llevar a cabo las funciones del Responsable del Sistema, éste podrá designar cuantos responsables del Sistema Delegados considere necesarios. Dicha designación deberá ser previamente aprobada por el Comité de Normativas ISO, efectuada con carácter formal y comportará la delegación de funciones, pero no de su responsabilidad.

5.2.6. ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA

Es el responsable de implantar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información.

Sus principales funciones y responsabilidades son:

- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad de los Sistemas de Información.
- Implantar, gestionar y mantener las medidas de seguridad aplicadas en los Sistemas de Información.
- Supervisar que las medidas de seguridad son aplicadas estrictamente.
- Monitorizar el estado de la seguridad del Sistema.

- Gestionar las autorizaciones concedidas a los usuarios del Sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el Sistema se ajusta a lo autorizado.
- Aplicar los Procedimientos Operativos de Seguridad de la Información y Explotación de los Sistemas de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Informar a los Responsables de la Seguridad de la Información y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

5.2.1. RESPONSABLE DE CALIDAD

El Responsable de Calidad se encarga de gestionar el Sistema de Gestión de Calidad (SGC) para garantizar que los servicios sean adecuados, coherentes y cumplan con los requisitos externos e internos.

Sus principales funciones y responsabilidades son:

- Mantener y gestionar toda la documentación y registros del SGC.
- Asegurar que el sistema de gestión de calidad funciona correctamente.
- Informar al resto de la organización de los cambios o modificaciones que suceden en el SGC.
- Planificar y establecer los procedimientos, estándares y especificaciones de calidad.
- Asegurar que todos los miembros de la organización (internos y externos), conozcan los objetivos de calidad, los entiendan y respeten.
- Elaboración de la documentación pertinente del SGC.
- Implementar la puesta en marcha del SGC en colaboración con los responsables de los departamentos de la organización, controlando para que se apliquen los procedimientos, registros y documentación aprobados por la alta dirección.
- Llevar a cabo la medición y supervisión de los indicadores, junto con el personal de apoyo que considere oportuno.
- Comunicar el Programa de auditorías y seguimiento de los resultados de las auditorías internas planificadas.
- Hacer sugerencias para cambios y mejoras y cómo implementarlas.
- Participar en la mejora de los procesos de trabajo.
- Revisar los requisitos del cliente y asegurarse de que se cumplan.
- Establecer, junto con el departamento de Compras, los requisitos de calidad de los proveedores externos, verificar que sigan los procedimientos y cumplimenten la documentación prevista en el SGC.
- Realizar seguimiento de los procedimientos y de las no conformidades que puedan surgir.
- Verificar la eficacia de las acciones correctivas implantadas con motivo de las no conformidades identificadas.

5.2.2. RESPONSABLE DE MEDIO AMBIENTE

El responsable de Medio Ambiente se encarga de gestionar el Sistema de Gestión Ambiental (SGA).

Sus principales funciones y responsabilidades son:

- Elaborar la documentación pertinente según el SGA.
- Mantener y gestionar toda la documentación y registros del SGA.
- Realizar la coordinación del desarrollo y el control de todos los documentos que forman parte del SGA.
- Informar a la alta dirección de la organización sobre el funcionamiento del SGA.

- Realizar la Política Ambiental de la organización.
- Definir los objetivos, metas, plazos, recursos y acciones de acuerdo a la Política Ambiental.
- Analizar el grado de cumplimiento de los objetivos medioambientales.
- Asegurar que el SGA está implantado y que se mantiene correctamente.
- Analizar las no conformidades detectadas en las diferentes áreas de trabajo.
- Establecer acciones correctivas y propuestas de mejora.
- Identificar, junto con los responsables de los departamentos, los aspectos ambientales asociados a las actividades de la organización.
- Asegurar que se cumple la legislación ambiental.
- Identificar las expectativas ambientales que tienen los clientes de la organización.
- Determinar cuál será la actuación ambiental de los proveedores.
- Implantar, organizar y gestionar la protección medioambiental en la organización.
- Organizar planes de formación y sensibilización del personal y de sus proveedores en relación con el respeto del medio ambiente en el trabajo.
- Analizar los resultados de las Auditorías Internas y Externas y archivar los informes de las mismas.
- Informar al Comité de Normativas ISO acerca de los resultados de las auditorías, tanto internas como externas, y las acciones correctivas establecidas

5.2.3. RESPONSABLE DE DOCUMENTACIÓN

El Responsable de Documentación se encarga de gestionar la documentación que afecta al Sistema de Gestión Integrado (SGI).

Sus principales funciones y responsabilidades son:

- Comunicar la Política al personal de la organización.
- Mantener actualizado el control de documentación.
- Codificación de los diferentes procedimientos, registros, protocolos, manuales, etc., de la organización.
- Comunicar las pautas de configuración del correo electrónico.
- Notificar los SGI al personal.
- Apoyar al Comité de Normativas ISO a definir, difundir y mantener la Política y los principios de gestión de calidad.
- Custodiar y recuperar la documentación generada con la eficacia necesaria para que no suponga un impedimento en la actividad de la empresa.
- Identificar y controlar los cambios y estado actual de los documentos.
- Asegurar que las versiones pertinentes de los documentos se encuentren disponibles en los puntos de uso.
- Asegurar que los documentos permanecen legibles y fácilmente identificables.
- Prevenir el uso no intencionado de documentos obsoletos y aplicarles una identificación adecuada en el caso que se mantengan por cualquier razón.
- Organizar de manera lógica, eficaz y categorizada la documentación.

5.3. PROCEDIMIENTOS DE DESIGNACIÓN Y RENOVACIÓN

La Dirección de Aire Networks es competente para:

- La creación del Comité de Seguridad de la Información (Comité de Normativas ISO)
- El nombramiento del Responsable de Seguridad y su sustituto.
- El nombramiento de los Responsables de la Información.
- El nombramiento de los Responsables del Servicio.

- El nombramiento del Responsable de Seguridad de la Información.
- El nombramiento del Responsable del Sistema.
- El nombramiento de los Administradores de Seguridad del Sistema.

Los Responsables de la Información y los Responsables del Servicio serán nombrados a propuesta del Comité de Normativas ISO.

Dicha competencia se verá excepcionada en el supuesto de que alguno de los nombramientos anteriores tenga incidencia en la organización de la Entidad.

Se entenderá renovados los cargos de forma anual desde su nombramiento a no ser que los órganos competentes indicados en este apartado realicen un nuevo nombramiento. En ese caso se asumirá como válido el último nombramiento y no se procederá a la renovación de los cargos nombrados previamente, puesto que cesaran en su cargo relativo al ENS y al sistema de gestión integrado.

6. Datos de carácter personal

En el desarrollo de las funciones atribuidas como operador nacional de telecomunicaciones trata datos de carácter personal, contando, en cumplimiento de la normativa de aplicación, con un Documento de Seguridad, en el que se recogen los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información de Aire Networks se ajustarán a las medidas de seguridad en base al enfoque del riesgo y demás requerimientos regulados en REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

Adicionalmente para mejorar el soporte normativo y dar mayor transparencia al cumplimiento de la protección de datos personales, se deben seguir los principios recomendados por la ISO 27018, entre otros, se enumeran algunos de ellos:

- Existirá una política que marque las líneas de actuación para las copias de seguridad y los requisitos relacionados con las obligaciones legales o contractuales relacionados con el borrado de datos personales contenidos en copias de seguridad
- Se definirá el periodo de retención de las políticas y directrices de seguridad administrativa
- Se restringirá la creación de material impreso o copias en papel
- Se llevará un control y registro de las restauraciones de datos personales
- Existirá una destrucción segura del soporte papel, en caso de tratarse por Aire Networks para los alcances definidos
- Se tendrán en cuenta las directrices de la ISO 27018 para la confección de los contratos
- Los proveedores serán gestionados mediante cláusulas de confidencialidad y requisitos sobre la subcontratación
- Existirán controles técnicos según la ISO 27018, se enumeran algunos: borrado seguro de archivos temporales, registro de eventos, protección de la información de registro, control sobre el espacio de almacenamiento de datos preasignado a otro cliente en los servicios ofrecidos bajo el entono de OASIX.

7. Gestión de riesgos

Respecto de todos los sistemas de información comprendidos en el alcance de esta Política se deberá realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el artículo 7 del mismo.

Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Normativas ISO establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Normativas ISO dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8. Auditoría

Si bien algunos de los sistemas de información de Aire Networks atienden una categoría básica, existen otros con una categorización de nivel ALTO. Consecuentemente, se establece como adecuado realizar una auditoría de acuerdo con lo establecido en el artículo 31 del ENS, en base a los siguientes periodos y criterios:

- **Ordinaria:** Periodo bienal.
- **Extraordinaria:** Siempre que se produzcan modificaciones sustanciales en el Sistema de Información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

9. Desarrollo de la Política

Esta Política se desarrollará mediante documentos más precisos que ayuden a llevar a cabo lo propuesto. Para ello se utilizarán:

- Normas de seguridad.
- Guías de seguridad.
- Procedimientos de seguridad.

Las normas de seguridad uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

Las guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

10. Concienciación y formación

Con el objetivo de lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todos los miembros de la plantilla de Aire Networks y a todas las actividades, de acuerdo al principio de Seguridad Integral recogido en el artículo 6 del ENS, el Comité de Normativas ISO establecerá un programa de

concienciación continua a todos los miembros de la plantilla de Aire Networks, en particular a los de nueva incorporación.

Así mismo el Comité de Normativas ISO elaborará y aprobará los requisitos de formación necesarios desde el punto de vista de seguridad de la información.

11. Obligaciones del personal

Todos los miembros de Aire Networks tienen la obligación de conocer y cumplir esta Política y la Normativa de Seguridad, siendo responsabilidad del Comité de Normativas ISO disponer los medios necesarios para que la información llegue a los afectados.

12. Terceras partes

Cuando Aire Networks preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación conjuntos para la reacción ante incidentes de seguridad.

Cuando Aire Networks utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se solicitará un informe del Responsable de Seguridad que concrete los riesgos en que se incurre y la forma de tratarlos. Será necesaria la aprobación de este informe por parte de los responsables de la información y los servicios afectados, previamente al uso de los servicios de terceros o cesión de información a los mismos.

13. Publicidad y Comunicación

Con el objeto de garantizar la máxima difusión de la Política entre los empleados y empleadas de Aire Networks se procederá a la publicación en los recursos internos de Aire Networks.

Asimismo, serán objeto de publicación en los recursos internos de Aire Networks las normas, guías y procedimientos de seguridad que en desarrollo del ENS se aprueben. Lo anterior podrá verse excepcionado respecto de aquellos documentos que por su contenido sean calificados de confidenciales.

Todo el equipo de Aire Networks es responsable de cumplir y hacer cumplir esta Política de Seguridad de la Información

Raúl Aledo Coy

CEO

Elche, 24 de Septiembre de 2024