D06 Política de Seguridad de la Información de Air Liquide Healthcare España SL y Care4Chronics SLU (ENS)

Versión 1.2

Enero 2026

CONTENIDO

1. INTRODUCCIÓN AL ENTORNO DE AIR LIQUIDE HEALTHCARE ESPAÑA S.L. Y CARE4CHRONICS, S.L.U. RESPECTO AL CUMPLIMIENTO DEL ENS

El presente documento de Política de Seguridad de la Información es un documento definido a alto nivel que recoge el significado de '**Seguridad de la Información'** en **Air Liquide Healthcare España S.L. y Care4Chronics S.L.U.** (en adelante **Air Liquide**).

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con celeridad a los incidentes.

En el Art. 2.3 Ámbito de Aplicación del R.D. 311/2022, de 3 de mayo, por el que se regula el ENS, señala que este real decreto también se aplica a los sistemas de información de las **entidades del sector privado**, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por éstas de sus competencias y potestades administrativas.

El art. 12 define que la **política de seguridad de la información** es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

Los sistemas 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.

Las diferentes áreas de Air Liquide deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el art. 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento.

Todas las áreas de Air Liquide deben cerciorarse de que la seguridad ITC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación.

2. OBJETIVO Y SERVICIOS PRESTADOS

Air Liquide es líder mundial en gases, tecnologías y servicios para la industria y la Salud, especializada en gases medicinales, equipamiento y servicios de valor a lo largo de toda la cadena de atención sanitaria.

La presente Política de Seguridad se aplica a las diferentes actividades en las que participa Air Liquide a través de medios electrónicos.

El alcance para la implantación del ENS en **Air Liquide Healthcare España SL** se establece en:

- **Servicio de atención a pacientes para el suministro de gases medicinales y equipamiento por prescripción facultativa** (Pública y Privada), siendo **VitalAire** la marca específica de Air Liquide Healthcare para las terapias respiratorias crónicas. Se trata de una oferta completa que permite atender en su domicilio a los pacientes con terapias respiratorias crónicas como oxigenoterapia, CPAP para apnea del sueño, aerosolterapia, ventilación mecánica, fisioterapia y otros servicios.

- **Servicio de suministro de gases medicinales y equipamiento a Centros Sanitarios** (Públicos y Privados), siendo **Medgas** la marca específica de Air Liquide Healthcare para la prestación de este servicio a Hospitales, Complejos Sanitarios, Clínicas, Consultas Médicas como por ejemplo Odontólogos o Dermatólogos que requieran el uso de gases medicinales, Centros de Biotecnología, Laboratorios, Centros de Reproducción Asistida, etc.
- **Servicio de atención a pacientes diabéticos**, que representa la actividad de diabetes de Air Liquide Healthcare bajo la denominación **Novalab**. Soluciones para la diabetes centradas en las personas mediante la utilización de herramientas para un cuidado eficaz tanto en el hogar como en la consulta.

El alcance para la implantación del ENS en **Care4Chronics SLU** se establece en:

- **Servicio de atención domiciliaria a pacientes de urgencias médicas domiciliarias** con un enfoque integral al tratamiento del mismo, atención domiciliaria enfocada en la prevención y la mejora de la calidad de vida del paciente en su entorno.

3. MARCO NORMATIVO

Como base normativa para la realización del presente documento se ha analizado la legislación vigente que afecta al desarrollo de las actividades de Air Liquide en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información. El marco legal en materia de cumplimiento normativo viene establecido en el **Registro de legislación y normativa aplicable**.

4. ORGANIZACIÓN DE LA SEGURIDAD

Niveles de la Estructura de Seguridad.

4.1. Definición de Roles, Funciones y Responsabilidades

4.1.1. Dirección

La Dirección es la responsable de que Air Liquide alcance sus objetivos a corto, medio y largo plazo. Respalda explícitamente y de forma notoria todas las actividades de Seguridad de la Información en la organización, expresando sus inquietudes al Comité de Seguridad Corporativa. Es el responsable de aprobar la Política de Seguridad de la Organización.

4.1.2. Comité de Seguridad de la Información

Coordina la Seguridad de la Información, recabando de forma regular del personal técnico propio o externo la información necesaria para la toma de decisiones. Podrán acudir a requerimiento del Comité cualesquiera

otros Jefes de Servicio o Área y responsables cuya intervención sea precisa por ser afectados por el Esquema Nacional de Seguridad y por el RGPD.

Entre sus cometidos está atender las inquietudes de la Alta Dirección e informar del estado de seguridad de la Información, informando regularmente del estado de la seguridad de la información.

Da instrucciones al Responsable de Seguridad para que se encargue de cumplimentar, y supervisar que administradores y operadores implementan las medidas de seguridad según lo establecido en ésta Política de Seguridad aprobada para Air Liquide.

Entre sus funciones están:

- Elaborar la estrategia de evolución en seguridad de la organización, así como de redactar, revisar y aprobar la Política de Seguridad y los procedimientos de uso de los servicios TIC.
- Promover la mejora del sistema de gestión, impulsa la realización de auditorías periódicas para verificar el cumplimiento de las obligaciones y supervisa que la seguridad se integre en todos los proyectos TIC desde su inicio.
- Definir los requisitos de formación y calificación para administradores y usuarios, asegurando que el personal tenga las competencias necesarias en materia de seguridad
- Coordinar todas las actividades de seguridad de la información, recabar datos técnicos para la toma de decisiones e informar regularmente a la Alta Dirección sobre el estado de la seguridad. Además, actúa como mediador para resolver conflictos de responsabilidad entre distintas áreas.

4.1.3. Responsable de Seguridad de la Información

Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. El responsable de la seguridad será **distinto** del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos.

En los servicios que se prestan de forma externalizada a entidades públicas, Air Liquide, como prestataria de dichos servicios tiene designado un POC (Punto o Persona de Contacto), que es el propio Responsable de Seguridad, para la seguridad de la información tratada y el servicio prestado, que cuenta con el apoyo de los órganos de dirección, y que canaliza y supervisa, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provee, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Entre sus funciones se encuentran:

- **Gestión de Riesgos y Planificación**: Liderar la elaboración y actualización periódica del Análisis de Riesgos y la Declaración de Aplicabilidad. Diseñar y realizar el seguimiento del Plan de Seguridad y los planes de mejora derivados.
- **Supervisión y Control**: Verificar que las medidas de seguridad técnicas y organizativas se aplican correctamente. Supervisar la seguridad en el ciclo de vida de los sistemas (desde el diseño hasta el borrado de datos). Promover y gestionar programas de formación y concienciación para todo el personal.
- **Gestión de Incidentes y Continuidad**: Coordinar la respuesta ante incidentes de seguridad y actuar como interlocutor con organismos externos (como el CCN-CERT). Validar los planes de continuidad de los sistemas para asegurar la resiliencia del servicio.
- **Reporte y Gobernanza**: Informar regularmente al Comité de Seguridad sobre el estado de la protección, los riesgos residuales y los incidentes detectados. Asesorar a la Dirección y a los Responsables de Información en la toma de decisiones sobre seguridad.

4.1.4. Responsable de la Información

Determinará los requisitos de la información tratada. *Su rol se centra en la protección y propiedad de los datos tratados.*

Entre sus funciones destacan:

- Actuar como Secretario del Comité de Seguridad de la Información. Convocar las reuniones del Comité. Preparar los temas a tratar aportando información pertinente para la toma de decisiones. Es responsable de la ejecución directa o delegada de las decisiones del Comité.
- Determinará los requisitos de seguridad de la información tratada, estableciendo los niveles de protección necesarios (confidencialidad, integridad y disponibilidad) según el Anexo I del Esquema Nacional de Seguridad.
- Velar por el uso correcto de la información dentro de su área, asegurando que se apliquen las medidas de protección definidas.
- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

4.1.5. Responsable del Servicio

Determinará los requisitos de los servicios prestados. *Su rol se centra en la operatividad y continuidad de la actividad o negocio.*

Le corresponden las siguientes funciones:

- Establecer los requisitos de seguridad específicos para la prestación de los servicios, priorizando su disponibilidad y continuidad.
- Asegurar que el servicio cuente con las medidas necesarias para no interrumpir la actividad ante incidentes técnicos
- Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.

4.1.6. Responsable del Sistema

Por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Le corresponden las siguientes funciones:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Elaborar y ejecutar los Planes de Continuidad del Sistema para garantizar que, ante un fallo, la tecnología se recupere en los tiempos exigidos por el Responsable del Servicio.

- Mantener actualizado el inventario de activos, la topología de red y los registros de configuración, asegurando que solo se ejecuten los cambios autorizados.
- Colaborar con el Responsable de Seguridad en la detección y resolución de anomalías

4.2. Procedimiento de designación/renovación de personas

La Dirección de la Organización nombrará formalmente:

- Al **Responsable de la Información**, puede ser un cargo unipersonal o un órgano.
- A los **Responsables del Servicio**, puede ser el mismo que el Responsable de la Información. Puede ser un cargo unipersonal o un órgano colegiado.
- Al **Responsable de la Seguridad**, que debe reportar directamente a la Dirección o, cuando exista, al Comité de Seguridad de la Información.
- Al **Responsable del Sistema**, que debe reportar directamente a la Dirección o, cuando exista, al Comité de Seguridad de la Información.

La Dirección de la Organización designa a la persona Responsable del Sistema:

- A propuesta del Responsable de la Información tratada, cuando el Sistema de información trate una única información.
- A propuesta del Responsable del Servicio prestado, cuando el Sistema de información preste un único servicio.
- Directamente cuando el Sistema de información trata diferentes informaciones o presta diferentes servicios, oídos los responsables de las informaciones y los servicios afectados.

5. REQUISITOS MÍNIMOS DE SEGURIDAD

Atendiendo al cumplimiento del Esquema Nacional de Seguridad (ENS), se garantizará el cumplimiento de los siguientes requisitos mínimos:

- **Organización e implantación del proceso de seguridad:** la seguridad de los sistemas de información compromete a todos los miembros de la organización. La presente Política de Seguridad deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento**.**
- **Análisis y gestión de los riesgos:** la organización realizará su propia gestión de riesgos, empleando alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos estarán justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.
- **Gestión de personal:** el personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en el RD 311/2022 del ENS, estará formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que será supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados por la Dirección.
- **Profesionalidad:** la seguridad de los sistemas estará atendida revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidentes y desmantelamiento. El personal de la organización recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración.

- **Autorización y control de los accesos:** el acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso exclusivamente a las funciones permitidas.
- **Protección de las instalaciones:** los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas permanecerán cerradas y dispondrán de un control de llaves.
- **Adquisición de productos de seguridad y contratación de servicios de seguridad:** Los productos y servicios de seguridad adquiridos deben contar con certificaciones de funcionalidad técnica alineadas con estándares internacionales y el nivel de riesgo.
- **Mínimo privilegio:** los sistemas se diseñarán y configurarán de manera que garanticen la seguridad por defecto:
    - El sistema proporcionará la **mínima funcionalidad** requerida para que la organización alcance sus objetivos.
    - Las **funciones de operación, administración y registro de actividad** serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
    - En un sistema de explotación **se eliminarán o desactivarán**, mediante el control de la configuración, las **funciones que no sean de interés**, sean **innecesarias** e, incluso, aquellas que sean **inadecuadas** al fin que se persigue.
    - Se garantizará que el **uso** ordinario del sistema sea **sencillo y seguro**, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
- **Integridad y actualización del sistema:** todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se monitoriza constantemente el estado de seguridad y las vulnerabilidades para aplicar actualizaciones con diligencia.
- **Protección de la información almacenada y en tránsito:** se aplica especial cuidado a la información en tránsito o almacenada en entornos inseguros (portátiles, móviles, redes abiertas) mediante cifrado y procedimientos de recuperación a largo plazo.

    Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el RD 311/2022 del ENS, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.
- **Prevención ante otros sistemas de información interconectados:** se protege el perímetro de red, especialmente en conexiones públicas, analizando y controlando siempre los puntos de unión con otros sistemas.
- **Registro de actividad y detección de código dañino:** con la finalidad exclusiva de lograr el cumplimiento del objeto del Esquema Nacional de Seguridad (ENS) con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

- **Incidentes de seguridad**: la organización dispone de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en su artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

  Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

- **Continuidad de la actividad:** los sistemas de la Organización dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

- **Mejora continua del proceso de seguridad:** el proceso integral de seguridad implantado será actualizado y mejorado de forma continua, aplicando los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

6. DATOS DE CARÁCTER PERSONAL

Para la prestación de los servicios previstos por la organización deben ser tratados datos de carácter personal. El Registro de Actividades del Tratamiento detalla los tratamientos afectados y los responsables correspondientes, así como las medidas adoptadas derivadas de las evaluaciones de impacto realizadas sobre los tratamientos. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro de Actividades del Tratamiento.

6.1. Responsable del Tratamiento. Funciones y obligaciones

A efectos de la organización se ha atribuido la condición de **Responsable de Tratamiento** a la persona jurídica, es decir, a Air Liquide Healthcare España S.L., de manera que se ha entendido que Air Liquide es Responsable del Tratamiento de los datos de carácter personal, que obran en sus sistemas de información, y que derivan de la prestación de los **servicios propios** atribuidos al nivel de sus competencias.

Las funciones del Responsable del tratamiento son:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.
- Deberá informar a los titulares de los datos los derechos que les asisten y en los términos en los que pueden ejercerlos.
- Deberá excluir del tratamiento los datos relativos al afectado que se oponga al tratamiento de los mismos.
- Deberá cesar en la utilización o cesión ilícita de los datos cuando así lo requiera el interesado.
- Obligación de hacer efectivo el derecho de rectificación o supresión del interesado.
- Notificar las rectificaciones o cancelaciones efectuadas en los datos personales a quien se haya comunicado dichos datos, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

6.2. Encargado del Tratamiento. Funciones y obligaciones

A efectos de la organización se ha atribuido la condición de **Encargado de Tratamiento** a la persona jurídica, es decir, a Air Liquide Healthcare España S.L., de manera que se ha entendido que Air Liquide es Encargada del Tratamiento de los datos de carácter personal, que obran en sus sistemas de información, y que derivan

de la prestación de los **servicios a las Entidades del Sector Público**, para el ejercicio por éstas de sus competencias y potestades administrativas.

El Encargado del Tratamiento deberá aplicar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado; estas medidas aparecerán estipuladas en el contrato con el Responsable del Tratamiento.

En concreto, sus funciones son las de:

- Tratar los datos del tratamiento.
- Realizar el control de tratamiento, calidad y seguridad de los datos.
- Controlar la forma y requisitos para proceder a las adiciones y cancelaciones.
- Controlar los soportes de seguridad.
- Control y acceso de contraseñas.
- Mantenimiento del registro de incidencias.
- Dar traslado al responsable del tratamiento de aquellas solicitudes de ejercicio de derecho que se reciban por parte de los interesados.

6.3. Delegado de Protección de Datos (DPD). Funciones y obligaciones

Air Liquide Healthcare España S.L. dispone de un Delegado de Protección de Datos (DPO) para el Grupo Air Liquide, cuya dirección de contacto es: https://contactprivacy.airliquide.com/.

El DPO actuará con plena independencia y contará con los recursos necesarios para velar y garantizar la privacidad. Sus funciones y responsabilidades se agrupan en los siguientes pilares de actuación:

A. Supervisión y Cumplimiento Normativo

El DPO audita y supervisa que todos nuestros tratamientos de datos respeten los principios de **minimización, exactitud y limitación de la finalidad**. Sus tareas incluyen:

- Gestionar y mantener el **Registro de Actividades de Tratamiento (RAT)**.
- Identificar las **bases jurídicas** y la normativa sectorial aplicable a cada actividad.
- Diseñar e implantar las **políticas de protección de datos** y realizar auditorías periódicas de cumplimiento.

B. Privacidad desde el Diseño y Gestión de Riesgos

Garantizamos que la seguridad esté presente desde el origen de cada proyecto:

- **Evaluaciones de Impacto:** Realiza análisis de riesgos y evaluaciones de impacto (EIPD) para tratamientos de alta sensibilidad.
- **Privacidad por Defecto:** Asegura la implantación de medidas técnicas y organizativas adecuadas a la naturaleza de los datos.
- **Gestión de Brechas:** Coordina los protocolos ante incidentes de seguridad, evaluando riesgos para los afectados y gestionando las notificaciones ante las autoridades competentes.

C. Transparencia y Relación con el Interesado

El DPO es el garante de sus derechos frente a la organización:

- **Atención al Cliente:** Gestiona los mecanismos para el ejercicio de sus derechos (acceso, rectificación, supresión, etc.) y valora cada solicitud de forma personalizada.
- **Información Clara:** Diseña las cláusulas y avisos de privacidad para asegurar que usted siempre sepa cómo usamos sus datos.

- **Control de Proveedores:** Supervisa la contratación de terceros (Encargados de Tratamiento) y valida las transferencias internacionales de datos.

D. Cultura y Enlace Institucional

- **Formación:** Lidera programas de sensibilización y formación continua para todo el personal de Air Liquide.
- **Autoridad de Control:** Actúa como el punto de contacto único y oficial con la **Agencia Española de Protección de Datos (AEPD)**.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

El DPO deberá reunir conocimientos especializados del Derecho y la práctica en materia de protección de datos. Se han identificado, en consecuencia, aquellos **conocimientos, habilidades o destrezas necesarias** que tiene que saber o poseer el Delegado de Protección de Datos para llevar a cabo una de las funciones propias de su puesto.

6.4. Usuarios con acceso a datos. Funciones y obligaciones

Todos los empleados de la entidad están sujetos a funciones y obligaciones. Todo el personal de la entidad que disponga de acceso a los datos de carácter personal debe cumplir con las siguientes obligaciones:

- No se permite la difusión de datos de carácter personal ni confidencial perteneciente a la entidad. Estando obligado a guardar secreto de la información incluso terminada la relación laboral.
- El usuario se responsabilizará de notificar toda incidencia según el procedimiento de gestión de incidencias, no notificar una incidencia será considerada una omisión del deber del trabajador.
- El usuario se responsabilizará de todos los accesos que se realicen bajo su identificador y contraseña, por tanto, no deberá revelar la contraseña.
- El usuario se responsabilizará siempre que abandone el puesto de trabajo de cerrar su sesión o bloquear el equipo con contraseña.
- No se podrán instalar aplicaciones en los sistemas de la entidad sin el consentimiento del delegado de protección de datos.
- No se permite la copia de datos de carácter personal, en soportes, sin la autorización expresa del delegado de protección de datos.
- El usuario se responsabilizará de guardar copias de todos los correos que incluyan anexos con datos personales vinculados a la entidad.

7. GESTIÓN DE RIESGOS

7.1. Justificación

Todos los sistemas sujetos a esta Política de Seguridad deberán 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 Gestión de la seguridad basada en los riesgos del RD 311/2022 del ENS.

7.2. Criterios de Evaluación de Riesgos

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

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios que afecten a los ciudadanos.

7.3. Directrices de Tratamiento

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo las inversiones de carácter horizontal que sean necesarias y proporcionales.

7.4. Proceso de Aceptación del Riesgo Residual

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información.

Los niveles de Riesgo residuales esperados sobre cada Información o sobre cada Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente, según corresponda, por el Responsable de esa Información o por el Responsable de ese Servicio.

Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

7.5. Necesidad de realizar o actualizar las Evaluaciones de Riesgos

El análisis de los riesgos y su tratamiento deben ser una actividad continua y permanentemente actualizada, según lo establecido en el artículo 7 del RD 311/2022 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada, en los servicios prestados o en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad o se reporten vulnerabilidades graves.

7.6. Riesgos que se derivan del Tratamiento de Datos Personales

Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

8. GESTIÓN DE INCIDENTES DE SEGURIDAD

8.1. Prevención

Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las áreas de negocio y divisiones de la organización 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. El ENS a través de su artículo 20 establece que los sistemas deben diseñarse y configurarse de forma que garanticen el principio de mínimo privilegio. De igual forma, el ENS establece que los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Para ello las áreas de negocio y divisiones de la organización 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 de Seguridad, las áreas de negocio y divisiones de la organización deben:

- Establecer áreas seguras para los sistemas de información crítica o confidencial.
- 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.

8.2. Detección

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

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 según lo establecido en el artículo 8 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 9 del ENS. 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.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la Organización, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones: (i) Sistemas de detección de intrusos a nivel de red; (ii) Sistemas de detección de intrusos a nivel sistema.

8.3. Respuesta

Las medidas de respuesta que se gestionarán en tiempo oportuno estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

Las áreas de negocio y divisiones de la organización deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otras áreas de negocio o divisiones de la organización.
- 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), Equipos de Respuesta a Incidentes de Seguridad (CSIRT), y los Centros de Operaciones de Seguridad (SOC).

8.4. Conservación

Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

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

9. CONCIENCIACIÓN Y FORMACIÓN

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

Todos los miembros de la organización atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Atendiendo a los requisitos de profesionalidad, las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos de la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

10. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 12 del ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

11. DOCUMENTACIÓN COMPLEMENTARIA

La Política de Seguridad de la Información se cumplimentará con documentos más precisos que ayudan a llevar a cabo el objetivo propuesto. Para ello se utilizará la documentación existente del Grupo Air Liquide:

- Normas de seguridad (Security Standards).
- Guías de seguridad (Security Guides).
- Procedimientos de seguridad (Security Procedures).

Las **normas** permiten uniformizar el uso de aspectos concretos del sistema, indican el uso correcto y las responsabilidades de los usuarios, y 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.

Los **procedimientos operativos** de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

En relación a la calificación de la información, aquella documentación que contenga información confidencial, se etiquetará como tal mediante la incorporación de marcas de agua en el propio documento, menciones al contenido confidencial en la cabecera y pie de página o fórmulas alternativas que dejen constancia de la restricción de acceso en el documento o soporte.

12. GLOSARIO DE TÉRMINOS

Análisis de riesgos: utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

Gestión de incidentes: plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Principios básicos de seguridad: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información: persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad: el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio: persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema: persona que se encarga de la explotación del sistema de información.

Servicio: función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.