INDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información está vigente desde la fecha de aprobación y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

AQLARA infraestructuras (AQI) depende de los sistemas de información para alcanzar sus objetivos, estos sistemas son administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que la organización pueda cumplir con sus objetivos, desarrollar sus funciones o competencias y prestar los servicios para la cual ha sido constituida 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.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos 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.

AQI debe cerciorarse de que la seguridad TIC 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, en la solicitud de ofertas, y en pliegos de licitación para proyectos donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

3. ALCANCE

Esta política es aplicable a todos los trabajadores de **AQI** y a cualquier persona ajena a **AQI** que tenga acceso a la información gestionada por o propiedad de la empresa. La política también es aplicable a toda la información en soporte digital y a los

Sistemas de Información propiedad de la empresa o gestionados por la misma. La información de **AQI** debe ser protegida conforme a su sensibilidad, valor y criticidad.

4. MISIÓN

La actividad de **AQI** contribuye al desarrollo sostenible y a la mejora de la calidad del agua. Garantizamos el acceso por parte de la ciudadanía a un recurso básico y aseguramos que cuando el agua vuelve a medio natural, lo hace en las mismas condiciones en que fue captada.

Los servicios incluidos dentro del ENS son los siguientes:

"El sistema de información que dan soporte a los procesos de Gestión de Servicios Públicos del ciclo integral del agua incluidos los procesos de atención al usuario ":

- Gestión de abonados (AQUAPRO o EUROPHA)

Con relación al documento de categorización vigente.

Estas actividades se realizan desde las instalaciones de **AQI** ubicadas en:

- Oficina en C/ Cobalto 12, Polígono San Cristóbal, 47012, Valladolid.

5. OBJETIVOS

Los objetivos en materia de seguridad que **AQI** pretende garantizar con la presente Política serán:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes respecto a la seguridad de la información.
- Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que se transmita a través de redes de comunicaciones sea adecuadamente protegida.

- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

6. PRINCIPIOS RECTORES DE LA POLITICA

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.
- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.
- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, danto una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.

- Vigilancia continua y reevaluación periódica: la entidad implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

7. MARCO NORMATIVO

Las principales normas que afectan a esta Política son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- 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 (Reglamento General de Protección de Datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- AQI se mantendrá cumpliendo y respetando la Ley de Propiedad Intelectual en lo que se refiere al uso del software, obteniendo las licencias correspondientes y llevando un registro y control de estas para el empleo adecuado de éstas en el desarrollo de las actividades.

AQI dispone de un registro de legislación aplicable en el que se identifica toda la legislación en materia de seguridad de la información y su adecuación y cumplimiento en la empresa.

8. ORGANIZACIÓN DE LA SEGURIDAD

La Dirección **AQI** tiene como responsabilidad fundamental la de liderar y comprometerse con respecto al Sistema de Gestión.

8.1 Comité: funciones y responsabilidades

Se designa como órgano responsable del sistema al Comité de Seguridad que dispone de las siguientes funciones:

- Atender las inquietudes que, en materia de seguridad, se planteen desde la Dirección de la entidad y de los diferentes departamentos.
- Informar y ser informado regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información, con la aprobación de planes específicos.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Controlar periódicamente el grado de cumplimiento de las medidas propuestas para reducir el riesgo residual (pudiendo proponer acciones de mejora) y el correcto funcionamiento del procedimiento de gestión e incidentes, velando por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección (o por el órgano competente) y aprobar la Normativa de Seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo/entidad en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque se respete el principio de seguridad desde el diseño, pudiendo requerir el asesoramiento el Responsable de la Seguridad, en todas aquellas iniciativas de la entidad que afecten a la seguridad de la información o de los sistemas. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas en el ámbito de aplicación del ENS.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización,

elevando a Dirección aquellos casos en los que no tenga suficiente autoridad para decidir.

El Comité de Seguridad de la Información estará formado por:

- Responsable de la Información
- Responsable de los servicios
- Responsable de la Seguridad
- Responsable del Sistema

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de nuestra empresa.

El Secretario del Comité de Seguridad será el responsable de Seguridad y tendrá como funciones:

- Convocar las reuniones del Comité de Seguridad de la Información, atendiendo a las instrucciones del presidente del Comité.
- Preparar los temas a tratar en las reuniones del Comité, recabando la información de los diferentes responsables.
- Elaborar el acta de las reuniones.
- Remitir el acta de las reuniones a los asistentes, recabando su firma.
- Conservar las actas, de acuerdo con los criterios de conservación documental de la entidad.

El Comité de Seguridad de la Información reportará a la Dirección de **AQI**

8.2 Roles: funciones y responsabilidades

Director general (CEO):

- Aprobar la Política de seguridad de la información y la Política de protección de datos.
- Facilitar los recursos adecuados para alcanzar los objetivos propuestos en materia de seguridad, siendo responsable último del cumplimiento de las obligaciones en materia de seguridad.
- Mantenerse informado regularmente del estado de seguridad de la información.
- Aprobar el Plan de Mejora de Seguridad con su dotación presupuestaria correspondiente.

- Responsabilidad última del uso que se haga de la información y, por tanto, de su protección.

Responsable de la información:

- Determinar los requisitos de la información tratada en materia de seguridad.
- Responsabilidad de la vigilancia del uso que se haga de la información y, por tanto, de su protección.
- Establecer los requisitos y los niveles de seguridad necesarios para la información en materia de seguridad.
- Responsable de determinar la valoración del sistema y de su aprobación.

Responsable del servicio:

- Determinar los requisitos de los servicios prestados.
- Establecer los requisitos del servicio en materia de seguridad, determinar los niveles de seguridad de los servicios.
- Aprobar el documento de Valoración del Sistema.

Responsable de Seguridad:

- Determinar las medidas de seguridad aplicables, en función de las valoraciones hechas por los Responsables de la Información y los Servicios.
- Proponer el nivel de riesgo aceptable y aprobar el análisis de riesgos.
- Elaborar y aprobar la Declaración de Aplicabilidad, atendiendo a los requerimientos del Responsable de la Información y del Servicio
- Determinar la categoría del sistema, atendiendo a las valoraciones del Responsable de la Información y del Servicio.
- Comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema.
- Participar en la elaboración y en la propuesta de la Política de Seguridad de la Información y los procedimientos, normativas e instrucciones en aplicación del ENS.
- Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y, en su caso, del Delegado de Protección de Datos y supervisar su despliegue.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Colaborar con el Delegado de Protección de datos en la gestión de los incidentes que afecten a datos personales y, en su caso, a la notificación a las autoridades de control y a las personas afectadas.

Responsable del Sistema:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Adoptar las medidas correctoras derivadas de las auditorías de seguridad.
- En la gestión de incidentes de seguridad (ciber incidentes) podrá, de acuerdo con el Responsable de la Seguridad, suspender de forma cautelar y urgente el tratamiento de la información y la prestación de los servicios como medida de contención. Dicha suspensión deberá ser comunicada al Titular de la entidad y a los responsables de la información y del servicio y, en caso de afección a datos personales al Delegado de Protección de Datos y si afecta a la tramitación administrativa, a los servicios jurídicos de la entidad para, en su caso, proceder a la suspensión de los plazos. 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.
- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- Aplicar los Procedimientos Operativos de Seguridad (POS).
- Informar al Responsable de seguridad 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.
- Comprobar que los controles de seguridad establecidos son adecuadamente observados.
- Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

8.3 Procedimiento de designación

La Dirección asegura que el personal dispone de la necesaria formación teórica y práctica en materia de seguridad de la información para el desempeño eficiente de sus funciones.

Las funciones y responsabilidades inherentes a cada puesto de trabajo, así como los requisitos de formación y experiencia necesarios, están recogidas en los perfiles de puesto de trabajo.

Las modificaciones de los roles y funciones de seguridad serán aprobados por la dirección de **AQI**.

Los nombramientos podrán ser revisados cada dos años, pudiendo realizarse antes cuando el puesto quede vacante o por un incumplimiento reiterado de sus funciones, previo apercibimiento.

AQI dispone de un mecanismo que permita la sustitución de los responsables designados en caso de ausencias de larga duración o aquellas de menor duración pero que puedan provocar ineficiencias en las funciones de cada uno de ellos que afecten al sistema.

9. TRATAMIENTO DE DATOS PERSONALES EN AQI

El tratamiento de datos de carácter personal se basará en la "Política protección datos personales", en la que se fijan las directrices que se deben seguir en **AQI** para garantizar la privacidad de los datos de los clientes, proveedores, empleados y, en general, de todos los colectivos de datos implicados, identificando la base de legitimación más adecuada para los tratamientos de datos personales llevados a cabo de acuerdo con la legislación vigente.

10. DETERMINACIÓN DE LA CATEGORIA Y DEL NIVEL DE SEGURIDAD REQUERIDO PARA LOS SISTEMAS

La categoría en materia de seguridad, de los sistemas de información en el alcance del Esquema Nacional de Seguridad, se determinará en función de la valoración del impacto que tendría un incidente que afecte a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

La valoración de las consecuencias del impacto se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

La facultad para determinar la categoría de un sistema le corresponde al responsable del servicio y al responsable de la información; y será de aplicación a todos los sistemas empleados para la prestación de los servicios incluidos en el alcance del Esquema Nacional de Seguridad.

El proceso de categorización de los sistemas se realizará a través de las siguientes actividades:

- Identificación del nivel correspondiente a cada servicio/información, en función de las dimensiones de seguridad.

- Determinación de la categoría del sistema, teniendo en cuenta que cuando un sistema maneja diferentes informaciones y presta diferentes servicios, el nivel del sistema en cada dimensión, será el mayor de los establecidos para cada información y servicios.

La identificación del nivel correspondiente a cada servicio/información en las dimensiones disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad se realizará considerando los siguientes criterios definidos en el Esquema Nacional de Seguridad:

- Nivel BAJO (B). Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel MEDIO (M). Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel ALTO (A). Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

La clasificación se realizará en base a las siguientes categorías: BÁSICA (B), MEDIA (M) y ALTA (A).

- Un sistema de información será de categoría ALTA (A) si alguna de sus dimensiones de seguridad alcanza el nivel ALTO (A).
- Un sistema de información será de categoría MEDIA (M) si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO (M), y ninguna alcanza un nivel superior.
- Un sistema de información será de categoría BÁSICA (B) si alguna de sus dimensiones de seguridad alcanza el nivel BAJO (B), y ninguna alcanza un nivel superior.

La calificación de la información será realizada por el responsable de la información considerando lo establecido legalmente sobre la naturaleza de la misma.

La valoración del sistema de información y la determinación de la categoría del sistema será documentada en el **Documento categorización del Sistema**, siendo el responsable de la información y del servicio el responsable de su documentación y aprobación formal. Además, en cada momento tendrá en exclusiva la potestad de

modificar el nivel de seguridad requerido, de acuerdo a los criterios descritos en el presente documento.

Considerando la categoría del sistema y los niveles asociados a cada dimensión de seguridad, se determinarán las medidas que se deberán aplicar a dicho sistema.

11. ESTABLECIMIENTO, IMPLANTACIÓN, MANTENIMIENTO Y MEJORA DEL SGSI Y DIRECTRICES PARA LA GESTIÓN DE LA DOCUMENTACIÓN

En cumplimiento del artículo 12 del Real Decreto del ENS, la presente Política de Seguridad se desarrollará aplicando los siguientes requisitos mínimos que se encuentran incluidos en la documentación del sistema:

a. Organización e implantación del proceso de seguridad.

Considerando las directrices desarrolladas en la Política de Seguridad del ENS, se desarrollarán un conjunto de procedimientos operativos que permitan garantizar la implantación de dichas directrices, y la consecución de los objetivos de la organización en materia de seguridad de la información.

b. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El proceso de análisis y gestión de los riesgos se realizará de acuerdo con las siguientes actividades:

- Identificación de activos.
- Análisis y valoración.
- Cálculo del riesgo.
- Determinación del riesgo residual.

El desarrollo de estas actividades se encuentra recogido en la metodología de análisis de riesgos.

Este análisis se repetirá:

- regularmente, al menos una vez al año.
- cuando se produzcan cambios en la información manejada.
- cuando se produzcan cambios en los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves, cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

c. Gestión de personal.

La Dirección se asegurará que el personal dispone de la formación necesaria teórica y práctica en materia de seguridad de la información para el desempeño eficiente de sus funciones.

Para lograr los objetivos de seguridad de la información todo el personal debe estar involucrado en el tratamiento y saber de qué forma se puede contribuir a su consecución.

d. Profesionalidad.

La Dirección deberá garantizar que el personal dispone del conocimiento y habilidades necesarias para el adecuado desempeño de sus funciones. Además, deberá proporcionar la formación necesaria cuando se detecten carencias en el cumplimiento de las actividades.

e. Autorización y control de los accesos.

Los sistemas de información deberán disponer de un mecanismo de control de accesos que limite su acceso a los usuarios y dispositivos que estén debidamente autorizados, restringiendo el acceso a las funciones que le son permitidas. Las medidas de seguridad aplicadas se encuentran descritas en el procedimiento de control de acceso.

f. Protección de las instalaciones.

La organización deberá disponer de un conjunto de controles de acceso físico a las instalaciones, que permita limitar el acceso únicamente a las personas autorizadas a las zonas de almacenamiento y/o procesamiento de información confidencial. Las medidas de protección se encuentran descritas en el procedimiento de seguridad de los equipos.

g. Adquisición de productos de seguridad y contratación de servicios de seguridad.

La adquisición de productos y servicios deberá considerar y garantizar el cumplimiento con los requisitos de seguridad establecidos por la Dirección, tal y como se detalla en la Política de arquitectura segura.

h. Mínimo privilegio.

Los sistemas deberán configurarse según las políticas y procedimientos de seguridad definidos. El procedimiento Gestión de Control de accesos desarrolla las medidas de seguridad que se deben aplicar a los sistemas de información en el que se considera siempre el principio de mínimo privilegio.

i. Integridad y actualización del sistema.

Se deberán aplicar medidas que permitan conocer el estado de seguridad de los sistemas, y que permitan identificar y gestionar los riesgos de seguridad de los mismos. Estas medidas se encuentran desarrolladas en el procedimiento Gestión del código malicioso.

j. Protección de la información almacenada y en tránsito.

Se deberán aplicar medidas de seguridad que permitan garantizar un adecuado nivel de protección de la información almacenada y en tránsito. Estas medidas se encuentran detalladas en el procedimiento de Cifrado e intercambio de información.

k. Prevención ante otros sistemas de información interconectados.

Se deberán analizar y gestionar los riesgos derivados de las conexiones de los sistemas de información con redes públicas, y aplicar las medidas necesarias de protección según el nivel de seguridad requerido por el sistema.

l. Registro de actividad y detección de código dañino.

Los sistemas de información deberán contar con registros de actividad de los usuarios que permitan custodiar la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas. Además, se deberá disponer de sistemas que permitan la detección de código dañino.

m. Incidentes de seguridad.

Los sistemas de información deberán contar con un sistema de detección y reacción frente a código dañino. Además, existirá un registro de incidentes de seguridad que permitirá realizar un seguimiento de la resolución de los mismos y aplicar mejoras a través de las lecciones aprendidas.

n. Continuidad de la actividad.

Se deberán establecer, en la medida de lo posible y según el nivel de riesgo asociado, los mecanismos necesarios para garantizar la recuperación de la información y la continuidad de las operaciones.

o. Mejora continua del proceso de seguridad.

La Dirección deberá llevar a cabo una revisión periódica del sistema para asegurarse de su conveniencia, adecuación y eficacia continua. Ante la ocurrencia de cualquier desviación respecto a los resultados esperados, se deberá iniciar el proceso de tratamiento de la misma mediante los procesos establecidos.

12. DOCUMENTACIÓN

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo con los requisitos generales del Sistema de Gestión de **AQI** que se recogen en el PG02 “Control de documentos”.

Toda la información documentada se aloja en los Sistemas de Información de **AQI**.

13. DESARROLLO DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de normativa de seguridad que abordará aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible por diversos medios a disposición de los usuarios en la Intranet.

14. OBLIGACIONES DEL PERSONAL

Todos los miembros de **AQI** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad de **AQI** a través del Comité de Seguridad y del área de personal de disponer los medios necesarios para que la información llegue a los afectados.

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

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.

15. TERCERAS PARTES / PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES

Cuando **AQI** preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de

respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando **AQI** utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las Guía de desarrollo.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

16. APROBACIÓN DE LA POLITICA Y ENTRADA EN VIGOR / EFECTIVIDAD

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información, que deberá revisarla anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo), que tendrá la obligación de aplicarla en la realización de sus actividades laborales.

La información documentada será clasificada en: **información de uso público, información privada, información de uso interno e información confidencial,** dando el uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en la Política de Clasificación de la información.

17. VIOLACIONES DE LA POLITICA DE SEGURIDAD

El cumplimiento de la Política de Seguridad de la Información es fundamental para garantizar la protección de los derechos legales de **AQI**. Cualquier incumplimiento será considerado una violación, y los responsables estarán sujetos a las medidas disciplinarias que determine la Dirección de **AQI**.

En Valladolid, a 14 de abril de 2026

Dirección General

09393325X JAVIER OLMOS (R: A47211214)

Firmado digitalmente por 09393325X JAVIER OLMOS (R: A47211214)
Fecha: 2026.04.14 08:33:14 +02'00'