Principios generales de seguridad de la información

2025

Lo principios de generales de seguridad de la información que rigen en AQUALIA tienen como objetivo la implantación y operatividad continuada de acciones destinadas a preservar los componentes básicos de la seguridad de la información:

- Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.
- Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos

Estos principios se aplican en todas las fases del ciclo de vida de la información: generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción, y de los sistemas que los procesan: análisis, diseño, desarrollo, implantación, explotación y mantenimiento.

La seguridad de la información incumbe a todo el personal de **AQUALIA** por lo que estos principios deben ser conocidos, comprendidos y asumidos por todos los niveles de la organización. Los principios se comunicarán fehacientemente a toda la organización, tanto al personal propio como a empresas colaboradoras externas, y estarán a disposición de las partes interesadas.

Las relaciones con terceras empresas colaboradoras deben de estar amparadas siempre por los correspondientes contratos de prestación de servicios, incluyendo cláusulas de garantías en el uso y tratamiento de la información

Aplicación

Con objetivo de aplicar los principios expuestos en esta política, se precisa la definición, elaboración, implantación y mantenimiento de planes estratégicos de seguridad. La elaboración de los planes estratégicos de seguridad deberá acompañarse de procesos formales de análisis y gestión de riesgos que permitan implantar las soluciones idóneas.

A nivel operativo, **AQUALIA** desarrollará sus propios procedimientos, estándares y guías de seguridad, que garanticen la integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad de la información.

Se implantarán los procesos de gestión de la seguridad necesarios, acordes con el estándar ISO 27001 y el Esquema Nacional de Seguridad para asegurar el seguimiento efectivo y eficiente de las acciones en seguridad, así como de los procesos de revisión y de mejora de los proyectos de seguridad y de las contramedidas definidas.

Conformidad legal

Por la naturaleza y objeto del negocio de **AQUALIA** se debe observar el cumplimiento de normas de rango superior (leyes, normas y disposiciones legales) que tendrán preferencia, cuando ello aplique sobre las directrices de esta política de seguridad de la información:

- Normas generales y/o deontológicas de **AQUALIA**.

- Normativa española que regule esta actividad.
- Normas españolas que provengan de organismos supranacionales de los que España sea miembro.
- Normativa comunitaria y /o extracomunitaria, en razón a las áreas de prestación de servicios por parte de **AQUALIA.**

Clasificación y tratamiento de la información

Toda información deberá estar clasificada en virtud de su importancia para la organización y ha de ser tratada según dicha clasificación, acorde a lo dispuesto en la normativa sobre clasificación y tratamiento de la información.

Formación y concienciación

El método más efectivo de mejorar la seguridad es mediante la formación continuada y su incorporación a la actividad laboral.

Dentro de los planes de formación se incluirán cursos específicos sobre seguridad de la información acorde con el área destinataria: dirección, técnicos, administradores y usuarios de los sistemas. Asimismo, se realizarán campañas de concienciación sobre seguridad dirigidas a todo el personal y proveedores a través del medio que se considere más efectivo.

Auditoría

Los sistemas de información se someterán periódicamente a auditorías internas y externas con la finalidad de verificar el correcto funcionamiento de los planes de seguridad, determinando grados de cumplimiento y recomendando medidas correctoras, consiguiendo, así, una mejora continua.