POLÍTICA

SEGURIDAD DE LA INFORMACIÓN

REVISADO POR:

SAMIR ARANA
Director de IT & Nuevos productos

APROBADO POR:

LELIO SOTOMONTE
Presidente

Código	AT-PL-36-V10
Fecha	Agosto 10 de 2024
Resumen	***El siguiente documento contiene la política del sistema de gestión de seguridad en la información de Atlantic Quantum Innovations S.A.S.***

TABLA DE CONTENIDO

1. DECLARACIÓN POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

En Atlantic Quantum Innovations S.A.S. compañía del sector de contact center y BPO, nos comprometemos a:

1.1. ***Proteger nuestros activos de información y los de nuestras partes interesadas contra diversas amenazas mediante la implementación de un Sistema de Gestión de Seguridad de la Información.***

1.2. Asegurar la confidencialidad, integridad y disponibilidad de la información propia y de ***nuestras partes interesadas.***

1.3. Mantener la estabilidad y disponibilidad de las operaciones que gestionamos, ***garantizando la continuidad del servicio.***

1.4. Generar valor al negocio de nuestros clientes ***mediante la implementación de prácticas de seguridad que protegen sus activos y fortalecen su confianza en nuestros servicios***.

1.5. Cumplir con ***todos*** los requisitos ***legales, regulatorios y/o contractuales*** aplicables a las ***jurisdicciones en las que operamos.***

Para lograr este objetivo, nos enfocamos en implementar controles estrictos de seguridad, mejorar continuamente nuestros procesos conforme a estándares internacionales, contar con un recurso humano altamente motivado y competente, y colaborar con aliados de negocios que compartan nuestra visión y estén comprometidos con la seguridad de la información.

Esta política será revisada y aprobada ***anualmente p***ara asegurar su adecuación y eficacia continúa ***adaptándose a los cambios en el entorno regulatorio, tecnológico y de negocio.***

2. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN.

a) Proteger los activos de información ***asegurando la confidencialidad, integridad y disponibilidad*** mediante la implementación de políticas, procedimientos y controles de seguridad.
b) Prevenir, controlar ***responder y aprender todos los incidentes de seguridad de la información.***
c) ***Asegurar el*** cumplimiento legal, regulatorio y/o contractual a través de la ***implementación y ejecución de los controles y procesos necesarios.***
d) ***Identificar, evaluar y mitigar los riesgos de seguridad de la información de manera proactiva y continua, mediante la implementación de un proceso de gestión de riesgos basado en las mejores prácticas de la industria, y tomando las medidas necesarias para minimizar la exposición de la empresa a amenazas internas y externas.***
e) ***Mantener un proceso continuo de revisión y mejora de las políticas, procedimientos y controles de seguridad de la información para adaptarse a cambios en el entorno y en las amenazas.***

f) Mantener una cultura de seguridad de la información al interior de la ***empresa donde todas las partes interesas se sientan empoderados para contribuir a la protección de la información y reportar cualquier riesgo o incidente de seguridad.***

g) ***Mantener la mejora continua del SGSI a través de la atención oportuna y eficaz de los planes de acción.***

3. RESPONSABILIDAD Y AUTORIDAD

La alta dirección designa la responsabilidad de implementar, mantener y mejorar este sistema, además de asegurar los recursos necesarios para su funcionamiento en Atlantic QI. Para más información, remitirse a AT-T-05 Matriz de Responsabilidades Seguridad en la información.

4. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

4.1. Política de Controles de Personas

La seguridad de la información es una responsabilidad compartida por todos los miembros de la organización. La dirección de Atlantic Quantum Innovations S.A.S. respalda activamente la seguridad de la información mediante un compromiso claro, apoyo continuo y la asignación explícita de responsabilidades.

Para reducir el riesgo de errores humanos, robos, fraudes, manejo indebido de la información y mal uso de las instalaciones, la alta dirección, a través de procesos de Talento Humano y Experiencia Interna, asegura el cumplimiento de los siguientes aspectos:

a) Selección y Vinculación de Personal:

Atlantic Quantum Innovations S.A.S. establece y sigue los lineamientos de la normativa vigente y los procedimientos internos para los procesos de selección y vinculación de personal. Cada proceso de selección debe incluir verificaciones exhaustivas, tales como consultas en bases de datos de listas restrictivas y antecedentes criminales en los portales del gobierno colombiano, como la Procuraduría General de la Nación, la Contraloría General de la Nación y la Policía Nacional, para confirmar la autenticidad de la información proporcionada por los candidatos, entre otras acordes a las necesidades de la organización. Para más información, remitirse Procedimiento de Reclutamiento y Atracción de Talento.

b) Verificación de Antecedentes y Exclusiones:

Los procesos de verificación de antecedentes y exclusiones están debidamente documentados en el procedimiento de reclutamiento y selección y en la política de verificación de exclusiones para programas de salud en EE. UU. Se deben realizar pruebas de detección para cualquier persona con

acceso a cuentas de Medicare y Medicaid, verificando las exclusiones antes del inicio de la relación laboral y de forma mensual en las siguientes bases federales de EE. UU.: LEIE (List Excluded Individuals/Entities), OIG (Office of Inspector General) y GSA (General Services Administration). Para más información, remitirse al RH-P-03Procedimiento de Reclutamiento y Atracción de Talento y AT-PL-42 Exclusion Authorities U.S. Healthcare Program.

c) Contratos de Empleados:

El proceso de Relaciones Laborales debe garantizar que los contratos de los empleados incluyan cláusulas que definan las responsabilidades del personal y de la organización en relación con la seguridad de la información.

d) Concientización, Educación y Capacitación:

Atlantic Quantum Innovations S.A.S. promoverá una cultura de seguridad de la información entre empleados y contratistas para minimizar riesgos, gestionar adecuadamente los activos y proteger las instalaciones, en línea con los procedimientos y controles del Sistema de Gestión de Seguridad de la Información (SGSI). La capacitación inicial sobre seguridad de la información será proporcionada por los procesos de Formación, Desarrollo Organizacional y Compras, abarcando responsabilidades del usuario, procedimientos y mejores prácticas. Todos los empleados y proveedores deben recibir esta capacitación anualmente. Los proveedores pueden presentar prueba de capacitación al gerente administrativo para su validación por el director de cumplimiento o su designado.

e) Responsabilidad y Reporte de Incidentes:

Todos los empleados y proveedores deben estar capacitados para reconocer e informar cualquier incidente de seguridad.

f) Contratos de Proveedores y Contratistas:

Los procesos de Obligacionales legales y Compras deben asegurar que en los contratos de proveedores y contratistas que manejan información sensible se incluyan cláusulas relacionadas con la propiedad intelectual, la confidencialidad y la seguridad de la información de Atlantic Quantum Innovations S.A.S. El personal de terceros debe cumplir con estas cláusulas antes de acceder a las instalaciones y plataformas tecnológicas de la organización.

g) Acuerdos de confidencialidad o no divulgación:

Se debe garantizar que todos los empleados, contratistas y proveedores y aquellas otras personas o terceros que, debido al cumplimiento de sus funciones u obligaciones, accedan, compartan, utilicen, recolecten, procesen, intercambien o consulten o accedan a la información de ATLANTIC QUANTUM

INNOVATIONS S.A.S. firmarán acuerdos relativos a la confidencialidad de la información de la empresa, que contendrán la siguiente información:

- ✓ ***Partes intervinientes;***
- ✓ ***Qué información tendrá carácter confidencial;***
- ✓ ***Compromisos por ambas partes;***
- ✓ ***Posibles sanciones y legislación aplicable.***

Cada empleado de la empresa debe asegurarse de leer, comprender y firmar cada uno de los acuerdos, contratos, cláusulas y documentos de políticas relacionados con la seguridad de la información.

h) Proceso Disciplinario:

Se debe elaborar un procedimiento para tomar medidas disciplinarias contra el personal y las partes interesadas que violen la política de seguridad de la información (fuga o pérdida de datos confidenciales o sensibles, actuaciones intencionadas, ataques a la reputación en redes sociales, permitir ataques de terceros como infecciones por malware, etc.). Este procedimiento debe ser notificado a los empleados y estar accesible en todo momento.

En caso de incumplimiento, el Proceso de Relaciones Laborales es responsable de aplicar las medidas necesarias conforme al procedimiento establecido. Para más información, remitirse al RH-I-07 Instructivo toma de medidas frente a faltas disciplinarias o de bajo desempeño y RH-T-02 Relación de Faltas y Medidas Disciplinarias

i) Terminación Laboral:

Las directrices de terminación laboral están claramente establecidas en el procedimiento de vinculación y desvinculación laboral.

Para evitar fugas de información es importante comunicar a los empleados las responsabilidades y obligaciones de seguridad y confidencialidad que deberán cumplir una vez finalizada la relación contractual. Para más información, remitirse al RH-P-34 Procedimiento Desvinculación de Personal.

j) Concesión autorizada de los permisos de acceso:

Garantizar que cada empleado solo acceda a la información oportuna, se debe dar de alta en los sistemas de acuerdo con las políticas de control de acceso (físico y lógico) correspondientes considerando:

- ***La entrega de su Carnet y tarjetas de acceso físico.***
- ***Asignación de las cuentas de correo electrónico.***
- ***Concediendo los permisos de acceso a servicios, aplicativos y recursos compartidos.***
  La asignación del puesto de trabajo, los dispositivos y equipos.

Cuando finalice su contrato laboral los derechos de acceso de todos los empleados, contratistas y proveedores a las instalaciones de procesamiento de información se eliminan inmediatamente después de la terminación del trabajo o se ajustan al cambiar. Para más información, remitirse a los documentos AT-PL-40 Política de Control de Acceso y IT-N-03 Norma control de acceso

5. POLÍTICA DE TELETRABAJO, TRABAJO EN CASA Y ACCESO REMOTO.

Atlantic QI establecerá los controles necesarios para proteger la confidencialidad, integridad, disponibilidad y privacidad de los activos de información en entornos de teletrabajo, en cumplimiento con la normativa vigente que regula y promueve el teletrabajo a nivel nacional y territorial, tales como la Ley 1221 de 2008, el Decreto Reglamentario 884 de 2012 del Ministerio de Trabajo, el Decreto 1227 de 2022 y el Decreto Distrital 050 de 2023.

Las medidas buscan garantizar el uso seguro de las tecnologías de la información mediante permisos, autenticación, y conexiones seguras, considerando la seguridad física y tecnológica. La protección de la información es clave, sin importar la modalidad de trabajo, y los equipos deben cumplir con los estándares de seguridad en su instalación y configuración. En concordancia con lo anterior, Atlantic QI debe:

- ***a) Otorgar los permisos de acceso necesarios a los usuarios que trabajen bajo las modalidades de teletrabajo, trabajo en casa o acceso remoto, de acuerdo con su rol y los activos de información que gestionan.***
- ***b) Acceso seguro: Para las credenciales de acceso se utilizarán contraseñas robustas y el doble factor de autenticación siempre que sea posible, forzando su cambio periódicamente.***
- ***c) Mantener un control sobre los usuarios que desempeñan sus actividades en estas modalidades.***
- ***d) Monitorear y hacer seguimiento a las conexiones remotas a los servicios corporativos.***
- ***e) Sensibilizar a los usuarios sobre cómo mitigar los riesgos asociados a la seguridad de la información y las consecuencias de posibles incidentes.***
- ***f) Habilitar una conexión segura a través de VPN cuando sea necesario.***
- ***g) Realizar la configuración de los equipos previamente por el personal de soporte de la organización (sistema operativo, antivirus, control de actualizaciones)***

Por su parte, los usuarios deben:

- ***h) Aplicar las políticas de seguridad de la información establecidas y reportar cualquier anomalía o actividad sospechosa que pueda comprometer el equipo o la información a la que tienen acceso, a través de la mesa de ayuda.***
- ***i) Realizar las funciones únicamente en el lugar previamente validado por la organización.***
- ***j) Implementar medidas de seguridad de la información en el lugar donde se esté trabajando de manera remota (teletrabajo, trabajo en casa o acceso remoto), para evitar el acceso accidental a la información corporativa por parte de otras personas; esto incluye configurar contraseñas y cuentas de usuario, así como activar el bloqueo automático por inactividad.***

Recomendaciones de seguridad para el uso de equipos portátiles (Si aplica):

- ***a) Contar con un espacio adecuado en casa que minimice el riesgo de pérdida de información por accidentes.***
- ***b) Utilizar cables de seguridad para asegurar el equipo.***
- ***c) Evita transportar el portátil si no es necesario, especialmente en transporte público, y nunca dejarlo desatendido. En caso de robo o pérdida, notifica de inmediato al responsable de Seguridad física. Usar un maletín adecuado que proteja el equipo en caso de desplazamiento.***
- ***d) No consumir líquidos cerca del equipo, y aplicar la política de Escritorio y Pantalla Limpio. Para más información, remitirse al AT-PL-37 Política de Escritorio Limpio.***
- ***e) Utilizar contraseñas seguras que incluyan números, letras y caracteres especiales cuando el sistema lo permita; asegurarse de cambiarlas periódicamente y mantenerlas para uso personal, conforme a la política de Control de Acceso. Para más información, remitirse al AT-PL-40 Política de Control de Acceso***
- ***f) Asegurarse de cerrar correctamente todas las conexiones con servidores y páginas web, utilizando, siempre que sea posible, las opciones de "desconectar" o "cerrar sesión".***
- ***g) Realizar copias de seguridad de forma periódica de la información manejada en los equipos utilizados para el teletrabajo, trabajo en casa, trabajo remoto, usando los medios de almacenamiento proporcionados por la Organización.***
- ***h) Evitar enviar archivos con información de la organización y/o de sus clientes mediante medios no oficiales o no institucionales como WhatsApp, Dropbox, WeTransfer, correos gratuitos, etc.***
- ***i) Cerrar la sesión del dispositivo cuando no esté en uso, tanto en casa como en espacios públicos.***
- ***j) Mantener el sistema operativo actualizado con los últimos parches de seguridad liberados por el fabricante, habilitando la actualización automática cuando sea posible.***
- ***k) Mantener actualizado el software antivirus para prevenir infecciones por virus o software malicioso, realizando escaneos regulares y habilitando la verificación automática del antivirus.***
- ***l) No gestionar información de la organización en equipos personales o que no estén dentro del dominio de Atlantic QI.***
- ***m) No instalar programas o extensiones de navegadores de fuentes no confiables, ya que podrían contener malware que comprometa el dispositivo y la información sensible.***
- ***n) Está prohibido que el usuario haga cambios en el hardware, instale software o modifique la configuración del equipo sin autorización del departamento competente.***
- ***o) Si se sospecha la infección por virus u otro software malicioso, se debe notificar a la mayor brevedad posible al personal técnico responsable.***
- ***p) Los equipos de cómputo para usuarios en modalidad de teletrabajo, trabajo en casa, trabajo remoto, deben contar con las siguientes características:***

- ✓ ***Tener un sistema operativo y aplicaciones de trabajo licenciadas.***
- ✓ ***Tener un Software de antivirus legal, con la base de firmas actualizada.***
- ✓ ***Si es un portátil y el sistema operativo cuenta con la opción de cifrado, se debe cifrar el disco duro donde se trabaja con la información de la entidad.***
- ✓ ***Activar el bloqueo automático por inactividad.***
- ✓ ***Manejar cuentas de usuario independientes.***

6. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

Atlantic QI asignará dispositivos móviles corporativos (Teléfonos móviles, Smart Phones) a sus empleados cuando sea necesario para sus funciones, sujeto a la disponibilidad y con la aprobación previa de su jefe inmediato y la dirección del área, además de la autorización del jefe de Gestión de Activos.

6.1. LINEAMIENTOS PARA USO DE DISPOSITIVOS MÓVILES

- ➢ ***Los dispositivos móviles de Atlantic QI, como teléfonos y tabletas, son herramientas de trabajo que deben usarse exclusivamente para facilitar la comunicación entre empleados. La administración y control de estos dispositivos son responsabilidad del área administrativa.***
- ➢ ***Los usuarios solo deben utilizar aplicaciones autorizadas y configuradas por personal autorizado.***
- ➢ ***La configuración inicial de los dispositivos y de las cuentas de correo corporativo será realizada únicamente por los equipos de IT. Microsoft Teams es el sistema de mensajería instantánea autorizado para estos dispositivos.***
- ➢ ***El uso de WhatsApp Web en los PCs de Atlantic QI está prohibido para líneas telefónicas personales, especialmente para enviar información clasificada como secreta o confidencial (por ejemplo: bases de datos, datos personales, información de clientes, entre otros) perteneciente a Atlantic QI o a sus partes interesadas.***
- ➢ ***El uso de WhatsApp Web se permite solo en teléfonos corporativos con permisos autorizados, que deben ser solicitados formalmente al proceso de Seguridad de la Información y aprobados por la dirección del área correspondiente, garantizando el cumplimiento de las políticas de seguridad. Excepciones: Los trabajadores en cargos de dirección o de confianza y/o manejo (directores, jefes, gerentes de cuentas, supervisores, coordinadores y asistentes), debido a su responsabilidad en la operación de Atlantic QI, deben utilizar la herramienta WhatsApp de manera permanente, adecuada y acorde a su rol.***
- ➢ ***Los sistemas de mensajería en dispositivos móviles corporativos de Atlantic QI deben usar cifrado de extremo a extremo.***
- ➢ ***Los dispositivos deben tener protección con contraseña, bloqueo automático, borrado remoto, cifrado de almacenamiento y solo deben usar la tarjeta SIM asignada por la organización, sin transferirla a otros equipos.***
- ➢ ***En caso de pérdida o hurto del dispositivo móvil, se debe notificar de manera inmediata al proceso de Seguridad Física, Seguridad de la Información y Gerencia Administrativa.***

- ***Los usuarios de dispositivos móviles corporativos no pueden cambiar configuraciones ni desinstalar software, solo aceptar actualizaciones.***
- ***Deben mantener desactivadas las redes inalámbricas (WiFi), infrarrojos y Bluetooth, y evitar redes públicas.***
- ***Para instalar aplicaciones adicionales, deben solicitarlo a través de su jefe y obtener la aprobación del Comité de Seguridad de la Información.***

6.2. PERFILES CONFIGURACIÓN DE ACCESO A CORREO ELECTRÓNICO CORPORATIVO EN DISPOSITIVOS MÓVILES PERSONALES.

- ***El acceso a correo electrónico institucional y otros servicios de ATLANTIC QI en dispositivos móviles personales solo se configura para empleados, previa firma de un acuerdo de confidencialidad.***
- ***Al desvincularse, los empleados deben devolver todos los activos y documentar sus conocimientos. Antes de reasignar dispositivos, se debe verificar que no contengan información organizacional de otros usuarios.***
- ***Está prohibido instalar juegos, imágenes, música, videos no corporativos, y visitar sitios web con baja seguridad en los dispositivos móviles asignados.***

7. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

7.1. Custodia de documentos y medios de almacenamiento:

- ***Todos los documentos, notas adhesivas, CD, dispositivos USB y cualquier otro medio de almacenamiento deben ser debidamente custodiados y, cuando no estén en uso, almacenados en lugares seguros (por ejemplo, archivadores bajo llave).***
- ***Al finalizar la jornada laboral o durante ausencias prolongadas, ningún documento o carpeta debe quedar visible en el escritorio.***

7.2. Bloqueo de estaciones de trabajo:

- ***Los usuarios deben bloquear su estación de trabajo cada vez que se ausenten de su puesto, utilizando la función de bloqueo de pantalla.***
- ***Las estaciones de trabajo deberán configurarse para bloquearse automáticamente tras un periodo definido de inactividad. Esta configuración será gestionada y controlada centralmente por la Dirección de IT a través del Directorio Activo.***

7.3. Gestión de la pantalla de inicio:

- ***La pantalla de inicio de las estaciones de trabajo debe mantenerse libre de archivos, con excepción de los accesos directos a las aplicaciones necesarias para el desempeño de las funciones del usuario.***

7.4. Impresión y manejo de documentos confidenciales:

- ***Los documentos confidenciales impresos deben ser recogidos de inmediato y no dejarse desatendidos en la impresora o en procesos comunes.***
- ***Los empleados deben asegurarse de que los documentos confidenciales estén resguardados cuando no estén en uso, y ser destruidos de forma segura cuando ya no sean necesarios, siguiendo los procedimientos establecidos.***

7.5. Responsabilidades

- ***Todos los empleados son responsables de cumplir con esta política y de reportar cualquier incidente de seguridad o incumplimiento.***
- ***La Dirección de IT es responsable de la gestión técnica de los controles de bloqueo automático y el cumplimiento de las configuraciones establecidas en el Directorio Activo.***

8. POLÍTICA PARA EL USO DE EQUIPOS PORTÁTILES EN ATLANTIC QI

Todo empleado de Atlantic QI debe recibir los recursos tecnológicos necesarios para el desempeño de sus funciones. Al ingresar a la organización, se le asignará un equipo de cómputo (PC o portátil), y deberá firmar el formato establecido para tal fin, y el acuerdo de confidencialidad y buen uso del recurso tecnológico.

8.1. Uso de Equipos Portátiles Personales

Solo está permitido el uso de los equipos portátiles asignados por la empresa para llevar a cabo las funciones laborales. En situaciones excepcionales, si se requiere el uso de un equipo portátil personal, se deberá seguir el siguiente procedimiento:

- ✓ ***El solicitante deberá presentar una solicitud formal que justifique la necesidad del uso de su equipo personal.***
- ✓ ***La solicitud debe contar con la aprobación del jefe inmediato y de la dirección de la dependencia involucrada.***

- ✓ ***La solicitud debe ser escalada a la Dirección de IT y al proceso de Seguridad de la Información para su análisis, revisión y aprobación, siempre y cuando no se incurra en incumplimientos contractuales o violación de políticas de seguridad de la información.***

8.2. Requisitos y Condiciones para el Uso de Equipos Personales

En caso de aprobarse la solicitud, el equipo deberá ser sometido a una revisión técnica por parte del proceso de Soporte de IT para verificar su estado y asegurar que cumpla con los requisitos mínimos de seguridad.

El uso de equipos personales deberá cumplir con las políticas y controles establecidos por Atlantic QI, incluyendo las siguientes medidas:

- ***Instalación de software antivirus y de protección actualizado.***
- ***Conexión obligatoria a través de la red VPN corporativa.***
- ***Cumplimiento de los requisitos de cifrado para la protección de datos sensibles.***

Está estrictamente prohibido descargar o almacenar información corporativa en dispositivos personales. Los equipos personales estarán sujetos a auditorías periódicas para verificar el cumplimiento de estas disposiciones.

8.3. Responsabilidades y Consideraciones

El empleado que utilice un equipo personal asume la responsabilidad de proteger los activos de información a los que tenga acceso. El uso de la información estará limitado exclusivamente al desarrollo de las funciones laborales dentro de la empresa.

En caso de incumplimiento de esta política, se podrán tomar medidas disciplinarias, incluyendo la revocación del permiso para utilizar equipos personales y acciones adicionales según las normativas internas.

9. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN SOBRE LA GESTIÓN DE PROYECTOS

La gestión de proyectos en Atlantic Quantum Innovations S.A.S. contempla los aspectos relacionados con la seguridad de la información asegurando la identificación y tratamiento de los riesgos implícitos en cada proyecto independiente de su categoría y alcance. Para tal fin se incluyen como parte integral de todo proyecto los puntos descritos a continuación:

a) Integración de la seguridad desde el inicio: La seguridad de la información debe ser una parte integral de la gestión de proyectos desde la fase de planificación, incluyendo la evaluación de riesgos, asignación de recursos y definición de roles.

b) Alineación de los objetivos del Proyecto con la política de Seguridad de la Información: se debe asegurar que los objetivos del proyecto no vayan en contravía de la política de la seguridad de la información.

c) ***Asignación de Roles y Responsabilidades de Seguridad en el Proyecto:*** Se ***deben*** definir y asignar claramente las responsabilidades en materia de la seguridad de la información a los roles especificados definidos en la matriz RACI dentro del equipo de cada proyecto.

d) Evaluación y Gestión de Riesgos de Seguridad: Durante todo el ciclo de vida del proyecto, se deben evaluar y mitigar los riesgos relacionados con la información, aplicando controles específicos donde sea necesario.

e) Documentación y Procedimientos Específicos para el Proyecto: Documentar los procedimientos de seguridad aplicables al proyecto y garantizar su cumplimiento.

10. GESTIÓN DE LOS ACTIVOS

Atlantic Quantum Innovations S.A.S. protege la información de la cual es propietaria o que tiene bajo su custodia según la naturaleza de la información y la exposición al riesgo para sus partes interesadas frente al acceso inapropiado o no deseado, la divulgación o la destrucción.

Establece métodos de protección para la propiedad legal del contenido de cualquier documento (físico, electrónico y digital) que se genere, obtenga, adquiera, transforme o controle durante el desarrollo de sus funciones.

El grado de protección provisto se relaciona directamente con la exposición al riesgo, independientemente de los medios de información. El grado de protección que se brinda a la información es consistente de principio a fin, incluida las actividades de creación, ***el manejo, el procesamiento, el almacenamiento y la eliminación.***

Atlantic Quantum Innovations S.A.S., se compromete mediante los líderes de los procesos y responsables, a identificar y proteger los activos de información considerando registrar aspectos tales como su tamaño, ubicación, servicios o departamentos a los que pertenecen, quienes son sus responsables, etc. Atlantic Quantum Innovations S.A.S. asegura que la información se clasifique, maneje y elimine de manera segura. El líder de seguridad de la información creará procedimientos para proteger los datos electrónicos y en papel. La empresa promueve el uso y almacenamiento mínimos de datos confidenciales para reducir riesgos.

Atlantic Quantum Innovations S.A.S. se adhiere estrictamente a la política de que los datos de tarjetas de pago solo se almacenan para completar la transacción y no más allá del tiempo necesario para el procesamiento de contratos. Nunca almacenará información protegida, como PII, PHI, CVV/CVC, CVV2/CVC2 o PIN, después de la autorización de la tarjeta.

Así mismo, es necesario tener en cuenta los siguientes lineamientos:

- ***Los responsables de los activos de información deben asegurarse de que los documentos clasificados como secretos cuenten con una versión que incluya solo las secciones aptas para su divulgación.***

- ***Se debe garantizar que los activos de información críticos estén ubicados en áreas seguras y protegidos contra posibles amenazas que puedan comprometer su uso adecuado, disponibilidad y confidencialidad.***
- ***Los activos de información críticos en formato digital deben estar protegidos mediante contraseñas.***
- ***Es esencial implementar controles o medidas basadas en la evaluación de los activos de información y los riesgos asociados.***
- ***Los empleados deben almacenar la información digital de la organización en las ubicaciones designadas para el respaldo de dicha información.***
- ***Etiquetado de la información.***

Los documentos secretos o clasificados serán manejados, preparados, copiados y distribuidos exclusivamente al personal autorizado. Se asignará un espacio físico adecuado para archivarlos, siguiendo la codificación con los lineamientos de gestión documental de Atlantic QI.

11. POLÍTICA DE CONTROL DE ACCESO

Atlantic Quantum Innovations S.A.S. prioriza la gestión segura de la información y la protección de datos personales, asegurando que solo personas autorizadas manejen estos activos. La organización definirá directrices para la creación de usuarios y contraseñas, asignación de derechos de acceso, y accesos privilegiados, siguiendo el principio de mínimo necesario. También implementará mecanismos de autenticación, revisará derechos de acceso periódicamente y ajustará o cancelará accesos en caso de suspensión o finalización de relaciones contractuales.

El acceso a los sistemas de información debe gestionarse independientemente del entorno en que se encuentren, ya sea de desarrollo, pruebas, preproducción o producción.

El derecho de acceso a los sistemas de información y centros de procesamiento de datos, independientemente de su naturaleza, conlleva una gran responsabilidad para el personal autorizado, por lo que este derecho es personal e intransferible, estando prohibido cederlo a terceros.

Los empleados, contratistas, proveedores de Atlantic Quantum Innovations S.A.S., no deben eludir ninguno de los controles de acceso que se han implementado.

Se recuerda que, en Colombia, el acceso no autorizado o fuera de lo acordado a los sistemas de información puede ser considerado un delito informático según lo establecido en la Ley 1273 de 2009.

12. POLÍTICA DE ALMACENAMIENTO EN LA NUBE Y CARPETAS COMPARTIDAS

a) ***El almacenamiento en la nube permite guardar y crear documentos, compartirlos con otros usuarios y tiene espacios personales y compartidos según el cargo. Todo contenido publicado o distribuido mediante OneDrive o SharePoint debe cumplir con la normativa de protección de datos personales.***

b) ***El contenido almacenado en las carpetas compartidas de Google Drive debe incluir únicamente documentos finales o aprobados. Las carpetas en cuentas personales pueden contener documentos de trabajo o finalizados. No se debe transferir información personal a estas carpetas, salvo que sea soporte de una actuación pública o parte de la gestión contractual con Atlantic QI.***

c) ***Está prohibido utilizar las cuentas de OneDrive y los servicios asociados para actividades personales, financieras, comerciales o publicitarias.***

d) ***Los usuarios son responsables de todas las acciones realizadas desde sus cuentas de OneDrive.***

e) ***Es una infracción grave permitir o facilitar el acceso a la cuenta a personas no autorizadas por Atlantic QI o su representante legal.***

f) ***La unidad compartida de OneDrive permite almacenar, buscar y acceder a archivos en un espacio común gestionado por un grupo, donde la información pertenece al grupo y no a un usuario individual.***

g) ***La información Organizacional manejada por las dependencias debe registrarse en la unidad compartida asignada a cada dependencia.***

h) ***La estructura de las carpetas y archivos en la unidad compartida estará a cargo de una persona designada por el jefe de cada dependencia.***

i) ***Cualquier modificación en el contenido de las carpetas o archivos debe ser gestionada por la dependencia a través del gestor designado.***

j) ***En esta unidad solo debe almacenarse información de Atlantic QI.***

k) ***Los administradores de cada dependencia son responsables de mantener actualizada y organizada la información en las carpetas, eliminando versiones preliminares o aquellas que no sean definitivas.***

l) ***Se deben asignar permisos sobre carpetas compartidas a grupos de usuarios.***

m) ***Es necesario habilitar la protección de los archivos de registro de eventos.***

n) ***Las cuentas de administración deben ser nombradas de manera que no se asocien fácilmente al administrador, para evitar exponer los privilegios de dicho usuario.***

13. POLÍTICA DE COPIAS DE RESPALDO DE SEGURIDAD DE LA INFORMACIÓN.

Atlantic QI protegerá su información y la de sus partes interesadas mediante mecanismos y controles periódicos que aseguren la confidencialidad, integridad y disponibilidad de la información. El proceso de Soporte debe realizar backups según la periodicidad establecida, y el proceso de Seguridad de la información verificará el cumplimiento mediante revisiones regulares. La información crítica debe estar

cifrada y respaldada en una ubicación diferente a las instalaciones originales, con controles de seguridad física y ambiental adecuados.

14. POLÍTICA DE CRIPTOGRAFÍA

Los controles criptográficos son clave en la protección de datos de Atlantic Quantum Innovations S.A.S. El gerente de Seguridad de la Información o quien haga sus veces debe establecer y mantener un programa de controles criptográficos alineado con ***las directrices*** de clasificación de información de la organización a través del cual se definen los estándares de encriptación, gestión de claves y validación de identidad, y asegura la protección de la información en tránsito y almacenamiento. Las claves se almacenan conforme a las directrices establecidas en las pautas de gestión de claves de cifrado de Atlantic Quantum Innovations S.A.S. y en el procedimiento IT-P-29 "Procedimiento de Cifrado de Información".

15. SEGURIDAD FÍSICA Y MEDIOAMBIENTAL

Atlantic Quantum Innovations S.A.S. protege las áreas de procesamiento y almacenamiento de información sensible, así como la infraestructura de servidores, mediante controles de acceso físico y métodos de protección para prevenir pérdidas o daños. Implementa controles de seguridad físicos, ambientales y administrativos para reducir riesgos de fallas o daños a la infraestructura debido a factores internos, externos, ambientales o de uso.

Cuando sea posible, todos los recursos de información deben residir en un entorno protegido. Se deben implementar controles de seguridad físicos y administrativos en cada instalación para proteger contra el acceso no autorizado.

Atlantic QI se compromete a gestionar constantemente sistemas de vigilancia y seguridad perimetral, así como planes de mantenimiento para la salvaguarda de un ambiente seguro e idóneo para las actividades desarrolladas en cada una de sus sedes. El acceso físico a instalaciones, centros de datos, sistemas, redes y datos en Atlantic Quantum Innovations S.A.S. está limitado a las personas autorizadas que requieren acceso para realizar las tareas asignadas y se realiza mediante control de acceso biométrico (huella o tarjeta inteligente).

Los visitantes a las instalaciones de Atlantic QI deben cumplir con los procedimientos internos y las normas establecidas con la empresa de vigilancia. Los colaboradores deben proteger sus identificaciones y credenciales de acceso, y serán responsables de cualquier acto realizado con su identificación en caso de negligencia o descuido.

Está restringido el ingreso de equipos personales (PC o Portátiles) o cualquier dispositivo de almacenamiento de información en las sedes de Atlantic QI.

El personal de vigilancia no está autorizado para guardar equipos tecnológicos (Portátiles Personales, PC), objetos personales. En caso de requerirse el ingreso de estos dispositivos debe ser solicitado previamente a la Dirección de IT y al área de Seguridad Física para su revisión y su aprobación.

Además de los controles de acceso, se implementan salvaguardas físicas para proteger sistemas sensibles y datos contra; incendios, robos u otros peligros.

16. SEGURIDAD DE LAS OPERACIONES

Existe un Sistema de gestión de la calidad (SGC) documentado en la Organización que detalla los procedimientos operativos relacionados con todos los negocios y funciones dentro de la Organización. El SGC está alojado en el portal central de Intranet (AIBrain - https:// http://conocimiento.aib.com.co/login.php) de la organización. Todos los empleados de Atlantic Quantum Innovations S.A.S., tienen acceso al AIBrain.

Los procedimientos operativos para las actividades de mantenimiento del sistema y el mantenimiento de las instalaciones de procesamiento de información, incluidos los sistemas informáticos operativos, equipos de telecomunicaciones, redes y sistemas de aplicaciones, se documentan y mantienen para garantizar operaciones seguras y eficientes. Estos procedimientos operativos son documentos formales y cualquier cambio en los procedimientos se realiza solo después de la autorización del comité de seguridad de la información conformado por: presidente, director de IT, gerente de telecomunicaciones, gerente de infraestructura tecnológica, gerente de seguridad de la información, jefe de seguridad de información. Este comité se reúne con una periodicidad mensual.

17. SEGURIDAD DE LAS COMUNICACIONES

La seguridad de las comunicaciones se preocupa por garantizar la integridad y disponibilidad de la información y los servicios, y mantener la confidencialidad de la información. Para garantizar que las comunicaciones sean seguras:

- Todos los dispositivos en la red de Atlantic Quantum Innovations S.A.S., deben ser autenticados con una contraseña segura.

- Los servidores que contienen datos restringidos deben estar separados del acceso público.

- Los datos o la información restringidos deben cifrarse cuando se envían a través de redes públicas.

18. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA

La política de adquisición de aplicaciones, desarrollo y mantenimiento de sistemas de información establece los siguientes lineamientos:

1. Todo software nuevo debe ser desarrollado cumpliendo con los estándares de la industria y aplicando técnicas de codificación segura.

2. El desarrollo de nuevas aplicaciones debe seguir una metodología formal, como la metodología ágil SCRUM o cualquier otra que sea adoptada oficialmente por la organización.

3. Las revisiones de seguridad son obligatorias y se realizan en las fases de recopilación de requerimientos, desarrollo y pruebas de los proyectos, garantizando que se identifiquen y mitiguen riesgos de seguridad antes de la implementación en producción.

4. Los desarrolladores deben recibir capacitación continua en prácticas seguras de codificación y aplicar principios de seguridad en el ciclo de vida de las aplicaciones, siguiendo las políticas y estándares de la organización.

19. RELACIONES CON LOS PROVEEDORES

a) Antes de que un proveedor acceda a los activos de Atlantic Quantum Innovations S.A.S., se deben acordar y documentar los requisitos de seguridad de la información para mitigar riesgos asociados con dicho acceso, siguiendo las directrices establecidas.

b) Se debe asegurar el cumplimiento de las siguientes indicaciones en el relacionamiento con proveedores de servicios de IT

c) Se debe definir y documentar los requisitos de seguridad de la información en los contratos.

d) Implementar y supervisar controles de seguridad relacionados con proveedores.

e) Establecer acuerdos de no divulgación de la información y asegurar su cumplimiento.

f) Identificar y aplicar controles adecuados para administrar el acceso de proveedores.

g) Establecer procesos para la revisión y monitoreo regular de los servicios de proveedores.

h) Implementar y mantener controles de inteligencia de amenazas en el acceso de proveedores.

i) Comunicación de Amenazas y Vulnerabilidades por Parte de los Proveedores:

Atlantic Quantum Innovations S.A.S. requiere que todos los proveedores informen de manera oportuna cualquier amenaza, vulnerabilidad o incidente de seguridad que pueda tener un impacto en la seguridad de los activos de la organización a través de los canales establecidos. Esto incluye, pero no se limita a:

a) Identificación de Amenazas: Los proveedores deben comunicar de inmediato cualquier amenaza potencial que identifiquen en sus entornos o en su cadena de suministro que pueda comprometer la seguridad de la información o de los servicios de Atlantic Quantum Innovations S.A.S.

b) Notificación de Incidentes: En caso de que un proveedor detecte un incidente de seguridad que pueda afectar a la organización, debe notificarlo de manera inmediata desde su detección.

c) Actualización de Vulnerabilidades: Los proveedores están obligados a mantener informada a la organización sobre cualquier vulnerabilidad detectada en los sistemas, aplicaciones o servicios que estén bajo su responsabilidad y que puedan representar un riesgo para Atlantic Quantum Innovations S.A.S.

d) Plan de Mitigación: Además de la notificación, los proveedores deben proporcionar un plan de acción y mitigación para abordar la amenaza o vulnerabilidad identificada, así como los tiempos estimados para su resolución.

20. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La respuesta a incidentes es la etapa final de un proceso que revisa eventos para determinar si han causado violaciones del sistema o compromisos de datos sensibles. Se debe designar un equipo de respuesta y mantener un plan para gestionar eficazmente los incidentes, contemplando:

1. Coordina todos los aspectos de la respuesta a incidentes y la notificación.
2. Monitorea y distribuye alertas de seguridad.
3. Proporciona un informe posterior a la acción con recomendaciones de mejora.
4. Proporciona capacitación sobre la seguridad, el fraude, el desperdicio y el abuso y el reporte de incidentes.
5. Proporciona un informe anual con métricas completas de eventos relacionados con la seguridad.

21. GESTIÓN DE LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CONTINUIDAD DEL NEGOCIO

Atlantic QI posee un BCP el cual tiene como propósito asegurar la reanudación de sus actividades oportuna de las operaciones, en caso de ocurrencia de eventos de interrupción de operaciones, que puedan poner en peligro la reputación y permanencia de la organización, definiendo procedimientos y estrategias para ejecutar en los momentos de interrupción y preparando al personal para una respuesta adecuada en la menor cantidad de tiempo posible considerando los SLAS definidos con sus clientes.

22. CUMPLIMIENTO

El Programa de seguridad de la información de Atlantic Quantum Innovations S.A.S. está diseñado para cumplir con las obligaciones legales, reglamentarias o contractuales de todos los empleados, contratistas y proveedores con acceso a las redes, infraestructura, equipos o instalaciones de Atlantic Quantum Innovations S.A.S., que contienen información confidencial y restringida propia o del cliente; así como activos de información restringida. Esto incluye todos los cumplimientos con HIPAA (Ley de Responsabilidad y Portabilidad del Seguro de Salud de 1996), CMS (Centros de Servicios de Medicare y Medicaid), PCI (Información de Tarjeta de Pago), ISO 27001 y demás normativas aplicables.

23. PRIVACIDAD Y CONFIDENCIALIDAD

Atlantic QI cuenta con una política de protección de datos personales e implementa controles técnicos y organizativos para proteger los datos de los usuarios según la normativa vigente (Ley 1581 de 2012 y Decreto 1377 de 2013), y demás normativas vigentes. La información recopilada solo se usará para los fines autorizados, con el consentimiento del titular, salvo excepciones legales.

Los datos personales incluyen:

1. Identificación: Información como nombre, número de identificación, fecha y lugar de nacimiento, firma, huella, características biométricas (ADN, iris, geometría facial), fotos y videos, etc.

2. Ubicación: Dirección, teléfono, correo electrónico y otros datos de contacto relacionados con actividades comerciales o privadas, etc.

3. Contenido socioeconómico: Información como nivel socioeconómico, datos financieros, historial laboral, nivel educativo y bienes patrimoniales, etc.

4. Datos sensibles: Información sobre salud (diagnósticos, tratamientos), afiliación a sindicatos u organizaciones, creencias religiosas, filosóficas o políticas, orientación sexual, origen étnico, y situaciones de vulnerabilidad (discapacidad, pobreza, víctimas de violencia), etc.

24. CUMPLIMIENTO

Atlantic QI sancionará cualquier violación de esta política y su cumplimiento se verificará a través de varios métodos, que incluyen, entre otros, recorridos periódicos, monitoreo de video y auditorías internas y externas, o cualquier otra metodología aplicable.

25. APLICACIÓN

Las violaciones de las políticas de seguridad de la información de Atlantic Quantum Innovations S.A.S. resultarán de acuerdo con la gravedad de la falta evidenciada en la aplicación de medidas disciplinarias, la finalización de la relación laboral y la responsabilidad civil y penal.

26. COMUNICACIÓN

Estas políticas deben ser publicadas en el aplicativo adoptado por Atlantic QI como repositorio del Sistema de Gestión, Intranet, Pagina web y debe ser comunicada a todos los empleados, proveedores y usuarios de Atlantic QI a través de las herramientas de comunicación interna y externa adoptadas por la organización, encaminadas a la apropiación de esta política.

27. REFERENCIAS A OTRAS POLÍTICAS Y PROCEDIMIENTOS INTERNOS Y DOCUMENTOS EXTERNOS

1. CMS: https://www.cms.gov/
2. HIPAA: http://www.hhs.gov/ocr/privacy/
3. Payment Card Industries: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-21.pdf?agreement=true&time=1547651733472
4. ISO 27001: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
5. Listado de individuos y entidades excluidas (LEIE) de la oficina del Inspector General (OIG) del Departamento de Salud y Servicios Humanos: https://exclusions.oig.hhs.gov/Default.aspx
6. Listado de exclusión del Sistema de Gestión de Premios (SAM) de la Administración de Servicios Generales (GSA): https://www.sam.gov/SAM/pages/public/searchRecords/advancedPIRSearch.jsf

CONTROL DE REVISIÓN:

Ver. Número	Capítulo	Fecha	Descripción
8.0	1.0	Marzo 16 de 2023	Se complementa la información detallada de los objetivos del negocio en la compañía.
9.0	1,2	Agosto 24 de 2023	Se elimina lo siguiente: Objetivo del documento y cuadro de definiciones. Se actualizan lo siguientes numerales: Resumen del documento, la declaración de la política (1), y objetivos de SGSI, (2) Dispositivos Móviles y Trabajo a distancia (A.6.2), Concientización, educación y capacitación en seguridad de la información A8 y Administración de Activos (A.9).
10.0	Todos	10 de septiembre 2024	Se actualiza toda la política.

CONTROL DE APROBACIONES:

Ver. Número	Actualizado por:	Verificado por:	Aprobado por:
8.0	**LISBETH OÑORO** Jefe de Seguridad de la Información **DARLYS ACOSTA P.** Tecnólogo de Soporte	**ARMANDO RODRIGUEZ** Director de IT	**LELIO SOTOMONTE** Presidente
9.0	**LISBETH OÑORO** Jefe de Seguridad de la Información **LINETH CAMARGO** Especialista Sistemas de Gestión	**JUAN SOLANO** Director de IT	**LELIO SOTOMONTE** Presidente
10.0	**LUZ SANTIAGO** Gerente de Seguridad de la Información **LINETH CAMARGO** Especialista Sistemas de Gestión	**SAMIR ARANA** Director de IT & Nuevos productos	**LELIO SOTOMONTE** Presidente