POLÍTICA

SEGURIDAD DE LA INFORMACIÓN

REVISADO POR:

JUAN SOLANO

Director de IT

APROBADO POR:

LELIO SOTOMONTE

Presidente

Código	AT-PL-36-V9
Fecha	Agosto 24 de 2023
Resumen	***El siguiente documento contiene la política del sistema de gestión de seguridad en la información de Atlantic Quantum Innovation 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. Asegurar la confidencialidad, integridad y disponibilidad de la información propia y de nuestros clientes.
2. Mantener la estabilidad y disponibilidad de las operaciones que gestionamos.
3. Generar valor al negocio de nuestros clientes.
4. Cumplir los requisitos ***legales, regulatorios y/o contractuales*** aplicables.

Para este fin nos soportamos en la implementación de controles estrictos de seguridad, el mejoramiento continuo de nuestros procesos, un recurso humano altamente motivado y competente y unos aliados de negocios alineados con nuestra visión de negocios.

Esta política será revisada y aprobada una vez al año con el fin de asegurar su adecuación y eficacia continua.

2. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN.

- Proteger los activos de información mediante la implementación de políticas, procedimientos y controles de seguridad necesarios para ***resguardar*** la infraestructura tecnológica de la organización.
- ***Prevenir y controlar*** los incidentes de seguridad de información para mantener la estabilidad y disponibilidad de las operaciones.
- Prevenir incumplimientos ***legales, regulatorios y/o contractuales*** a través del seguimiento continuo al cumplimiento de las políticas de seguridad y privacidad de la información.
- ***Mantener*** una cultura en seguridad de la información al interior de la empresa.
- Mantener la mejora continua del SGSI a través de la atención oportuna y eficaz de los planes de acción.

3. NORMAS DE SEGURIDAD DE LA INFORMACIÓN

A5. Políticas para Seguridad de Información

A.6.1.5 Seguridad de la información en 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:

1. Se definen y asignan las responsabilidades para la seguridad de la información a los roles especificados definidos en la matriz RACI de cada proyecto.
2. Se incluyen los objetivos de seguridad de la información en los objetivos de cada proyecto.
3. Se realiza una evaluación de riesgos de seguridad de la información en una etapa temprana del proyecto para identificar los controles necesarios.
4. Se incluye la gestión de seguridad de la información en todas las fases de la metodología de proyectos utilizada.

A.6.2 Dispositivos Móviles y Trabajo a distancia.

Las personas en posesión de computadores portátiles, laptops, tablets, entre otros dispositivos móviles y equipos transportables o medios de almacenamiento que contengan información no pública, deben asegurarse ***de que el activo* no** se quede sin supervisión en ningún momento, a menos que la información se haya salvaguardado adecuadamente. Estas personas asumen toda la responsabilidad por el equipo y los datos que este contiene.

Los usuarios deben tener especial cuidado al utilizar los dispositivos móviles, equipo transportables y medios de almacenamiento en lugares públicos para proteger la información de accesos no autorizados.

A.7 Seguridad de Recursos Humanos

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., apoya activamente la seguridad de la información dentro de la organización con un rumbo claro, el compromiso demostrado y la asignación explícita de responsabilidades.

Con el fin de reducir el riesgo de errores humanos, robos, fraudes, mal manejo de la información y mal uso de las instalaciones, la alta dirección a través de la dirección talento humano y experiencia interna, con la participación de sus procesos constitutivos, asegura el cumplimiento de los siguientes aspectos:

1. Se realizan verificaciones de antecedentes previas al empleo para garantizar que los candidatos se seleccionen adecuadamente.
2. 2Se ejecutan pruebas de detección adecuadas para cualquier persona en Atlantic Quantum Innovations S.A.S. que tenga acceso a las cuentas de Medicare y Medicaid, las exclusiones se verifican antes del inicio de la relación laboral y con una periodicidad mensual a partir de entonces en las siguientes bases federales de los EEUU: LEIE (List Excluded Individuals/Entities)/(Lista de personas / entidades excluidas), OIG (Office of Inspector General)/(Oficina del Inspector General) and GSA (General Services Administration) (Administración de Servicios Generales).
3. Se validan los antecedentes criminales en los portales del gobierno colombiano: Base de datos de la Procuraduría General de la Nación; Base de datos de la Contraloría General de la Nación y Base de datos de la Policía Nacional. Los procesos de verificación de antecedentes y verificación de

exclusiones se encuentran debidamente establecidos y documentados en el procedimiento de reclutamiento y selección y en la política de verificación de exclusiones para programas de salud en EE. UU.

Concientización, educación y capacitación en seguridad de la información

La capacitación inicial de concientización sobre la seguridad de la información es provista por ***los procesos de formación, Desarrollo organizacional y compras*** abordando las responsabilidades del usuario, los procedimientos y las mejores prácticas de seguridad de la información.

Todos los empleados y proveedores deben recibir la capacitación de concientización sobre seguridad de la información de Atlantic Quantum Innovations S.A.S. con una periodicidad anual. Los proveedores pueden proporcionar una prueba de capacitación al gerente administrativo de Atlantic Quantum Innovations S.A.S. para este caso el director de cumplimiento o su designado debe aprobar que la capacitación cumpla con los estándares de Atlantic Quantum Innovations S.A.S.

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

Es necesario asegurar que todos los usuarios estén conscientes de las amenazas y asuntos de seguridad de la información, y que estén equipados para respaldar la política de seguridad de la organización en el curso de su trabajo diario
Minimizar los daños causados por incidentes de seguridad y mal funcionamiento, y monitorear y aprender de dichos incidentes.
Garantizar que se firmen los formatos y autorizaciones requeridas por parte de todos los empleados, contratistas y proveedores antes iniciar con sus trabajos en las instalaciones de la organización.
Implementar un proceso disciplinario formal para manejar al personal cuando ocurre una violación de seguridad.
Los procesos de terminación laboral se encuentran debidamente establecidos en el procedimiento de vinculación y desvinculación laboral.

A.8 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. 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., debe garantizar que la información en todos los medios se clasifique, se maneje y se elimine de manera segura. El jefe de seguridad de la información desarrollará procedimientos y pautas para proteger la información mientras se procesa o almacena en forma electrónica o en papel. Atlantic Quantum Innovations S.A.S., fomenta el uso y almacenamiento mínimos de sus datos confidenciales para reducir el riesgo de que se comprometan los datos.

Este principio debe observarse rigurosamente en el tratamiento de todos los datos de tarjetas de pago procesados por Atlantic Quantum Innovations S.A.S. El almacenamiento de todos los datos de la tarjeta de

pago se guardará solo para completar la transacción de pago y no se almacenará durante más tiempo del que permita el procesamiento de los contratos. En ningún momento después de la autorización de la tarjeta, en ninguna circunstancia, Atlantic Quantum Innovations S.A.S. almacenará información de PII, PHI (o cualquier tipo de información protegida), para incluir datos de CVV / CVC, CVV2 / CVC2 y PIN de bloqueo de datos.

A.9 Control de Acceso

Atlantic Quantum Innovations S.A.S., otorga y proporciona la menor cantidad de acceso a los datos sobre una base de "necesidad de saber del negocio", "mínimo privilegio" y “mínimo necesario”. A los usuarios se les otorga una cantidad mínima de acceso requerido para cumplir con éxito sus requisitos de trabajo.

Los controles de acceso se establecen de acuerdo con el valor y la clasificación de los activos de información que se están protegiendo. El departamento de TI garantiza que todos los sistemas de autenticación y autorización apliquen los principios de "negar todo" para el control de acceso.

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

Se realizan pruebas y se supervisan los programas diseñados para determinar si los sistemas de control y sus componentes funcionan de la manera prevista y ofrecen un nivel aceptable de protección a medida que avanza el tiempo y la tecnología.

Se realizan revisiones gerenciales de los controles de acceso, como mínimo, anualmente.

“Los empleados de Atlantic Quantum Innovations S.A.S. acceden únicamente a la información relacionada con las funciones de su cargo. Los administradores de los sistemas de información deben seguir los estándares de configuración establecidos. Los contratistas acceden a la información necesaria para el desarrollo del objeto del contrato. Los empleados deben seguir las guías de contraseñas seguras al momento de seleccionar credenciales de autenticación fuertes y las guías de como los usuarios deben proteger sus credenciales de autenticación. Los empleados no deben reusar las contraseñas usadas anteriormente y deben cambiar sus contraseñas si ellos sospechan que sus contraseñas han sido comprometidas”

A.10 Criptografía

Los controles criptográficos desempeñan un papel importante en el sistema de controles que Atlantic Quantum Innovations S.A.S. emplea para proteger sus activos de datos. Con este fin, el jefe de Seguridad de la Información establece y mantiene un programa de controles criptográficos alineado con la política de clasificación de la información.

El programa de criptografía establece estándares para la fuerza de encriptación mínima de los datos en cada clasificación de datos, cuando los controles criptográficos son apropiados, la administración de claves de encriptación y la validación de la identidad de transmisión saliente.

Este programa aborda la información de extremo a extremo durante el tránsito y el almacenamiento, tanto dentro como fuera de las redes Atlantic Quantum Innovations S.A.S. que cumplen con todos los requisitos legales.

La administración de claves se implementa a un nivel acorde con la función crítica que cumplen estas claves. Las claves se almacenan de acuerdo con las pautas de administración de claves de cifrado de Atlantic Quantum Innovations S.A.S. La información se describe en el procedimiento IT-P-29 Procedimiento Cifrado de información.

A.11 Seguridad Física y medioambiental

Atlantic Quantum Innovations S.A.S. protege sus recursos de información a través de la implementación de controles de seguridad físicos, ambientales y administrativos "sólidos" diseñados para reducir el riesgo de falla física o de daños a la infraestructura debidos a riesgos ambientales.

Donde 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.

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).

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

A.12 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, jefe de seguridad de información. Este comité se reúne con una periodicidad mensual.

A.13 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.

A.14 Adquisición, desarrollo y mantenimiento del sistema

La política de adquisición de aplicaciones, desarrollo y mantenimiento de sistemas de información aborda los siguientes requisitos:

1. El nuevo software se desarrolla en base a los estándares de la industria y las técnicas de codificación segura.
2. El desarrollo de todas las aplicaciones nuevas debe seguir el ciclo de la metodología ágil SCRUM o cualquier otra adoptada por la organización.
3. Las revisiones de seguridad se llevan a cabo durante las fases de recopilación de requerimientos, desarrollo y pruebas de todos los proyectos antes de la implementación.
4. Los desarrolladores reciben capacitación y siguen prácticas seguras de codificación y principios básicos de seguridad de aplicaciones.

A.15 Relaciones con los proveedores

Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y documentarse antes de que el proveedor tenga acceso a los activos de Atlantic Quantum Innovations S.A.S. Asegurar que se ejecuten los acuerdos de no divulgación para proteger la información confidencial. Los controles apropiados se identifican y aplican para administrar el acceso del proveedor a los activos de información de la organización. Los controles de seguridad de la información para proveedores se abordan a través de los acuerdos con proveedores que consideran la cadena de suministro y el monitoreo regular de los servicios de los proveedores.

A.16 Gestión de Incidentes de seguridad de la información

La respuesta a incidentes es la etapa final de un proceso que escala los eventos a través de un proceso de revisión para determinar si un evento observado en un sistema de procesamiento de información podría haber causado una violación del sistema o un compromiso de datos sensibles. Se debe designar un equipo de respuesta a incidentes y mantener un plan para guiar efectivamente la respuesta a un incidente. El programa también:

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.

A.17 Gestión de los aspectos de seguridad de la información para la continuidad del negocio

Atlantic Quantum Innovations S.A.S. planifica, documenta e implementa procesos para contrarrestar las interrupciones del negocio, para proteger o mitigar razonablemente los procesos críticos de los efectos de las fallas de los sistemas u otras interrupciones y para facilitar su reanudación oportuna.

A.18 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.

4. CUMPLIMIENTO

El cumplimiento de esta política 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.

5. 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.

6. 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
7.0	4.0	Enero 24 de 2023	Se modifica numeral 4, se simplifican los objetivos de Seguridad de la Información.
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).

CONTROL DE APROBACIONES:

Ver. Número	Actualizado por:	Verificado por:	Aprobado por:
7.0	**LISBETH OÑORO** Jefe de Seguridad de la Información **JESUS DAVID DÍAZ** Ing. Seguridad de la Información	**ARMANDO RODRIGUEZ** Director de IT	**LELIO SOTOMONTE** Presidente
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