Política de Gestión de la Seguridad de Proveedores

Versión 1

Tabla de contenido

1. Objetivos

- Proteger la información confidencial mediante la implementación de controles adecuados en todas las interacciones y acuerdos con proveedores.
- Asegurar el cumplimiento de requisitos de seguridad por parte de los proveedores y su cadena de suministro, garantizando que sus prácticas y sistemas cumplen con las normativas y políticas de la organización.
- Mitigar riesgos asociados con la gestión de proveedores mediante la evaluación continua y el monitoreo de la seguridad de la información compartida o gestionada por terceros.
- Garantizar que se extiendan los controles de seguridad de la información que le apliquen al proveedor a toda su cadena de suministro.

2. Alcance

Aplica a todo el personal de Quantic Vision, tanto interno como externo; así como a las personas que directa o indirectamente prestan sus servicios profesionales dentro de la misma, y a toda la información obtenida, creada, procesada, almacenada o intercambiada dentro y desde la organización.

3. Políticas de seguridad de la información en las relaciones con proveedores

3.1. Para la selección del proveedor se debe seguir el procedimiento definido para tal fin, e implementar los controles de seguridad de la información que le correspondan.

3.2. Todos los proveedores y contratistas que manipulen información en el desarrollo de sus funciones deberán firmar un acuerdo de confidencialidad de la información, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información.

3.3. Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal a la Gerencia de Ingeniería, en concordancia con la política de control de acceso de Quantic Vision.

3.4. Las políticas y procedimientos de seguridad de la información de Quantic Visión deben ser aplicadas por los proveedores. Se debe incluir una cláusula contractual que

exija el cumplimiento de estas políticas y es responsabilidad del supervisor del contrato que sea monitoreada esta condición.

3.5. Se deben generar Acuerdos de Niveles de Servicio (ANS), Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con todos los proveedores. Estos acuerdos deben contener una responsabilidad civil y penal para proveedores y el monitoreo de su cumplimiento es responsabilidad del supervisor del contrato.

3.6. Los proveedores deben cumplir con el uso aceptable de los activos de información que queden bajo su responsabilidad, esto define acciones como almacenamiento, transmisión, impresión y procesamiento; de acuerdo con los lineamientos definidos para la Gestión de Activos de Información.

3.7. Todas las actividades realizadas en los sistemas de información de Quantic Vision, durante la ejecución del contrato, por parte de proveedores, deben ser monitoreadas por el líder del proceso a quien se le presta el servicio. En caso de evidenciar abuso en los accesos se debe informar inmediatamente a la Gerencia de Ingeniería.

3.8. El envío, copia o manipulación de información de propiedad de Quantic Vision por parte de los proveedores debe contar con la autorización escrita del Líder del proceso a quien se le preste el servicio.

3.9. Los accesos a los sistemas de información corporativa solo deben ser brindados a los proveedores o contratistas de Quantic Vision en caso de ser necesario para el cabal cumplimiento de las actividades a realizar.

3.10. Todo sistema externo utilizado por los proveedores para acceder a la información de Quantic Vision, debe ser autorizado por la Gerencia de Ingeniería.

3.11. Cualquier actividad realizada por un proveedor en los sistemas de información de Quantic Vision, debe ser monitoreada por la Gerencia de Ingeniería. En el caso que se identifiquen riesgos de seguridad sobre la información, inmediatamente será revocada su autorización y el sistema será bloqueado.

3.12. El software utilizado por cualquier proveedor o contratista debe ser legal y contar con su respectiva licencia que acredite su uso.

3.13. La información de Quantic Vision que haya sido accedida por sistemas externos, debe ser validada en su integridad, confidencialidad y disponibilidad antes del retiro del proveedor.

3.14. Realizar la gestión de vulnerabilidades de las plataformas que estén bajo su responsabilidad. Esto incluye el reporte oportuno a Quantic Vision de las vulnerabilidades identificadas y las medidas a implementar para mitigar los riesgos asociados.

3.15. El proveedor debe entregar a Quantic Vision, si aplica, la documentación que demuestre el cumplimiento de las políticas de seguridad de la información en toda la cadena de suministro que involucra los servicios contratados.

3.16. Para la ejecución de controles de cambios se deben seguir las directrices definidas a nivel contractual y el Procedimiento de Gestión de Cambios de la empresa.

3.17. Reportar los eventos de seguridad de la información de acuerdo con el Procedimiento de Gestión de Incidentes de Seguridad de la Información de Quantic Vision.

4. Continuidad de la operación para proveedores de servicios

4.1 El proveedor contará con un Plan de Continuidad de Negocio de acuerdo con el bien, servicio u obra adquirido por Quantic Vision; además si la empresa requiere el envío y resultado de las pruebas de este plan, debe ser suministrado sin inconveniente por el proveedor.

4.2 Cuando ocurra un evento de interrupción de los servicios prestados por el proveedor que sea imputable totalmente a éste, asegurará la prestación del servicio cumpliendo con el Tiempo Objetivo de Recuperación (RTO) requerido por el (los) proceso (s) de Quantic Vision según las necesidades expuestas en el documento de Análisis de Impacto al Negocio – BIA.

4.3 El proveedor deberá informar los datos de contacto y horarios de disponibilidad de los responsables que durante la vigencia del contrato atenderán situaciones críticas y de indisponibilidad de los servicios suministrados, y deberá garantizar que el recurso disponible para la atención cuente con los conocimientos técnicos requeridos.

5. Sanciones

El incumplimiento significa toda conducta de cualquier miembro de la Comunidad Empresarial de Quantic Vision que no respete las políticas. Entre los ejemplos de incumplimiento se incluyen, sin limitarse a estos:

a) Los colaboradores y/o partes interesadas que sean negligentes en la aplicación de medidas de seguridad y control dentro de la organización.

b) Una acción o inacción por parte de un colaborador y/o partes interesadas que contribuye a la violación de las normas orientadas al buen uso de la información.

c) Un colaborador y/o parte interesada que no resuelve o remite inmediatamente a una autoridad superior los problemas de seguridad de la información que sean detectados.

d) Los colaboradores y/o partes interesadas que no tomen las medidas correspondientes ante una queja o un incidente de seguridad.

e) Todos los miembros de la Comunidad Empresarial de Quantic Vision serán responsables de implementar las políticas y procedimientos de seguridad que se contemplan o son referenciados en este documento y sus complementarios.

f) Cualquier incumplimiento de las políticas y procedimientos de seguridad es considerado como falta disciplinaria por incumplimiento de las obligaciones y deberes del colaborador, y será sancionada según el reglamento interno de trabajo y/o proceso disciplinario de la empresa.

g) Los colaboradores temporales y de terceros que estén involucrados en incidentes de incumplimiento, pueden ver terminado su contrato de acuerdo con las condiciones que en este se han establecido.

6. Normatividad

- ISO 27001 – Sistemas de Gestión de Seguridad de la Información.

7. Anexos y documentos relacionados

- SGSI-MA-002 - Manual de políticas de seguridad de la información.
- SGSI-PR-013 - Procedimiento de seguridad de la información con proveedores.

8. Control de cambios

Versión	Descripción de cambios	Fecha de actualización
1	Creación del documento	04/03/2025

9. Control del documento

Elaboró	Revisó	Aprobó	Fecha de aprobación
Nombre: Sandra Barrios Cargo: Oficial de Cumplimiento	Comité de Seguridad de la Información	Comité de Seguridad de la Información	04/03/2025