	POLITICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACION	Código	PC-01SG
		Versión	05
		Fecha de creación: Fecha de actualización:	03/06/2022 08/05/2025

POLÍTICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por	***Revisado y Aprobado por***
Alejandra Ramirez	Juan Guillermo Bobadilla
Cargo: Coordinadora administrativa	Cargo: Representante Legal
Firma:  	Firma: 

	POLITICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACION	Código	PC-01SG
		Versión	05
		Fecha de creación: Fecha de actualización:	03/06/2022 08/05/2025

Contenido

	POLITICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACION	Código	PC-01SG
		Versión	05
		Fecha de creación: Fecha de actualización:	03/06/2022 08/05/2025

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

En GJX, reconocemos nuestra responsabilidad en la creación de soluciones innovadoras y eficientes para mejorar los procesos de negocio, generando valor a través de la tecnología de vanguardia. Somos conscientes de la importancia crítica de identificar, proteger y gestionar adecuadamente nuestros activos de información, los de nuestros clientes y proveedores. Por ello nos comprometemos a implementar, mantener y mejorar continuamente nuestro Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022. Nos esforzamos por prevenir y mitigar los riesgos asociados con la distribución, destrucción, modificación y uso no autorizado de la información, la infraestructura tecnológica y los sistemas de información, asegurando la confidencialidad, integridad y disponibilidad de los datos, cumpliendo con los marcos legales, normativos, regulatorios y contractuales.

Nos esforzamos por prevenir y mitigar los riesgos asociados con la distribución, destrucción, modificación y uso no autorizado de la información, la infraestructura tecnológica y los sistemas de información, asegurando la confidencialidad, integridad y disponibilidad de los datos así como gestionar los riesgos de seguridad de la información incluyendo aquellos derivados de posibles efectos del cambio climático" Nuestro compromiso se materializa a través de:

1. Establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI): Implementamos un SGSI estructurado que define claramente los roles, responsabilidades y procesos para garantizar la seguridad de la información. Este Sistema está en constante evolución para adaptarse a las cambiantes amenazas y vulnerabilidades, así como a los desarrollos tecnológicos.

2. Gestión de Riesgos: Realizamos evaluaciones periódicas de riesgos para identificar, analizar y tratar los riesgos relacionados con la información, asegurando que se mantengan dentro de niveles aceptables y alineados con la estrategia de negocio.

3. Control y Medidas de Seguridad: Aplicamos controles técnicos, administrativos y físicos apropiados para proteger los activos de información, basados en los resultados del análisis de riesgos. Esto incluye el uso de metodologías ágiles y la minimización de errores humanos para fortalecer la seguridad de la información.

4. Cumplimiento Normativo: Nos comprometemos a cumplir con todas las leyes, regulaciones y requisitos contractuales aplicables en materia de seguridad de la información. Esto incluye el cumplimiento de los requisitos legales, reglamentarios y contractuales de nuestros clientes, de los países y de los sectores donde desarrollamos nuestra labor.

5. Roles y responsabilidades de seguridad de la información: GJX establece los roles y responsabilidades respecto a la seguridad de la información. En la matriz de roles y responsabilidades.

6. Formación y Concienciación: Promovemos una cultura de seguridad de la información, proporcionando formación y concienciación periódica a todos los empleados, asegurando que comprendan sus responsabilidades individuales y colectivas en la protección de los activos de información.

7. Gestión de Incidentes y Mejora Continua: Establecemos mecanismos para la gestión de incidentes de seguridad de la información y aprendemos de ellos para mejorar continuamente nuestro SGSI.

8. Revisión y Evaluación del SGSI: Realizamos revisiones periódicas del SGSI para asegurar su adecuación, suficiencia y eficacia, ajustándolo a las necesidades cambiantes del negocio, el entorno tecnológico y el panorama de amenazas.
9. Principio de Menor Privilegio: Implementamos el principio de menor privilegio, asegurando que los usuarios, sistemas y procesos tengan solo los privilegios mínimos necesarios para realizar sus funciones. Este principio se aplica para minimizar el riesgo de accesos no autorizados o acciones malintencionadas.

   Asignación de Privilegios: Los accesos a sistemas y datos serán asignados basándose en las necesidades específicas del rol y las responsabilidades del usuario.

   Revisión de Privilegios: Realizaremos revisiones periódicas de los privilegios de acceso para asegurarnos de que solo se mantengan aquellos estrictamente necesarios.

10. Necesidad de conocer: Implementamos el principio de necesidad de conocer, limitando el acceso a la información a aquellas personas cuyo trabajo requiere dicho acceso.

11. Clasificación de Información: Clasificamos la información según su nivel de sensibilidad y criticidad para asegurar que solo los individuos autorizados tengan acceso a datos específicos.

12. Controles de Acceso Basados en Roles: Utilizamos controles de acceso basados en roles para garantizar que los usuarios solo tengan acceso a la información necesaria para sus funciones.

13. Segregación de deberes: La segregación de deberes y áreas de responsabilidad tiene como objetivo separar los deberes en conflicto entre diferentes empleados para evitar que ejecuten deberes potencialmente conflictivos por su cuenta. La organización determina los deberes y áreas de responsabilidad que deben segregarse.

14. Revisión independiente de la seguridad de la información
    En GJX se realiza revisión independiente de la seguridad de la información de manera periódica por parte del oficial de cumplimiento al sistema de gestión de seguridad de la información, así como al cumplimiento de las políticas para garantizar la idoneidad, eficacia y gestionar la seguridad de la información.

15. Desarrollo seguro
    En GJX desarrollamos las soluciones de manera segura diferenciando entornos de desarrollo, prueba y producción garantizando la integridad, confidencialidad, disponibilidad en cada etapa del desarrollo.

Esta política será revisada anualmente o tras cualquier cambio significativo en nuestra organización o en el entorno de amenazas para garantizar su relevancia y efectividad continuas. Además, nos comprometemos a comunicar y a tener disponible esta política para todas las partes interesadas pertinentes.

Con esta política, GJX reafirma su compromiso con la seguridad de la información, la mejora continua y la satisfacción de las necesidades y expectativas de nuestros clientes y otras partes interesadas.
Esta la política debe ser comunicada a todos los empleados, contratistas, terceros y todas las partes interesadas pertinentes, incluyendo clientes y socios.

	POLITICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACION	Código	PC-01SG
		Versión	05
		Fecha de creación: Fecha de actualización:	03/06/2022 08/05/2025

OBJETIVOS

1. Gestionar los riesgos identificados proponiendo controles que garanticen minimizar su ocurrencia.
2. Fortalecer el conocimiento y concientización del personal en Seguridad de la Información implementando mecanismos de comunicación, capacitación y entrenamiento.
3. Realizar la gestión de incidentes de manera eficaz garantizando el correcto reporte, análisis y gestión de los incidentes reportados.
4. Garantizar la identificación, valoración y control de los activos de información.
5. Garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información en los desarrollos de aplicaciones a clientes y aliados.
6. Mantener una conectividad constante en los servicios de comunicación y en la disponibilidad de aplicativos.

	POLITICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACION	Código	PC-01SG
		Versión	05
		Fecha de creación: Fecha de actualización:	03/06/2022 08/05/2025

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS				
No. de Versión.	***Fecha***	***Modificaciones***	***Responsable***	***Aprobado Por***
V1	03/06/2022	Agregar y modificar política según el nuevo Mapa de procesos	**Camila Rodriguez** Coordinadora Administrativa	**Juan Bobadilla** Gerente General
V2	02/02/2024	Se actualizo la política de seguridad de la información se incluyeron roles y responsabilidades	**Alejandra Ramirez** Coordinadora Administrativa	**Juan Bobadilla** Gerente General
V3	13/06/2024	Se incluyo controles de acceso y clasificación de información	Alejandra Ramirez Coordinadora administrativa	**Juan Bobadilla** Gerente General
V4	05/02/2025	Se actualizaron conceptos	Alejandra Ramirez Coordinadora administrativa	Juan Bobadilla Gerente General
V5	08/05/2025	Se actualiza la política se agregan los objetivos	Alejandra Ramirez Coordinadora administrativa	Juan Bobadilla Gerente General