POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Platica

Tabla de contenido

1. Antecedentes

GEEK OUT STUDIO S.A.S., constituida y existente bajo las leyes de la República de Colombia, en adelante **Platica**, con el propósito de proteger la seguridad de la información de **Platica** y garantizar la confidencialidad, integridad, disponibilidad y continuidad de los servicios que presta, la organización ha adoptado un Sistema de Gestión de Seguridad de la Información (SGSI) basado en el estándar internacional ISO/IEC 27001:2022.

El SGSI se implementa como un marco integral que articula la seguridad de la información, la ciberseguridad y la protección de la privacidad, en concordancia con la normatividad vigente, los compromisos contractuales y las buenas prácticas internacionales, apoyando así el cumplimiento de los objetivos estratégicos de **Platica**.

2. Propósito

La presente política establece los principios, lineamientos y compromisos generales que rigen la gestión de la seguridad de la información en **Platica**, con el fin de asegurar la confidencialidad, integridad, disponibilidad y, cuando aplique, la privacidad de la información, así como orientar la toma de decisiones y el comportamiento de los colaboradores y terceros.

3. Alcance

Esta política aplica a todos los colaboradores y terceros vinculados a **Platica**.

4. Definiciones

De conformidad el estándar internacional ISO/IEC 27001:2022 sobre la materia, se establecen las siguientes definiciones, las cuales serán aplicadas e implementadas acogiendo los criterios de interpretación que garanticen una aplicación sistemática e integral:

I. *Activo*: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas.) que tenga valor para la organización.
II. *Ciberseguridad*: Conjunto de prácticas, procesos, controles y tecnologías destinados a proteger la información, los sistemas de información y los activos digitales frente a amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad en el entorno digital.
III. *Confidencialidad*: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
IV. *Control:* Medida por la que se modifica el riesgo.
V. *Disponibilidad:* Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
VI. *Incidente de seguridad de la información:* Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
VII. *Integridad*: Propiedad de la información relativa a su exactitud y completitud.
VIII. *Política*: Intenciones y dirección de una organización, expresada formalmente por su alta dirección.
IX. *Riesgo*: Efecto de la incertidumbre sobre los objetivos.
X. *Seguridad de la información*: Preservación de la confidencialidad, integridad y disponibilidad de la información.

XI. *SGSI [Sistema de Gestión de Seguridad de la Información]*: Conjunto de políticas, procedimientos, directrices y recursos que gestionan colectivamente la seguridad de la información, basado en un enfoque de riesgos.

5. Directrices

5.1. Política del Sistema de Getión de Seguridad de la Información

Platica reconoce que la información es un activo estratégico y esencial para el cumplimiento de su misión organizacional. En consecuencia, se compromete a planear, implementar, mantener y mejorar continuamente su Sistema de Gestión de Seguridad de la Información (SGSI), de conformidad con la norma ISO/IEC 27001:2022, alineado con su estrategia organizacional, su estructura de gobierno y su modelo de gestión.

Este compromiso incluye:

- La protección de la confidencialidad, integridad, disponibilidad y privacidad de la información.
- La definición, seguimiento y revisión periódica de objetivos de seguridad de la información, medibles y coherentes con el contexto organizacional.
- La identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información, considerando amenazas cibernéticas, riesgos tecnológicos, operativos y de privacidad.
- La asignación de roles, responsabilidades y recursos necesarios para la operación eficaz del SGSI.
- El cumplimiento de los requisitos legales, regulatorios, contractuales y otros aplicables, incluidos los relacionados con la protección de la privacidad.
- La integración del SGSI con los procesos del negocio y la adopción de un enfoque de mejora continua, basado en el ciclo Planear-Hacer-Verificar-Actuar (PHVA).

5.2. Objetivos del Sistema de Gestión de Seguridad de la Información

Platica establece como objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) los siguientes:

- Desarrollar e implementar iniciativas y proyectos de mejora continua que fortalezcan la eficacia del Sistema de Gestión de Seguridad de la Información de **Platica**.
- Identificar, evaluar y reducir el nivel de los riesgos de seguridad de la información dentro del alcance del SGSI a un estado aceptable, mediante la implementación de controles que protejan la confidencialidad, integridad y disponibilidad de la información.
- Detectar, gestionar y responder oportunamente a los incidentes de seguridad de la información, conforme a los procedimientos establecidos, minimizando su impacto operativo, legal y reputacional.
- Promover la conciencia y cultura de seguridad de la información en los colaboradores y terceros que hacen parte del SGSI, mediante programas de capacitación, comunicación y sensibilización.
- Garantizar la observabilidad y monitoreo de los activos de información que soportan los servicios tecnológicos críticos dentro del alcance del SGSI.

5.3. Directrices generales de seguridad de la información

Platica establece las siguientes directrices generales de seguridad de la información:

- La responsabilidad de la implementación de un SGSI, se encuentra a cargo de la Gerencia de Tecnología y su área de Seguridad de información.
- Todos los colaboradores y terceros de **Platica** son responsables de cumplir las directrices de seguridad de la información establecidas en las políticas, manuales, procedimientos y procesos del sistema de gestión de seguridad de la información.
- El uso de la información debe cumplir con las políticas y estándares de la organización para la protección de su confidencialidad, integridad y disponibilidad, así mismo para dar cumplimiento a los requerimientos contractuales y normativos.
- Los documentos que conforman el SGSI son de uso confidencial y/o interno de **Platica**.

6. Consecuencias del no cumplimiento

En caso de evidenciar una falta o incumplimiento de esta política, se deberá informar al superior jerárquico quien determinará la gravedad del incumplimiento y escalará a Gestión del Talento Humano para definir el manejo correspondiente. Si la falta o incumplimiento se da por parte de un contratista o un proveedor, se deberá notificar a la Central de Contratación quien evaluará las repercusiones legales conforme a los términos de cada contrato.

7. Controles aplicables

ISO 27001:2022.