Política de Seguridad de la Información

Empresa: TechNova S.A.S.

1. Introducción

En **TechNova S.A.S.**, reconocemos que la información es uno de nuestros activos más valiosos. Nuestra actividad como empresa desarrolladora de software implica el manejo constante de datos sensibles, tanto internos como de nuestros clientes. Esta Política de Seguridad de la Información (PSI) se implementa con el fin de establecer un marco que garantice la protección de dichos activos, previniendo accesos no autorizados, alteraciones indebidas y pérdidas de información. La política busca establecer una cultura organizacional enfocada en la seguridad, asegurando la continuidad del negocio y el cumplimiento de los estándares legales y contractuales.

2. Propósito

El propósito de esta política es definir los lineamientos que permitan a **TechNova S.A.S.** proteger la confidencialidad, integridad y disponibilidad de la información. Asimismo, esta política busca:

- Apoyar la continuidad de las operaciones del negocio.
- Cumplir con requisitos legales y normativos relacionados con la seguridad de la información.
- Fortalecer la confianza de nuestros clientes y aliados.
- Proporcionar un marco para establecer controles de seguridad efectivos.

3. Alcance

Esta política aplica a todos los empleados, contratistas, socios estratégicos y terceros que tengan acceso a los recursos de información de **TechNova S.A.S.** Abarca:

- Todos los sistemas de información (servidores, bases de datos, aplicaciones internas).
- Equipos de cómputo, dispositivos móviles y de almacenamiento que contengan información corporativa.
- Infraestructura en la nube utilizada para proyectos de clientes.
- Procesos internos de desarrollo, pruebas, soporte y gestión de proyectos tecnológicos.

La PSI cubre tanto los entornos físicos como los digitales, sin importar si los recursos se encuentran en las oficinas de la empresa o en esquemas de teletrabajo.

4. Principios Fundamentales

Nuestra PSI se basa en los tres principios clave de la seguridad de la información:

- **Confidencialidad**: Solo las personas autorizadas deben tener acceso a la información sensible.
  Ejemplo: Los contratos de clientes solo son accesibles para el área legal y gerencial mediante autenticación de doble factor.
- **Integridad**: La información debe mantenerse completa y sin alteraciones indebidas.
  Ejemplo: El sistema de control de versiones para código fuente (Git) garantiza que los cambios estén registrados y autorizados.
- **Disponibilidad**: Los sistemas y datos deben estar accesibles para quienes los necesiten, cuando los necesiten.
  Ejemplo: La infraestructura en la nube de TechNova cuenta con respaldo automático y tolerancia a fallos.

5. Roles y Responsabilidades

En **TechNova S.A.S.**, cada miembro del equipo tiene un papel importante en la protección de la información. A continuación se describen los roles clave:

- **Gerente de Seguridad de la Información (CISO)**: Responsable de diseñar, aplicar y supervisar la PSI. Encargado de evaluar riesgos y liderar respuestas ante incidentes.
- **Comité de Seguridad**: Conformado por líderes de áreas clave (TI, legal, desarrollo y recursos humanos). Aprueban políticas, evalúan auditorías y toman decisiones estratégicas.
- **Colaboradores**: Deben conocer y cumplir la PSI, asistir a formaciones y reportar cualquier anomalía de seguridad.
- **Proveedores y Terceros**: Están obligados a cumplir con acuerdos de confidencialidad y políticas de acceso definidas por la empresa.

6. Clasificación de la Información

La información se clasifica en:

- **Confidencial:** Contratos, credenciales, datos financieros.
- **Restringida:** Código fuente, documentación técnica interna.
- **Pública:** Información de marketing y publicaciones en el sitio web.

7. Control de Acceso

- Autenticación multifactor (MFA).
- Revisión de permisos cada 6 meses.

- Registro de accesos y auditoría de accesos fallidos.

8. Gestión de Incidentes de Seguridad

- Flujo de respuesta estructurado.
- Formulario de reporte accesible para empleados.
- Registro del tipo de incidente, hora y persona afectada.

9. Política de Uso Aceptable

- Se permite el uso de recursos tecnológicos para fines laborales.
- Se prohíbe la instalación de software no autorizado y uso personal de credenciales corporativas.

10. Gestión de Riesgos

- Evaluación de riesgos en nuevos proyectos.
- Identificación de los 5 principales riesgos:
    1. Fuga de datos
    2. Ransomware
    3. Acceso indebido
    4. Fallas de configuración
    5. Errores en respaldo

11. Formación y Concienciación

- Capacitación semestral: “Reconociendo amenazas digitales: phishing y ransomware”.
- Simulacros trimestrales de phishing con un 90% de éxito esperado.
- Guías sobre creación de contraseñas seguras y buenas prácticas.

12. Gestión de Proveedores

- Cláusulas de seguridad en contratos (cifrado obligatorio).
- Evaluación de proveedores mediante auditorías de cumplimiento.

13. Revisión y Auditoría

- Auditorías internas semestrales.
- Verificación de configuraciones de firewall, accesos, y sistemas críticos.

14. Consecuencias del Incumplimiento

- Primera infracción: Advertencia formal.
- Segunda infracción: Suspensión temporal.
- Tercera infracción: Posible terminación del contrato.

15. Referencias

- **ISO/IEC 27001**: Sistema de Gestión de Seguridad de la Información.
- **Ley de Protección de Datos Personales (país de origen)**.
- Buenas prácticas de la **Academia Cisco**.