POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

INOVABIZ
Innovation & Business

VERSIÓN 1.3

Versión	Fecha	Descripción	Autor
1.0	11-10-2021	Documento original	Inovabiz
1.1	18-02-2022	Evaluación con gerencia e incorporación comentarios	Inovabiz
1.2	22-01-2023	Ajustes de responsabilidades	Inovabiz
1.3	10-06-2024	Ajustes de títulos para compliance	Inovabiz

Tabla de Contenidos

1 DECLARACION INSTITUCIONAL

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de Inovabiz. Es de aplicación para cualquier persona que de alguna manera esté relacionada con Inovabiz. En particular, debe ser conocida y cumplida por toda la planta de personal de Inovabiz, funcionarios de planta, técnicos, y contratados, sea cual fuere su nivel jerárquico y su situación.

2 DEFINICIÓN DE LOS REQUERIMIENTOS DE LA ORGANIZACIÓN

Inovabiz se compromete a proteger la información y los sistemas informáticos contra amenazas internas y externas, garantizando la confidencialidad, integridad y disponibilidad de los datos. Esto se logra mediante la implementación de controles y medidas de seguridad adecuadas, conforme a las normativas legales y los estándares aplicables.

3 OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se conforma por una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

- **Organización de la Seguridad:** Administrar la seguridad de la información dentro de Inovabiz y establecer un marco gerencial para controlar su implementación.
- Clasificación y Control de Activos: Mantener una adecuada protección de los activos de Inovabiz.
- **Seguridad del Personal:** Reducir los riesgos de error humano, comisión de ilícitos contra Inovabiz o uso inadecuado de instalaciones.

- **Seguridad Física y Ambiental:** Impedir accesos no autorizados, daños e interferencia a las dependencias e información de Inovabiz.
- **Gestión de las Comunicaciones y las Operaciones:** Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.
- **Control de Acceso:** Controlar el acceso lógico a la información.
- Desarrollo y Mantenimiento de los Sistemas: Garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.
- **Administración de la Continuidad de las Actividades de Inovabiz:** Contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.
- **Cumplimiento:** Impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

4 DEFINICIÓN DEL ALCANCE

Esta política es aplicable a todos los empleados, contratistas, socios comerciales, y cualquier otra parte interesada que maneje o acceda a la información de Inovabiz. Incluye todas las instalaciones, equipos, software y datos pertenecientes a Inovabiz.

5 DEFINICIÓN DE LAS PARTES INTERESADAS

Las partes interesadas incluyen:

- Empleados de Inovabiz
- Contratistas y proveedores
- Clientes
- Autoridades regulatorias
- Socios comerciales y tecnológicos

6 DEFINICIÓN DE ROLES, RESPONSABILIDADES, DERECHOS Y DEBERES DEL PERSONAL

- **Equipo de Seguridad de la Información:** Responsable de la detección, análisis y mitigación de vulnerabilidades. Así como también la implementación, revisión y actualización de la política de seguridad
- **Responsable de Seguridad de la Información:** Responsable de la gestión de la seguridad de la información.

- Empleados: Deben cumplir con las políticas y procedimientos establecidos, reportar incidentes de seguridad, y participar en capacitaciones de seguridad.

7 DEFINICIÓN DE EXCEPCIONES Y SANCIONES

Cualquier excepción a esta política debe ser aprobada por el Comité de Seguridad de la Información. Las violaciones a esta política pueden resultar en acciones disciplinarias, que pueden incluir el despido y la persecución legal, según corresponda.

8 PRÁCTICAS DEL MANEJO DE LA CIBERSEGURIDAD

Las siguientes son las prácticas que manejar en este contexto:

- Asignar un rol dedicado a las amenazas internas, manejado entre el líder del proyecto y el gerente de operaciones o CTO.
- Todo inicio de un proyecto debe superar los puntos mencionados en la presente política, incluyendo contar con firewall y antivirus adecuados, y acceder únicamente mediante mecanismos autorizados.
- Las contraseñas son únicamente conocidas por cada miembro del equipo y no pueden ser compartidas.
- Todos los miembros de Inovabiz deben participar anualmente en la actualización de esta política.
- No se deben descargar aplicaciones no relacionadas con la labor, ni acceder a archivos adjuntos de correos de origen desconocido.
- La seguridad física incluye apagar equipos no utilizados durante periodos prolongados para evitar acceso no autorizado.
- Hacer copias de seguridad de documentos críticos y almacenarlas en ubicaciones separadas.
- La política de gestión de vulnerabilidades será revisada y actualizada anualmente o cuando sea necesario para asegurar su efectividad y alineación con las mejores prácticas.

9 ÁMBITO DE APLICACIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Para clasificar el ámbito de aplicabilidad, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación se establece el criterio de clasificación de la información en función a cada una de las mencionadas características.

Confidencialidad:

- Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de Inovabiz o no.
- Información que puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves a Inovabiz o terceros. CLASIFICADA – USO INTERNO
- Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a Inovabiz o a terceros. CLASIFICADA - CONFIDENCIAL
- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de Inovabiz, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves a Inovabiz o a terceros. CLASIFICADA - SECRETA

Integridad:

- Información cuya modificación no autorizada, si no es detectada, no afecta la operatoria de Inovabiz.
- Información cuya modificación no autorizada, si no es detectada, podría ocasionar pérdidas leves para Inovabiz o terceros.
- Información cuya modificación no autorizada, si no es detectada, podría ocasionar pérdidas significativas para Inovabiz o terceros.
- Información cuya modificación no autorizada, si no es detectada, podría ocasionar pérdidas graves a Inovabiz o a terceros.

Disponibilidad: Se distinguen dos casos

- **Inaccesibilidad transitoria**.
  - Información cuya inaccesibilidad transitoria no afecta la operatoria de Inovabiz.
  - Información cuya inaccesibilidad transitoria durante 1 semana podría ocasionar pérdidas significativas para Inovabiz o terceros.
  - Información cuya inaccesibilidad transitoria durante 1 día podría ocasionar pérdidas significativas a Inovabiz o a terceros.
  - Información cuya inaccesibilidad transitoria durante 1 hora podría ocasionar pérdidas significativas a Inovabiz o a terceros.
- **Inaccesibilidad permanente**:
  - Información cuya inaccesibilidad permanente no afecta la operatoria de Inovabiz.
  - Información cuya inaccesibilidad permanente podría ocasionar pérdidas leves para Inovabiz o terceros.
  - Información cuya inaccesibilidad permanente podría ocasionar pérdidas significativas para Inovabiz o terceros.
  - Información cuya inaccesibilidad permanente podría ocasionar pérdidas graves a Inovabiz o a terceros.

CRITICIDAD BAJA: ninguno de los valores asignados superan el 1.
CRITICIDAD MEDIA: alguno de los valores asignados es 2.
CRITICIDAD ALTA: alguno de los valores asignados es 3.

Inovabiz se compromete a seguir las prácticas recomendadas, incluyendo pero no limitándose a:

- **Gestión de Riesgos:**
  - Identificación, evaluación y tratamiento de riesgos de ciberseguridad de acuerdo con las mejores prácticas internacionales. –
- **Protección de Datos:**
  - Implementación de controles de protección de datos personales y sensibles
- **Respuesta a Incidentes:**
  - Establecimiento de procedimientos para la detección y respuesta efectiva a incidentes de seguridad
- **Auditorías y Revisiones:**
  - Realización de auditorías internas para asegurar el cumplimiento con los procedimientos y políticas.
- **Capacitación y Concientización:**
  - Programas de formación continua para empleados sobre políticas de ciberseguridad y procedimientos de protección de datos.

10 GLOSARIO DE TERMINOS

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asi mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la empresa