Política de Seguridad de la Información

Introducción

El Directorio de Inceptia S.R.L., ha fijado sus objetivos en función de su estrategia general. Por consiguiente, ha considerado necesario definir políticas claras, las que serán la base de sustentación para la administración y desarrollo de las actividades de las áreas responsables de tecnología, desarrollo, comunicaciones y operaciones.

Objetivo del Manual

El objetivo de la Política General de la Seguridad de la Información es establecer los lineamientos y directivas relativas a la protección de la información y activos de Inceptia S.R.L.

Alcance

Todos los activos Informáticos de la Organización, a sus recursos y procesos relacionados, como así también a los grupos de influencia de Inceptia S.R.L., proveedores de tecnología y sistemas de información, clientes de todo tipo, operadores de telecomunicaciones, organismos de regulación y control, y otros entes externos vinculados directa o indirectamente.

Revisiones y Recomendaciones

El Directorio, el responsable de Tecnología e Infraestructura y los responsables operativos de Seguridad de la Información, deberán cuidar que la presente política se mantenga alineada con los objetivos estratégicos de Inceptia S.R.L., y plantear las actualizaciones que se juzguen necesarias para el cumplimiento de las disposiciones legales y reglamentarias que se dicten sobre el tema.

Responsabilidad en la Determinación

- Directorio.
- Responsable de Tecnología (CTO).

Responsabilidad en la Implementación

- Responsable de Tecnología (CTO).
- Responsables operativos de Seguridad de la Información (ROSIs)

Áreas y Sectores Intervinientes

- Responsable de Tecnología (CTO).
- Responsables operativos de Seguridad de la Información (ROSIs)

Obligatoriedad de Cumplimiento

La Política descripta en el presente Manual es de cumplimiento obligatorio para el personal afectado al Seguridad de la Información, Desarrollo de Aplicaciones, Tecnología Informática y el personal del resto de las Áreas involucradas de Inceptia S.R.L..

Términos Utilizados

- Información: Se considera información a los diferentes conjuntos organizados de datos que utiliza Inceptia S.R.L..
- Recurso o activo de tecnología Informática y comunicaciones (RTI): Se considera un RTI a todos aquellos recursos técnicos que almacenan, procesan o transmiten información de la Organización.
- Política: Se considera Política a la declaración, por parte de la dirección de la Organización, de un conjunto de objetivos para regir y proteger los activos de información de esta. Dentro de estos objetivos se encuentran prácticas generalmente aceptadas para llevar a cabo tareas de control interno, requerimientos de protección de la información, etc.
- Directivas: Una directiva es una declaración que provee a los miembros de la Organización información acerca de los objetivos planteados en las políticas. Las directivas son diseñadas para proveer una descripción más específica de los objetivos de la Organización, de modo que son modificadas más frecuentemente que las políticas debido a cambios en el entorno de negocios de la Organización. El cumplimiento de las directivas asegura el cumplimiento de los objetivos planteados en las políticas.
- Estándar: un estándar es una declaración que provee una guía o lineamiento para concretar los objetivos estipulados por las directivas e indicados por las políticas.
- Procedimiento: un procedimiento es una declaración que indica cómo realizar un conjunto de actividades que permitan lograr los objetivos establecidos. Un procedimiento puede tomar la forma de un manual de instalación, una guía de usuario, un manual administrativo, una lista de verificación o cualquier otro tipo de documentación operacional.

Introducción

Las definiciones y lineamientos presentados en esta Política establecen las bases para la implementación de controles y medidas de la Seguridad de la Información que permitirán al Inceptia S.R.L. minimizar y/o controlar adecuadamente los riesgos que afectan a su información y a sus activos de tecnología Informática y comunicaciones de la Organización.

La responsabilidad por la seguridad de la información no debe ser concedida sólo a los Responsables operativos de Seguridad de la Información. La responsabilidad de la protección de los activos de información día a día es deber de cada funcionario. La información de la Organización debe ser administrada activamente para asegurar la seguridad, confidencialidad, integridad y disponibilidad de esta.

Disposiciones Generales y Transitorias

Los criterios y directivas emitidos en revisiones anteriores de esta Política y los referidos en cualquier otra norma al respecto, quedan totalmente sustituidos a partir de la vigencia de la presente.

Esta Política será revisada anualmente por los Responsables operativos de Seguridad de la Información de Inceptia S.R.L.. Los resultados de la revisión, y los cambios que se sucedan, serán reportados al CEO y comunicados a los involucrados antes de ser implementados.

La falta de cumplimiento de las definiciones emanadas de la presente Política, y de las políticas y normas derivadas sobre seguridad y protección de la información, estará sujeta a las sanciones disciplinarias que amerite cada caso.

Roles y Responsabilidades

La implementación satisfactoria de la Política General de Seguridad de la Información, y de las medidas que de ella se desprendan, requiere la plena cooperación y la asistencia de todos los colaboradores de Inceptia S.R.L. Es imperativo, por lo tanto, que todo el personal sea consciente de, y opere de acuerdo con, los requisitos de seguridad aquí detallados.

A los efectos de definir e implementar adecuados niveles de seguridad en la información, Inceptia S.R.L. ha designado un área de trabajo, a saber:

- Reponsable de Tecnología (CTO): será el encargado de gestionar la protección de la información y los RTI, implementando las medidas de seguridad que se desprendan de la estrategia y las políticas definidas por la Dirección, y controlando su eficacia para los fines buscados. Asimismo, proveerá los recursos necesarios para asegurar que todo el personal del Inceptia S.R.L. reciba la capacitación adecuada sobre los procedimientos de seguridad relevantes, y que se brinden los medios y recursos para cumplir con dichos procedimientos.

Adicionalmente, se definen los siguientes roles relativos al cumplimiento de los requisitos de la Seguridad de la Información:

- Propietario: persona a la que, por su cargo y/o responsabilidad, Inceptia S.R.L. reconoce como responsable de un RTI determinado.
    - Su nivel deberá ser consistente con la autoridad requerida para evaluar los riesgos a los que está expuesto el RTI, respetar las medidas de protección para reducirlos, o para asumir los riesgos que no desee minimizar, dentro de los rangos de riesgos aprobados por la Organización.
    - Es responsable de establecer el nivel de criticidad y confidencialidad del RTI del que es dueño.
- Usuario: persona que accede a información y/o utiliza un RTI de Inceptia S.R.L. en el desarrollo de su tarea específica. Deben firmar su conformidad con las políticas de seguridad de la Organización, y los estándares y procedimientos que regulan sus actividades.

Diagrama de Roles

ROLES	RESPONSABILIDADES
DIRECTORIO / CEO (GC)	Establece la estrategia y asegura que el SGSI esté alineado con los objetivos del negocio.
	Tiene la última palabra en la aprobación de políticas y procedimientos clave
CTO (GM)	Lidera la definición estratégica del SGSI desde el punto de vista técnico y organizacional.
	Asegura que todas las políticas, normas y procedimientos cumplan con los objetivos del SGSI y las expectativas regulatorias.
Compliance Manager (MB)	Garantiza el diseño de normas y procedimientos alineados con estándares y regulaciones externas (ej., GDPR, regulaciones locales).
	Supervisa el cumplimiento del SGSI y coordina auditorías internas y externas.
Responsables Operativos (LDV, DP, AD)	Detallan normas y procedimientos específicos que aseguren la operatividad del SGSI en sus áreas de influencia (productos, operaciones, infraestructura).
Usuarios	Son responsables de seguir y adherirse a las políticas, normas y procedimientos.
Auditor	Proveen una evaluación independiente del cumplimiento y efectividad del SGS

Política General de Seguridad de la Información

El principal objetivo de la Seguridad de la Información es cumplir con los siguientes principios:

- Confidencialidad: Asegurar que todos sus recursos Informáticos estén protegidos contra uso no autorizado o revelaciones accidentales acorde a la clasificación otorgada por el origen y la función de esta. Sólo las personas calificadas y autorizadas tendrán acceso a la información requerida bajo el criterio de “la necesidad de conocer” y el principio de otorgar el “mínimo privilegio” requerido para la realización de las tareas asignadas.
- Integridad: Tender a la ausencia de errores y/o corrupción en toda su información y garantizar que la información sea exacta, completa y válida de acuerdo con los valores y las expectativas de Inceptia S.R.L., y regulaciones externas.
- Disponibilidad: Minimizar las amenazas de interrupción del negocio y preservar la continuidad de la operatoria normal. Por lo tanto debe garantizar que:
    - La información de alta criticidad sea resguardada;
    - La capacidad de procesamiento sea recuperada en tiempo y forma.

La adecuada implementación y vigencia de la Política de Seguridad de la Información deberá:

- Garantizar la protección adecuada de las informaciones y los sistemas contra acceso, modificación, destrucción y divulgación no autorizados;
- Garantizar el cumplimiento de la presente Política y de las Normas Corporativas de Seguridad de la Información de la Organización.
- Asegurar que los activos de información sean utilizados solamente para las finalidades aprobadas por la Organización, estando sujetos a monitoreo y auditoría;
- Asegurar la participación de los colaboradores en el Programa Corporativo de Concienciación y Educación en Seguridad de la Información.

Principales Directivas

Las siguientes directivas regirán la implementación de la Seguridad de la Información en Inceptia S.R.L.:
Política General de Seguridad de la Información: Inceptia S.R.L. define que su Política General de Seguridad de la Información, y todas las políticas derivadas, estén alineadas a las Regulaciones aplicables a la empresa y aquellas derivadas de los servicios ofrecidos a sus clientes y Sanas Prácticas (Best Practices), que garantizan el uso eficiente de los recursos informáticos, según las necesidades y particularidades de Inceptia S.R.L. Esta definición también regirá para los estándares específicos y procedimientos apropiadamente detallados que constituyen el marco completo de cobertura de la seguridad de la información de Inceptia S.R.L.

Organización de Seguridad: para la Administración de la Seguridad de la Información, Inceptia S.R.L. ha definido un Responsables de gestión estratégica y operativa de Seguridad de la Información, la cual reporta al Responsable de Tecnología (CTO) y al Directorio.

- Clasificación y Control de Activos de Información: La información de negocio de Inceptia S.R.L., y todos los RTI relacionados, deberán encontrarse inventariados, tener asignado un Propietario, y deberán estar clasificados según su nivel de confidencialidad y criticidad para el negocio de Inceptia S.R.L.
- Administración de Riesgos de Seguridad: Se evaluarán los riesgos a los que están sometidos los activos RTI de Inceptia S.R.L. El Responsables operativos de Seguridad de la Información en conjunto con el Propietario del RTI, establecerán los riesgos que pueden afectar a dicho recurso, las implicancias de su exposición, modificación o acceso no autorizado y cuáles son las medidas de protección que se deberán implementar de acuerdo con el análisis de riesgo efectuado.
- Competencia del personal en materia de seguridad de la información: El personal de Inceptia S.R.L., ya sea permanente, temporal, o perteneciente a empresas proveedoras del mismo, deberá ser informado desde el momento de su ingreso de las responsabilidades y derechos en materia de uso y protección de los RTI de Inceptia S.R.L., se revisará anualmente estas responsabilidades. Se capacitará con y para el fin de crear conciencia acerca de la importancia que adquiere este aspecto para la Organización.

- Programa de Concientización y Educación en Seguridad de la Información: El personal de Inceptia S.R.L., ya sea permanente, temporal, deberá ser informado y/o participar, desde el momento de su ingreso de los Programas de Concientización y Educación en Seguridad de la Información, se revisará anualmente estas responsabilidades. Se capacitará con y para el fin de crear conciencia acerca de la importancia que adquiere este aspecto para la Organización.
- Administración de Equipamiento, Operaciones y Comunicaciones: Se deberá asegurar la disponibilidad de los equipamientos, la integridad de los procesos operativos y la seguridad en las comunicaciones para garantizar un correcto procesamiento de la información y resguardar la confidencialidad de esta. Todas las comunicaciones electrónicas con el exterior deberán prever la Encripción de los datos.
- Controles de Acceso: El acceso a los RTI deberá ser restringido de acuerdo con los requerimientos de control establecidos por sus Propietarios y el Responsables operativos de Seguridad de la Información, bajo el criterio de "la necesidad de conocer" y el principio de mínimo privilegio. Dicho acceso se asegurará a través de procesos de autenticación, autorización, monitoreo y posterior auditoría.
- Tratamiento de Incidentes o Violaciones de Seguridad de la Información: En casos de ocurrencias de eventos clasificados como Incidente de Seguridad, se debe comunicar inmediatamente al Responsable de Seguridad de la Información. El correcto relato de incidentes garantiza que los asuntos de seguridad sean encaminados y resueltos en tiempo hábil evitando que los mismos incidentes se repitan.
- Prevención de software malicioso: Versiones actualizadas de software Antivirus deben estar instaladas en los servidores y configuradas para ejecutar automáticamente con periodicidad diaria para servidores que ejecuten sistemas vitales y periodicidad semanal para el resto de los servidores.
- Directivas de Privacidad: La protección y privacidad de los datos de los clientes reflejan los valores de la Organización y reafirma su compromiso con la mejora continua de la eficacia del proceso de Protección de Datos.
- Las informaciones de nuestros clientes siguen las siguientes directivas:
    - La información es recopilada en forma ética y legal, con el conocimiento del usuario, para propósitos específicos y debidamente informados.
    - La información recibida por Inceptia S.R.L. es tratada y almacenada en forma segura e íntegra, con métodos de criptografía o certificación digital, cuando es aplicable.
    - La información sólo será accedida por personas autorizadas y capacitadas para su uso adecuado.
    - La información podrá estar disponibles a las empresas contratadas para prestación de servicios, siendo exigido de tales organizaciones el cumplimiento de nuestras directrices de seguridad y privacidad de datos.
    - La información de los clientes solamente será proporcionada a terceros, mediante previa autorización del cliente o para el cumplimiento de la exigencia legal o reglamentaria;
    - La información y datos que constan en nuestros registros, así como, otras solicitaciones que garanticen los derechos legales o contractuales sólo serán

entregadas a los propios interesados, mediante pedido formal, siguiendo los requisitos legales vigentes.

- Desarrollo y Mantenimiento de Sistemas: Los principios de Seguridad de la Información deberán ser incorporados a los sistemas aplicativos en todo el ciclo de vida de estos, incluyendo los procesos de desarrollo, prueba, mantenimiento y puesta en producción de los sistemas aplicativos.
- Se deberán prevenir pérdidas, modificaciones o uso inadecuado de los datos, proyectos y sistemas aplicativos de Inceptia S.R.L..
- Administración de la Continuidad del Negocio: Se deberá desarrollar y mantener los planes de recuperación tecnológica y continuidad de negocio requeridos por los propietarios de los RTI y el Responsables operativos de Seguridad de la Información, de forma tal de poder responder a eventos no deseados que impacten de manera negativa sobre los procesos de negocio críticos para la Organización.
- Conformidad con Leyes, Regulaciones y Normas Internas: Se deberá garantizar que la utilización de los recursos RTI no provoque infracciones o violaciones de leyes, regulaciones, ni de las obligaciones establecidas por estatutos, normas, reglamentos o contratos vigentes en cada ámbito de actuación. Asimismo, se deberá evaluar y asegurar el cumplimiento de las normas internas (políticas, reglas, estándares, procedimientos) relativos a la Seguridad de la Información

Objetivos del Sistema General de Seguridad de la Información

OBJETIVO	METRICA	KPI	META 2025	Frecuencia Medición
Garantizar la disponibilidad y continuidad del servicio	Disponibilidad de Plataforma Voice Bots y ChatBots	% Disponibilidad de Plataforma Voice Bots y ChatBots	**99%**	**Anual**
	Frecuencia pruebas Plan de Continuidad	Cantidad de Pruebas planes de continuidad por año	**1**	**Semestral**
Proteger la Confidencialidad y privacidad de los datos	Cifrado de Datos en Tránsito	% Datos cifrados en Tránsito	**100%**	**Trimestral**
	Restricción de Accesos	% Accesos restringidos por perfil usuario y con Logs de Control	**100%**	**Trimestral**
Actuar dentro del marco de los requisitos legales y reglamentarios aplicables a la organización.	Frecuencia Revisiones Matriz Legal	Cantidad de Revisiones Matriz Legal por año	**2**	**Semestral**
Gestionar de manera adecuada las vulnerabilidades técnicas de la plataforma de Servicios	Remediación de vulnerabilidades según SLA establecido por la organización	% de Remediación de vulnerabilidades	**90%**	**Anual**
	Frecuencia Escaneos preventivos de búsqueda de vulnerabilidades	Cantidad de Pentest	**1**	**Anual**
Fortalecer la cultura de seguridad en la organización	Competencias en Personal	Cumplimiento de Planes de capacitación, técnica y cultural de Seguridad según roles	**100%**	**Anual**
Asegurar Mejora Continua SGSI	Frecuencia Auditorías Internas al SGSI	Cantidad de Auditorías Internas por año	**1**	Anual
	Cumplimiento Auditorías Externas	Cumplimiento de calendario de AE acordadas con el organismo de certificación	**100%**	Anual