SIJISA S.A. DE C.V.

SI08 Política de seguridad a TI

Los requisitos de la norma ISO 27001:2013

Documento Ref.:	SI08 Política de seguridad TI
Versión:	1
Fecha de la versión:	15/may/2017
Autor:	Raúl Torres.
Aprobado por:	José Ricardo Jiménez Sánchez.
Nivel de confidencialidad:	Controlados: si imprime es copia no controlada.

Lista de Distribución

Esta política de seguridad de las TI es un documento controlado y se mantiene en el Intranet de SIJISA S.A. DE C.V. como de sólo lectura. Las consultas a los documentos de SGSI se realizarán vía intranet sin tener acceso a cambios. El coordinador del SGSI debe garantizar que todas las modificaciones y revisiones se realicen y se mantengan actualizadas en la intranet y en las copias controladas. Se podrán utilizar copias controladas de documentos para entrenamiento y auditorías internas las cuales serán distribuidas de la siguiente manera.

La copia No.	Titular
1	Coordinador del SGSI.
2	Redes e Implementación.
3	Soporte administrativo.
4	Soporte financiero.
5	Ventas.

Control de Cambios

Este documento se revisa periódicamente, al menos una vez al año, y se mantiene durante un período de 6 años. Los cambios y revisiones se mantienen en la intranet y las copias son controladas por los líderes de área para fines de entrenamiento, concientización y auditoria interna. El historial de los cambios y las revisiones se registran a continuación.

Fecha	Enmendar. No.	Nº de página	Nueva edición No.	Motivo del cambio	Autorizado por
15/may/2017	-	Todos	1	Versión inicial.	José Ricardo Jiménez Sánchez
	1		2		
	2		3		
	3		4		
	4		5		
	5		6		
	6		7		
	7		8		
	8		9		
	9		10		
	10		11		
	11		12		
	12		13		
	13		14		
	14		15		
	15		16		
	16		17		

Copias de este documento distinto a los mencionados anteriormente no será revisado; dicha copia será marcada como la no controlada.

Tabla de contenido

0. Los controles de referencia

Control Ref.	Título
A.5.1.1	Políticas de seguridad de la información
A.5.1.2	Revisión de las políticas de seguridad de la información
A.6.1.1.	Roles y responsabilidades de seguridad de la información
A.18.1.1	Identificación de la legislación aplicable y los requisitos contractuales

1. Introducción

SIJISA S.A. DE C.V. reconoce que la información y los sistemas de TI son activos valiosos los cuales son esenciales en el apoyo de sus objetivos estratégicos. SIJISA S.A. DE C.V. También reconoce su obligación de proteger la información de amenazas internas y externas, así como la importancia de la gestión eficaz de la seguridad de la información es esencial para garantizar el éxito del establecimiento de las TI y cumplimiento de las funciones de negocio y servicio. SIJISA S.A. DE C.V. se compromete a preservar la confidencialidad, integridad y disponibilidad de todos los activos físicos y electrónicos.

La gestión de la seguridad de la información es un ciclo continuo de una actividad encaminada a la mejora continua en respuesta a las nuevas y cambiantes amenazas y vulnerabilidades. Puede definirse como el proceso de protección de la información del acceso no autorizado, revelación, modificación o destrucción y es vital para la protección de la información y reputación de SIJISA S.A. DE C.V.

Los detalles de enfoque de la política de la tecnología de la información (TI) en Gestión de la seguridad SIJISA S.A. DE C.V. no contiene información confidencial o restringida y puede ser publicada libremente a las partes pertinentes. Una versión actual de este documento está disponible en intranet de la organización y está a disposición de las partes externas en el website www.sijisa.net

El enfoque se basa en las recomendaciones contenidas en la norma ISO27002 para la gestión de la seguridad de la información.

2. Alcance

Esta política se aplica a la seguridad de las TI:

- Los sistemas TI pertenecientes a, o bajo el control de SIJISA S.A. DE C.V.
- Información almacenada o en uso, en SIJISA S.A. DE C.V.
- Información en tránsito a través de SIJISA S.A DE C.V en redes de voz o datos.
- Control de la información en SIJISA S.A. DE C.V.
- Recursos de acceso a la información.
- Todas las partes que tienen acceso a, o el uso de los sistemas de TI e información perteneciente a, o bajo el control de SIJISA S.A. DE C.V., incluyendo:
    - Empleados de SIJISA S.A. DE C.V.
    - Contratistas
    - Personal temporal
    - Las organizaciones asociadas/partners.
    - Cualquier otra parte utilizando recursos de TI en SIJISA S.A. DE C.V.

La aplicación de esta política se aplica a lo largo del ciclo de vida de la información desde la adquisición / creación, utilización, almacenamiento y/o eliminación.

3. Declaración de política

La política de seguridad de la información se basa en los principios enunciados en la Norma Internacional para la seguridad de la información - *ISO/IEC 27001:2015.*

SIJISA S.A. DE C.V. está comprometida con el desarrollo y mantenimiento de un sistema de gestión de seguridad de información basado en el estándar internacional y ha desarrollado esta Política de seguridad TI buscando:

- Proporcionar orientación y apoyo para la seguridad de las TI, de conformidad con los requisitos de la empresa, regulaciones y requisitos legales.
- Definir responsabilidades a los empleados, socios/partners, contratistas y cualquier otra persona u organización que tenga acceso a la empresa SIJISA S.A. DE C.V.
- Conocer el estado de la administración con la intención de apoyar los objetivos y principios de la seguridad en concordancia con la estrategia de negocio y objetivos.
- Proporcionar un marco en el que la confidencialidad, integridad y disponibilidad de recursos de TI puede ser mantenida.
- Optimizar la gestión de los riesgos, mediante la prevención y minimización del impacto de los incidentes de seguridad en la TI.
- Asegurar que todas las infracciones de la seguridad de las TI son reportadas, investigadas y tomar las medidas adecuadas cuando sea necesario.
- Asegurar que las políticas y procedimientos de seguridad apoyan las TI y se revisan periódicamente para garantizar la continuidad de las buenas prácticas y la protección frente a nuevas amenazas.
- Garantizar que los requerimientos de la seguridad de la información TI se comunican periódicamente a todas las áreas pertinentes.

Uso autorizado

El acceso a las TI y sistemas de información de los cuales SIJISA S.A. DE C.V. es responsable permite el acceso de las áreas de negocio o en conexión con la organización. Los usuarios autorizados se definen como: empleados, contratistas autorizados, empleados temporales o las organizaciones asociadas/partners al uso de los servicios de información proporcionados por SIJISA S.A. DE C.V.

Política de Uso Aceptable

Todos los usuarios de los sistemas de TI e información de SIJISA S.A. DE C.V. son responsables de aceptar y acatar los términos de la SI02 Política de Uso Aceptable de la organización, y políticas de seguridad asociadas a los códigos de conexión o de conducta.

Conciencia de seguridad

SIJISA S.A. DE C.V. se compromete a promover prácticas de trabajo seguras. Todos los empleados recibirán formación sobre asuntos de seguridad en consonancia con la clasificación de la información y los sistemas a los que tienen acceso. El personal que trabaja en las funciones especializadas recibirán la capacitación adecuada, relevantes para su función. Políticas de seguridad de la información pertinente, los procedimientos y las directrices serán accesibles y se difundirán a todos los usuarios. Seguirá siendo responsabilidad de los empleados, el asegurarse que están adecuadamente informados de las políticas y procedimientos de seguridad de la información.

Continuidad de negocio

SIJISA S.A. DE C.V. ha desarrollado y mantiene una estrategia de continuidad empresarial basada en la evaluación de riesgos específica para mantener funciones críticas para el negocio en caso de cualquier interrupción significativa de servicios o instalaciones en las cuales SIJISA S.A. DE C.V. soporta sus actividades.

Vigilancia y presentación de informes

SIJISA S.A. DE C.V. se reserva el derecho de supervisar el uso de las TI y sistemas de información, incluido el correo electrónico y el uso de internet, para proteger la confidencialidad, integridad y disponibilidad de los activos de información y garantizar el cumplimiento de las políticas de SIJISA S.A. DE C.V. La organización, a su discreción, o cuando sea requerido por ley, informara de los incidentes de seguridad a las autoridades mexicanas para proseguir la investigación. Como parte de la auditoria interna implementada por SIJISA S.A. DE C.V. evaluara sistemáticamente el cumplimiento de políticas de seguridad y controles e informes referidos a la ISO27001 informando cuando se requiera al Director General. Los incidentes de seguridad mencionados en la política y procedimientos de gestión de incidentes de seguridad, informará sobre la eficacia de los controles de ISO27001 y ayudara en la identificación de necesidades de capacitación, sensibilización y mejoras mediante el procedimiento de mejora.

Evaluación de riesgos

SIJISA S.A. DE C.V. ha desarrollado una estrategia de gestión de riesgo y el riesgo a sus sistemas de las TI y la información será administrado bajo este marco con referencia a las políticas y procedimientos del SGSI, en específico el procedimiento de tratamiento y evaluación de riesgos. Las revisiones son independientes, imparciales y verificadas por la auditoría interna o de partes externas cuando sea necesario.

Revisión de la política de seguridad de TI

SIJISA S.A. DE C.V. realizará un examen anual de la política o después de cualquier incidente de seguridad, importantes cambios en la legislación mexicana o cambio en SIJISA S.A. DE C.V. en requisitos de negocio o estructura.

Administración de activos

SIJISA S.A. DE C.V. mantendrá un inventario compuesto de todos los activos de información que será administrada de conformidad con políticas y procedimientos de seguridad de la información implementados en la organización.

Las sanciones

El fracaso en el cumplimiento de la política de seguridad de la información por los empleados de SIJISA S.A. DE C.V. puede conducir a la adopción de medidas disciplinarias con arreglo a los lineamientos establecidos en la declaración de las políticas. En relación a la falla en el cumplimiento de la política de seguridad de contratistas, personal temporal, partners u organizaciones de tercera parte de SIJISA S.A. DE C.V. puede resultar en terminación del contrato y relaciones, suspensión de servicios y/o aspectos legales.

4. El cumplimiento de las obligaciones legales y contractuales

SIJISA S.A. DE C.V. acatará toda la legislación mexicana relativa al procesamiento y almacenamiento de información, tomara en consideración:

- Ley Federal de protección de datos personales.
- Disposiciones de legislación en base a requerimientos de clientes.
- Requerimientos de cumplimiento de leyes establecidas de manera contractual, cuando sean referidas en la relación comercial.

SIJISA S.A. DE C.V. también cumplirá con cualquiera de los requisitos contractuales, normas y principios necesarios para mantener las funciones de negocios de la organización, incluyendo:

- Protección de los derechos de propiedad intelectual.
- Protección de registros de SIJISA S.A. DE C.V.
- Verificación de cumplimiento y procedimientos de auditoría.
- La prevención del uso indebido de instalaciones.
- Los códigos de conexión a redes y servicios de terceros.

Se tiene un listado de normatividad que se revisa para mantener al día los requerimientos relacionados a la empresa.

5. Responsabilidades

Coordinador de SGSI: SIJISA S.A. DE C.V. coordina la gestión de la seguridad de la información, monitoreo, auditorias, es responsable ante la dirección del SGSI. Mantiene la información de regulaciones y normas, para apoyo en el contexto interno y externo de la norma. Garantizar el que la documentación del sistema del SGSI este en el intranet para su consulta, y este debidamente actualizada.

Líderes de área: son responsables de garantizar que políticas y procedimientos estén en su lugar para cubrir todos los aspectos de los sistemas de TI y seguridad de la información. Todas las políticas serán comunicadas para asegurar buenas prácticas de trabajo y minimizar el riesgo en la reputación de SIJISA S.A. DE C.V.

Director General: Es responsable de garantizar que la información y los sistemas de la TI de SIJISA S.A. DE C.V. dentro de sus áreas de servicio se gestionan de conformidad con la política de seguridad de las TI. Día a día la responsabilidad de la gestión de los sistemas de TI e información puede ser delegada al personal designado como información o propietarios del sistema dentro de los departamentos.

Los usuarios de los recursos: Es responsabilidad de cualquier persona u organización que tenga acceso a TI y sistemas de información de SIJISA S.A. DE C.V. e cumplir con la política de seguridad de TI, políticas y procedimientos asociados y el adoptar las medidas adecuadas para salvaguardar la seguridad de los sistemas de TI y la información a la que tengan acceso. Cualquier sospecha o debilidad de seguridad, amenazas, incidentes o eventos debe ser comunicado de inmediato a través del procedimiento de gestión y de notificación de incidentes. Usando la guía de Plataforma de registro de incidentes de seguridad.

Roles y responsabilidades se establecen también en SI13 Política de seguridad del SGSI.

6. Desarrollo de políticas de TI específicas, Procedimientos y Políticas

SIJISA S.A. DE C.V. está comprometido con el desarrollo continuo y la revisión de políticas de TI, procedimientos y políticas para gestionar el riesgo de las amenazas a sus sistemas y servicios. Este trabajo será administrado por el coordinador del SGSI. Una lista actualizada de los documentos de soporte se incluyó en los Apéndices A-B. Las nuevas políticas y procedimientos se distribuirán a todas las partes interesadas en el momento de la emisión. Los Apéndices A-B de esta política se actualizan durante la reunión anual de revisión de seguridad de las TI.

7. Las infracciones de la política

Las infracciones de esta política y/o incidentes de seguridad son definidos como eventos que tienen como resultado, pérdidas o daños en activos de SIJISA S.A. DE C.V. o eventos que violan procedimientos y políticas de seguridad de SIJISA S.A. DE C.V.

Todos los empleados de SIJISA S.A. DE C.V., contratistas, proveedores, partners o socios tienen la responsabilidad de informar sobre los incidentes de seguridad y las infracciones a esta política, tan pronto como sea posible aplicando el procedimiento de presentación de informes de incidentes de SIJISA S.A. DE C.V. Esta obligación se extiende también a cualquier organización externa contratada para apoyar o acceder a la información de los sistemas de información de SIJISA S.A. DE C.V.

En el caso de tercera parte, consultores o contratistas el incumplimiento podría resultar en la eliminación inmediata de acceso al sistema. En caso de dañar o comprometer los sistemas de TI o los resultados de la red por el incumplimiento, SIJISA S.A. DE C.V. estudiará acciones legales contra el tercero.

SIJISA S.A. DE C.V. adoptará las medidas apropiadas para remediar cualquier violación de la política, procedimientos y directrices a través de los marcos pertinentes en sitio. En una situación individual el caso se podría tratar como un proceso disciplinario.

Reportes de incidencias

Los usuarios serán continuamente alentados a informar de cualquier infracción por la Plataforma de tickets vía web para el registro de incidente. Las infracciones pueden involucrar no sólo a los equipos de tecnología de la información, sino también los datos que se manejan de forma incorrecta, perdidos , con abuso o cualquier otro incidente que pueda provocar un problema de seguridad y que puedan infringir las políticas asociadas de SIJISA S.A. DE C.V. La Plataforma de tickets de incidentes de seguridad basada en el Procedimiento de gestión de incidencias es una herramienta para realizar el proceso de acciones correctivas y mejora.

Gestión de incidencias

Durante la presentación de una infracción, los detalles del incidente se introducirán mediante el reporte por la persona que reporte la incidencia mediante la Plataforma de tickets. Una vez que el reporte ha sido introducido en el sistema, se realizara seguimiento en concordancia con el procedimiento de gestión de incidentes de seguridad. El coordinador de área realizara la gestión para que en conjunto de las partes involucradas se tomen las medidas correctivas apropiadas. Los líderes de área y el coordinador del SGSI en base al análisis y solución de los incidentes de seguridad, verificaran el estado de la incidencia para proceder a su cierre.

8. Los documentos y registros asociados

Documento / Nombre de registro	Ubicación de almacenamiento	Propietario	Control de protección	Programación de retención
Todos los procedimientos y políticas de TI. (Apéndice A)	Intranet SIJISA	SIJISA	Restringido. Edición en la website. Acceso Publico	6 años

9. Gestión de documentos

Este documento es válido desde [15/may/2017].

Este documento se revisa periódicamente y por lo menos una vez al año para garantizar que se cumplen los siguientes criterios establecidos.

- La conformidad con los requisitos de la norma ISO 27001:2013
- Requisitos legislativos definidos por la ley, cuando corresponda

Director General.
José Ricardo Jiménez Sánchez.

Apéndice A: Lista de las políticas de seguridad del SGSI

Título	El estado	Fecha de revisión
SI00 Procedimiento del Comité SGSI	Publicado	15/may/18
SI01 Declaración de Aplicabilidad (SOA)	Publicado	15/may/18
SI02 Política de Uso Aceptable.	Publicado	15/may/18
SI03 Política de control de acceso	Publicado	15/may/18
SI04 Política de administración de activos	Publicado	15/may/18
SI05 Política de Conservación de registros digitales	Publicado	15/may/18
SI06 Políticas de administración de registros organizacionales.	Publicado	15/may/18
SI07 Política de cifrado.	Publicado	15/may/18
SI08 Política de seguridad	Publicado	15/may/18
SI09 Política de mejora.	Publicado	15/may/18
SI10 Política de respaldo y restauración de información	Publicado	15/may/18
SI11 Política de manejo y clasificación de la información.	Publicado	15/may/18
SI12 Política de Uso Aceptable de Internet y correo electrónico	Publicado	15/may/18
SI13 Política de SGSI.	Publicado	15/may/18
SI14 Política para la Gestión Operativa	Publicado	15/may/18
SI15 Política para contraseña.	Publicado	15/may/18
SI16 Política de eliminación de Registros.	Publicado	15/may/18
SI18 Política de escritorio seguro.	Publicado	15/may/18
SI20 Política de Gestión de incidentes de seguridad	Publicado	15/may/18
SI21 Política de seguridad del Servidor.	Publicado	15/may/18
SI22 Política de seguridad del proveedor.	Publicado	15/may/18
SI23 Política de conexión de tercera parte.	Publicado	15/may/18
SI24 Política de red inalámbrica.	Publicado	15/may/18

Apéndice B: Lista de procedimientos de seguridad del SGSI

Título	El estado	Fecha de revisión
SI25 Procedimientos de protección de datos y manejo de soporte de almacenamiento	Publicado	15/may/18
SI26 Procedimiento de seguridad de PC de Escritorio.	Publicado	15/may/18
SI27 Procedimiento de retiro de equipo de TI.	Publicado	15/may/18
SI28 Procedimiento de control de documentos y registros	Publicado	15/may/18
SI29 Plan de Continuidad de negocio de TI	Publicado	15/may/18
SI30 Procedimiento de mejora	Publicado	15/may/18
SI31 Procedimiento de informes y gestión de incidencias	Publicado	15/may/18
SI32 Procedimientos de manejo y clasificación de la Información	Publicado	15/may/18
SI34 Procedimiento de auditoría interna	Publicado	15/may/18
SI35 Procedimientos de seguridad de portátiles y dispositivos móviles.	Publicado	15/may/18
SI36 Procedimiento de antivirus y Software malintencionado	Publicado	15/may/18
SI37 Procedimiento de uso de teléfono móvil	Publicado	15/may/18
SI38 Procedimiento de infraestructura física y ambiental	Publicado	15/may/18
SI39 Procedimiento para la evaluación de registros.	Publicado	15/may/18
SI40 Procedimiento para análisis, tratamiento y evaluación de riesgos.	Publicado	15/may/18
SI41 Procedimiento de concientización en seguridad	Publicado	15/may/18
SI42 Procedimientos de trabajo móvil y Teletrabajo.	Publicado	15/may/18