Política de Tratamiento y Seguridad de la Información y Documentación

Nombre	Fecha de elaboración:	Revisión	Requisito de la Norma:	Página
ANEXO 1 Política de tratamiento y seguridad de la información	**23/02/2023**	01	**270012022:** 6.2	1 de 22

Contenido del documento

1. Control de documento

Número de Revisión	Fecha de Revisión dd/mm/aaaa	Descripción del cambio
00	03/10/2021	Creación del Documento
01	17/01/2022	

2. Términos y definiciones

Término	Definición
Auditoría	Proceso sistemático y documentado ejercido de forma interna o por personas externas, para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.
Autoridad Reguladora	Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, del ámbito federal, local y/o autoridad Internacional cuya competencia sea reglamentar y/o verificar la protección y seguridad de la información.
Aviso de privacidad	Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.
Bases de datos	Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Término	Definición
Código fuente	El conjunto de líneas de textos, que son las directrices que debe seguir la computadora para realizar dicho programa; por lo que es en el código fuente, donde se encuentra escrito el funcionamiento de la computadora.
Cliente	Persona física o moral con la que VENSI celebra contrato de prestación de servicios de forma tácita o expresa, por el cual recibe el pago de una cantidad cierta en dinero como contraprestación de los servicios otorgados
Datos personales	Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
Datos personales sensibles	Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones.
Derechos ARCO	Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.
Derecho de Acceso	Aquel que tiene el titular de la información o documentación de solicitar el acceso a sus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes de VENSI, así como de conocer información relacionada con el uso que se da a tu información personal.
Derecho de Rectificación	Aquel que tiene el titular de la información o documentación de solicitar la rectificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados.
Derecho de Cancelación	Aquel que tiene el titular de la información o documentación de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos de VENSI cuando proceda la cancelación ya sea por prescripción de la acción o porque ya haya transcurrido el periodo de bloqueo de la información.
Derecho de Oposición	Aquel que tiene el titular de la información o documentación de solicitar que sus datos personales no se utilicen para ciertos fines, o de requerir que se concluya el uso de los mismos a fin de evitar un posible daño o perjuicio; siempre y cuando la información o documentación no sea necesaria legalmente para algún proceso o procedimiento pendiente de resolución o para el cumplimiento de obligaciones pendientes.
Disociación	Proceso al que puede someterse la información a fin de que no pueda asociarse con algún titular, documento y/o con alguna otra información que permita por su estructura, contenido o grado de desagregación, su identificación.
Documento de Seguridad	Instrumento que describe y da cuenta, de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos

Término	Definición
	Personales.
Información confidencial	Aquella que contiene datos concernientes a la información reservada y sensible que por sus características no pueda ser objeto de disociación y/o involucre derechos de terceros que deban de ser resguardados.
Información cotidiana	Aquella cuyo tratamiento se desarrolla de forma rutinaria, ya que no contiene datos personales, datos personales sensibles, información sensible, confidencial, reservada o pública.
Información pública	Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados en el ámbito federal o local; accesible a cualquier persona de acuerdo con lo establecido por la Ley General de Transparencia y Acceso a la Información, la Ley Federal de Transparencia y Acceso a la Información, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. La característica principal de este tipo de información es que el público en general puede desarrollar su tratamiento ya que es de libre acceso, fácil, gratuito y en muchos casos expedito.
Información reservada	Aquella cuyo tratamiento debe ser restringido, por contener datos personales, secreto comercial, industrial, fiscal, bancario, fiduciario, bursátil, postal u otro considerado como tal por alguna disposición legal; la relacionada con procedimientos penales, judiciales, y/o que involucren investigaciones administrativas y en general toda aquella que por sus características deba ser tratada por personal determinado que por sus facultades y/o funciones deba tener conocimiento de la información y/o documentación.
Información sensible	Aquella que por sus características contenga datos, documentación y cualquier otra que se refiera a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones.
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Lineamientos/ regulación	Normatividad aplicable en materia de Seguridad de la Información y/o Protección de Datos Personales para el privado.
Medidas de seguridad administrativas	Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de seguridad de la información y protección de datos personales.
Medidas de seguridad físicas	Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.
Medidas de seguridad técnicas	Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital y la ciber seguridad de la información, de los datos personales y los recursos involucrados en su tratamiento.

Término	Definición
Responsable	Sujeto obligado por la Ley General de Protección de Datos Personales en Posesión los Particulares o por cualquier otro ordenamiento nacional o internacional, a la protección de la información y documentación que trate, mismo que decide sobre su tratamiento.
Revisión	Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de la protección y seguridad de la información y documentación que VENSI trate.
Riesgo	Combinación de la probabilidad de un evento y su consecuencia desfavorable.
Titular	Persona física a quien corresponden los datos personales y la información tratada por VENSI.
Transferencias	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado
Tratamiento	Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de información y datos personales.

3. Alcance

Aplica para todos los colaboradores contratados directamente por VENSI, socios de negocios, socios, proveedores o cualquier persona que tenga relación con la organización, ya sea que provengan de sus titulares, clientes, proveedores, responsables o encargados del tratamiento de la información, con independencia del soporte, espacio o lugar que se resguarden.

4. Objetivo del procedimiento

La presente política tiene como finalidad regular cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados al tratamiento, obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia, disposición, resguardo, archivo, destrucción y/o extinción de los documentos e información a los cuales VENSI tenga acceso a través de sus colaboradores, socios de negocios, socios, proveedores o cualquier persona que tenga relación con la organización, ya sea que provengan de sus titulares, clientes, proveedores, responsables o encargados del tratamiento de la información, con independencia del soporte, espacio o lugar que se resguarden.

5. Políticas

5.1. Obligaciones generales

1. La Dirección debe asegurarse de que existan los recursos humanos, materiales y tecnológicos para implementar planes y programas en aspectos de seguridad de la información y protección de datos personales.

2. La Dirección tiene la responsabilidad de promover la seguridad de la información y la protección de los datos personales por lo cual, debe nombrar un "Responsable de la seguridad de la información", mismo que tendrá la obligación de implantar y mantener un Sistema de Gestión de la Seguridad de la Información.

3. La Dirección es responsable de asegurar la alineación operativa de Tecnologías de la Información a la normativa aplicable en materia de seguridad de la Información y protección de datos personales.

4. La Dirección implementará los estándares funcionales, operativos y tecnológicos, que deben incorporarse en el desarrollo de servicios , componentes de tecnologías de información y comunicación que permitan como resultado la protección y seguridad de la información, confidencialidad y protección de los datos personales.

5. La Dirección se asegurará que todos los equipos móviles y electrónicos que VENSI asigne al personal para el cumplimiento de sus funciones, cuenten con las herramientas necesarias para propiciar la seguridad de la información. Estas herramientas, incluyen, en forma enunciativa, más no limitativa: antivirus, software de cifrado, aplicaciones seguras, entre otras.

Los equipos móviles de uso personal, no otorgados por VENSI, que requieran acceso a los servicios de la organización, deben contar con la validación de que se cuenta con los elementos tecnológicos de seguridad informática, ya sea de la Dirección de normatividad o de su jefe inmediato. Se privilegian los antivirus que incorporan funcionalidades de protección contra malware y cortafuegos (firewall), también conocidos como "suites de seguridad", así mismo se deberá evitar tener dos antivirus en un mismo dispositivo. Tener dos antivirus activos no significa mayor protección; de hecho, puede ocasionar diferentes problemas en el sistema. Un antivirus que esté trabajando se convertirá en un "software malicioso" a los ojos del otro, el cual intentará bloquearlo y eliminarlo, y se corre el riesgo de afectar el desempeño del sistema por el consumo extra de recursos.

6. Todas las instalaciones y actualizaciones de programas y aplicaciones deben hacerse desde el sitio web oficial del fabricante o desde las tiendas oficiales de apps, verificando la identidad del autor de la aplicación, evitando descargar e instalar aquéllas de dudosa procedencia.

7. La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el servicio y facultades encomendadas en la descripción del puesto debiéndose aplicar criterios de buen uso en su utilización.
8. Por ningún motivo se podrá hacer uso de la información para otros fines que no sean estrictamente los necesarios y relacionados con su operación y funciones, esto incluye la

impresión, transmisión, retransmisión, almacenamiento, procesamiento, extracción, copia, uso remoto o cualquier otro medio físico o lógico sin el permiso expreso del cliente, titular, encargado y/o responsable de la información.

9. Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario, cuya revisión de validez será efectuada por la Dirección cuando el caso concreto lo amerite.

10. El personal está obligado a alertar, de manera inmediata, oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos establecidos en el manejo de incidentes, que se establecerán más adelante.

11. Está absolutamente prohibido reproducir, copiar, hacer pública o divulgar a terceros cualquier información y/o documentación a la que se tenga acceso, obligándose a tomar las providencias necesarias para evitar el tratamiento erróneo y/o no autorizado.

12. Todo el personal se compromete a proteger los equipos electrónicos, móviles y de acceso remoto que se le han asignado para el desempeño de sus funciones siguiendo las medidas de seguridad que a continuación se describen, como mínimo:

    a. No exponer el equipo a condiciones de inseguridad física y/o ambiental.
    b. Proteger las claves de acceso que le han sido asignadas.
    c. No dejar el equipo desatendido en lugares públicos o en lugares donde pueda ser sustraído o dañado con relativa facilidad, a manera de ejemplo: autos, maletas de viaje, cerca de ventanas, en el piso, inmuebles externos u oficinas ajenas a la organización, lugares de venta de comida o bebida, entre otros.

13. La selección del personal es responsabilidad del proveedor del jefe directo en conjunto con el proveedor de Recursos Humanos, quien realizará la evaluación integral del personal, asegurando que el perfil de competencias del candidato es el más adecuado para cumplir con el puesto requerido y que se encuentra en condiciones de cumplir con los términos y condiciones de confidencialidad, seguridad de la información y protección de los datos personales.

14. El jefe directo deberá notificar al Responsable de la seguridad de la información de los nuevos ingresos para que esté a su vez, informe de la existencia de Políticas de Seguridad de la Información, aviso de confidencialidad y protección de datos; así mismo como parte de la inducción al personal de nuevo ingreso, se deberá proporcionar el material informativo necesario sobre seguridad de la información.

15. Se deberá privilegiar la separación del puesto de una manera ordenada, disminuyendo así el riesgo hacia los activos de información que son propiedad de VENSI, en caso de terminación de la relación laboral y/o contractual, también se dará el término al tratamiento de la información a la que pudiera tener acceso el usuario, por lo que se restringirán e inhabilitarán privilegios, usuarios, contraseñas y demás permisos de forma inmediata.

16. Se acatarán las medidas de seguridad y confidencialidad necesarias ante la finalización del contrato individual de trabajo, cambio de puesto o funciones de los empleados,

prestadores de servicios o terceros; ante la inhabilitación de un usuario, se tomarán medidas para resguardar la información cuyo tratamiento de forma provisional decidirá la Dirección para disminuir riesgos en la operación de VENSI.

17. El consultor jurídico deberá asegurarse de que el formato de los contratos de prestación de servicios, cuente con cláusulas que promuevan el cumplimiento de esta política.

18. El consultor jurídico deberá asegurarse de establecer y mantener actualizado el contenido de todos los acuerdos de confidencialidad y de no revelación de información, que debe incluirse en los contratos, tanto para personal interno como proveedores.

19. El consultor jurídico coadyuva en el cumplimiento de los requerimientos legales, contractuales o regulatorios a los que está sujeto VENSI; así como está obligada a fomentar la revisión y seguimiento a eventos que provoquen una interrupción total o parcial de los servicios prestados, evitando violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.

20. Se deberá promover en todo momento, la participación en los procesos de concientización, capacitación y prevención a incidentes de seguridad, a todo el personal, para fortalecer una cultura de seguridad de la información.

21. En este documento se establecen las directrices generales sobre el tratamiento y seguridad de información y documentación en VENSI, que tiene efecto inmediato a partir de la fecha de su autorización y difusión por cualquier medio a colaboradores, socios, socios de negocios, proveedores y cualquier persona física o moral que tenga relación con la organización; cuya revisión debe ser de manera anual para cumplir las necesidades al interior de VENSI, en materia de seguridad de la información y protección de datos personales.

22. Todos los colaboradores en general que presten sus servicios a VENSI, son responsables de conocer y cumplir las Políticas de seguridad de la información, confidencialidad y protección de datos personales.

23. En caso de ocurrir algún incidente de seguridad que involucre algún contacto con las autoridades reguladoras en materia de seguridad de la información, será el Responsable de la seguridad de la información, quien tendrá el trato directo con las mismas, por medio de los procesos y procedimientos establecidos para tal efecto.

24. De acuerdo con el procedimiento de manejo de incidentes, todo el personal deberá reportar cualquier falta u omisión a los lineamientos o normatividad de Seguridad de la Información, para que de acuerdo a la gravedad, se informe a la Dirección General y al Asesor Jurídico, para que en el ámbito de sus competencias resuelvan lo conducente.
25. El presente documento, será revisado cuando menos una vez al año; así mismo, será actualizado cuando se requiera o derive de:

    a. Modificaciones al marco jurídico y normativo aplicable.
    b. Observaciones y/o recomendaciones por parte de las partes interesadas, así como, de las autoridades competentes.
    c. Cambios en la estructura organizacional de la sociedad; y,

d. Perfeccionamiento del proceso de Control de calidad, Seguridad de la Información y mejora continua.
e. Mejoras al proceso de tecnologías de la información o cualquier otro de la sociedad.

A fin de desarrollar la revisión y actualización correspondiente, el Responsable de la seguridad de la información en conjunto con el Consultor jurídico realizará las siguientes acciones:

1. Gestionar la actualización de esta política.
2. Elaborar propuestas de modificaciones y mejoras al presente documento.
3. Coordinar la revisión y actualización del presente documento cuando se requiera o derive de alguno de los supuestos mencionados en los incisos a) al e) del presente numeral.
4. Enviar a la Dirección General para la valoración y aprobación correspondiente.
5. Gestionar la publicación y difusión de este documento por cualquiera de los medios autorizados para tal efecto.

5.2. Inventario de activos

Los activos de información son aquellos elementos reconocibles que almacenan datos, registros, información, documentación en cualquier medio y que tiene las características de ser valioso por la información contenida en él y ser de imposible o difícil reemplazo. Por lo cual es responsabilidad de todo el personal identificar sus activos de información.

El Responsable de la seguridad de la información, contará con un registro actualizado sobre los activos físicos e informáticos con la información que previamente le proporcione todo el personal.

Todos los activos, son propiedad de VENSI y todo activo de información debe ser asignado a un responsable o custodia y autorizado por su jefe inmediato.

<u>La persona responsable del activo debe:</u>

A. Salvaguardar la integridad, disponibilidad y confidencialidad del activo.

B. Hacer uso del activo únicamente para los propósitos y actividades de la Institución.

C. Reportar cualquier incidente o problema relacionado con el activo de información, de manera inmediata, oportuna y adecuada al Responsable de la seguridad de la información, para que, de acuerdo con la gravedad, se informe a Dirección General.

D. Cualquier omisión (con dolo o involuntaria) de reportar algún incidente relacionado a cualquier activo bajo su guarda y custodia, se considera una falta hacia la seguridad de la información que en su caso debe reportarse a las autoridades competentes.

E. Realizar lo necesario para mantener el activo de información en buenas condiciones que garanticen y cumplan su función.

F. Salvaguardar los activos e información de cualquier alteración o modificación no autorizada, daño o destrucción que límite su disponibilidad para el adecuado desarrollo

de sus actividades.

G. Evitar daños temporales o permanentes a los activos de información, causados por accidentes, imprudencias o daños dolosos.

H. Reportar cualquier falla o mal funcionamiento detectado mediante el Formulario para Reporte de Incidencias SGSI.

I. Informar a los jefes inmediatos, de cualquier falla o vulnerabilidad de los activos de información mediante el Formulario para Reporte de Incidencias SGSI.

J. Notificar de cualquier necesidad de protección o mejora, en los controles para los activos de información mediante el Formulario para Reporte de Incidencias SGSI.

K. Usar los activos de información únicamente para los propósitos establecidos por VENSI.

L. Reportar cualquier uso no adecuado del activo de información.

M. Todo el personal al concluir sus servicios y/o funciones, tiene la obligación de entregar los activos informáticos, móviles, electrónicos y/o físicos asignados, en buen estado físico y de operación, así como los activos de información y la documentación correspondiente.

N. El uso de medios removibles de almacenamiento debe apegarse a los deberes de seguridad y confidencialidad, priorizando el buen uso y mejores prácticas del manejo de medios removibles de almacenamiento, para el traslado de la información.

O. Todo activo informático que contenga información, debe contar con procedimientos de migración, respaldo y borrado seguro antes de que el activo sea eliminado. Así mismo la información deberá ser respaldada de forma semestral en todas las áreas de la organización, al respaldar se debe realizar copias de seguridad de la información que se almacena en los dispositivos (configuraciones, logs, file systems, bases de datos, etc.) para garantizar el acceso a la información almacenada, ya sea personal o vinculada a las actividades de trabajo. Así, en caso de que ocurra cualquier incidente de seguridad (robo, pérdida del dispositivo, o avería, etc.) se podrá mantener el acceso a la misma. Se debe revisar y validar periódicamente la información respaldada, para evitar que se pierda, se vuelva obsoleta o se deteriore; asegurando que la información sea recuperable y que cumple con los principios de integridad y disponibilidad, es decir, garantizar que los respaldos no sean alterados.

P. Todo activo de información debe contar con programas de soporte y mantenimiento, para su correcto funcionamiento y disponibilidad. El Responsable de la seguridad de la información debe validar que los mantenimientos que se lleven a cabo, sean realizados por personal capacitado, de acuerdo a las especificaciones del fabricante. Asimismo, asegurarse que se conserve un registro de todos los mantenimientos preventivos y correctivos efectuados.

Q. El Responsable de la seguridad de la información debe solicitar al proveedor de TI un calendario de mantenimiento preventivo y llevar un registro de las actividades de mantenimiento (preventivo y correctivo).

R. Solo el proveedor de TI puede instalar software en los equipos, por lo que debe asegurarse de que contenga las licencias autorizadas por el fabricante, siendo permitidas para descargar actualizaciones solo páginas oficiales. Es importante mantener actualizados los sistemas operativos y las aplicaciones de los dispositivos. Estas actualizaciones normalmente incluyen cambios importantes que mejoran el rendimiento y la seguridad de los equipos; muchos de estos programas, incluso, se actualizan de manera automática.

S. Toda información que ya no sea tratada o utilizada por haberse cumplido la finalidad para la cual fue recabada, deberá ser objeto de bloqueo, cuya conservación será únicamente para determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual; transcurrido este periodo, se procederá a su devolución, cancelación, supresión o destrucción según sea lo que corresponda.

5.2.1. Directrices de clasificación:

En VENSI, es importante la protección de los activos, de los datos personales y la seguridad de la información, por ello en la obtención, uso, divulgación, almacenamiento, acceso, manejo, aprovechamiento, transferencia o disposición y en general el tratamiento de la información y documentación se deberán observar los siguientes criterios de clasificación:

- Información confidencial: Aquella que contiene datos concernientes a la información reservada y sensible que por sus características no pueda ser objeto de disociación y/o involucre derechos de terceros que deban de ser resguardados.

- Información cotidiana: Aquella cuyo tratamiento se desarrolla de forma rutinaria, ya que no contiene datos personales, datos personales sensibles, información sensible, confidencial, reservada o pública.

- Información pública: Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados en el ámbito federal o local; accesible a cualquier persona de acuerdo a lo establecido por la Ley General de Transparencia y Acceso a la Información, la Ley Federal de Transparencia y Acceso a la Información, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. La característica principal de este tipo de información es que el público en general puede desarrollar su tratamiento ya que es de libre acceso, fácil, gratuito y en muchos casos expedito.
- Información reservada: Aquella cuyo tratamiento debe ser restringido, por contener datos personales, secreto comercial, industrial, fiscal, bancario, fiduciario, bursátil, postal u otro considerado como tal por alguna disposición legal; la relacionada con procedimientos penales, judiciales, y/o que involucren investigaciones administrativas y en general toda aquella que por sus características deba ser tratada por personal determinado que por sus facultades y/o funciones deba tener conocimiento de la información y/o documentación.

- Información sensible: Aquella que por sus características contenga datos personales sensibles, documentación y cualquier otro dato que se refiera a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles

los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones.

En atención a lo anterior, cualquier persona que efectúe el tratamiento, custodie y/o conserve de forma temporal, constante o definitivamente la información, deberá observar, cumplir y respetar el etiquetado o colocación de la marca de identificación que a efecto cada activo contenga con motivo de su clasificación en el inventario de activos correspondiente.

Toda la información y documentación deberá tratarse conforme a los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, así como los deberes de seguridad y confidencialidad previstos en la LFPDPPP, su Reglamento y demás normativa aplicable.

Todo activo esta registrado en la base de datos con un ID para su tratamiento, identificación y trazabilidad.

El control de acceso, donde se establece qué personas son las autorizadas para el manejo de la información o activo, es determinado en el perfil correspondiente.

5.2.2. Protección de datos personales

Se deberá cumplir por la LFPDPPP, su Reglamento y demás normativa aplicable. Todo tratamiento de datos personales que se efectúe en VENSI, se deberá justificar con un fin concreto, lícito, explícito y legítimo, relacionado con las atribuciones que la normatividad le aplique. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, todo colaborador deberá considerar y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como cuidar su confidencialidad e integridad.

5.3. Control de acceso

Para proteger la confidencialidad, autenticidad o la integridad de la información que se encuentre en los documentos y/o archivos digitales o físicos, VENSI tomará las medidas y controles cumpliendo todos los acuerdos y reglamentos pertinentes según aplique.

Con el fin de asegurar que sólo los usuarios designados accedan a los servicios de información en VENSI, se otorgarán privilegios adecuados a su perfil o rol en la organización y según el servicio requerido.

Es responsabilidad del coordinador de Área informar al Responsable de la seguridad de la información de las bajas o cambios del personal, para que a su vez, este notifique al proveedor de la ejecución del cambio o remoción de los derechos de acceso.

El Responsable de la seguridad de la información debe asegurar la confidencialidad de la entrega de contraseñas en todos los procesos, otorgará sólo los niveles de permisos mínimos necesarios para que cada usuario pueda realizar sus actividades en VENSI, y estos deberán ser entregados

al usuario, por medios diversos a fin de que los privilegios de acceso no se encuentren en un solo documento y/o archivo.

Toda contraseña, es confidencial y debe mantenerse en VENSI, por lo que todo personal, ingresará con la cuenta asignada para tal efecto; en ningún caso accederán usando una cuenta diferente a la autorizada para el usuario en concreto.

Los derechos de autor de toda aplicación y herramienta de software utilizada en las estaciones de trabajo y todo el software instalado en las computadoras de la organización debe ser legal.

Las claves y certificados del cifrado que se utilicen en el almacenamiento y transmisión de la información deben ser asignadas por el proveedor de TI y resguardadas por cada usuario.

Antes de abrir cualquier enlace, archivo anexo, mensaje de texto o llamada de un remitente desconocido, todo colaborador deberá hacerse los siguientes cuestionamientos:

- ¿Espero esa información? Si el mensaje proviene de un remitente desconocido (persona u organización), analizar bien antes de responder o hacer clic y/o descargar cualquier archivo adjunto.

- ¿Reconozco al remitente? Comprobar si la dirección está bien escrita (verificar que no haga falta ninguna letra, por ejemplo) y si el dominio (la terminación del correo electrónico) es de confianza y corresponde a quien envía el mensaje.

- ¿Solicitan que haga algo? Los correos electrónicos fraudulentos (phishing) o los mensajes de texto de este tipo (smishing) suelen pedir que se realice alguna acción como: hacer clic en un hipervínculo, descargar algún archivo, responder al mensaje proporcionando información personal, etc. Con frecuencia, buscan generar una sensación de urgencia y provocar una reacción inmediata e irracional. Es necesario analizar antes de proporcionar cualquier información.
- Se debe desconfiar, particularmente, de los mensajes que parecerían genéricos (como “Estimados:”, “A quien corresponda:”, etc.).

- Algunos correos electrónicos de phishing son más sofisticados que otros, por lo que resulta muy útil saber identificar las pistas más obvias, que incluyen: imágenes de logotipos de baja calidad, errores ortográficos o gramaticales, se dirigen al usuario como “querido amigo” en lugar de por su nombre o se refieren a un mensaje anterior inexistente, etc.

- En el caso de comunicaciones referentes a instituciones bancarias y financieras, se recomienda NUNCA dar clic en los enlaces contenidos en un correo o mensaje de texto y NO proporcionar información de acceso a cuentas. Ante alguna duda, se deberá contactar directamente a tu institución financiera para más orientación.

Todo aquel que por motivo de sus funciones tenga acceso a los Activos de Información y activos de soporte o almacenamiento, al concluir la relación jurídica con VENSI, no podrán conservar en su poder, sustraer o tratar cualquier tipo de Información, debiéndose entregar de forma inmediata (al instante) a su jefe directo o a la persona designada por la Dirección. En atención a lo anterior, el Responsable de la seguridad de la información notificará al proveedor para que a

su vez, revoque o suspenda, los permisos de accesos físico, electrónico o cualquier otro que se le hubiera otorgado de forma inmediata, es decir al instante de la conclusión de la relación jurídica, para el caso de cambios de facultades se deberá reflejar con la eliminación de todos los derechos de acceso dados inicialmente para ser modificadas o eliminadas, después de la terminación o el cambio de empleo, contrato o acuerdo.

No obstante, lo anterior, subsistirá hasta por el periodo de diez años contados a partir del mismo día de la conclusión de la relación jurídica, la obligación de confidencialidad y seguridad.

5.4. Controles contra el código malicioso:

El Responsable de la seguridad de la información debe asegurar que todos los equipos de escritorio, móviles (laptops) dispositivos utilizados en la red, tengan instalado el software antivirus, anti-malware, anti-xploits, anti-spam y anti-spyware institucional y mantenerlo actualizado, tanto en versión como en definición de firmas. Así mismo, deben cumplir con una configuración base de parches de seguridad.

El software de antivirus debe permitir:

1. Ejecutar búsqueda automática, manual o programable.
2. Limpiar archivos infectados.
3. Mantener en cuarentena los archivos que no puedan ser limpiados.
4. Contar con mecanismos para prevenir y contener amenazas, así como, negación de servicios.
5. Proveer la capacidad de actualizaciones automáticas y programables.
6. Registrar los incidentes de virus y contar con la capacidad de análisis de registro.
7. Detectar código malicioso.
8. Generar alertas.
9. Llevar una administración centralizada.

El software contra código malicioso y sus componentes deben ser actualizados cuando exista una nueva versión o definición de firmas, con base a los contratos con el fabricante.

5.5. Seguridad física

En caso de ser requerido el acceso físico a las instalaciones, el proveedor asignará una tarjeta de acceso, de acuerdo a las indicaciones del jefe directo; en caso de que el colaborador no requiera tarjeta de acceso, deberá seguir el protocolo de general de entrada a las instalaciones:

a) Presentarse en en el lobby general con una identificación oficial (INE, pasaporte, licencia de manejo, etc)
b) En caso de ser colaborador de Vensi: Indicar que es colaborador
c) En caso de ser un proveedor: indicar el motivo de la visita, personal que le atenderá y la empresa a la que pertenece.
d) En el área de recepción de Vensi: indicar el motivo de la visita, personal que le atenderá y la empresa a la que pertenece.

El proveedor cuenta con un listado de los colaboradores que cuentan con tarjeta de acceso otorgada por VENSI.

VENSI proporcionará a cada colaborador un espacio físico asignado que cuente con mobiliario protegido para el resguardo de información física.

Todo equipo que almacene, procese o transmita información esencial para la operación de VENSI, debe ser protegido para disminuir riesgos y amenazas ambientales o físicas; tales como, inundaciones, rayos, sismos, radiaciones, polvo, humedad, vandalismo, explosión, humo etc.

El proveedor de TI debe realizar el respaldo de la información por medio de discos duros externos y de manera digital en google drive, lo cual permitirá el acceso de manera remota y garantizara la continuidad de la operación en caso de contingencia.

Al finalizar la jornada laboral, o ausentarse temporalmente del área de trabajo, todo colaborador, debe cumplir con los siguientes lineamientos:

• Cajones o archiveros, éstos deben cerrarlos con llave.
• Retirar del escritorio cualquier tipo de información, sin importar el medio en que se encuentre (papel, post-its, discos, medios magnéticos) y resguardarse en gabinetes con llave o cualquier otro mueble con acceso controlado.
• No dejar documentos con información sobre impresoras, copiadoras, etc.
• No utilizar la información impresa que sea confidencial o de uso restringido para reciclaje
• No dejar a la vista de otras personas información relevante, como aquélla sensible o claves de acceso.
• Mantener siempre la computadora, teléfono celular o cualquier otro dispositivo, en un lugar seguro y con contraseña, a fin de restringir el acceso a éstos por parte de personas no autorizadas.
• Al alejarse de los dispositivos, es importante bloquear la sesión.
    • Mantener cubierta la cámara web cuando no se esté utilizando, para limitar el acceso que pudieran llegar a tener a ésta aplicaciones o programas no autorizados.
    • Deshabilitar la autoejecución de memorias USB para evitar que, por ese medio, se ejecuten programas maliciosos.
    • En medios digitales, bloquear su equipo utilizando como mecanismo un protector de pantalla protegido por contraseña, cuando el usuario suspenda sus actividades por un lapso menor a 15 minutos de tiempo o concluir las sesiones activas al finalizar sus tareas.

5.6. Registro de eventos

Todos los sistemas y aplicaciones críticos de la organización, bases de datos y dispositivos de red y servidores, deben contar con registros de eventos y bitácoras de seguridad protegidos debidamente. El Responsable de la seguridad de la información, debe resguardar por un periodo de al menos cinco años todos los registros de incidentes, alarmas, cambios, configuraciones, entre otros, que deben estar disponibles para su extracción y revisión por parte de las autoridades reguladoras, cuando sean requeridos. Se debe asegurar que los registros de acceso a sistemas, bitácoras, bases de datos y cualquier otro registro de seguridad de los aplicativos; se almacenen en un repositorio accesible para cualquier tipo de revisión o análisis.

5.7. Gestión de vulnerabilidades

La organización debe asegurarse de que los medios de almacenamiento digital o software utilizado para el almacenamiento de información cuente con los certificados que avalen la seguridad de la información (SOC 2).

6. Controles de auditoría de los sistemas de información

Las actividades de auditoría deben ser calendarizadas y planeadas para prevenir interrupciones en la operación, cada seis meses, en caso de auditores externos se debe observar lo relacionado con la aplicabilidad de los Proveedores.

6.1. Controles de red

6.2. Mensajería electrónica

El proveedor de TI, debe contar con herramientas de seguridad y de filtrado de contenido, que permitan la segmentación de navegación conforme a la operación de las áreas.

Está prohibido descargar programas de internet "no autorizados" o sin licencia de uso institucional. La instalación y actualización de programas y aplicaciones deben hacerse desde el sitio web oficial del fabricante o desde las tiendas oficiales de apps, verificando la identidad del autor de la aplicación, evitando descargar e instalar aquéllas de dudosa procedencia. Por parte del proveedor de TI, se efectuará la validación periódica que evite instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, dicho programa será incorporado en el programa de mantenimiento a los equipos de cómputo que se lleva a cabo de forma semestral, será excluido el software que se encuentra precargado de fábrica en los equipos de cómputo.

En caso de detectarse la instalación de programas o software no autorizados en las estaciones de trabajo o equipos portátiles, se deberá hacer de conocimiento al Responsable de la seguridad de la información a efecto de que se determinen las acciones y medidas correctivas correspondientes de acuerdo con el riesgo y severidad de las mismas.

Esta área debe cuidar el cumplimiento de los requerimientos de seguridad mínimos para cada elemento de la red tales como:

01. Zona de acceso – debe contar con, al menos, los siguientes controles de seguridad:
    a. Acceso desde internet:
    b. Firewall
    c. Sistema de Prevención de Intrusiones (IPS)
    d. Servidor de autenticación de dominio
    e. Acceso hacia internet
    f. Filtrado de contenido

02. Zonas de distribución – debe contar con al menos los siguientes controles:
    a. Tarjetas de Acceso, en ruteadores y switches

03. Zona interna – debe contar al menos con los siguientes controles de seguridad:
    a. Tarjetas de Acceso , en ruteadores y switches

04. Zona centro o núcleo – debe protegerse por los siguientes controles de seguridad:
    a. Firewalls

6.2. Mensajería electrónica

El Responsable de Seguridad de la Información, debe cuidar la disponibilidad y confiabilidad del correo electrónico institucional, teniendo la facultad de suspender el servicio mediante el proveedor de TI del correo electrónico institucional al colaborador que haga mal uso de este.

El correo electrónico institucional, es una herramienta de trabajo, comunicación e intercambio de información, por ende, solo es posible realizar actividades que estén relacionadas con los propósitos y funciones institucionales de operación, que debe ser utilizado de manera racional, eficaz y eficiente.

Dado que es una herramienta de trabajo, el Responsable de Seguridad de Información, tiene el derecho de efectuar la revisión y monitorización de este, por lo que su uso indebido, podrá ser motivo de suspensión temporal de la cuenta de correo, del usuario o de acuerdo a la gravedad la eliminación o inhabilitación de la misma de forma inmediata; así como de las sanciones a que se refiere el Reglamento interior del Trabajo y demás normatividad aplicable al caso en concreto.

Las comunicaciones, remisiones, almacenamiento y uso de la información serán por medios seguros debiendo el usuario garantizar la integridad y confidencialidad de la información, así mismo se debe utilizar los servicios de información seguros como https, ftp, proxy y cualquier medio de software que permita el proceso, envío, recepción o redirección de información de forma segura, confidencial y/o encriptada de extremo a extremo.
Todo el personal se obliga a utilizar de forma adecuada los servicios de red y el servicio de correo electrónico institucional.

No está permitido el uso del correo electrónico de la Institución para:

- Difundir cadenas de correos.
- Difundir mensajes de discriminación racial, religiosa, política o de cualquier otra naturaleza.
- Difundir mensajes que promocionen negocios personales o particulares.

Los usuarios deben borrar, sin abrir, todos los correos electrónicos que procedan de cuentas de correo que les sean desconocidas o cuyo “asunto” pueda relacionarse con publicidad o virus (SPAM).

Los mensajes de correo electrónico no deben borrarse porque pueden formar parte de una evidencia en los casos de auditorías. Se solicita al personal a no hacer uso de mensajería instantánea o redes sociales, para compartir información confidencial, reservada, y/o sensible; no obstante lo anterior, los respaldos correspondientes a los mensajes de correo electrónico, serán almacenados por un periodo de cinco años.

El usuario será responsable de la información que sea enviada con su cuenta, pero todos los correos electrónicos que se emitan desde cuentas de correo de la organización deben contar con la leyenda:

.

7. Planificación de la continuidad de la seguridad de la información

Los titulares de cada una de las áreas actúan como responsables para mantener la continuidad de los procesos, operaciones y servicios críticos de VENSI para casos de contingencias, acciones deliberadas, accidentales, fallas de los sistemas o desastres naturales etc.

8. Medidas de seguridad de apoyo en condiciones de teletrabajo

La Dirección define las circunstancias y requisitos para realizar trabajo a distancia, de igual forma, suministra las herramientas y controles necesarios para que se realicen de manera segura.

Cualquier persona que realice trabajo a distancia debe cumplir con las siguientes normas:

I. Cumplir en su totalidad con la presente política
II. Analizar y aprobar los métodos de conexión remota
III. Seguir los métodos y controles de seguridad implementados
IV. Verificar la efectividad de los controles aplicados sobre las conexiones remotas
V. Deberá contar con un antivirus actualizado
VI. Instalar y utilizar sólo software conocido y confiable.
VII. Mantener el software actualizado
VIII. No instalar software que permita la explotación de riesgos que comprometan la seguridad de la información o el incumplimiento de leyes o regulaciones.
IX. Queda prohibido el envío de cadenas, chistes y en general, de información que no esté relacionada con la actividad laboral de los usuarios de correo.
X. Agregar a los contactos de los que se espera respuesta o responsables directos del correo en el campo Para: las personas a las que se incluye de manera informativa agregarlas en el campo CC:, Cuando se requiere enviar copia del correo a más de 5 destinatarios, se deberán agregar en el campo CCO.
XI. En caso de requerir el envío de archivos cuyo tamaño es mayor al autorizado para el correo electrónico, se deberá utilizar la herramienta institucional para compartir documentos (DRIVE)
XII. Depurar periódicamente el buzón de entrada, elementos enviados y elementos eliminados. Una buena práctica para mantener un correo depurado es borrar los mensajes no deseados inmediatamente después de recibirlos.
XIII. Las reuniones virtuales son una herramienta para trabajar a distancia. Las soluciones de videoconferencia permiten la comunicación audiovisual a través de las redes ya con infraestructuras locales, en la nube y con soluciones híbridas con terminales físicos o soluciones software ejecutándose en diferentes plataformas hardware (portátiles, móviles y tabletas), con aplicativo de software (MS Windows, iOS, Android).
XIV. El Responsable de Seguridad de la Información deberá llevar un registro de la persona autorizada para realizar trabajo a distancia.

9. Falta u omisión

Las acciones que se enumeran a continuación, en manera enunciativa más no limitativa, constituyen infracciones a la Política de Seguridad de la información:

a) No firmar los acuerdos de confidencialidad o de responsabilidad de activos de información.
b) No actualizar la información de los activos de información a su cargo.
c) No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ellos.
d) No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral.
e) Dejar información en carpetas compartidas, no autorizadas o en lugares distintos al servidor de archivos institucional, obviando las medidas de seguridad
f) Dejar las gavetas abiertas o con las llaves puestas en los escritorios.
g) Permitir que personas ajenas a la organización, deambulen sin acompañamiento en el interior de las instalaciones, en áreas no destinadas al público.
h) Solicitar cambio de contraseña de otro usuario.
i) Utilizar claves de acceso de un usuario distinto al propio para ingresar a los sistemas y/o aplicativos.
j) Hacer uso de la red de datos, para acceder, almacenar, mantener o difundir en o desde los equipos institucionales, material con contenido sexual u ofensivo, cadenas de correos y correos masivos no autorizados.
k) La utilización de software no relacionado con la actividad laboral que pueda degradar el desempeño de la plataforma tecnológica institucional.
l) Actuar con negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de VENSI.
m) Conectar equipos de cómputo personal u otros sistemas electrónicos personales a la red de datos institucional, sin la debida autorización o utilizar los recursos tecnológicos institucionales para beneficio personal
n) Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por VENSI.
o) Destruir, dañar, borrar, deteriorar activos informáticos, sin autorización.
p) Distribuir, enviar, introducir software malicioso u otros programas de computación de efectos dañinos en las plataformas tecnológicas.
q) Alterar datos personales de las bases de datos institucionales.
r) Realizar cambios no autorizados en las plataformas tecnológicas.
s) Acceder sin autorización expresa a todo o en parte a los sistemas
t) Suplantar a un usuario ante los sistemas de autenticación y autorización establecidos.
u) No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información o permitir que otras personas accedan con el usuario y clave del titular a éstos.
v) Otorgar el acceso o privilegios a la infraestructura de VENSI a personas no autorizadas.
w) Retirar de las instalaciones de la Institución, estaciones de trabajo o equipos portátiles que contengan información institucional, sin la autorización pertinente.
x) Sustraer de las instalaciones de VENSI documentos con información institucional, o abandonarlos en lugares públicos o de fácil acceso.

y) Entregar, enseñar y divulgar información institucional, a personas o entidades no autorizadas.
z) Copiar sin autorización los programas de VENSI o violar los derechos de autor o acuerdos de licenciamiento.

10. Sanciones

Se estará a lo dispuesto por el Reglamento Interior del Trabajo y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y ante el incumplimiento de cualquiera de las determinaciones consignadas en la presente política de seguridad, descriptiva de puesto, contrato individual de trabajo, en materia de tratamiento y seguridad de la información; así como los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, así como los deberes de seguridad y confidencialidad, la LFPDPPP, su Reglamento y demás normativa aplicable.