TILLIT
Asesores Empresariales

Identificación de las medidas de seguridad y Análisis de Brecha

En cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en lo sucesivo, LFPDPPP), se informa que el responsable del tratamiento de sus datos personales es TILLIT AE S.C., (en adelante "TILLIT", "nosotros", la "Firma"), tiene con domicilio fiscal en Calle Napoles 2578, Italia Providencia, C.P. 44630 Guadalajara, Jalisco.

En cumplimiento con el artículo 6 de la LFPDPPP) se documentan las medidas de seguridad administrativas, técnicas o físicas que permiten disminuir los riesgos.

Objetivo de Control	Descripción
Políticas del SGSDP	
Políticas de gestión de datos personales	Se cuenta con Política de Privacidad, Aviso de Privacidad, Formato para ejercer Derechos ARCO.
Revisión y evaluación	La Política se revisa de forma Anual.
Documentación del SGSDP	Se cuenta con banco de formatos. Se cuenta con evidencia de entrega de Aviso de Privacidad a Empleados.
Cumplimiento legal	
Identificación de la legislación/regulación aplicable	Se respeta lo contenido en el Contrato de Prestación de Servicios celebrado con el cliente.
Salvaguarda de registros organizacionales	Se debe mantener el resguardo de todos los registros y documentación que pudieran ser evidencia o bien, requeridos en cumplimiento de la LFPDPPP y protegerlos contra pérdida, destrucción, falsificación, acceso o revelación no autorizados.
Prevención del mal uso de activos	Se cuenta con un Sistema particular "SIBYL" donde se almacena y gestiona la información, cuenta con medidas de seguridad para su ingreso y niveles de autorización.
Recolección de evidencia	Se recolecta la información qué se requiere para cumplir con los servicios que señalan los Contratos de Prestación de Servicios y la envía "Electrónica" y "Física" voluntariamente el Titular.
Revisión de cumplimiento técnico	La calidad de la información se verifica en la calidad probatoria de cada documento, se analizarán los resultados de los procedimientos en los que se utilizaron.
Controles de auditoría de sistemas	Los Socios revisan mensualmente que la información se integre a los expedientes según los Contratos de Prestación de Servicios.
Protección del soporte de auditoría del sistema	La revisión queda documentada mediante las entrevistas con el Titular de la información.
Estructura organizacional de la seguridad	
Administración y Coordinación de la seguridad de la información	Se recaban las iniciativas generadas por el equipo, apoyadas en la comunicación efectiva entre las diferentes áreas de la organización para la implementación de controles de seguridad, coordinados por la persona a cargo de la seguridad de la información personal.
Designación de deberes en seguridad y protección de datos personales	El Organigrama limita privilegios.
Recomendaciones de un especialista en seguridad de la información.	Cuando sea adecuado, obtener el consejo y recomendaciones de un especialista en protección de datos y seguridad de la información.
Cooperación con organizaciones	Por la forma de gestionar los Datos no se detecta ninguna vulnerabilidad.
Revisión de implementación	Realizar una revisión periódica de la implementación del SGSDP por auditores internos o externos.
Identificación de riesgos de terceros	No hay involucramiento de terceros en el tratamiento de los datos personales.
Requerimientos de seguridad en contratos con terceros	No se comparten Datos con terceros.
Requerimientos de seguridad en contratos con servicios de	Se tiene limitado el acceso a las carpetas a integrantes de TILLIT

<table>
<tr><td>almacenamiento de información y computo en la nube</td><td></td></tr>
<tr><td colspan="2">Clasificación y acceso a los activos</td></tr>
<tr><td>Inventario y clasificación de datos personales</td><td>Se alimenta en SIBYL y los correos en Gmail, ambos con acceso restringido.</td></tr>
<tr><td>Inventario de activos</td><td>Se alimenta en SIBYL y los correos en Gmail, ambos con acceso restringido.</td></tr>
<tr><td>Identificación de procesos de datos personales</td><td>Los Datos los entrega le cliente para su defensa legal y regresan al mismo al terminar los juicios.</td></tr>
<tr><td colspan="2">Seguridad del Personal</td></tr>
<tr><td>Acuerdo de confidencialidad</td><td>Se debe firmar un acuerdo de confidencialidad o no revelación de información por los nuevos empleados de la organización involucrados en el tratamiento de los datos personales.</td></tr>
<tr><td>Términos y condiciones de empleo</td><td>Dentro de los términos de contratación, la organización debe informar ampliamente a los nuevos empleados sobre sus deberes y compromisos respecto a la seguridad de la información y protección de datos personales.
También deberá considerarse la presentación de un aviso de privacidad al personal interno del cual recabaremos datos personales de distintos tipos.</td></tr>
<tr><td>Proceso disciplinario</td><td>Debe existir un proceso disciplinario en la organización para aquellos que no cumplan o violenten lo establecido en la política o procedimientos.</td></tr>
<tr><td colspan="2">Seguridad física y ambiental</td></tr>
<tr><td>Perímetro de seguridad</td><td>El archivo de expedientes físicos se encuentra dentro de la oficina y dentro de la oficina se encuentra en el área de Litigio donde hay puerta y se abre con llave específica. Se identifica con un número consecutivo.
El archivo electrónico de expedientes se encuentra en Google DRIVE, se tiene en carpetas donde solo miembros de TILLIT pueden acceder con su usuario de correo y contraseña.
Los expedientes terminados se entregan dentro de los 60 días siguientes a su archivo y se recaba un acuse de recibo, el acuse tiene el siguiente:
<table>
<tr><th></th><th>Expediente Cerrados</th><th></th></tr>
<tr><td>1</td><td>Verificar correo en que se avisa que se cierra juicio</td><td></td></tr>
<tr><td>2</td><td>Baja en Sibyl</td><td></td></tr>
<tr><td>3</td><td>Solicitud de baja en BUZÓN ELECTRÓNICO (de ser aplicable)</td><td></td></tr>
<tr><td>4</td><td>Aparece en Boletin acuerdo de baja de BUZÓN</td><td></td></tr>
<tr><td>5</td><td>Pasa a terminados en DRIVE</td><td></td></tr>
<tr><td>6</td><td>Se hacen cambios en REPORTE</td><td></td></tr>
<tr><td>7</td><td>Se da de baja en archivo de cálculo</td><td></td></tr>
<tr><td>8</td><td>Formato de acuse y copia</td><td></td></tr>
<tr><td>9</td><td>Acuse firmado guardado en consecutivo</td><td></td></tr>
</table>
El archivo electrónico tiene una vigencia de dos años.
Los expedientes vigentes sólo pueden abandonar la oficina para a) Audiencias y b) Citas con el cliente
Los expedientes no vigentes sólo abandonan la oficina para ser entregados.
ambos podrán excepcionalmente abandonar la oficina en caso de cambio de domicilio.</td></tr>
<tr><td colspan="2">Gestión de comunicaciones y operaciones</td></tr>
<tr><td>Protección contra software malicioso</td><td>Se utilizan los del proveedor Gmail</td></tr>
<tr><td>Respaldo de la información</td><td>Se generan respaldos de la información de forma mensual en SIBYL y diarios en Google Drive.Las copias de seguridad se suben a los servidores de Google y se encriptan con la contraseña de tu Cuenta de Google</td></tr>
<tr><td>Registros de operadores</td><td>Tanto SIBYL como Gmail informan fallas.</td></tr>
<tr><td>Registro de fallas</td><td>Tanto SIBYL como Gmail informan fallas.</td></tr>
<tr><td>Controles de red</td><td>N/A</td></tr>
<tr><td>Gestión de soportes informáticos extraíbles</td><td>No se permite el uso de soportes informáticos extraíbles como memorias USB, discos, cintas magnéticas, etc. fuera de la oficina.</td></tr>
</table>

Documentación de seguridad del sistema	Toda la documentación de los sistemas y activos de información debe ser protegida de acceso no autorizado.
Seguridad de medios en tránsito	Se debe asegurar el traslado de soportes físicos/electrónicos que contengan datos personales contra robo, acceso, uso indebido o corrupción.
Comercio electrónico seguro	No se comercia con los Datos Personales.
Mensajería electrónica	Solo se permite recibir y compartir la información con los clientes que se tiene celebrado contrato de prestación de servicios. Principalmente se utilizará correo electrónico y por excepción el uso de mensajería por teléfono móvil.
Seguridad en sistemas electrónicos	El sistema propio tiene usuario y contraseña.
Otras formas de intercambio de información	Solo puede ser vía correo o física y para los fines autorizados.
Disociación y Separación	La información solo se utiliza para los fines contratados.
Reglas de control de acceso	Existen reglas y privilegios para cada usuario.
Uso de servicios de red	Se tiene red única para la gestión de litigios.
Autenticación de usuario para conexiones externas	Se tiene habilitada en Google Drive y Gmail así como la paquetería que se notifique cualquier intento de ingreso de usuario nuevo o desconocido.
Proceso de inicio de sesión	Sólo se debe tener acceso a los sistemas de datos personales a través de un inicio de sesión seguro, esto minimiza los accesos no autorizados.
Alerta de coerción a usuarios	N/A
Trazabilidad de tratamiento	El sistema SIBYL y la herramienta Google Drive y Gmail permiten observar la trazabilidad y la posibilidad de identificar quién tuvo acceso a los datos personales y los tratamientos realizados.
Sincronización de relojes	No se opera con relojes en tiempo real qué requieran sincronización.
Dispositivos móviles internos.	No se permite utilizar móviles diversos a los registrados por el personal.
Dispositivos móviles externos.	No se permite utilizar móviles diversos a los registrados por el personal.
Almacenamiento privado dentro del entorno de operación	Se almacena y usa solo equipo y correos corporativos.
Teletrabajo	N/A
Validación de datos de entrada	Los sistemas propios y de terceros solicitan usuarios y contraseña.
Validación de datos de salida	En el caso de aplicaciones se debe asegurar que los datos entregados sean los esperados y que se proporcionen en las circunstancias adecuadas.
Cifrado	No se usa cifrado de “salida”. Se respeta el cifrado de recepción en los casos que las personas con las que se celebren contratos lo requieran.
Firmas electrónicas	N/A
Servicios de no- repudio	N/A
Control de software y sistemas	Se deben tener controles y procesos para integrar software al ambiente operacional, para minimizar el riesgo de corrupción de datos. Se debe probar cualquier cambio o actualización de sistemas críticos antes de implementarse en la organización. Se deben aplicar los cambios a una copia concreta del software original y evaluar su funcionamiento.
Procedimientos de notificación de vulneraciones de seguridad a titulares	Vía correo o conforme a los contratos de prestación de servicios.

Atentamente
TILLIT ASESORES EMPRESARIALES S.C.

Luis Raúl Meza Mora / Representante
(Actualizado a Diciembre 10 2022)

Francisco Arturo Rivera Morales / Responsable de Privacidad