

DOCUMENTO DE SEGURIDAD

DEFINICIONES PARA EL DOCUMENTO DE SEGURIDAD

Para los efectos del presente documento, se tomarán las definiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, sin perjuicio de lo previsto en la normativa aplicable en la materia, se entenderá por:

Áreas responsables: Instancias de los sujetos obligados **previstas en los respectivos reglamentos interiores**, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento y ser responsables o encargadas de los datos personales y que deciden sobre el tratamiento de datos personales.

Aviso de privacidad: Documento a disposición del titular de forma física, electrónica, o en cualquier formato generado por el responsable, 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 referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de dichas responsabilidades. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Consentimiento: Manifestación de la voluntad libre, específica, e informada, del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

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 políticas y preferencia sexual.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación, y oposición de datos personales.

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Documento de seguridad: Instrumento que describe y da cuenta de manera general de 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.

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

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 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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, a sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y
- d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

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 de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y
- d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Supresión: La **baja archivística** de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Transferencia: 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 datos personales.

SECRETARÍA DE INNOVACIÓN Y GOBIERNO DIGITAL DEL
ESTADO DE AGUASCALIENTES **(SIGOD)**
DOCUMENTO DE SEGURIDAD

PRESENTACIÓN

La Secretaría de Innovación y Gobierno Digital (SIGOD) del Estado de Aguascalientes, acepta que la información que se recaba, genera, procesa y resguarda, debe ser tratada en estricto apego al marco legal aplicable durante todo su ciclo de vida y preservando, en todo momento, el derecho de protección de datos personales de todas las personas, incluyendo servidores públicos, lo cual es responsabilidad de todas las áreas previstas en el artículo 8° del Reglamento Interior de la Secretaría de Innovación y Gobierno Digital, en el estricto apego a sus funciones, tratan esta información.

MARCO NORMATIVO

Artículos 6°, Base A, fracciones II y III, y 16 párrafo segundo de la Constitución de los Estados Unidos Mexicanos; Artículo 3, Título Primero, Capítulos I y II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; Títulos Sexto y Séptimo de la Ley General de Transparencia y Acceso a la Información Pública.

SISTEMA DE GESTIÓN

1.- INVENTARIO DE DATOS PERSONALES Y SISTEMAS DE TRATAMIENTO

INVENTARIO DE DATOS PERSONALES				
Fecha de Recepción de Datos Personales	Datos Personales Sometidos a Tratamiento	Finalidad del Tratamiento	Transferencia de Datos Personales	Periodo de Conservación de Datos Personales
17/feb/2023	Nombre (opcional en el caso de solicitudes de transparencia, y necesario en ejercicio de Derecho ARCO) Domicilio (Opcional, para notificaciones) Correo (Opcional como medio de notificación) Teléfono (Opcional como medio de contacto)	Podrán ser utilizados para fines estadísticos, así como para dar cumplimiento a las facultades propias de la SIGOD contempladas en la Ley Orgánica de la Administración Estatal, en su artículo 40, y las demás que señalen las leyes, reglamentos y ordenamientos de carácter general y demás supuestos que se encuentran previstos en el artículo 22 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en correlación al 24 Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Aguascalientes y sus Municipios	Sus datos personales no serán transferidos, difundidos, ni distribuidos, salvo lo señalado en el artículo 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 24 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Aguascalientes y sus Municipios	De conformidad con el artículo 58 de la Ley General de Archivo, el archivo de concentración se conservará por un periodo de siete años.

SECRETARÍA DE INNOVACIÓN Y GOBIERNO DIGITAL DEL
ESTADO DE AGUASCALIENTES (**SIGOD**)
DOCUMENTO DE SEGURIDAD

Etapas del Ciclo de Vida en la que se Encuentran los Datos Personales			
Obtención	Uso	Bloqueo	Supresión
X	X		No se ha dado el supuesto

SISTEMAS DE TRATAMIENTO Bases de Datos	
Físicos	Digitales
Recepción de Información Documental; Archivo de Trámite;	Plataforma Nacional de Transparencia Word, Excel,

Ejercicio de Derechos ARCO				
Acceso	Rectificación	Cancelación	Oposición	No aplica
X	X	X	X	
Consentimiento Expreso del Titular de los Datos Personales				
Difundir	Distribuir	Comercializar	No se otorgó consentimiento expreso	
X	X	No aplica	No aplica	

2.- FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

Unidad administrativa:	De conformidad con el artículo 8° del Reglamento Interior de la Secretaría de Innovación y Gobierno Digital son: Unidades Administrativas serán las siguientes: A) Dirección General de Innovación y Mejora Regulatoria; B) Dirección General de Sistemas de Información; C) Dirección General de Servicios de Tecnologías de Información (TI); D) Coordinación Administrativa; E) Coordinación Jurídica; y F) Unidad de Política Informática
Empleo, Cargo o Comisión del Responsable o Encargado:	A) Directora (o) General de Innovación y Mejora Regulatoria B) Directora (o) General de Sistemas de Información C) Directora (o) General de Servicios de Tecnologías de Información (TI); D) Coordinador (a) Administrativa; E) Coordinador (a) Jurídica F) Jefa (e) de Departamento de la Unidad de Política Informática.
Atribuciones de la Unidad Administrativa y Fundamento Jurídico que habilita el tratamiento:	A) Dirección General de Innovación y Mejora Regulatoria, de conformidad con el artículo 14 del Reglamento Interior de la Secretaría de Innovación y Gobierno Digital son; B) Dirección General de Sistemas de Información, de conformidad con el artículo 15 del Reglamento Interior de la Secretaría de Innovación y Gobierno Digital son; C) Dirección General de Servicios de Tecnologías de Información (TI) , de conformidad con el artículo 16 del Reglamento Interior de la Secretaría de Innovación y Gobierno Digital son; D) Coordinación Administrativa, de conformidad con el artículo 17 del Reglamento Interior de la Secretaría de Innovación y Gobierno Digital son; E) Coordinación Jurídica, de conformidad con el artículo 18 del Reglamento Interior de la Secretaría de Innovación y Gobierno Digital son; y F) Unidad de Política Informática, de conformidad con el artículo 19 del Reglamento Interior de la Secretaría de Innovación y Gobierno Digital son

SECRETARÍA DE INNOVACIÓN Y GOBIERNO DIGITAL DEL
ESTADO DE AGUASCALIENTES **(SIGOD)**
DOCUMENTO DE SEGURIDAD

3.- ANÁLISIS DE RIESGOS

Tipo de Datos Personales	Número de Personas que dan Tratamiento de Datos Personales	Sitios de Resguardo	Nivel de Riesgo Inherente (Bajo, Medio, Alto, Reforzado)
Los datos personales que recabe la Secretaría de Innovación y Gobierno Digital del Estado de Aguascalientes, es ingresada por los ciudadanos y/o usuarios dentro de la página https://www.aguascalientes.gob.mx/SIGOD/ y se informa que podrán ser utilizados para fines estadísticos, así como para dar cumplimiento a las facultades propias de la SIGOD contempladas en la Ley Orgánica de la Administración Estatal, en su artículo 40, y las demás que señalen las leyes,	(6)	En las Oficinas de la SIGOD, en cada una de las áreas de las Unidades Administrativas	<p>(Bajo: considera información general concerniente a una persona física identificada o identificable)</p> <p>(Medio: permiten conocer la ubicación física de la persona, su patrimonio, datos de autenticación o jurídicos)</p> <p>(Alto: contempla datos personales sensibles)</p> <p>(Reforzado: de acuerdo a su naturaleza pueden derivar en mayor beneficio para un atacante, por ejemplo: información adicional como códigos de seguridad, números de identificaciones personales, o relacionados con niveles de primer mando, figuras públicas, líderes, o información relacionada con la impartición de justicia o seguridad nacional)</p>

AMENAZAS		
Origen de la Amenaza	Motivación/Causa	Posibles Consecuencias
Hacker; Cracker; Criminal Cibernetico,	Desafío; Dinero; Ego; Estatus; Rebelión; Alteración no Autorizada de Información; Intereses Geopolíticos; Destrucción de Información; Ganancia Económica; Revelación Ilegal de Información.	Acceso No Autorizado al Sistema; Pérdida Económica; Pérdida de Credibilidad; Reducción de la Productividad, Riesgos legales o falta de cumplimiento normativo; Intrusión en los Sistemas; Robo de Información, Código Malicioso, Interrupción de Servicios
Interno. - Personal No Capacitado; Descontento; Negligente	Curiosidad; Ego; Errores No Intencionales u Omisiones; Venganza,	Abuso en la Operación de los Sistemas; Acceso No Autorizado a los Sistemas;

POSIBLES VULNERABILIDADES	
Personal	Uso Incorrecto de Software y Hardware
Daño Físico	Posibilidad de Fuego (baja); Afectaciones por Agua o Lluvias (Baja vulnerabilidad)
Eventos Naturales	Fenómenos Climáticos o Meteorológicos; Fenómenos Sísmicos
Pérdida de Servicios Básicos	Falla en el Sistema de Aire Acondicionado o Suministro de Agua; Pérdida de Suministro Eléctrico; Falla en los Equipos, Falla en la Planta de Emergencia; Falla en el Sistema Extinción de Incendios.
Hardware y Software	Robo de Equipo; Alteración de Hardware; Alteración de Software; Fallas del Equipo o Malfuncionamiento del Equipo; Saturación de los Sistemas de Información; Malfuncionamiento del Software; Falla en el Mantenimiento del Sistema de Información, Interrupción Servicio

SECRETARÍA DE INNOVACIÓN Y GOBIERNO DIGITAL DEL
ESTADO DE AGUASCALIENTES **(SIGOD)**
DOCUMENTO DE SEGURIDAD

Recursos Involucrados en el Tratamiento de Datos Personales			
Físico	Internet	Hardware	Software
X (opcional)	X	X	X



4.- ANÁLISIS DE BRECHA

Medidas de Seguridad Existentes	Medidas de Seguridad Faltantes
Físicas: Controles de Acceso Técnicas: Usuarios y Perfiles limitados Software y Hardware: Firewalls, Red Interna o Intranet	Mayores Capacitaciones. Fallas o Causas de Fuerza Mayor respecto los servicios brindados por terceros. Fortalecimiento (mejora continua) en los procesos de seguridad internas

SECRETARÍA DE INNOVACIÓN Y GOBIERNO DIGITAL DEL ESTADO DE AGUASCALIENTES (SIGOD) DOCUMENTO DE SEGURIDAD

5.- PLAN DE TRABAJO

La SIGOD, en cumplimiento al Control Interno, ha establecido el plan de trabajo el cual se encuentra publicado en el siguiente link:
<https://www.aguascalientes.gob.mx/SIGOD/ControlInterno/CI/PTCI%202023.pdf>

<div>  <div> Secretaría de Innovación y Gobierno Digital </div> </div> <div> GOBIERNO DEL ESTADO DE AGUASCALIENTES NOMBRE DE LA DEPENDENCIA O ENTIDAD IMPLEMENTACIÓN Y FORTALECIMIENTO DEL SISTEMA DE CONTROL INTERNO INSTITUCIONAL PROGRAMA DE TRABAJO DE CONTROL INTERNO DEL EJERCICIO 2023 </div> <div>  </div>												
No	NGCI	Elemento de Control	Ref. Eval.	% de Cumplimiento SI/No	% de Cumplimiento con base en la evidencia	Acción de Mejora	Fecha de Inicio	Fecha de término	Unidad Administrativa	Responsable	Medio de Verificación	Indicador de Avance
AMBIENTE DE CONTROL												
1	Art. 12, fracc II, inciso b), 2, 4	Actualización de las Descripciones de Puestos de la SIGOD	0.5	SI	50%	Realizar las modificaciones en el Sistema de Descripciones de Puestos	junio	septiembre	Coordinación Administrativa	Encargada de Capital Humano	Plataforma de Descripción de Puestos	Avanzado
2	Art. 12, fracc II, inciso e), 5, 9	Publicación de los Manuales del Operación y Organización de la SIGOD	0.5	SI	50%	Creación de los Manuales para la Dependencia	febrero	septiembre	Dirección General de Innovación y Mejora Regulatoria	Jefe del Depto. De Organización y Simplificación Administrativa	Portal de SIGOD, Manuales publicados	Avanzado
EVALUACIÓN DE RIESGOS												
3	MEMICI Principio 8 Considerar el Riesgo de Corrupción	Realización, evaluación y seguimiento del Programa de Trabajo de Administración de Riesgos	1	SI	100%	Realización del PTAR	marzo	abril	Coordinación Administrativa	Coordinadora Administrativa	PTAR	Avanzado
ACTIVIDADES DE CONTROL												
4	Art. 14, fracc I, incisos b) y c), 2 y 3, 2.3 y 4	Seguimiento al cumplimiento de Objetivos y Metas	1	SI	100%	Evaluación de Objetivos y Metas	enero	septiembre	Unidades Administrativas	Mandos Medios	Evaluaciones en el SEDE	Óptimo
5	Art. 14, fracc III, inciso d), 4, 5	Creación de resguardos de los bienes de la SIGOD	0	SI	0%	Creación y validación constante de los resguardos de bienes	enero	septiembre	Coordinación Administrativa	Coordinadora Administrativa	Resguardos	Inicial
6	Art. 14, fracc III, inciso f), 6, 1-7	Creación y actualización de controles en materia de TICS	0.5	SI	50%	Análisis de los controles necesarios para el área de TICS para su creación y correcta implementación	abril	septiembre	Dirección General de Servicios de TI	Director General de Servicios de TI	Documentos de control	Inicial
INFORMACIÓN Y COMUNICACIÓN												
7	Art. 15, fracc II, inciso e), 5, 5	Formato de quejas y denuncias	1	SI	100%	Creación del formato de quejas y denuncias	abril	abril	Coordinación Administrativa	Encargada de Capital Humano	Formato de quejas y denuncias	Óptimo
8	Art. 15, fracc I, 1, 1 y 2	Llevar un registro de los acuerdos tomados en las reuniones comités, etc.	0	SI	0%	Toma de notas de reuniones donde se tomen decisiones importantes sobre la SIGOD para tener un seguimiento de esos temas	abril	septiembre	Todas las Unidades Administrativas	Director General o Coordinador a cargo de la reunión	Notas de las reuniones con los acuerdos	Inicial
SUPERVISIÓN												
9	Art. 16 Segundo párrafo	Informar a el titular de la Dependencia así como al CE sobre los avances en temas de Control Interno	1	SI	50%	Informes trimestrales sobre tema de Control Interno en la Dependencia	enero	septiembre	Coordinación Administrativa	Coordinadora Administrativa	Informes	Inicial

SECRETARÍA DE INNOVACIÓN Y GOBIERNO DIGITAL DEL
ESTADO DE AGUASCALIENTES **(SIGOD)**
DOCUMENTO DE SEGURIDAD

Se elaborará un Plan de Trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales; entre las cuales se pueden encontrar las siguientes:

Control	Parámetro
Políticas	
Políticas de Gestión de Datos Personales	Implementación y mantenimiento de los diferentes controles establecidos para salvaguardar los datos personales que efectuara cada una de las Unidades Administrativas en cumplimiento a su normatividad para dar cumplimiento a sus objetivos y metas
Revisión y Evaluación	Medidas implementadas deberán ser revisadas y evaluadas de conformidad con el Programa de Control Interno del Ejercicio correspondiente.
Identificación y Documentación	Identificar y documentar cada una de las Unidades Administrativas de acuerdo al Catálogo de Disposición Documental.
Cumplimiento Legal	
Legislación/Regulación Aplicable	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; Títulos Sexto y Séptimo de la Ley General de Transparencia y Acceso a la Información Pública.
Salvaguarda de Registros	En cumplimiento a la Ley General de Archivos, cada una de las Unidades Administrativas de cumplirá con los plazos de conservación de acuerdo al Catálogo de Disposición Documental.
Prevención del Mal Uso de la Información	Se deberá cumplimiento al Código de Conducta de la Administración Pública Centralizada del Estado de Aguascalientes, de manera destacada cumpliendo los Principios de Legalidad Honradez, Lealtad, Objetividad. Controlar la identificación, asignación, ubicación y uso o utilidad de los activos inventariados.
Recolección de Evidencia	En caso de una vulneración o incidente de seguridad no borrar archivos, ni logs ya que servirán de evidencia para el análisis forense
Revisión de Cumplimiento Técnico	Se deben revisar los activos y sus controles de seguridad, tal que se verifique su correcto funcionamiento, así como las posibles amenazas y vulnerabilidades relacionadas.
Controles de Auditoría de Sistemas	Se debe tener un proceso para la revisión y evaluación del funcionamiento de los sistemas, tal que se minimicen las consecuencias de posibles vulneraciones y se logre un ciclo de mejora continua.
Protección del Soporte de Auditoría del Sistema	Se deben proteger las herramientas, el software y los archivos de datos que surjan o se utilicen en una auditoría, para evitar comprometer la seguridad de la información de la organización.
Estructura Organizacional de la Seguridad	
Administración y Coordinación de la Seguridad de la Información	Cada una de las Unidades Administrativas deberá tener claros sus objetivos y metas; apoyados en la comunicación efectiva y la implementación de controles de seguridad.
Designación de Deberes en Seguridad y Protección de Datos Personales	Cada una de las Unidades Administrativas deberá designar persona que funja como responsable y enlace de protección de datos personales.
Clasificación y Acceso a la Información	
Inventario y Clasificación de Datos Personales	Cada una de las Unidades Administrativas deberá primeramente Identificar los Datos Personales, los datos personales recolectados y tratados en cualquier soporte físico o electrónico, teniendo especial atención en los datos sensibles, financieros y patrimoniales.
Identificación de Procesos de Datos Personales)	Cada una de las Unidades Administrativas deberá identificar el ciclo de vida de los datos personales en cada uno de sus procesos, desde la obtención, almacenamiento, procesamiento, cancelación o cualquiera que sea su tratamiento. Esto es especialmente importante para conocer dónde se resguardan y qué se hace con los datos personales, lo cual contribuye también en agilizar la respuesta al ejercicio de los derechos ARCO por parte de un titular.
Seguridad del Personal	

**SECRETARÍA DE INNOVACIÓN Y GOBIERNO DIGITAL DEL
ESTADO DE AGUASCALIENTES (SIGOD)
DOCUMENTO DE SEGURIDAD**

Identificar Responsabilidades de Seguridad en cada Puesto de Trabajo	Cada una de las Unidades Administrativas deberá identificar que personas de acuerdo con sus funciones efectúan tratamiento de datos personales, para efecto de concientizar y responsabilizar respecto a la seguridad y protección de datos personales.
Capacitación	Las personas que tengan tratamiento de datos personales, se deberán comprometer a tomar capacitaciones en la materia.
Proceso Disciplinario	De conformidad con el Título Decimo Primero de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con Capítulo VI del Título Octavo de la Ley General de Transparencia y Acceso a la Información Pública, así como las responsabilidades que resulten de los procedimientos administrativos en término de la Ley de Responsabilidades Administrativas del Estado de Aguascalientes.
Seguridad Física y Ambiental	
Perímetro de Seguridad	Mecanismos de seguridad, puertas con control de acceso, vigilancia por guardias de seguridad.
Seguridad en Entornos de Trabajo	Cada una de las Unidades Administrativas deberá Implementar mecanismos para mantener las áreas de resguardo y el resguardo de su documentación.
Protección de Propiedad	Revisar e identificar los activos, como equipo y/o software que sean susceptibles de sustracción o alteración
Gestiones de Comunicaciones y Operaciones	
Control de Cambios Operacionales	Cada una de las Unidades Administrativas deberá Implementar de acuerdo a sus procedimientos cualquier cambio que pueda afectar las operaciones relacionadas con datos personales.
Protección Contra Software Malicioso	Deben existir diferentes controles respecto al software malicioso: Prohibir el uso de software ilegal y/o no autorizado. Aplicar difusión (campañas, boletines, via correo electrónico institucional). Mantener en los dispositivos de procesamiento de información como computadoras, las respectivas herramientas actualizadas que las protejan contra software malicioso.
Respaldo de la Información	Cada una de las Unidades Administrativas deberá generar respaldos y el respectivo almacenaje de los soportes físicos y/o electrónicos, especialmente para el ejercicio de derechos ARCO.
Registro de Fallas	Las fallas en sistemas y activos deben poder reportarse y gestionarse, esto incluye la corrección de la falla y revisión de los registros, debiendo las de reportar a sus jefes inmediatos, y en casos de falla informática a la mesa de ayuda extensión 5001.
Mensajería Electrónica	Se debe hacer uso adecuado del correo electrónico institucional, procurando efectuar resguardos en las PC asignada a los servidores publicos
Divulgación de Información de manera Pública	La información que tenga el carácter de pública deberá de publicarse en la PNT, https://www.plataformadetransparencia.org.mx/ De conformidad con la Ley General de Transparencia.
Control de Acceso	
Reglas de Control de Acceso	Reglas y privilegios para cada usuario o grupo de usuarios conforme a sus responsabilidades o perfiles.
Gestión de Usuarios y Contraseñas	Las cuentas de usuario serán únicas e intranferibles y estarán formadas por la siguiente nomenclatura: Nombre +. (Punto) + Primer apellido + una letra adicional para evitar duplicidad en caso de homonimia, preferentemente primera letra del segundo apellido La contraseña de inicio de sesión asignada deberá cambiarse, cada 90 días, por una particular con el fin de evitar robo y/o acceso no autorizado y deberá estar conformada bajo los siguientes requisitos. 8 caracteres como mínimo. Al menos una mayúscula. Al menos una minúscula. Al menos un número. Al menos un carácter especial El personal deberá memorizar la contraseña asignada, o bien asegurarse de resguardarlo, absteniéndose de dejarla disponible y a la mano en su escritorio, computadora o cualquier

SECRETARÍA DE INNOVACIÓN Y GOBIERNO DIGITAL DEL
ESTADO DE AGUASCALIENTES **(SIGOD)**
DOCUMENTO DE SEGURIDAD

	medio físico o electrónico expuesto en su lugar de trabajo ni ser compartida, divulgada y/o publicada
Restricción de Acceso a Datos Personales	El Tratamiento de datos personales será exclusivo a las finalidades y en cumplimiento de las facultades y obligaciones de Cada una de las Unidades Administrativas, y solamente por quien cuente con dichas facultades.
Registro de Eventos	Cada una de las Unidades Administrativas deberá de documentar y/o registrar eventos de excepciones y eventos relevantes de seguridad en los sistemas y activos, los cuales deben almacenarse un periodo acordado para investigación y control de acceso.
Desarrollo y Mantenimiento de Sistemas	
Control de Acceso a Software de Configuración	El acceso a los usuarios se efectuará con las correspondientes contraseñas vigentes.
Reporte y Manejo de Incidentes)	Reporte de Incidentes de Seguridad causados por: Reporte por daño físico/lógico, robo/vandalismo. Ataque con código malicioso desde la LAN. Ciberataque, desde la WAN. Fuga de información o Posible Fuga de Información Bloqueo de acceso al sistema en el equipo de cómputo.
Procedimientos de Acción en caso de Incidente	Se deberá de Reportar Mesa de Ayuda, extensión 5001, levantará el ticket, registrando: Datos del solicitante (nombre, teléfono, área, correo, fecha). Detalles del requerimiento de soporte. Detalles del incidente, como: • Tipo de incidente. • Fecha en que se descubrió. • Clasificación del incidente
Revisión y Actualización)	Contar con el antivirus institucional instalado y actualizado Aplicar los parches de seguridad y actualizaciones del sistema operativo del equipo.

6.- MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Bitácora de las Vulneraciones a la Seguridad			
Descripción de la Vulneración de Seguridad	Fecha en la que Ocurrió	Motivo de la Vulneración	Acciones Correctivas Implementadas de Forma Inmediata y Definitiva
La pérdida o destrucción no autorizada	(Día, Mes y Año)		Contar con el antivirus institucional instalado y actualizado Aplicar los parches de seguridad y actualizaciones del sistema operativo del equipo
El robo, extravío o copia no autorizada			
El uso, acceso o tratamiento no autorizado			
El daño, la alteración o modificación no autorizada)			

SECRETARÍA DE INNOVACIÓN Y GOBIERNO DIGITAL DEL
ESTADO DE AGUASCALIENTES **(SIGOD)**
DOCUMENTO DE SEGURIDAD

7.- PROGRAMA GENERAL DE CAPACITACIÓN

Cada una de las Unidades Administrativas propondrá al Comité de Transparencia de la SIGOD, programas de capacitación de acuerdo a las necesidades de las Unidades Administrativas, de no hacer propuesta las unidades dentro de los primeros cinco días de enero de cada año, el Comité de Transparencia designara Capacitaciones que puedan ser tomadas en Línea o por Correo Institucional.

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente documento de Seguridad es un esbozo, que se irá actualizando conforme:

Evento por el cual se Actualiza el Documento de Seguridad			
Se produjeron modificaciones sustanciales al tratamiento de datos personales que derivan en un cambio en el nivel de riesgo	Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión	Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida	Implementación de acciones correctivas y preventivas ante una vulneración de seguridad