Movimiento Ciudadano Jalisco

Documento de Seguridad

Última Actualización

03/11/2026

Contenido

Catálogo de Sistemas de Tratamiento....2
Sistema de Tratamiento de Afiliaciones y Círculos Ciudadanos....2
Sistema de Tratamiento de Asuntos Jurídicos y Electorales....3
Sistema de Tratamiento de Vinculación de las Estructuras Juveniles Municipales, Distritales y Estatales....5
Sistema de Tratamiento de Vinculación de las Estructuras de Movimientos Sociales....6
Sistema de Tratamiento de Solicitudes de Acceso a la Información y de Derechos ARCO....7
Sistema de Tratamiento de Procesos Internos.....9
Sistema de Tratamiento de Datos Personales del Padrón de Proveedores/Contratos de Prestación de Servicios....10
Sistema de Tratamiento de Vinculación con los Actores....12
Controles y mecanismos de seguridad para las transferencias....14
Controles de Identificación y Autentificación de Usuarios....15
Procedimientos de respaldo y recuperación de datos personales....15
Técnicas de supresión y borrado seguro de datos personales....16
Análisis de Riesgo....16
Gestión de Vulneraciones....20
Plan de Contingencia....21
Mecanismos de monitoreo y revisión de las medidas de seguridad....23
Análisis de Brecha....23
Plan de trabajo....26
Programa General de Capacitación....27
Anexos....27

Catálogo de Sistemas de Tratamiento

Sistema de Tratamiento de Afiliaciones y Círculos Ciudadanos	
Administrador	Ricardo Joaquín Ramírez Franco
Cargo	Encargado
Área	Secretaría de Afiliaciones
Funciones y Obligaciones	Se solicita al interesado su credencial INE para llenar una cedula de afiliación, se le saca una copia fotostática y el propietario la firma donde da su consentimiento que la copia es exclusivamente para afiliación, se sube a la plataforma del partido, se guarda un tiempo y después se manda al nacional para su validez.
Personal autorizado para el tratamiento	
Nombre	Hilda Maritza Oropeza Silva
Cargo	Auxiliar
Funciones y Obligaciones	Se solicita al interesado su credencial INE para llenar una cedula de afiliación, se le saca una copia fotostática y el propietario la firma donde da su consentimiento que la copia es exclusivamente para afiliación, se sube a la plataforma del partido, se guarda un tiempo y después se manda al nacional para su validez.
Inventario de datos personales	Nombre, correo, teléfono, domicilio, INE, firma.
Bases de datos	Base de datos de afiliaciones y círculos de ciudadanos
Número de titulares	Entre 501 hasta 5 mil
Tipo de soporte	
Físico	Archivero el cual se encuentra bajo llave y solo dos personas tienen acceso a mismo.
Electrónico	Red interna
Características del lugar de resguardo	Tres computadoras con claves, archiveros con llave y seguridad en la oficina
Programas en los que se utilizan los datos	Excel
Controles de seguridad	Solo el personal antes mencionado tiene acceso a las claves de las computadoras, y llaves del archivero. Así como vigilancia en la oficina.
Transferencias	Interinstitucionales entre dependencias, entidades de la administración pública, entidades federativas y municipios. Con entes privados u organizaciones civiles públicas o privadas.
Tipo de traslado	Traslado físico de soportes electrónicos
Bitácora de acceso y operación cotidiana	
Bitácora electrónica	BAOC-2019

Bitácora física	N/A		
Bitácora de vulneraciones			
Tipo de soporte	Electrónico		
Fecha	**Vulneración**	**Número de titulares afectados**	**Medidas correctivas**

Sistema de Tratamiento de Asuntos Jurídicos y Electorales	
Administrador	Diego Noe Salazar Rodríguez
Cargo	Abogado
Área	Secretaría de Asuntos Jurídicos
Funciones y Obligaciones	Quien tiene la función de dar seguimiento a todo lo inherente en el área, entiéndase la elaboración de contratos, redacción de instrumentos jurídicos, así como los documentos necesarios para efectuar el debido registro de precandidatos y candidatos del partido Movimiento Ciudadano
Personal autorizado para el tratamiento	
Nombre	Ana Paulina Arias Canisales
Funciones y Obligaciones	Elaboración de contratos, redacción de instrumentos jurídicos, así como los documentos necesarios para efectuar el debido registro de precandidatos y candidatos del partido Movimiento Ciudadano
Nombre	Janitzio Nahieli Sandoval Madrigal
Funciones y Obligaciones	Interactúa en el área de Asuntos Jurídicos y Electorales con motivo de la información que se requiere para la cabal contestación de las solicitudes de Acceso a la Información
Nombre	
Funciones y Obligaciones	Interactúa en el área de Asuntos Jurídicos y Electorales con motivo de la información que se requiere para la cabal contestación de las solicitudes de Acceso a la Información
Inventario de datos personales	Nombre, domicilio, teléfono, CV, INE, RFC, firma, correo, fecha de nacimiento, escolaridad.

Bases de datos	Base de datos regidores, base datos presidentes municipales, base de datos Daniel, base de datos juicios, base de datos denuncias, base de datos quejas, base datos registros de candidatos
Número de titulares	Entre 501 hasta 5 mil
Tipo de soporte	
Físico	1 archivero, 20 cajas
Electrónico	Red inalámbrica
Características del lugar de resguardo	1.- Archivero color negro (sin número de control patrimonial) 2.- cajas de documentación de cartón mismos que se encuentran dentro de la oficina de asuntos
Programas en los que se utilizan los datos	Microsoft Word Microsoft Excel Sistema Nacional de Registros de Precandidatos y Candidatos de Instituto Nacional y Electoral (SNR).
Controles de seguridad	• Contraseñas en cada una de las computadoras que manejan la información que se genera en el área de Asuntos Jurídicos y Electorales • Llave de la puerta de ingreso a la oficina de Asuntos Jurídicos y Electorales • Personal de seguridad privada al ingreso de las instalaciones de la Comisión Operativa Estatal de Movimiento Ciudadano Jalisco, lugar donde se encuentra la información.
Transferencias	Interinstitucionales entre dependencias, entidades de la administración pública, entidades federativas y municipios. Con entes privados u organizaciones civiles públicas o privadas.
Tipo de traslado	Traslado de soportes físicos y Traslado físico de soportes electrónicos
Bitácora de acceso y operación cotidiana	
Bitácora electrónica	BAOC-2019
Bitácora física	N/A
Bitácora de vulneraciones	

Tipo de soporte	Electrónico		
Fecha	**Vulneración**	**Número de titulares afectados**	**Medidas correctivas**

Sistema de Tratamiento de Vinculación de las Estructuras Juveniles Municipales, Distritales y Estatales	
Administrador	Rodrigo Ramos Enriquez
Cargo	Delegado
Área	Coordinación Delegación de Jóvenes en Movimiento
Funciones y Obligaciones	Delegado Estatal de Jóvenes en Movimiento: La creación y capacitación de estructuras político-electoral juvenil en el estado de Jalisco.
Personal autorizado para el tratamiento	
Nombre	Diego Gerardo Arroyo León
Cargo	Auxiliar
Funciones y Obligaciones	Auxiliar en la creación y capacitación de estructuras político electoral juvenil en el estado de Jalisco.
Inventario de datos personales	Nombre, correo, teléfono, domicilio, INE, firma.
Bases de datos	Base de datos de vinculación de las estructuras juveniles, municipales, distritales, estatales.
Número de titulares	Entre 501 hasta 5 mil
Tipo de soporte	
Físico	Archivero el cual se encuentra bajo llave.
Electrónico	Red interna, 3 servidores
Características del lugar de resguardo	1. Computadora portátil, marca lenovo modelo B41-35 en carpetas de orden: respaldo/jóvenes. 2. Computadora portátil Mac pro modelo A1278 en carpeta de orden: trabajo/jóvenes 3. Los documentos se encuentran en un archivero en la oficina de comunicación en las instalaciones del partido.
Programas en los que se	Microsoft Word, descripción de actividades. Microsoft Excel: base de datos.

utilizan los datos	Microsoft Power Point: presentación de actividades Correo gmail
Controles de seguridad	Solo el personal antes mencionado tiene acceso a las claves de las computadoras, y llaves del archivero. Así como vigilancia en la oficina.
Transferencias	Interinstitucionales entre dependencias, entidades de la administración pública, entidades federativas y municipios. Con entes privados u organizaciones civiles públicas o privadas.
Tipo de traslado	Traslado de soportes físicos
Bitácora de acceso y operación cotidiana	
Bitácora electrónica	BAOC-2019
Bitácora física	N/A

Bitácora de vulneraciones			
Tipo de soporte	Electrónico		
Fecha	**Vulneración**	**Número de titulares afectados**	**Medidas correctivas**

Sistema de Tratamiento de Vinculación de las Estructuras de Movimientos Sociales	
Administrador	Jenifer Hinojosa Correa
Cargo	Coordinadora
Área	Coordinación de Movimientos sociales
Funciones y Obligaciones	Capacitación y sensibilización a las estructuras municipal y distrital sobre diversos temas.
Personal autorizado para el tratamiento	
Nombre	N/A
Cargo	N/A
Funciones y Obligaciones	N/A
Inventario de datos personales	Nombre, correo, teléfono, domicilio, INE, firma.
Bases de datos	Base de datos movimientos sociales

Número de titulares	Hasta 500 personas		
Tipo de soporte			
Físico	N/A		
Electrónico	Red interna		
Características del lugar de resguardo	1. Computadora portátil, marca lenovo modelo B41-35 en carpetas de orden: respaldo/movimientos sociales		
Programas en los que se utilizan los datos	Microsoft Word, descripción de actividades. Microsoft Excel: base de datos. Microsoft Power Point: presentación de actividades Correo Gmail		
Controles de seguridad	Solo el personal de transparencia tiene acceso y se cuenta con oficina la cual se cierra con llave. Las medidas preventivas consisten en resguardo físico en sitios con llave, sistema de video vigilancia y personal de guardia 24 horas los 7 días de la semana		
Transferencias	Interinstitucionales entre dependencias, entidades de la administración pública, entidades federativas y municipios. Con entes privados u organizaciones civiles públicas o privadas.		
Tipo de traslado	Traslado de soportes físicos y Traslado sobre redes electrónicas		
Bitácora de acceso y operación cotidiana			
Bitácora electrónica	BAOC-2019		
Bitácora física	N/A		
Bitácora de vulneraciones			
Tipo de soporte	Electrónico		
Fecha	**Vulneración**	**Número de titulares afectados**	**Medidas correctivas**

Sistema de Tratamiento de Solicitudes de Acceso a la Información y de Derechos ARCO	
Administrador	Flor Janet Lobos Robles
Cargo	Titular de la Unidad de Transparencia
Área	Unidad de Transparencia

Funciones y Obligaciones	1 Recibir, admitir, gestionar y resolver las solicitudes de información pública que sean de su competencia. 2 Remitir al Instituto de Transparencia e Información Pública del Estado de Jalisco las solicitudes de información que no sean de su competencia.
Personal autorizado para el tratamiento	
Nombre	Flor Janet Lobos Robles
Cargo	Titular de la Unidad de Transparencia
Funciones y Obligaciones	1 Recibir, admitir, gestionar y resolver las solicitudes de información pública que sean de su competencia. 2 Remitir al Instituto de Transparencia e Información Pública del Estado de Jalisco las solicitudes de información que no sean de su competencia.
Inventario de datos personales	Nombre, domicilio y correo
Bases de datos	Base de datos de solicitudes de información y derechos ARCO
Número de titulares	Hasta 500
Tipo de soporte	
Físico	
Electrónico	Red interna
Características del lugar de resguardo	1 Archivero 2 Cajas de Documentación 1 servidor 2 computadoras: BENQ modelo GL950-TA y VORAGO modelo LED-W18-200
Programas en los que se utilizan los datos	Excel y Word
Controles de seguridad	Solo el personal de transparencia tiene acceso y se cuenta con oficina la cual se cierra con llave. Las medidas preventivas consisten en resguardo físico en sitios con llave, sistema de video vigilancia y personal de guardia 24 horas los 7 días de la semana
Transferencias	Interinstitucionales entre dependencias, entidades de la administración pública, entidades federativas y municipios. Con entes privados u organizaciones civiles públicas o privadas.
Tipo de traslado	Traslado de soportes físicos y Traslado sobre redes electrónicas
Bitácora de acceso y operación cotidiana	
Bitácora electrónica	BAOC-2019
Bitácora física	N/A

Bitácora de vulneraciones			
Tipo de soporte	Electrónico		
Fecha	**Vulneración**	**Número de titulares afectados**	**Medidas correctivas**

Sistema de Tratamiento de Procesos Internos.	
Administrador	Cesar Francisco Padilla Chavez
Cargo	Secretaria de Acuerdos
Área	Secretaría de Acuerdos
Funciones y Obligaciones	Titular del área de la cual dependen los procesos internos de Movimiento Ciudadano.
Personal autorizado para el tratamiento	
Nombre	Oscar Amézquita González
Cargo	Secretario de Asuntos Municipales
Funciones y Obligaciones	Encargado de recabar los datos personales de manera física y/o virtual.
Nombre	Mirza Flores Gomez
Cargo	Coordinadora Estatal de movimiento Ciudadano Jalisco
Funciones y Obligaciones	Se envía se envía la información para efecto de llevar a cabo convocatorias y envío de información a los integrantes del partido; así como para el análisis político de la misma.
Inventario de datos personales	Nombre, domicilio, teléfono, INE, RFC, firma, correo, fecha de nacimiento, escolaridad, experiencia laboral, información patrimonial, procedimientos administrativos, ingresos y egresos.
Bases de datos	Base de datos órganos de dirección
Número de titulares	Entre 501 hasta 5 mil
Tipo de soporte	
Físico	Si
Electrónico	Red Internet
Características del lugar de resguardo	1 Archivero metálico con tres cajones o gavetas protegido con llave. 1 Laptop Toshiba, modelo L775-S7105, serie G66C002GC10

Programas en los que se utilizan los datos	Paquete de software Microsoft Office (Word, Excel). Adobe Acrobat. Sistema Nacional de Registro de Candidatos del Instituto Nacional Electoral (SNR). Plataforma interna de contabilidad. Plataforma "Google" para envío de correos electrónicos y administración de contactos.
Controles de seguridad	Vigilante en la puerta de acceso. Bitácora de visitas en recepción. Llave en puerta de acceso a oficina de Secretaría de Acuerdos. Llave en gaveta para acceder a archivo físico y servidor. Contraseña para acceder al servidor (Computadora)
Transferencias	Interinstitucionales entre dependencias, entidades de la administración pública, entidades federativas y municipios. Con entes privados u organizaciones civiles públicas o privadas.
Tipo de traslado	Traslado de soportes físicos y Traslado sobre redes electrónicas
Bitácora de acceso y operación cotidiana	
Bitácora electrónica	BAOC-2019
Bitácora física	N/A
Bitácora de vulneraciones	
Tipo de soporte	Electrónico

Fecha	**Vulneración**	**Número de titulares afectados**	**Medidas correctivas**

Sistema de Tratamiento de Datos Personales del Padrón de Proveedores/Contratos de Prestación de Servicios	
Administrador	Gilberto Mendoza Cisneros
Cargo	Tesorero
Área	Coordinación de Tesorería
Funciones y Obligaciones	Adquisiciones, registro contable y pago a proveedores bajo los lineamientos del Reglamento de Fiscalización del INE.
Personal autorizado para el tratamiento	
Nombre	Miguel Ángel García Santiago
Cargo	Consejero

Funciones y Obligaciones	Adquisiciones, registro contable y pago a proveedores bajo los lineamientos del Reglamento de Fiscalización del INE.
Nombre	
Cargo	Secretaria de Fomento Deportivo
Funciones y Obligaciones	Adquisiciones, registro contable y pago a proveedores bajo los lineamientos del Reglamento de Fiscalización del INE.
Nombre	Miguel Ángel García Santiago
Cargo	Contador
Funciones y Obligaciones	Adquisiciones, registro contable y pago a proveedores bajo los lineamientos del Reglamento de Fiscalización del INE.
Nombre	Miguel Ángel García Santiago
Cargo	Contador
Funciones y Obligaciones	Adquisiciones, registro contable y pago a proveedores bajo los lineamientos del Reglamento de Fiscalización del INE.
Nombre	Gustavo Uriel Medina López
Cargo	Auxiliar Administrativo
Funciones y Obligaciones	Adquisiciones, registro contable y pago a proveedores bajo los lineamientos del Reglamento de Fiscalización del INE.
Nombre	Miguel Ángel García Santiago
Cargo	Auxiliar
Funciones y Obligaciones	Adquisiciones, registro contable y pago a proveedores bajo los lineamientos del Reglamento de Fiscalización del INE.
Nombre	Gilberto Mendoza Cisneros
Cargo	Tesorero
Inventario de datos personales	Nombre, domicilio, teléfono, correo, RFC, INE, CURP, cuentas bancarias, CV, firma.
Bases de datos	Base de datos recursos humanos, base de datos drive
Número de titulares	Entre 501 hasta 5 mil
Tipo de soporte	
Físico	Si
Electrónico	Si
Características del lugar de resguardo	4 archiveros tipo armario de 4 repisas cada uno Vacp 9052175CON 113 001 058 004, RJ 113 009 001 002, Vacp 9052175CON 113 001 056 0002,Vacp 9052175CON 115 001 066 001, 2 Armarios de la instalación fija sin número de inventario. 7 Gavetas tipo escritorio 35 cajas de cartón de archivo muerto 1 Servidor físico instalado en las oficinas de Movimiento Ciudadano

	7 computadoras de escritorio 1 Monitor Samsung 115 001 035 001 cpu Intel core 3 active Cool 2 Monitor Samsung 115 001 035 0008 cpu HDMI RY ZEN5 3 Monitor Asus E9LMTF084732 cpu LG 4 Monitor Samsung Z46FH4LDC09116k 5 Monitor Vorago 5930714180203 cpu Active Cool 6 Monitor BENQ cpu HDMI 7 Monitor HACER AS5735 1 Lap Top Toshiba YE11360835 1 Lap Top LENOVO 953776
Programas en los que se utilizan los datos	Sistema Integral de Fiscalización propiedad del Instituto Electoral / Excel y Word
Controles de seguridad	Personal de vigilancia 24/7 Llaves de puertas de acceso a oficinas y mobiliario Contraseñas de acceso en computadoras
Transferencias	Interinstitucionales entre dependencias, entidades de la administración pública, entidades federativas y municipios. Con entes privados u organizaciones civiles públicas o privadas.
Tipo de traslado	Traslado de soportes físicos y Traslado sobre redes electrónicas
Bitácora de acceso y operación cotidiana	
Bitácora electrónica	BAOC-2019
Bitácora física	N/A

Bitácora de vulneraciones			
Tipo de soporte	Electrónico		
Fecha	**Vulneración**	**Número de titulares afectados**	**Medidas correctivas**

Sistema de Tratamiento de Vinculación con los Actores	
Administrador	Tecutli Gomez Villalobos
Cargo	Secretario de Organización y Acción Política
Área	Secretaría Organizacional y Acción Política

Funciones y Obligaciones	Realizar base de datos o listados, para tener la vinculación con los actores tanto personal como por correo o telefónica.
Personal autorizado para el tratamiento	
Nombre	Ricardo Joaquín Ramírez Franco
Cargo	Coordinador
Funciones y Obligaciones	Realizar base de datos o listados, para tener la vinculación con los actores tanto personal como por correo o telefónica.
Nombre	Oscar Amézquita González
Cargo	Secretario de Asuntos Municipales
Funciones y Obligaciones	Realizar base de datos o listados, para tener la vinculación con los actores tanto personal como por correo o telefónica.
Nombre	Tecutli Gómez Villalobos
Cargo	Secretaría de Vinculación y Participación Ciudadana
Inventario de datos personales	Nombre, Teléfono, Correo Electrónico
Bases de datos	Base de datos regidores, base datos presidentes municipales, base de datos Daniel
Número de titulares	Entre 501 hasta 5 mil
Tipo de soporte	
Físico	4 carpetas
Electrónico	Red Internet
Características del lugar de resguardo	1 Computadores blanca marco Sony y en ella se encuentran las 4 carpetas con los datos de los titulares
Programas en los que se utilizan los datos	Excel Word
Controles de seguridad	Hay una puerta de alambrado con candado y posterior a esa hay una puerta de metal negra con llave, la computadora con la que se trabaja y en la que se encuentra la información cuenta con una contraseña.
Transferencias	Interinstitucionales entre dependencias, entidades de la administración pública, entidades federativas y municipios.
Tipo de traslado	Traslado de soportes físicos y Traslado físico de soportes electrónicos
Bitácora de acceso y operación cotidiana	
Bitácora electrónica	BAOC-2019
Bitácora física	N/A

Bitácora de vulneraciones			
Tipo de soporte	Electrónico		
Fecha	**Vulneración**	**Número de titulares afectados**	**Medidas correctivas**

Controles y mecanismos de seguridad para las transferencias

Traslado de soportes físicos:

- El envío se realiza a través de personal autorizado por su superior jerárquico.
- Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas.
- La información sólo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial.
- Toda entrega de información requiere acuse de recibo.
- Todas las transmisiones serán registradas en las bitácoras de transferencia de cada área.

Traslado físico de soportes electrónicos:

- El envío se realiza a través de personal autorizado por su superior jerárquico.
- Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas;
- La información sólo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial
- Toda entrega de información requiere acuse de recibo.
- Todas las transmisiones serán registradas en las bitácoras de transferencia de cada área.
- Cifrado de las memorias USB, discos compactos u otros soportes físicos de medios electrónicos.

Traslados sobre redes electrónicas:

- Todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán ser sometidos a un proceso a través del cual la información puede ser codificada para no ser accedida por otros, a menos que tengan la clave del cifrado.

Controles de Identificación y Autentificación de Usuarios

A. Modelo de control de acceso.

1. La autenticación consiste en el proceso de identificación de un individuo sobre la base de sus credenciales (nombre de usuario y contraseña).

2. La autorización, es el proceso que determina a qué documentos o información tiene acceso un usuario.

B. Perfiles de usuario, contraseñas y administradores en el sistema operativo de red.

1. La designación de perfiles de usuario y contraseñas en el sistema operativo de red, se realiza a través de los administradores designados.

2. El nombre de usuario no tiene relación a datos personales del usuario.

3. La contraseña es personal debe contener ocho caracteres, alfanumérica, intercalando mayúsculas y minúsculas y números.

4. Cada usuario es responsable de resguardar y proteger su contraseña.

Procedimientos de respaldo y recuperación de datos personales

El proceso de respaldo de los datos personales, se lleva a cabo a través de la digitalización de los documentos que contienen dichos datos. Estas digitalizaciones se resguardan en soporte digital, cada área es responsable del soporte físico de los medios electrónicos durante el tiempo que señalen las disposiciones legales correspondientes.

Para la recuperación de los datos personales que se encuentren en los equipos de cómputo, se realiza una copia de seguridad en medios físicos externos como memorias USB o Discos Duros cuyo resguardo y acceso sea únicamente de los administradores de cada sistema de tratamiento.

En caso de pérdida, robo o extravío de los datos personales en los casos en los que sea materialmente imposible de recuperar los datos, se cuenta con su respaldo digitalizado para su posterior impresión, dejando constancia de dicho proceso.

Técnicas de supresión y borrado seguro de datos personales

La supresión y borrado seguro de los datos personales tiene como objetivo la confidencialidad, integridad y disponibilidad de los datos personales. Para lo anterior se cuenta con técnicas de supresión y borrado seguro que garantizan que no sea posible recuperar la información, ya sea de manera física o digital, una vez suprimidos los datos, para evitar el acceso no autorizado a los mismos.

Dichas técnicas consisten en la destrucción de documentos mediante la trituración cruzada, así como la destrucción física de discos compactos y memorias externas.

Análisis de Riesgo[1]

El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

El nivel de riesgo por tipo de dato es igual al beneficio que representa la información para un atacante, y para calcularlo se requieren dos elementos principalmente:

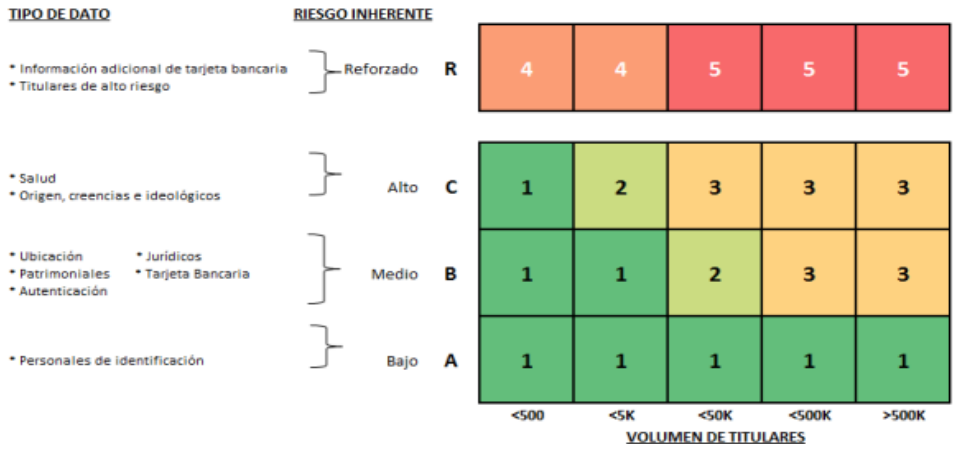
1. Tener el nivel de riesgo inherente de cada tipo de dato que se trate, y;
2. Calcular el volumen de titulares, cuantificando el número de personas de las que se traten datos personales.

[1] http://inicio.inai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf

El nivel de riesgo inherente de cada tipo de dato se determina de acuerdo a al beneficio que representa la información para un atacante por medio de la identificación y clasificación de datos personales. Mientras que el volumen de titulares se calcula acotando la cantidad de personas en un sistema de tratamiento de datos personales:

<500: Datos de hasta 500 personas
<5k: Datos entre 501 hasta 5,000 personas
<50k: Datos entre 5,001 hasta 50,000 personas
<500k: Datos entre 50,001 hasta 500,000 personas
>500k: Datos de más de 500,000 personas

Al definir el nivel de riesgo inherente por cada tipo de dato y el volumen de titulares, se podrá identificar el nivel de riesgo por tipo de dato para ello se han establecido cinco niveles posibles nombrados con valor numérico del 1 al 5, tal como se muestra en la siguiente imagen, donde 1 es el nivel más bajo y 5 el más alto:



Sistema de Tratamiento de Afiliaciones y Círculos Ciudadanos			
Tipo de Dato	**Nivel de Riesgo Inherente**	**Volumen de Titulares**	**Nivel de riesgo por tipo de dato**
Identificativos	Bajo	**<5k**	1
Laborales	Bajo	**<5k**	1
Procedimientos Administrativos o Jurisdiccionales	Medio	**<5k**	1
Salud	Alto	**<5k**	2

Origen/étnicos	Alto	**<5k**	2
Ideológicos	Alto	**<5k**	2
Características personales	Alto	**<5k**	1
Preferencia sexual	Alto	**<5k**	2

Sistema de Tratamiento de Asuntos Jurídicos y Electorales			
Tipo de Dato	**Nivel de Riesgo Inherente**	**Volumen de Titulares**	**Nivel de riesgo por tipo de dato**
Identificativos	Bajo	**<5k**	1
Laborales	Bajo	**<5k**	1
Procedimientos Administrativos o Jurisdiccionales	Medio	**<5k**	1
Académicos	Alto	**<5k**	2
Patrimoniales	Alto	**<5k**	1

Sistema de Tratamiento de Vinculación de las Estructuras Juveniles Municipales, Distritales y Estatales			
Tipo de Dato	**Nivel de Riesgo Inherente**	**Volumen de Titulares**	**Nivel de riesgo por tipo de dato**
Identificativos	Bajo	**<5k**	1
Procedimientos Administrativos o Jurisdiccionales	Medio	**<5k**	1

Sistema de Tratamiento de Vinculación de las Estructuras de Movimientos Sociales			
Tipo de Dato	**Nivel de Riesgo Inherente**	**Volumen de Titulares**	**Nivel de riesgo por tipo de dato**
Identificativos	Bajo	**<500**	1
Procedimientos Administrativos o Jurisdiccionales	Medio	**<500**	1

Sistema de Tratamiento de Solicitudes de acceso a la Información y de Derechos ARCO			
Tipo de Dato	**Nivel de Riesgo Inherente**	**Volumen de Titulares**	**Nivel de riesgo por tipo de dato**
Identificativos	Bajo	**<500**	1
Procedimientos Administrativos o Jurisdiccionales	Medio	**<500**	1
Salud	Alto	**<500**	1
Origen/étnicos	Alto	**<500**	1
Ideológicos	Alto	**<500**	1
Preferencia Sexual	Alto	**<500**	1
Características Personales	Alto	**<500**	1

Sistema de Tratamiento de Procesos Internos			
Tipo de Dato	**Nivel de Riesgo Inherente**	**Volumen de Titulares**	**Nivel de riesgo por tipo de dato**
Identificativos	Bajo	**<5k**	1
Laborales	Bajo	**<5k**	1
Académicos	Medio	**<5k**	1
Patrimoniales	Medio	**<5k**	1
Procedimientos Administrativos o Jurisdiccionales	Medio	**<5k**	1
Salud	Alto	**<5k**	2
Origen/étnicos	Alto	**<5k**	2
Ideológicos	Alto	**<5k**	2

Sistema de Tratamiento de Datos Personales del Padrón de Proveedores/Contratos de Prestación de Servicios			
Tipo de Dato	**Nivel de Riesgo Inherente**	**Volumen de Titulares**	**Nivel de riesgo por tipo de dato**
Identificativos	Bajo	**<5k**	1
Laborales	Bajo	**<5k**	1

Patrimoniales	Medio	**<5k**	1

Sistema de Tratamiento de Vinculación con los Actores			
Tipo de Dato	**Nivel de Riesgo Inherente**	**Volumen de Titulares**	**Nivel de riesgo por tipo de dato**
Identificativos	Bajo	**<5k**	1
Procedimientos Administrativos o Jurisdiccionales	Medio	**<5k**	1

Gestión de Vulneraciones[2]

Para identificar un incidente de seguridad, se requiere de la detección y/o registro de alertas de seguridad, los cuales son advertencias respecto a cambios en los sistemas de tratamiento.

Ejemplos de alertas de seguridad	
Categoría	**Ejemplos**
Desastre natural (más allá del control humano)	Terremoto, erupción de un volcán, tsunami, huracán, etc.
Inestabilidad social	Huelgas, terrorismo, guerra.
Daño físico (accidental o deliberado)	Incendio, inundación, malas condiciones ambientales (contaminación, polvo, corrosión, congelamiento), radiación o pulso electromagnético, destrucción parcial o toral de medios de almacenamiento físico o electrónico.
Falla de la infraestructura	Falla en el suministro de servicios como: energía, agua, telecomunicaciones y redes, aire acondicionado.
Falla técnica	Fallas del hardware, mal funcionamiento del software, sobrecarga o saturación en el uso de los sistemas, falta de mantenimiento.
Software malicioso[7]	Diferentes categorías de software malicioso (malware) como virus, troyanos, software de acceso y control remoto (RAT, por sus siglas en inglés), amenazas persistentes avanzadas (APT, por sus siglas en inglés), Ransomware.
Ataques técnicos	Explotación de vulnerabilidades de la configuración, protocolos o programas, normalmente a la fuerza. Escaneo de redes, utilización de puertas traseras en el software, intentos de acceso no autorizado, inferencia de contraseñas, ataques de denegación de servicio.
Incumplimiento de reglas o políticas (accidental o deliberado)	Uso no autorizado de activos, uso de activos autorizados, pero para finalidades no autorizadas, uso de software, o dispositivos no permitidos, instalación de programas o aplicaciones no autorizadas o ilegales, copia o sustracción de documentos o información no autorizada.
Información dañada	Sobre escritura accidental, error de captura o de almacenamiento.
Intercepción de información	Espionaje, intervención de comunicaciones, ingeniería social, robo, pérdida o extravío de información.
Divulgación de contenido perjudicial	Difusión en medios masivos de comunicación de contenido ilegal, malicioso, abusivo o que pueda dañar los derechos morales o patrimoniales de las personas.

[2] http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

Procedimiento a seguir:

a) Informar a los titulares de los datos personales lo siguiente:

1. La naturaleza del incidente.
2. Los datos personales afectados.
3. Las recomendaciones al titular acerca de las medidas que éste puede adoptar para protegerse.
4. Las acciones correctivas realizadas de forma inmediata.
5. Los medios donde los titulares pueden obtener más información.
6. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente.
7. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

b) Informar al ITEI de la vulneración de seguridad ocurrida.
c) La actualización del documento de seguridad correspondiente.
d) Contar con una bitácora de las vulneraciones en la que se describa:

1. En qué consistió la vulneración.
2. La fecha en la que ocurrió.
3. El motivo o causa de la vulneración.
4. Las acciones correctivas implementadas de forma inmediata y a largo plazo.

Plan de Contingencia

El Plan de contingencia contiene las medidas preventivas, las acciones inmediatas y reactivas para ayudar a controlar un incidente y minimizar las consecuencias negativas del suceso. En este apartado se proponen una serie de procedimientos alternativos al funcionamiento normal de esta Institución cuando alguna de sus funciones usuales se ven perjudicadas por causas internas o externas. El objetivo es garantizar la continuidad de la operación en los procesos de protección de datos personales, que consiste en primer lugar en clasificar la gravedad de la contingencia, como a continuación se describe:

Grado 1: situaciones de bajo riesgo que pueden ser resueltas por el personal del Responsable, como fallas eléctricas o fallas en la conexión de internet.

Grado 2: aquellas que para su atención se requiera el apoyo del personal y de personas externas al Responsable, como inundaciones o ataques cibernéticos.
Grado 3: contingencias que por su alcance afecten severamente la operatividad del Responsable y que requiera apoyo externo, como incendios o terremotos.

Dentro de las acciones previstas para evitar la pérdida o vulneración de los datos personales, se determinará el grado de la contingencia, después cada área debe tomar en cuenta lo siguiente:

- En caso de inundaciones, se deben de realizar las siguientes acciones:

1. Realizar la revisión y reparación de la hermeticidad de las ventanas y puertas, impermeabilizar los techos para evitar goteras.
2. Retirar expedientes y documentos del piso y elevarlos lo mayor posible.
3. Colocar barreras para evitar que el agua se propague.
4. Los documentos húmedos serán llevados a áreas ventiladas para que se sequen.
5. En caso de expedientes mojados, colocar papel secante entre las hojas o congelarlos inmediatamente para comenzar el proceso de recuperación.
6. Seguir el procedimiento señalado en el apartado de gestión de vulneraciones.

- En caso de ciberataques:

1. Revisar el inventario de los equipos de cómputo, impresoras, escáneres y copiadoras.
2. Desconectar el internet para detener el ataque.
3. Contactar inmediatamente al personal de soporte y a los proveedores, para evaluar y reparar los daños ocasionados.
4. Seguir el procedimiento señalado en el apartado de gestión de vulneraciones.

- En caso de incendios:

1. Llamar a los servicios de emergencia para el apoyo de los bomberos.
2. Localizar los extintores y utilizarlos solamente en los casos donde no se ponga en peligro la vida del personal.
3. Evacuar al personal de las instalaciones y esperar a los servicios de emergencia.
4. Una vez apagado el incendio, evaluar los daños a los documentos.
5. Si los documentos fueron dañados por el incendio, se debe de contar con un respaldo digital para poder recuperarlos.

6. Seguir el procedimiento señalado en el apartado de gestión de vulneraciones.

- En caso de terremoto:

1. Activar la alerta sísmica.
2. Evacuar al personal de las instalaciones.
3. Ingresar solamente un par de personas para evaluar los daños, en caso de grietas, derrumbes u otros daños, prohibir el reingreso del personal y esperar a protección civil para la evaluación del daño estructural.
4. Una vez que las autoridades permitan el reingreso, evaluar los daños a los documentos y comenzar la recuperación de los mismos a través de su respaldo digital.
5. Seguir el procedimiento señalado en el apartado de gestión de vulneraciones.

Mecanismos de monitoreo y revisión de las medidas de seguridad

a) Mantenimiento de los equipos de cómputo dos veces al año.
b) El personal deberá de cambiar sus contraseñas cada mes, dichas contraseñas deberán ser alfanuméricas, de al menos ocho caracteres, alternando mayúsculas y minúsculas.
c) Revisión cada dos meses de las instalaciones eléctricas.
d) Impermeabilización de los techos antes del temporal de lluvias.
e) Cada seis meses, remitir memorándum a las áreas para gestionar algún cambio en el tratamiento de los datos personales.
f) Solicitar al personal que notifique inmediatamente cualquier fallo a las cerraduras de los archiveros o de las puertas de su área.

Análisis de Brecha

El análisis de brecha es un proceso que consiste en identificar los riesgos y definir las medidas actuales de su tratamiento, para así conocer las medidas faltantes y planear su implementación. Para realizar dicho análisis, se utilizarán parámetros comparándolos con la situación actual.

Parámetro	Situación Actual
Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Identificado en el apartado de bitácoras de acceso y operación cotidiana del presente documento de seguridad.
Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo	No implementado.
Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	No implementado.
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	No implementado.
Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	No implementado.
Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	No implementado.

Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Identificado en el apartado de mecanismos de monitoreo y revisión de las medidas de seguridad del presente documento de seguridad.
Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad	Identificado en el apartado de gestión de vulneraciones del presente documento de seguridad.
Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Identificado en el apartado de mecanismos de monitoreo y revisión de las medidas de seguridad del presente documento de seguridad.
Todas las responsabilidades de seguridad deben estar claramente definidas.	Identificadas en el catálogo de sistemas de tratamiento del presente documento de seguridad.
Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	No implementado.
Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Identificados en el apartado de técnicas utilizadas para la supresión y borrado seguro de los datos personales del presente documento de seguridad.
Cualquier medio que contenga información deberá ser protegido	No implementado.

contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización	

Plan de trabajo

Se deberán realizar las siguientes acciones:

De 1 a 6 meses:

- Los documentos deben de encontrarse uniformemente integrados.
- Digitalizar todos los documentos para tener un respaldo digital, dicho respaldo deberá contenerse en un medio externo.
- Implementar los mecanismos y controles de seguridad para las transferencias fuera de las instalaciones del Responsable.
- Debe de evitarse archivar documentación cerca de aparatos eléctricos.
- Evitar colocar documentos directamente en el piso.
- Las instalaciones eléctricas deben encontrarse en buen estado.
- Todos los equipos eléctricos que estén en el archivo deben quedar apagados y desconectados durante la noche o cuando no se utilicen.
- No colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.
- Identificar los documentos de mayor valor para resguardarlos en las zonas con más seguridad y realizar su respectivo respaldo.
- Contar con un inventario de los equipos de cómputo, impresoras, escáneres, copiadoras y mantener contacto con los proveedores y técnicos.
- Remover los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.

De 6 a 12 meses:

- Los archiveros deben de garantizar la conservación de los documentos, siendo de metal u otro material inflamable.
- Los estantes deben encontrarse lejos del suelo para facilitar la limpieza y evitar la proliferación de humedad o plagas.
- Se debe de guardar la información en una zona segura de preferencia donde el calor de algún incendio no alcance los dispositivos o en lugares cercanos a extintores.
- Capacitar al personal para el uso de extintores y sobre los planes de evacuación y contingencia.

De 12 a 18 meses:

- Cambiar los botes de basura de plástico por metal.
- Fijar los equipos de cómputo a los escritorios.
- Bloquear de los equipos donde no sea necesario las entradas USB.

De 18 a 36 meses:

- Todos los escritorios deberán ser de cristal.
- Los documentos deberán ser resguardados en zonas sin ventanas, techos sin filtraciones de agua y cubiertas de material inflamable.

Programa General de Capacitación

Personal	Tema	Temporalidad
Titulares y Directivos	Generalidades	1 a 6 meses
Personal de base	Generalidades	1 a 6 meses
Titulares y Directivos	Sistema de Gestión	6 a 12 meses
Personal de base	Sistema de Gestión	6 a 12 meses
Titulares y Directivos	Documento de Seguridad	1 a 6 meses

Anexos

Bitácora de Transferencias

Datos Transferidos	Persona que autoriza	Fecha de la transferencia	Responsable que recibe	Firma de quien recibe	Fecha de devolución en su caso