POLÍTICAS DE SEGURIDAD

Fecha del Documento	17 enero 2022
	Versión 2.2

Índice

Para los efectos de este documento se entenderá por:

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

Comité: Autoridad máxima en materia de protección de datos personales, en la organización;

Acceso: El titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento;

Rectificación: Rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados;

Cancelación: Eliminación de determinados datos de un sistema de datos personales;

Oposición: Oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo;

Datos personales: La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable, concerniente a su origen étnico, características físicas, morales o emocionales, vida afectiva y familiar, domicilio y teléfono particulares, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, huella digital, ADN y número de seguridad social, u otros similares;

Sistema de datos personales: Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso;

Responsable del Sistema de Datos Personales: Persona que decide sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos;

Administrador del Sistema de Datos Personales: Es el encargado de administrar o mantener el entorno operativo del Sistema; utilizando herramientas de administración que permiten el acceso a los datos protegidos;

Usuario del Sistema de Datos Personales: Es aquel personal autorizado por el responsable del sistema para el tratamiento de datos personales, ya sea de manera física o automatizada;

Responsable de Seguridad del Sistema de Datos Personales: Es el encargado de garantizar la confidencialidad e integridad de cada sistema de datos personales, con la finalidad de proteger los datos de posibles incidencias que puedan provocar su pérdida, alteración o acceso no autorizado;

Tratamiento de Datos Personales: 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;

Centros de tratamiento: Aquellos espacios donde se realizan tratamientos de datos personales;

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;

Titular: La persona física a quien corresponden los datos personales;

Incidencia: Cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales.

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

Ámbito de aplicación

El Presente documento es de carácter general y de observancia obligatoria para todos los responsables, usuarios, encargados y demás personal que realice tratamiento de datos personales contenidos en los sistemas físicos y automatizados de datos personales de la Secretaría de Salud y del Organismo Público Descentralizado Servicios de Salud de Veracruz.

Recursos protegidos

La protección de los datos personales se deberá realizar mediante el control de todas las vías por las que se tenga

acceso a dicha información. Se deberá coordinar el trabajo que realicen las Unidades Administrativas respecto al buen manejo y resguardo de Datos Personales estableciendo sistemas y medidas de seguridad. Sin importar el tipo de contenedor en el que se encuentren, ya sea físico o automatizado.

Los recursos que por servir de medio directo o indirecto para acceder a los datos, deberán ser controlados son los siguientes:

1.- Los centros de tratamiento donde se encuentren ubicados los documentos o se almacenen los soportes que los contengan, su descripción figura en el Anexo C;

2.- Las áreas o estaciones de trabajo (local o remoto), desde los que se pueda tener acceso a los datos personales. La relación de esos puestos de trabajo está descrita en el Anexo C;

3.- Los servidores y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicada la información, que está descrito en el Anexo B;

4.- Los sistemas de datos personales físicos o informáticos o aplicaciones que permiten acceder a los datos, descritos en el Anexo A.

Medidas generales que debe observar el personal involucrado en el tratamiento de los Sistemas de Datos Personales.

1. El personal que haga uso de datos personales en el área de trabajo garantizará que la información que se administre no pueda ser visible o tratada por personas no autorizadas;
2. Los documentos, expedientes, pantallas, así como las impresoras u otro tipo de dispositivos del área de trabajo deberán estar físicamente ubicados en lugares que garanticen la confidencialidad de los datos del sistema;
3. Respecto a la información electrónica, se deberá establecer un protector de pantalla con clave de activación que impida la visualización de los datos;
4. Asegurarse que en las impresoras los documentos impresos en la bandeja de salida no contengan datos personales. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos, los responsables de cada sistema deberán retirar los documentos conforme vayan siendo impresos;
5. Queda expresamente prohibida la conexión a redes o sistemas exteriores en el centro de trabajo; de ser necesaria el uso de este tipo conexiones se deberá

reportar al Responsable del Sistema de Datos Personales. La revocación de esta prohibición será autorizada por el responsable del sistema, quedando constancia de esta modificación en el Libro de incidencias.

6. Los usuarios de los datos personales deberán Abstenerse de portar información con datos personales fuera del área correspondiente a su resguardo.
7. Se deberán implementar controles de acceso a las áreas que realicen tratamiento de Datos Personales ya sea de manera física o electrónica.
8. Las áreas encargadas de la administración de los datos personales, deberán establecer funciones y obligaciones del personal que realice algún tratamiento a la información confidencial, esto de acuerdo a las características del sistema.
9. De acuerdo al nivel de seguridad del sistema de Datos Personales, se deberá nombrar un Responsable de Seguridad del Sistema de Datos Personales, el cual deberá realizar auditorías internas para observar la adecuada protección de la información confidencial.
10. Evaluar las condiciones de vulnerabilidad de los espacios en los que resguarda la información.
11. Identificar los factores humanos o materiales que pudieran poner en peligro los acervos referentes a Datos Personales.
12. Revisar las instalaciones y áreas de resguardo de los acervos considerando en todo momento la seguridad.
13. Evitar accesar a la información sin autorización.
14. Identificar donde se deberá establecer controles de acceso.
15. Identificar vulneraciones por falta de identificación del personal autorizado.
16. Una vez identificados los riesgos, se establecerá un programa de metas concretas.
17. Se aplicará un esquema de actividades para eliminar o mitigar la cantidad de riesgos posibles;
18. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
19. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando.
20. Evitar tomar fotografías de pacientes o personas externas a la institución.
21. No hacer entrega información confidencial de manera económica, es decir deberá realizarse de manera oficial y con autorización.
22. No se deberán crear grupos en redes sociales para transferirse información confidencial.
23. No destruir documentación si no existe el aval del Archivo General del Estado.

24. No se deberá divulgar información de manera oral, física y electrónica sin autorización del responsable del sistema o administrador.
25. Se deberá establecer un programa de capacitación para el personal que de tratamiento a la información confidencial.

Funciones y obligaciones del personal que interviene en el tratamiento de los sistemas de datos personales

El personal afectado por esta normativa se clasifica en cuatro categorías:

Responsable del Sistema: Persona física que decide sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos. Anexo D;

Administrador del Sistema: Es el encargado de administrar o mantener el entorno operativo del Sistema; utilizando herramientas de administración que permitan el acceso a los datos protegidos. Anexo D;

Usuario del Sistema: Es aquel personal autorizado por el responsable del sistema para el tratamiento de datos personales. Anexo D;

Responsable de Seguridad del Sistema: Es el encargado de garantizar la confidencialidad e integridad de cada sistema de datos personales, con la finalidad de proteger los datos de posibles incidencias que puedan provocar su pérdida, alteración o acceso no autorizado. Anexo D.

Funciones del Responsable del Sistema

1. Implantar las medidas de seguridad establecidas en este Sistema de Gestión;
2. Garantizar la difusión de este Sistema de Gestión entre todo el personal que vaya a utilizar el sistema de datos personales;
3. Notificar al administrador del sistema de las incidencias que surjan con el sistema de datos personales;
4. Mantener actualizado el sistema siempre que se produzcan cambios relevantes en él o en la organización del mismo;
5. Autorizar la salida de soportes físicos e informáticos que contengan datos personales fuera de los sitios de tratamiento de los mismos;
6. Cualquier otra que, derivado de sus funciones, considere necesarias para la protección de los datos personales.

Funciones del Administrador del Sistema

1. Garantizar la operación continua del Sistema de Datos Personales;
2. Establecer y otorgar los permisos autorizados por el responsable del sistema y los usuarios;
3. Atender las incidencias;
4. Coordinar las acciones de mantenimiento de los sistemas y aplicaciones;
5. Respecto a la información electrónica, se establecerá un usuario, que será el único asociado a la contraseña correspondiente, para el personal descrito en el Anexo D;

6. Solo cuando las condiciones no permitan la existencia de un responsable de seguridad del sistema, el administrador deberá suplir las funciones descritas para este;
7. Notificar al responsable de seguridad de los cambios de usuarios de los sistemas y contraseñas;
8. Cualquier otra que, derivado de sus funciones, considere necesarias para la protección de los datos personales.

Funciones del Responsable de Seguridad del Sistema

1. Garantizar la seguridad del sistema y sus aplicaciones;
2. Mantener el control de los usuarios de los sistemas y salvaguardar y proteger las contraseñas personales;
3. Coordinar las actividades de respaldo y recuperación de los datos;
4. Asegurar la integridad de la información física o electrónica;
5. Proponer la adquisición de terminales o consolas de trabajo que disminuyan los riesgos de fuga de información;
6. Guardar en lugar protegido las copias de seguridad y respaldo de la información;
7. Cualquier otra que, derivado de sus funciones, considere necesarias para la protección de los datos personales.
8. Realizar auditorías internas para observar la adecuada protección de la información confidencial.

Funciones del Usuario del Sistema

1. Operar el sistema de datos personales;
2. Vigilar y proteger la información tratada;
3. Informar al responsable del sistema de las incidencias que presenta el sistema;
4. Solo cuando las condiciones no permitan la existencia de un administrador del Sistema, el usuario deberá suplir las funciones descritas para este;
5. Cualquier otra que, derivado de sus funciones, considere necesarias para la protección de los datos personales.

Incidencias

El mantener un registro de las incidencias que comprometan la seguridad de los datos personales es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para deslindar responsabilidades de los mismos.

El responsable de seguridad de la información habilitará un Libro de incidencias a disposición de todo el personal autorizado para acceder al sistema de datos personales.

El personal que tenga conocimiento de una incidencia en los sistemas de datos personales, la reportará a la instancia correspondiente para el registro en el Libro de incidencias del sistema.

La omisión de registro y omisión de notificación de una incidencia, será considerada como una falta contra la seguridad de restricción a datos personales por parte de los mismos.

La notificación y/o registro de una incidencia deberá contener como mínimo los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir, descripción detallada de la misma. El procedimiento está descrito en el **Anexo F**.

Se mantendrá el registro de las incidencias otorgándole un valor administrativo, conforme lo establecen los Lineamientos para Catalogar, Clasificar y Conservar los Documentos y la Organización de Archivos, por lo que su guarda será de 6 años.

Entorno del sistema operativo y de comunicaciones

Son los sistemas informáticos, programas o aplicaciones con las que se puede acceder a la información, y que son usualmente utilizados por los usuarios para acceder a ella.

Estos sistemas pueden ser aplicaciones informáticas expresamente diseñadas para acceder a los datos, o sistemas pre programados de uso general como aplicaciones o paquetes disponibles en el mercado informático.

El sistema operativo y de comunicaciones deberá tener al menos un responsable de seguridad. descrito en el Anexo D.

Solo se permitirá el acceso al sistema de datos a través de las herramientas o programas de utilidad establecidas para tal efecto y por el personal que este expresamente autorizado en el Anexo D.

Si la aplicación o sistema de acceso a la información utiliza documentos temporales o cualquier otro medio en el que puedan ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no sean accesibles posteriormente por personal no autorizado.

Si el equipo de cómputo en el que está ubicada la información está integrado en una red de comunicaciones de forma tal que desde otros equipos de cómputo conectados a la misma sea posible el acceso a la información de datos personales, el administrador del sistema deberá asegurarse que dicho acceso no se permita a personas no autorizadas.

Si la aplicación informática que permite el acceso a la información no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado mediante el control de usuario y contraseñas.

Salvaguarda y protección de las contraseñas personales

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos y deben por tanto estar especialmente protegidas.

Cada usuario será responsable de la confidencialidad de su contraseña y en caso de robo, extravío o alguna otra vulneración, deberá reportarlo al administrador del sistema y proceder al cambio.

El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

Resguardo, Respaldo y Recuperación

La seguridad de los datos personales no sólo supone la confidencialidad de estos, sino que también con lleva la integridad y la disponibilidad de esos datos.

Para garantizar estos aspectos fundamentales de la seguridad es necesario que existan procesos de resguardo, respaldo y de recuperación, que permitan proteger recuperar, y en su caso, reconstruir los datos del sistema. Anexo E.

Existirá un responsable de seguridad (Anexo D) cuando el nivel de seguridad del sistema de datos personales los exija que será el encargado de obtener periódicamente una copia de seguridad de la información, a efectos de respaldo y posible recuperación en caso de fallo.

En caso de pérdida total o parcial de los datos, existirá un procedimiento, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del sistema al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en el Anexo E. Apartado llamado procedimiento de respaldo y recuperación.

Los soportes que contengan datos personales deberán ser almacenados en lugares con acceso exclusivo solo al personal relacionado en el Anexo D, según corresponda.

Normas y procedimientos de seguridad

Áreas de tratamiento

Las áreas de tratamiento deberán contar con las medidas mínimas de seguridad que eviten la indisponibilidad de los datos personales que pudieran producirse como consecuencia de incidencias. La relación de los centros de tratamiento se encuentra en el Anexo C.

Estaciones de trabajo

Son todos aquellos medios desde los cuales se puede acceder a los datos personales.
Se consideran también estaciones de trabajo aquellas terminales de administración del sistema, por ejemplo, las consolas de operación donde en algunos casos también pueden aparecer los datos protegidos.

Cada estación de trabajo estará bajo la responsabilidad de una persona de las autorizadas en el Anexo D, que garantizará que la información que muestra no pueda ser vista por personas no autorizadas.

Las pantallas, así como las impresoras u otro tipo de dispositivos conectados a la estación de trabajo deberán estar físicamente ubicadas en lugares que garanticen esa confidencialidad.

Cuando el responsable de una estación de trabajo la abandone, bien temporalmente o bien al finalizar su jornada laboral, deberá dejarlo en un estado que impida la visualización de los datos personales. Esto podrá realizarse a través de un

protector de pantalla que impida la visualización de tales datos.

En el caso de las impresoras, deberá asegurarse que no quedan documentos impresos en la bandeja de salida que contengan datos personales protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de los sistemas, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso a los datos personales. La revocación de esta prohibición será autorizada por el responsable de la información. Quedando constancia de esta modificación en el Libro de incidencias.

Gestión de medios

Son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona el sistema de información.

Dado que la mayor parte de los soportes que hoy día se utilizan, tales como CD-ROM, memorias flash USB, discos duros portátiles, cintas magnéticas y almacenamientos (SAN), entre otros, son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos tiene el control de estos medios.

Los soportes que contengan datos, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué documentos se trata, qué tipo de datos contiene, proceso que los ha originado y fecha de creación.

Aquellos medios que sean reutilizables, y que hayan contenido copias de datos, deberán ser borrados antes de su reutilización, de forma que los datos personales que contenían no sean recuperables.

Los soportes que contengan datos personales deberán ser almacenados en lugares de acceso exclusivo al personal relacionado en el Anexo D, según corresponda.

La salida de soportes informáticos que contengan datos personales fuera de los locales donde están ubicados los sistemas de datos personales deberá ser expresamente

autorizada por el responsable del sistema, utilizando para ello el documento adjunto en el Anexo E.

Anexos

Anexo A. Descripción del Sistema de Acceso a la Información.

Descripción del sistema de acceso a los datos personales

Nombre del sistema:
Plataforma del sistema o ubicación del área responsable del tratamiento:
Alojamiento del sistema (ubicación física):
Tipos de acceso físico o sistema (web, local)[1]:
Autentificación (usuario y password)[2]: Sí ( ) No ( )
Manera de interrelación de la información[3]:
Origen o manera de recolección de la información[4]:
Nivel de seguridad de acuerdo a los datos recabados[5]:

[1] Especificar si la interacción con el sistema se hace físicamente o se requiere ingresar a alguna aplicación informática, tanto en internet como una aplicación localmente instalada.
[2] Especificar si se requiere ingresar por medio de autentificación con usuario y contraseña.
[3] Describir si la información es compartida y con quién.
[4] Señalar cuál es la forma en que la información es obtenida, por ejemplo a través de un formato de ingreso.
[5] Especificar si el nivel de seguridad es Básico, Medio o alto de acuerdo a los datos recabados.

Anexo B. Entorno de Sistema Operativo y de Comunicaciones

Entorno de sistema operativo y de comunicaciones de la información
(A ser complementado por el administrador del sistema)

El servidor deberá contener al menos los siguientes datos y aspectos:

Sistema operativo y aplicaciones:

Tipo de servidor[6]	**Nombre y versión del S.O.**[7]	**Memoria Ram.**[8]	**Procesador**[9]	**Capacidad en disco duro**[10]	**Administrador del sistema**[11]

Entorno de comunicaciones

Conexión de red[12]	**Tipo de enlace**[13]	**Velocidad de conexión**[14]

[6] Si los datos están en un servidor de archivos Web, FTP, Correo Electrónico, etc.
[7] Cuál es el sistema Operativo y su versión, por ejemplo, Windows 7, Windows 10, Mac OSX high sierra, Linux 5.4.7
[8] Cantidad de memoria para ejecutar procesos en un equipo de cómputo.
[9] El cerebro en un equipo de cómputo; determina la velocidad de operaciones por segundo que el equipo puede hacer.
[10] Capacidad de almacenamiento. Determina la cantidad de archivos y aplicaciones que puede guardar una computadora.
[11] Persona cuyo usuario permite acceder a todos los recursos del sistema. También llamada súper cuenta.
[12] Telefónica conmutada, digital RDSI, digital ADSL, por cable, inalámbrica, etc.
[13] Enlace dedicado, asimétrico, punto a punto, etc.
[14] Velocidad en bauds por segundos y sus múltiplos, en que la información se trasfiere por la red.

Anexo C. Centros de Tratamiento

Áreas o Centros de tratamiento

Nombre del área o nombre y versión del S.O.[15]	Nombre del Sistema de Datos Personales	No. de usuarios que acceden a la información físicamente o equipo de cómputo[16]	Responsable del sistema	Indique su forma de conexión local/remota (¿cómo se comparte información o se interrelaciona)[17]	Indique la ubicación física

[15] El nombre del área donde se encuentra el sistema o bien, si es un sistema informático, el nombre y versión del sistema operativo, por ejemplo, Windows 10.
[16] Cantidad de personas que cuentan con acceso al sistema o a la aplicación.
[17] Indicar si es un sistema localizado o instalado dentro del área responsable o se accede y comparte vía remota (internet).

Anexo D. Personal autorizado para acceder al sistema físico o electrónico.

Nombre del sistema_____
Nivel de Seguridad del Sistema_____

Nombre y Apellidos.....
.....
Cargo……..
.....
.....
Fecha.....

Declaración de recepción y aceptación del documento

Declaramos haber leído EL Sistema de Gestión adjunto y aceptamos el cumplimiento de las normas expresadas en el, asumiendo las consecuencias que en caso contrario pudieran derivarse por ley.

RESPONSABLE DEL SISTEMA

Nombre y apellidos	Cargo	Firma

ADMINISTRADOR DEL SISTEMA

Nombre y apellidos	Organismo / Unidad administrativa	Firma

RESPONSABLE DE SEGURIDAD DEL SISTEMA

Nombre y apellidos	Unidad administrativa	Nombre del sistema	Firma	Tipo de acceso

USUARIOS DEL SISTEMA

Nombre y apellidos	Unidad administrativa	Nombre del sistema	Firma	Tipo de acceso

Anexo E. Procedimientos de control de accesos, respaldo y recuperación y gestión

Procedimientos de control y seguridad (contiene los siguientes procedimientos)

Procedimiento de identificación, asignación y cambio de contraseñas.

a) Corresponde al administrador del sistema, la identificación del personal que accede a algún determinado sistema, así mismo la asignación de cuentas y/o contraseñas de acceso;

b) El acceso y tratamiento de la información confidencial, las cuentas de usuario y/o contraseñas deberán utilizarse exclusivamente para actividades que estén relacionadas con los propósitos y funciones institucionales que desempeñen los servidores públicos;

c) El responsable del sistema determinará los usuarios que tengan acceso al sistema por medio de controles de acceso, cuentas de usuario y/o contraseñas;

d) Las cuentas de usuario y/o contraseñas de acceso deberán ser identificadas y registradas por el administrador del sistema y procurará ajustar para mayor seguridad la nomenclatura de las mismas a los siguientes estándares:

   1. El nombre de usuario puede conformarse por 6 caracteres como mínimo y 25 caracteres como máximo;
   2. Para formar el nombre de usuario es necesario utilizar únicamente los siguientes caracteres: letras minúsculas "a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z.", dígitos "0, 1, 2, 3, 4, 5, 6, 7, 8, 9". y el guión "_" solo para casos especiales;
   3. No incluir letras con acentos, "ñ", ni ningún otro carácter especial como: espacios en blanco" / [] : ; I = , + * ? < >.;
   4. Las contraseñas deberán tener como mínimo 6 caracteres y como máximo 25 caracteres, su composición deberá ser alfanumérica (letras mayúsculas, minúsculas, números y algún signo de puntuación);
   5. Si hubieren duplicados o algún caso especial, estos deberán resolverse a criterio del administrador del sistema.

e) Es responsabilidad del usuario reportar si ha existido algún cambio de personal en el manejo de personal, así como cambiar cada determinado tiempo su contraseña, de acuerdo al grado de confidencialidad de la información que maneje; Se recomienda cambiar la contraseña cada 90 días naturales como mínimo o antes si el administrador o

responsable de seguridad del sistema lo considera necesario;

f) Para establecer o cambiar la contraseña no deberán relacionar la misma con datos personales como son fecha de nacimiento, nombre, apellidos, nombre de sus hijos, sobrenombre, entre otros;

g) El usuario deberá notificar al administrador del sistema de manera fehaciente e inmediata cualquier uso no autorizado de la información del sistema, de su cuenta o cualquier otra vulnerabilidad de su seguridad, para la evaluación del impacto del uso no autorizado y tomar las medidas necesarias para la solución del incidente;

h) En el caso de que un usuario olvide su contraseña deberá notificarlo al administrador del sistema para su recuperación, si requiere cambiar su contraseña, podrá utilizar las opciones disponibles cuando el propio sistema de que se trate lo permita; este cambio deberá ser notificado y/o solicitado según corresponda inmediatamente al administrador del sistema;

i) Los accesos, las cuentas de usuario y/o claves de acceso estarán vigentes en tanto el responsable del sistema no solicite la cancelación correspondiente.

Proceso para Respaldar

a) Identificar el número de bases de datos para respaldo;
b) Determinar los mecanismos de respaldo de datos: manual o automática;
c) Determinar la periodicidad del respaldo de datos;
d) Determinar los medios en los que se resguardarán los datos una vez realizado el respaldo de información. En caso de reutilización de medios deberá eliminar la información contenida en ellos a fin de procurar la integridad de la información;
e) Iniciar la copia de datos;
f) Verificar que los datos respaldados se encuentren íntegros;
g) Comprimir las copias de información en un archivo: zip, rar, etc.;
h) Verificar que los archivos comprimidos puedan ser descomprimidos correctamente y la información se encuentre íntegra;
i) Etiquetar el medio que contiene los archivos de respaldo con la siguiente información:
    1. Ubicación de los datos respaldados;
    2. Nombre de los datos respaldados;
    3. Fecha de creación del respaldo;

j) Resguardar el medio que contiene los datos en un lugar protegido.
k) Llevar a cabo un proceso de digitalización de sistemas de datos personales en físico si es necesario, para tener un respaldo y por ende de recuperación.

Proceso para Recuperar

a) Identificar el tipo de incidencia que impide el acceso a los datos desde su ubicación original;
b) Identificar los datos corruptos o la información a recuperar;
c) Solicitar el medio de resguardo que contiene la información a recuperar;
d) Copiar los archivos de respaldo y verificar su correcto acceso;
e) Asentar la incidencia en la bitácora de incidencias.

Proceso para la Gestión de Medios

Ingreso

a) Verificar que el soporte se encuentre correctamente identificado e incluya la información descrita;
b) Registrar el ingreso del soporte físico o electrónico;
c) Resguardar el soporte físico o electrónico en un lugar protegido.

Egreso

a) Verificar que el soporte contenga la información solicitada y se encuentre correctamente identificado;
b) En caso de reutilización, verificar que el soporte a asignar no cuente con ningún tipo de información, en caso contrario, los datos que se encuentren en el soporte deberán ser eliminados;
c) Registrar el egreso del soporte;
d) En caso de ser necesario, asegurarse del reingreso del soporte.

SISTEMA:	**Nombre del sistema**				
ALTAS		BAJAS			
N° de orden	Fecha de copia	Motivo			Fecha
		Reutilización	Destrucción	Otros	
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /

Los documentos de datos se enviarán a los responsables de la información en sobre cerrado, por mensajero y con acuse de recibo para garantizar e identificar su recepción.

Cualquier salida de soportes deberá ser autorizada por el responsable del sistema, de acuerdo con el siguiente documento:

AUTORIZACION DE SALIDA DE SOPORTES

Fecha de salida del soporte	

Soporte	
Identificación	
Contenido	
Documento de donde proceden los datos	
Fecha de creación	

Finalidad y Destino	
Finalidad	
Destino	
Destinatario	

Forma de Envío	
Medio de envío	
Remitente	
Precauciones para el transporte	

Autorización	
Persona que autoriza	
Cargo / Puesto	
Observaciones	
Firma	

Anexo F. Procedimiento de notificación y gestión de incidencias

Procedimiento de notificación y gestión de incidencias

Se describirá el procedimiento de notificación y gestión de incidencias.

En la notificación se hará constar:

a) *Tipo de incidencia;*
b) *Fecha y hora en que se produjo;*
c) *Persona que realiza la notificación;*
d) *Persona a quien se comunica;*
e) *Efectos que puede producir la incidencia;*
f) *Descripción detallada de la misma.*

Las incidencias registradas, se les otorgará un valor administrativo, conforme lo establecen los Lineamientos para Catalogar, Clasificar y Conservar los Documentos y la Organización de Archivos, por lo que su guarda será de 6 años.

A continuación, se adjunta el impreso de notificación manual que podrá ser utilizado para la notificación de incidencias.

Impreso de notificación de incidencias

Incidencia n°: |_____| (A ser rellenado por el responsable de seguridad).	
Fecha de notificación: /__/__/____/	
Tipo de incidencia: (Anotar todos los detalles de interés de la incidencia).	
Descripción detallada de la incidencia:	
Fecha y hora en que se produjo la incidencia:	
Persona(s) que realiza(n) la notificación: (Especificar si son usuarios o no del sistema).	
Persona(s) a quien(es) se comunica:	
Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella).	
Nombre y firma de quien recibe: _____	

Dado en la ciudad de Xalapa de Enríquez, Veracruz de Ignacio de la Llave, el día 17 de enero del año 2022.