PLAN DE RECUPERACIÓN DE DESASTRES Y DE CONTINUIDAD DE LA OPERACIÓN PARA LOS SISTEMAS INFORMÁTICOS

Contenido

GENERALIDADES

I. OBJETIVO

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen las Tecnologías y Sistemas de Información.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen los Sistemas de Información.
- Contar con una estrategia planificada compuesta por un conjunto de procedimientos que garanticen la disponibilidad de una solución alterna que permita restituir rápidamente los sistemas y tecnologías informáticas de la institución, esto ante la eventual presencia de siniestros que los paralicen parcial o totalmente.
- Identificar las acciones que se deben llevar a cabo y los procedimientos a seguir en el caso de la presencia de un siniestro que restrinja el acceso a los sistemas de información. ·
- Establecer las secuencias que se han de seguir para organizar y ejecutar las acciones de control de emergencias.
- Minimizar las pérdidas asociadas a la presencia de un siniestro relacionado con la gestión de los datos.

II. ALCANCE

El plan de contingencias es un análisis de los posibles riesgos y eventuales siniestros a los cuales puede estar expuesto equipos de cómputo, programas, archivos, sistemas y bases de datos a nivel institucional. En este documento se hace un análisis de los riesgos y siniestros a los cuales se encuentra sujeta el Área de Informática, así como, de las acciones a seguir para tratar de reducir su posibilidad de ocurrencia y los procedimientos apropiados en caso de la presencia de cualquiera de tales situaciones.

El alcance del plan de contingencia incluye los elementos básicos y esenciales, componentes y recursos informáticos que conforman las tecnologías y sistemas de información que maneja la Secretaría de Salud, mismas que se relacionan a continuación:

- ***Datos***: En general se consideran datos todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (Bases de Datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colecciones de bits.
- ***Aplicaciones***: Son los archivos y programas desarrollados o adquiridos por la entidad.
- ***Tecnología***: Incluye los equipos de cómputo como computadoras de escritorio, laptops, equipos de videoconferencia, servidores, cableados, switches, etc. en general, conocidos como hardware y los programas, archivos, bases de datos, etc. denominados software para el procesamiento de información.
- ***Instalaciones***: Lugares físicos de la Entidad donde se encuentren el Hardware y software.

III. DEFINICIONES

- ***Acceso***: Es la lectura o grabación de datos que han sido almacenados exitosamente en un sistema de computación. Tiene un resultado positivo de una autentificación cuando se consulta una Base de Datos, los datos son primero accedidos y suministrados a la computadora y luego transmitidos a la pantalla del equipo.
- ***Amenaza***: Cualquier evento que pueda interferir con el funcionamiento de un sistema y/o computadora y causar la difusión no autorizada de información. Ejemplo: Fallas del suministro eléctrico, virus, saboteos o descuido del usuario
- ***Ataque***: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o el intento de obtener de modo no autorizado la información confiada a una computadora.
- ***Privacidad*:** Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.
- ***Seguridad*:** Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados. En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos. El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.
- ***Integridad***: Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.
- ***Datos*:** Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.
- ***Base de Datos*:** Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan. También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

  Las características que presenta un DBMS son las siguientes:

  - Brinda seguridad e integridad a los datos.
  - Provee lenguajes de consulta (interactivo).
  - Provee una manera de introducir y editar datos en forma interactiva.

- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

- ***Incidente*:** Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.
- ***Sistemas de Información***: Es el término empleado en el ambiente del procesamiento de datos para referirse al almacenamiento de los datos de una organización y ponerlos a disposición de su personal. Pueden ser registros simples como archivos de Word y Excel, o pueden ser complejos como una aplicación de software con base de datos. Estos ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.

- ***Cortafuegos (Firewall)***: Es un sistema diseñado para bloquear el acceso no autorizado de comunicaciones. Se trata de un dispositivo configurado para permitir, limitar, cifrar y descifrar el tráfico de mensajes entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos se utilizan para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.

IV. CONDICIONES GENERALES Y GUIA DE ACCIONES.

Se indica a continuación los procedimientos y actividades generales que se deben tener en cuenta para la correcta ejecución del plan de contingencia que aplica para toda la Institución.

4.1 PLAN DE CONTINGENCIA:

TIPO DE RIESGO	FACTOR DEL RIESGO	PREVENCIÓN Y MITIGACIÓN
Incendio: destrucción de equipos y archivos	Bajo	Extintores, aspersores automáticos, detectores de humo, pólizas de seguros.
El robo común: pérdida de equipos y archivos.	Alto	Copias de respaldo (BackUp), Seguros sobre robos de equipos y contra todo riesgo, alarmas.
Vandalismo: daño a los equipos y archivos	Medio	Seguro contra todo riesgo, copias de respaldo
Fallas en los equipos: daño a los archivos	Medio	Mantenimiento, equipos de respaldo, garantía y copias de respaldo.
Equivocaciones: daño a los archivos.	Medio	Capacitación, copias de respaldo, políticas de seguridad.
Acción de Virus: daño a los equipos y archivos	Alto	Actualizaciones del sistema operativo, Antivirus actualizados, copias de respaldo
Terremotos: destrucción de equipo y archivos	Bajo	Seguro contra todo riesgo, copias de respaldo.
Accesos no autorizados: filtrado no autorizado de datos	Alto	Cambio de claves de acceso mínimo cada seis meses. Política de seguridad para acceso a personal competente.
Robo de datos: difusión de datos sin el debido permiso o acceso permitido.	Medio	Cambio de claves de acceso mínimo cada seis meses, custodia de las copias de respaldo.
Fraude: modificación y/o desvío de la información y fondos de la institución.	Bajo	Sistemas de información seguros con dos usuarios para autorizar transacciones, procedimiento de control.

4.2 PLAN DE RESPALDO

Para asegurar que se consideran todas las posibles eventualidades, se relacionan las actividades que se deben realizar con el objeto de prever, mitigar o eliminar los riesgos conocidos para la funcionalidad informática de la Secretaría:

No.	ACTIVIDAD	ELEMENTOS
1.	Copias de seguridad de la información y documentos residentes en los discos duros.	Documentos en formatos Word, Excel, PDF, artes, imágenes, audio y correos electrónicos
2.	Copias de seguridad de los sistemas de información y Bases de Datos	Aplicaciones WEB e intranet de información. Aplicaciones y Bases de Datos de los procesos y archivos.
3.	Contar mínimo con un kit de instalación para restaurar los archivos del sistema operativo y aplicaciones de una computadora o servidor en caso de falla o virus.	Sistema operativo (Windows, Linux, etc.) Paquetes de ofimática y diseño. (Office, Corel) Bases de datos (Sql, MySql, FoxPro, etc.) Drivers y utilitarios de impresoras, redes, computadoras, etc.
4.	Mantenimientos, revisiones preventivas y correctivas de equipos de cómputo y comunicación, extintores, alarmas y sistemas contra incendio, para mantenerlos en óptimas condiciones.	Equipos de cómputo y comunicación periféricos, sistemas eléctricos UPS, Aire acondicionado, Alarmas, Sistemas contra incendio, Extintores,
5.	Actualizar las claves o contraseña de acceso a las aplicaciones y bases de datos	Base de Datos, y sistemas de información
6.	Mantener actualizados los sistemas operativos, antivirus y aplicaciones	Sistemas operativos de equipos de cómputo, antivirus y aplicaciones. Entrega de una actualización cada vez que salga una nueva versión de las aplicaciones. Configuración de actualizaciones automáticas en los sistemas operativos.
7.	Mantener como respaldo un inventario adicional con equipos de cómputo, repuestos, consumibles, para su reemplazo	Equipos de computación, videoconferencias y de comunicación de la Entidad.

Se recomienda realizar una copia de seguridad de todos los sistemas institucionales y archivos del PC al menos para ser realizados cada viernes al término de la jornada laboral.

4.3 GUIA DE ACCIONES Y RECOMENDACIONES PROPUESTAS ANTE EMERGENCIAS

Este apartado corresponde a una guía general de las acciones que pueden seguir los responsables informáticos para enfrentar las emergencias tecnológicas dentro del área.

a) EMERGENCIA FÍSICA EN SERVIDOR

1. Error Físico de Disco de un Servidor.

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

a. Ubicar el disco crítico.
b. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
c. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
d. Bajar el sistema y apagar el equipo.
e. Retirar el disco dañado y reponerlo con otro del mismo tipo, formatearlo y darle partición.
f. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
g. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
h. Habilitar las entradas al sistema para los usuarios.

2. Error de Memoria RAM

En este caso se dan los siguientes síntomas:

i. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
j. Ante procesos mayores se congela el proceso.
k. Arroja errores con mapas de direcciones hexadecimales.
l. El servidor deberá contar con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.
m. Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo inmediatamente.
n. Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Ubicar las memorias dañadas.
- Retirar las memorias dañadas y reemplazarlas por otras iguales o similares.
- Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para

estaciones en las cuales se realizarán las pruebas.
- Probar los sistemas que están en red en diferentes estaciones.
- Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

3. Error de Tarjeta(s) Controladora(s) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

o. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
p. El servidor debe estar apagado, dando un correcto apagado del sistema.
q. Ubicar la posición de la tarjeta controladora.
r. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
s. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
t. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
u. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

4. Caso de Incendio Total

La mejor manera de **prevenir** un incendio es no provocarlo. Observe las prohibiciones de no fumar y las normas de prevención institucional.

En presencia del fuego tenga en cuenta que:

- Puede tratar de apagar un fuego en una oficina siempre que tenga detrás una puerta que le permita salida.
- Si el fuego prende en sus ropas, no corra, tírese al suelo y ruede. Si el hecho ocurre a otra persona cúbrala con alguna prenda o con una toalla humedecida, si se encuentra próximo a un aseo. No se quite la ropa si tiene quemaduras.
- En presencia de aparatos eléctricos, no eche agua al fuego**.** Tampoco debe hacerlo ante líquidos inflamables (alcohol, aceite, gasolina, etc).
- Si hay mucho humo póngase un pañuelo en la boca y nariz, a ser posible mojado, y salga agachado o gateando. Respire profundamente para evitar desvanecimientos.
- Al salir de la dependencia, procure cerrar las ventanas y las puertas, pues las corrientes avivan el fuego.
- Si se encuentra aislado y no puede ponerse a salvo, diríjase a la habitación más alejada del fuego (pero no a un nivel superior a menos que esté seguro de que los equipos de rescate se encuentran muy cerca y provistos de escaleras largas u otro equipo.
- Si se ve obligado a huir a través de las llamas para ponerse a salvo, no se entretenga en recoger nada, cúbrase (incluyendo la cabeza) con una manta, una toalla, una cortina o un abrigo mojados si es posible, luego aguante la respiración y corra.

- Si tiene que desalojar el edificio siga las normas de “Evacuación”

5. Caso de Inundación

v. Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.

w. En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.

x. Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.

y. Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.

z. Proveer cubiertas protectoras para cuando el equipo esté apagado.

6. Caso de Fallas de Fluido Eléctrico

Se puede presentar lo siguiente:

aa. Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.

bb. Las tareas de supervisión y vigilancia de funcionamiento de los servidores tras el incidente y/o falla eléctrica, están a cargo por personal designado por el titular del Área de Informática de la Secretaría de Salud.

7. <u>Generalidades con respecto a la seguridad ante emergencia</u>

En el momento que se dé aviso por los altavoces de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos.

cc. Ante todo, se debe conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, se debe tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

dd. Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

b. EMERGENCIAS DE DATOS (CASO)

1. Caso de Virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

a. Contar con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación.

b. El antivirus muestra el nombre del archivo infectado y quién lo usó.

c. Si los archivos de sistema han sido afectados por el virus, estos archivos serán reemplazados del disco original de instalación o del backup.

d. Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras:

Se revisará las computadoras y laptops con antivirus preferentemente portable.

De suceder que una computadora se haya infectado con uno o varios virus ya sea en la memoria o a nivel disco duro, se debe proceder a realizar los siguientes pasos:

a. Utilizar un antivirus (preferentemente portable en usb o cd) igual o mayor en versión al instalado en la computadora infectada. Reiniciar la computadora con dicho dispositivo portable.

b. Retirar el dispositivo portable con el que arrancó la computadora e insertar el antivirus portable, luego activar el programa de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, se borrará el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del Scaneado. Finalizado el scaneado, reconstruir el Master Boot del disco duro.

c. En cualquier caso de que se realice el escaneo de equipos de cómputo y/o laptops por fallas o daños causados por virus, se debe realizar un respaldo de archivos y documentos, esto en la medida de lo posible y si así lo permite el equipo de cómputo.

c. RESPECTO A LA ADMINISTRACIÓN DE LOS BACKUPS

a. Se administrará bajo la lógica de un almacén, esto implica ingreso y salida de medios magnéticos (USB, discos removibles, CD's, etc.) obviamente teniendo más cuidado con las salidas y cuidando que el grado de temperatura y humedad sean los adecuados.

b. Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.

c. El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

d. RESPECTO A LA ADMINISTRACIÓN DE IMPRESORAS

a. Todo listado que especialmente contenga información confidencial, debe ser destruido.

b. Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.

c. Establecer controles respecto a los procesos remotos de impresión.

e. PARA EL MANTENIMIENTO DE LOS DISCOS DUROS

a. Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.

b. El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.

c. Evitar que la computadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.

d. No mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

e. para mantener la velocidad en el equipo, se debe realizar una vez al mes el proceso de desfragmentación para conservar en óptimo estado la respuesta del equipo; Windows incluye un desfragmentador de disco fácilmente localizable en el menú Inicio/Todos los programas/Accesorios/Herramientas del Sistema/Desfragmentador de disco.

f. Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un equipo de cómputo.

f. RESPECTO A LOS MONITORES

a. Usar medidas contra la refección para reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día.

b. Sentarse por lo menos a 60 cm. de la pantalla. No sólo esto reducirá su exposición a las emisiones (que se disipan a una razón proporcional al cuadrado de la distancia), sino que puede ayudar a reducir el esfuerzo visual.

c. También manténgase por lo menos a 1 m. o 1.20 m. del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.

d. Finalmente apague su monitor cuando no lo esté usando

g. PARA EL CUIDADO DEL EQUIPO DE CÓMPUTO

a. Teclado. Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función. Para eliminar el polvo del teclado, lo más conveniente es voltearlo y soplar el aire comprimido para que éste salga completamente. Se debe evitar en lo posible quitar las tapas de las teclas de la PC para lavarlas, ya que su reposición puede generar fallas mecánicas.

b. Mouse. El mouse percibe los movimientos a través de una esfera de caucho, la cual mueve dos rodillos; por lo general, en éstos se acumula suciedad con el uso, impidiendo el correcto funcionamiento, para limpiarlos se debe quitar con cuidado la tapa para liberar la esfera y usar un hisopo para limpiar los rodillos. Antes de realizar cualquier movimiento, se sugiere observar cómo están colocados, por si ocurre algún accidente, no haya ningún problema para colocarlos nuevamente. Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste. Para el caso de Mouse de led alejarlo de zonas con polvo y se recomienda el uso de mouse pad.

c. CD-ROM. Antes de usar cualquiera de estos componentes, se debe verificar que el CD-ROM/DVD o CDRW del equipo se encuentren limpios, de igual forma, cada CD o DVD que se utilicen deben encontrarse libres de polvo y partículas para forzar menos al láser y prolongar su duración.

d. Protectores de pantalla. Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.

e. Impresora. El manejo de las impresoras, en su mayoría, es a través de los botones y cuidar el cambio de cartuchos de tinta/ toner.

f. En caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado.

g. Papelera de reciclaje. Windows reserva un 10 por ciento de la capacidad del disco duro para mantener algo de la información que ya se haya eliminado, con la finalidad de que en cualquier momento se pueda recuperar. No obstante, la papelera de reciclaje, ubicada en el Escritorio de la computadora, debe limpiarse con regularidad para no llenarse de basura que le estará quitando espacio en disco duro.
Se debe seleccionar el ícono y hacer clic derecho, posteriormente elegir la opción Explorar, podrá ver todos los archivos ubicados en su papelera y eliminar aquéllos que no necesite o, en su caso, vaciar la papelera de reciclaje.

h. Término de sesión o apagado. En muchas ocasiones, por la prisa o mal uso de la computadora, no se cierran las aplicaciones correctamente o bien, no se apaga la computadora de forma adecuada, esto provoca pérdida de información y daña el sistema operativo.

h. MANTENER LAS ÁREAS OPERATIVAS LIMPIAS Y PULCRAS

Para proteger a nuestras computadoras del polvo, resulta muy conveniente adquirir algunas fundas para los CPU, monitor, teclado, escáner, y/o cualquier otro equipo de cómputo para evitar que entre el polvo a los componentes más sensibles y cause daño; no se debe olvidar que la limpieza es necesaria, para ello se pueden emplear aire comprimido, espumas y una pequeña franela (Soporte técnico).

V. REPORTE DE PROBLEMA Y SOLICITUD DE MEJORA

Los funcionarios y/o personal de la institución pueden solicitar la solución de un problema presentado o realizar una solicitud de mejora del sistema o percance presentado, comunicándolo al Área de Informática quienes son los encargados de gestionar cualquier solicitud por parte de los usuarios finales, presentando una solución de acuerdo con el nivel de importancia, los niveles de servicio y tipo de problema presentado.

COLABORADORES:

Dr. José Manuel Cruz Castellanos
Secretario de Salud y Director General del Instituto de Salud

Dra. Alejandra Martínez Meneses
Directora de Planeación y Desarrollo

Ing. Rolando Humberto Gómez Hernández
Jefe del Área de Informática