SERVICIOS DE SALUD DE HIDALGO

SALUD
SECRETARÍA DE SALUD

Estado Libre y Soberano de Hidalgo

SERVICIOS DE SALUD DE HIDALGO
DIRECCIÓN DE PLANEACIÓN, PRESUPUESTO Y EVALUACIÓN
SUBDIRECCIÓN DE INFORMACIÓN EN SALUD

PLAN DE RECUPERACIÓN DE DESASTRES EN MATERIA DE TECNOLOGÍAS DE INFORMACIÓN

Fecha de elaboración	Elaborado por	Revisado por	Validado por
dic- 2023	Ing. Jorge Héctor Samperio Gallardo Ing. Edgar Bautista Cuadrilla	Ing. Zeltzin Xiutlaizin Viveros Estrada	L.A.P. Mireya Gutierrez García

SERVICIOS DE SALUD DE HIDALGO

SALUD
SECRETARÍA DE SALUD

Estado Libre y Soberano de Hidalgo

Tabla de contenido

OBJETIVO GENERAL

Proporcionar a las áreas que utilizan Tecnologías de Información de los Servicios de Salud de Hidalgo una guía de referencia que indique los procedimientos e instrucciones para dar continuidad a las operaciones, procesos y servicios informáticos de orden crítico, en caso de que se llegara a presentar algún desastre o contingencia.

1. OBJETIVOS ESPECÍFICOS

- Proteger los recursos de la Institución, buscando su adecuada administración ante posibles riesgos que los afecten.
- Definir y aplicar medidas para prevenir los riesgos en materia de tecnologías de la información.
- Establecer responsables para la administración de riesgos y la atención de contingencias.
- Establecer los procedimientos y elementos mínimos requeridos para afrontar las contingencias.
- Proveer una solución para mantener los procedimientos administrativos, sistemas de información y equipos de cómputo fundamentales de la institución, funcionando correctamente.
- Definir las consecuencias y evitar una posible pérdida de información relacionada con un evento inesperado, en un nivel aceptable, al ejecutar procedimientos de respaldo apropiados.
- Estimular la creación de una cultura digital entre los miembros de la Institución.

2. ALCANCE

Este documento aplica a todo el personal que tenga acceso a los bienes informáticos, sistemas de información, telecomunicaciones y tecnología de los Servicios de Salud de Hidalgo.

3. DEFINICIONES

Acceso: Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación.

Ataque: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a un computador.

Amenaza: Cualquier cosa que pueda interferir con el funcionamiento adecuado de un computador o causar la difusión no autorizada de información confiada en un servidor. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

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, hojas de cálculo, imágenes, vídeo, etc.

Equipos de cómputo: Elementos o dispositivos de hardware, software, redes y telecomunicaciones interconectados que son utilizados para lleva a cabo las actividades operativas sistematizadas de la Institución.

Incidente: Cuando se produce un ataque o se materializa una amenaza, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

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.

Plan de contingencia: Estrategia planificada con una serie de procedimientos que faciliten y orienten a tener una solución alternativa que permita restituir rápidamente los servicios de la Institución ante la eventualidad de todo lo que la pueda paralizar, ya sea de forma parcial o total.

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.

Sistema de Información: Organización sistemática para almacenar los datos de una organización y ponerlos a disposición de su personal.

Los sistemas están estrechamente relacionados entre usuarios, equipos y rutinas o procedimientos automatizados; estos elementos son necesarios entre sí, por lo tanto, es imprescindible tomar medidas que permitan una continuidad en la operatividad de los sistemas para no ver afectados los objetivos y no perder la inversión de costos y tiempo.

4. POLÍTICAS GENERALES DE SEGURIDAD Y USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y TELECOMUNICACIONES

- El acceso a los espacios físicos donde se ubiquen los bienes tecnológicos deberá ser restringido y solo permitir el ingreso y uso de los elementos antes descritos al personal debidamente identificado y autorizado para tal efecto.
- Todos los equipos de cómputo deben contar con protección por contraseña establecida por el encargado de TI en el área. En caso de que el funcionario defina la contraseña, debe informar al encargado de TI o a su jefe inmediato vía oficio.
- Es responsabilidad del funcionario, analizar todos los dispositivos de almacenamiento externos que se conecten a su equipo de cómputo, para evitar infecciones de programas maliciosos y corrupción del sistema o de la información.
- El funcionario debe realizar los respaldos pertinentes y con la frecuencia que considere adecuada, con base a la criticidad de los datos que tiene bajo su responsabilidad.
- Es responsabilidad del funcionario leer los manuales de operación de los bienes informáticos antes de utilizarlos, con esto se evita un mal funcionamiento o daños permanentes en los equipos.
- El acceso a los sistemas de información deberá ser restringido mediante un pasaporte, consistente en un nombre de usuario y contraseña, el

cual debe ser entregado al funcionario mediante oficio, indicando la responsabilidad que tiene sobre la operación del sistema y el uso, explotación o difusión de la información generada por el mismo.

- En caso de sistemas nominales, el funcionario debe firmar una carta de confidencialidad, en la cual se notifique sobre las disposiciones legales que implica el incorrecto uso de los datos que se procesan.
- Para la instalación de software requerido para desempeñar las funciones encomendadas al personal, se deberá solicitar al encargado de TI del área el apoyo para verificar los términos de licenciamiento, legitimidad y derechos de autor del mismo. Para elementos que no se cuente con alguno de los elementos anteriores se recomienda el uso de software libre.
- Es responsabilidad del funcionario evitar la instalación de software que no cuente con el aval del área de TI así como de aquel que fomente la piratería, pornografía o cualquier actividad ilícita.
- Es responsabilidad del funcionario utilizar la infraestructura para desempeñar las tareas propias de la institución sin buscar un bien personal ya sea para económico o de ocio.
- No se utilizarán los bienes informáticos de la institución para almacenar, reproducir, ejecutar o transmitir copias no autorizadas de software o información digital (incluyendo música, videos o juegos).
- El área de TI Estatal establecerá las políticas de uso aceptable para indicar que el uso del Internet es un bien público por lo que deberá coadyuvar a las tareas definidas por la institución.
- El encargado de TI establecerá los filtros necesarios para optimizar el consumo de Internet entre los funcionarios, priorizando las tareas definidas por la institución.

5. ATENCIÓN DE CONTINGENCIAS

A. FALLO DEL SERVICIO DE INTERNET

Acciones para restablecer el servicio:

- Elaborar documento de apertura de incidencia con fecha, hora, diagnóstico inicial, persona que lo reporta y persona que atiende la primera acción.
- Notificar a los usuarios sobre la falla.

- Verificar cableado: integridad física, continuidad, envío y recepción de paquetes.
- Verificar conexión inalámbrica: alcance, potencia, envío y recepción de paquetes.
- Verificar que los equipos Router, Access Point, Switch estén encendidos.
- Verificar dirección IP, puerta de enlace y DNS.
- Verificar reglas de antivirus y políticas de firewall local para descartar bloqueos o restricciones.
- Verificar políticas de Firewall/UTM para identificar que el usuario pertenece a un grupo permitido para el acceso a internet y descartar bloqueos o restricciones por categorización de sitios o contenido.
- Verificar actualizaciones, plugins, extensiones o barras de herramientas del browser que impidan el acceso a Internet.
- Analizar el equipo para eliminación de virus o malware.
- Verificar disponibilidad del servicio con proveedor.

Cuando se restablezca el servicio:

- Verificar acceso, continuidad y velocidad del servicio.
- Emitir documento de cierre de incidencia con fecha, hora, diagnóstico final y personas que atendieron el caso.

B. FALLO DE CONECTIVIDAD ALÁMBRICA O INALÁMBRICA

Acciones para restablecer el servicio:

- Elaborar documento de apertura de incidencia con fecha, hora, diagnóstico inicial, persona que lo reporta y persona que atiende la primera acción.
- Verificar cableado: integridad física, continuidad, envío y recepción de paquetes.
- Verificar conexión inalámbrica: alcance, potencia, envío y recepción de paquetes.
- Verificar contraseña de acceso inalámbrico.
- Verificar que los equipos Router, Access Point, Switch estén encendidos.
- Verificar dirección IP, puerta de enlace y DNS.
- Verificar políticas de Firewall/UTM para identificar que el usuario pertenece a un grupo permitido para el acceso a la red.
- Verificar funcionamiento de dispositivos físicos de conexión como tarjetas de red o adaptadores inalámbricos.

Cuando se restablezca el servicio:

- Verificar acceso, continuidad y velocidad del servicio.
- Emitir documento de cierre de incidencia con fecha, hora, diagnóstico final y personas que atendieron el caso.

C. FALLO DE DISPOSITIVOS DE IMPRESIÓN

Acciones para restablecer el servicio:

- Elaborar documento de apertura de incidencia con fecha, hora, diagnóstico inicial, persona que lo reporta y persona que atiende la primera acción.
- Verificar cable de datos, cable de red o conexión inalámbrica.
- Verificar disponibilidad de papel.
- Verificar nivel de consumibles.
- Verificar peso y tipo de papel.
- Verificar atasco de papel.
- Verificar inyectores.
- Verificar el fusor.

Cuando se restablezca el servicio:

- Verificar posibilidad de impresión desde distintas ubicaciones.
- Emitir documento de cierre de incidencia con fecha, hora, diagnóstico final y personas que atendieron el caso.

D. FALLO DE SISTEMAS DE INFORMACIÓN

Acciones para restablecer el servicio:

- Elaborar documento de apertura de incidencia con fecha, hora, diagnóstico inicial, persona que lo reporta y persona que atiende la primera acción.
- Verificar servicio de Internet.
- Verificar servicio de red alámbrica o inalámbrica.
- Verificar políticas de Firewall/UTM para identificar que el usuario pertenece a un grupo permitido para el acceso a internet y descartar bloqueos o restricciones por categorización de sitios o contenido.

- Verificar pasaporte: usuario y contraseña, para ingreso al sistema. Si se ha olvidado cualquiera de estos elementos, proceder con el proceso de restablecimiento.
- Verificar la vigencia del pasaporte de ingreso al sistema. Si se ha vencido, solicitar al administrador de sistema para su renovación.
- Verificar con el área propietaria del sistema, la disponibilidad en línea, en red o por versión de sistemas operativos.
- Verificar con el área propietaria del sistema, la configuración y archivos requeridos para la operación.

Cuando se restablezca el servicio:

- Verificar la disponibilidad y operación del sistema.
- Emitir documento de cierre de incidencia con fecha, hora, diagnóstico final y personas que atendieron el caso.

E. PÉRDIDA DE DATOS EN EQUIPOS DE CÓMPUTO

- Elaborar documento de apertura de incidencia con fecha, hora, diagnóstico inicial, persona que lo reporta y persona que atiende la primera acción.
- Analizar por posible infección de virus.
- Verificar si existen puntos de restauración.
- Verificar respaldos.
- Aplicar herramientas de recuperación de datos, autorizados por la Subdirección de Información en Salud.
- Al finalizar el diagnóstico y la posible recuperación de datos, emitir documento de cierre de incidencia con fecha, hora, diagnóstico final y personas que atendieron el caso.

F. ROBO

- Elaborar, junto con el responsable administrativo, Acta de hechos y proceder a realizar la denuncia ante el Ministerio Público con apoyo de Jurídico.
- Si existiese circuito cerrado de video, revisar los registros en busca de evidencia.
- Realizar las entrevistas al personal operativo y personal de seguridad en busca de personas sospechosas.

- Entregar copia del Acta emitida por el Ministerio Público al responsable de la unidad, con copia a la Subsecretaría de Administración y Finanzas, Contraloría y Jurídico.
- Aplicar, si fuese el caso, la reposición del equipo a las personas que tienen bajo su resguardo el equipo.

G. DAÑO INTENCIONADO A EQUIPO

- Elaborar, junto con el responsable administrativo, Acta de hechos.
- Realizar las entrevistas al personal operativo y personal de seguridad en busca de personas sospechosas.
- Entregar copia del Acta de hechos al responsable de la unidad, con copia a la Subsecretaría de Administración y Finanzas y Contraloría.
- Aplicar, derivado del diagnóstico y adjudicación de responsables, la reposición del equipo o las sanciones que correspondan.

6. RECOMENDACIONES SOBRE AMENAZAS

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

A continuación, se enlistan los peligros recurrentes y las acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

A. INCENDIOS

- Prohibido fumar en todas las áreas.
- Deben emplearse muebles de materiales incombustibles y cestos metálicos para papeles.
- El piso y el techo de las áreas con equipo de cómputo, de telecomunicaciones y de almacenamiento de los medios magnéticos deben ser impermeables.
- Contar con áreas debidamente ventiladas.
- Instalar alarmas de detección de incendios.

- La temperatura no debe sobrepasar los 18° C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Las áreas con equipos de cómputo deben estar provistas de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes (cuarto de servidores).
- Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel.

B. INUNDACIONES

- Verificar el mantenimiento hidráulico de los edificios, así como impermeabilización de techos y sellado de muros.
- Revisar frecuentemente el sistema de drenaje en busca de obstrucciones.
- Diseñar los espacios para que los equipos electrónicos, de cómputo u otro que utilice energía eléctrica se encuentre lejos de ventanas o accesos al exterior.
- Revisar las acometidas eléctricas y los paneles de control para que permitan el corte de energía eléctrica en caso de ser necesario.
- Mantener limitado el acceso solo a personal autorizado a los sitios de concentración de energía eléctrica.

C. INSTALACIONES ELÉCTRICAS

- Diseñar una red eléctrica de acuerdo a los estándares vigentes.
- Proveer una red de energía regulada para los contactos destinados a equipos informáticos.
- Proveer de tierra física.
- Instalar infraestructura pararrayos.
- Diseñar los espacios para que los equipos electrónicos, de cómputo u otro que utilice energía eléctrica se encuentre lejos de ventanas o accesos al exterior.
- Revisar las acometidas eléctricas y los paneles de control para que permitan el corte de energía eléctrica en caso de ser necesario.
- Mantener limitado el acceso solo a personal autorizado a los sitios de concentración de energía eléctrica.

- Proveer de extinguidores para componentes eléctricos.
- Proveer de reguladores y sistemas ininterrumpidos de energía para equipos informáticos.
- Contar con un inventario de equipo eléctrico y electrónico para identificar cargas o consumos altos de energía.

D. CABLEADO DE RED

- Diseñar el cableado de acuerdo a la disposición de equipos y personal en el edificio considerando futuros cambios, esto para minimizar el contacto con el personal, daños al cableado y costos de reubicación.
- Evitar ubicar los cables cerca de maquinaria pesada o equipos de radio o microondas.
- Utilizar materiales certificados.
- Elaborar la certificación de nodos y conectividad.
- Elaborar la memoria técnica.
- Utilizar materiales blindados para instalaciones en el exterior.
- Ubicar el SITE de comunicaciones bajo los estándares vigentes.
- Instalar equipos de aire acondicionado con la capacidad suficiente para mantener el SITE a temperatura adecuada.
- Proveer de extinguidores para componentes eléctricos.

E. AIRE ACONDICIONADO

- Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de servidores y equipos de proceso de datos en forma exclusiva.
- Revisar las acometidas eléctricas y los paneles de control para que permitan el corte de energía eléctrica en caso de ser necesario.
- Proveer de extinguidores para componentes eléctricos.

F. AMENAZAS OCASIONADAS POR EL HOMBRE

Los componentes de la infraestructura tecnológica son posesiones valiosas de la Institución y pueden estar expuestas. Es frecuente que los usuarios utilicen los equipos de cómputo de la institución para realizar trabajos privados y de esta manera reduzca su productividad o incremente la vulnerabilidad a ataques.

- Todos los equipos que componen la infraestructura tecnológica de la institución deben estar instalados de manera no fácil de sustraer o acceder.
- Su posicionamiento y ubicación se debe registrar incluyendo número de serie del equipo, modelo, marca, especificaciones técnicas, número de inventario y persona responsable.
- El uso que los funcionarios de la institución dan a los diferentes componentes de la infraestructura tecnológica debe estar registrado y se deben comunicar las políticas de uso aceptable (PUA).

G. DISTURBIOS, SABOTAJES INTERNOS Y EXTERNOS DELIBERADOS

- Para el control de acceso al cuarto de servidores a cualquier personal ajeno a la institución y/o División de sistemas se le tomarán los datos y se registrará el motivo de la visita, hora de ingreso y de salida.
- El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a las distintas áreas de la Institución.
- Proveer de un sistema de circuito cerrado de televisión para el control y monitoreo de los espacios libres y algunos cerrados a fin de chequear el curso normal de actividades.

H. SEGURIDAD LÓGICA

- Mantener actualizados los sistemas operativos
- Instalar y mantener actualizado el software antivirus.
- Informar a los usuarios sobre los peligros digitales como malware, ransomware, virus, phishing, spyware, spam, pharming, spoofing, hacking, phreaking, hijackware, password stealer, adware, hoax, etc.
- Instalar equipos UTM como parte de la infraestructura tecnológica.
- Cifrar información crítica o sensible.
- Realizar respaldos frecuentes en medios externos y cifrados.
- Crear cuentas separadas de administrador y de usuario en los equipos de cómputo.

I. CONTROLES DE ACCESO

- Establecer pasaportes mediante identificación y autentificación
- Crear roles
- Crear transacciones
- Diseñar limitaciones a los servicios
- Establecer modalidades de acceso
- Generar protocolos de acceso mediante ubicación y horario
- Mantener protocolos para el control de acceso interno y externo
- Establecer y responsabilizar al personal de administración

7. TABLA DE RIESGOS

Riesgo	Tipo de riesgo	Probabilidad de ocurrencia	Grado de impacto
Incendios	Tecnológicos	Remota	Muy Severo
Sismos	Naturales	Remota	Muy Severo
Inundaciones	Sociales	Aleatoria	Grave
Fallas en la conexión de red	Tecnológicos	Poco Frecuente	Moderado
Inoperatividad de los Servidores	Tecnológicos	Poco Frecuente	Moderado
Inconvenientes eléctricos	Tecnológicos	Frecuente	Moderado
Pérdida de Información	Tecnológicos	Poco Frecuente	Grave
Acción de virus informático	Sociales	Poco Frecuente	Grave
Alteración de la información	Sociales	Poco Frecuente	Grave
Robo común de equipos y archivos	Sociales	Remota	Grave
Robo de información y datos	Sociales	Poco Frecuente	Grave
Ausencia del Personal de TI	Sociales	Poco Frecuente	Moderado

8. MODELO DE ESCALAMIENTO

Al momento de identificar un riesgo, amenaza o cuando se presente un desastre o contingencia el ciclo de notificación debe ser el siguiente, considerando que, si no se resuelve o atiende el evento en el primer contacto, subirá de nivel hasta su resolución: