SALUD

SECRETARÍA DE SALUD

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARÍA DE SALUD

Proyecto 1.0

UNIDAD DE ADMINISTRACIÓN Y FINANZAS
Dirección General de Tecnologías de la Información

Contenido

I. INTRODUCCIÓN

La Secretaría de Salud, como dependencia del Gobierno de México, encabeza el Sector Salud por tanto es a la que le corresponde formular, establecer y controlar las políticas de salud para el país. En conjunto con sus Unidades Administrativas, así como los Órganos Desconcentrados de la Secretaría de Salud, son los responsables de consolidar estas políticas de salud pública, junto con otros organismos autónomos descentralizados, lo que hace que sea una organización con alto grado de complejidad.

Aun cuando cada Institución es un organismo autónomo en su administración, existe una alta interdependencia para el cumplimiento en la consolidación de la información relevante la cual sirve tanto para el cuidado de la salud de la población en sus distintos niveles, así como para los procesos de planificación, programación, monitoreo, control y evaluación de las políticas y programas en materia de Salud.

Para que los principios de la Política de Seguridad de la Información sean efectivos, resulta necesaria la implementación de una Política de Seguridad de la Información que forme parte de la cultura organizacional y laboral en la Secretaría de Salud, lo que implica contar con el compromiso de todos los servidores públicos de la Institución vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

Por lo anterior, el rol de la Dirección General de Tecnologías de la Información (DGTI) es, además de otras actividades sustantivas, operativas y administrativas, generar y aplicar políticas de seguridad informática para garantizar la integridad de los datos que se procesan, almacenan, comparten, divulgan y transfieren a otras dependencias, aprovechando el uso eficiente de tecnologías de la información, y aportando al logro de los objetivos institucionales de manera confiable, integra y oportuna.

Como consecuencia de lo expuesto, se han realizado las tareas de implementar sus propias políticas de seguridad de la información, basándose en las características establecidas en el Modelo de Política de Seguridad de la Información ISO27002, si bien es cierto, la Secretaría de Salud no busca obtener la certificación ISO, sí considera los parámetros que deben cumplir los Sistemas de Gestión de la Seguridad de la Información (SGSI) a implementarse.

El presente documento, es un documento vivo, es decir, se deberá actualizar conforme a las necesidades actuales de la Secretaría de Salud y a la gestión de los recursos tecnológicos a cargo de la DGTI, a fin de establecer los mecanismos de seguridad, estándares y mejores prácticas requeridas para mantener de forma segura la información que se almacena, procesa y transfiere a través de la infraestructura tecnológica que administra, gestiona y se provee a las UA/OAD.

La DGTI en el desempeño de las funciones que actualmente tiene establecidas en el Reglamento Interior de la Secretaría de Salud, gestiona y administra entre otros, los siguientes servicios de aplicación general a las UA/OAD, mismos que se enuncian a continuación:

- Equipo de Cómputo,
- Red local e Internet,
- Servicios de Centro de Datos,
- Correo Electrónico Institucional,
- Gestión Documental
- Servicio de Videoconferencias
- Publicación de portales y páginas dentro del dominio salud.gob.mx.
- Desarrollo y mantenimiento de software

II. MARCO JURÍDICO

- Constitución Política de los Estados Unidos Mexicanos, DOF 05-II-1917. Última Reforma D.O.F. 28-05-2021

LEYES

- Ley Orgánica de la Administración Pública Federal. D.O.F. 29-12-1976. Última Reforma 05-04-2022.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Nueva Ley D.O.F 26-01-2017.
- Ley General de Transparencia y Acceso a la Información Pública. D.O.F 04-05-2015. Última Reforma D.O.F 20-05-2021.
- Ley General de Responsabilidades Administrativas. D.O.F 18-07-2016. Última Reforma D.O.F 22-11-2021
- Ley Federal de Telecomunicaciones y Radiodifusión. D.O.F 14-07-2014.
- Ley Federal de Transparencia y Acceso a la Información Pública. Última Reforma D.O.F 20-05-2021.

REGLAMENTOS

- REGLAMENTO INTERIOR DE LA SECRETARÍA DE SALUD. D.O.F 19-01-2004. Última reforma D.O.F 7-02-2018

ACUERDOS

- Plan Nacional de Desarrollo 2019-2024. D.O.F. 12-07-2019.
- Programa Sectorial de Salud 2020-2024. D.O.F. 17-08-2020.
- Programa Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública 2019-2024. D.O.F. 30-08-2019.
- Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal. D.O.F. el 06-09-2021.
- ACUERDO por el que se expide la Estrategia Digital Nacional 2021-2024. D.O.F. 06-09-2021.

NORMAS Y ESTÁNDARES

- ISO 27001:2013 norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI).
- ISO 27000, Tecnologías de la Información-Resumen y vocabulario.
- ISO 27002, Tecnologías de la Información-Técnicas de Seguridad.
- ISO 27005, Tecnologías de la Información-Técnicas de Seguridad
- DISPOSICIONES Y CRITERIOS EMITIDOS POR LA COORDINACIÓN DE ESTRATEGIA DIGITAL NACIONAL Difundidas en https://www.gob.mx/cedn.
- Bases Técnicas de Seguridad Informática para las Dependencias y Entidades de la Administración Pública Federal. 12/03/2020.
- Políticas digitales alineadas al Plan Nacional de Desarrollo.
    - ✓ Coordinación de la política tecnológica en la Administración Pública Federal
    - ✓ Mayor impulso y eficiencia en el aprovechamiento de la Infraestructura de TIC
    - ✓ Política nacional de fomento a las compras de TIC
    - ✓ Análisis técnico de proyectos de TIC
    - ✓ Gobierno electrónico
    - ✓ Innovación tecnológica
    - ✓ Proceso de planeación para el desarrollo de la Estrategia Digital Nacional u de la Política Tecnológica
    - ✓ Priorizar el software libre y los estándares abiertos
    - ✓ Máximo aprovechamiento de sistemas e infraestructura
- Proceso de Planeación de la Estrategia Digital Nacional y de la Política Tecnológica. 12/2018.
- PROTOCOLO NACIONAL HOMOLOGADO DE GESTIÓN DE INCIDENTES CIBERNÉTICOS. Secretaría de Seguridad y Protección Ciudadana. Guardia Nacional. 10/2021

III. GLOSARIO DE TÉRMINOS

Acuerdo. El Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información, en la Administración Pública Federal.

Administrador del Servicio: Servidor público adscrito a la Dirección General de Tecnologías de la Información, designado como responsable de la verificación, supervisión y aceptación de los servicios TIC que conforme al ámbito de su competencia le correspondar.

Auditabilidad. Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Autenticidad. Asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Confiabilidad de la Información. - es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad. Garantizar que la información sea protegida para que no sea divulgada sin consentimiento de la persona.

Disponibilidad. Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, en términos de las disposiciones aplicables.

DGTI. Dirección General de Tecnologías de la Información.

Enlace Informático. El servidor público designado por la unidad administrativa u órgano administrativo desconcentrado de la Secretaría de Salud, como responsable para comunicar, informar, apoyar y acordar con la DGTI todo lo relacionado con la coordinación de la función informática al interior de la unidad administrativa u órgano administrativo desconcentrado de su adscripción.

Enlace de Seguridad de la Información. Servidor público designado por el Responsable de la Seguridad de la Información para coadyuvar y vigilar el cumplimiento y aplicación de las presentes Políticas y de las disposiciones normativas aplicables en materia de seguridad de la información.

Grupo de Trabajo. Grupo de Trabajo de la Seguridad de la Información ce la Secretaría de Salud.

Información. Toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad. Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.

Legalidad. Cumplimiento de las leyes, normas, reglamentaciones o disposiciones que resulten aplicables en la materia.

MGSI-SSA. Marco de Gestión de Seguridad de la Información de la Secretaría de Salud alineado a la política general de Seguridad de la Información.

No repudio. Evitar que una entidad que haya enviado o recibido información, alegue ante terceros que no la envió o recibió.

Normas. Normas y estándares relacionados con sistemas de información y seguridad de la información.

Políticas de Seguridad. Políticas de Seguridad de la Información de la Secretaría de Salud.

Protección a la duplicación. Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Responsable de la Seguridad de la Información. La persona titular de la Dirección General de Tecnologías de la Información de la Secretaría de Salud, de conformidad con el artículo 77 del Acuerdo.

Seguridad de la información: Capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma

Sistemas de Información. Conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

TIC. Tecnologías de la Información y Comunicación.

UA/OAD: Unidades Administrativas y Órganos Administrativos Desconcentrados de la Secretaría de Salud.

Usuario Final: El servidor público de la Secretaría de Salud que consume o utiliza los bienes o servicios TIC.

IV. OBJETIVO

Las presentes políticas de seguridad de la información dan cumplimiento al Marco de Gestión de Seguridad de la Información (MGSI) de la Institución previsto en el "**Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información, en la Administración Pública Federal**", y está orientada a garantizar certidumbre en la continuidad de la operación y la permanencia e integridad de la información institucional, así como a los servicios y procesos descritos en las presentes Políticas y su aplicación dentro de la Secretaría de Salud.

Las presentes Políticas tienen por objeto establecer los criterios institucionales en materia de seguridad de la información aplicables a los servicios y procesos que gestiona y administra la DGTI, para la protección y el uso correcto de los recursos tecnológicos y de la información que en ellos se almacena y para aplicar las medidas que permitan mantener la confidencialidad, integridad y disponibilidad de la Información.

Las presentes Políticas son de observancia general y obligatoria para las Unidades Administrativa y Órganos Administrativos Desconcentrados de la Secretaría de Salud y los servidores públicos adscritos a las mismas, como usuarios de los servicios y procesos que gestiona y administra la DGTI.

V. RESPONSABILIDADES

Para el cumplimiento de las presentes Políticas de Seguridad, procesos y servicios por cada una de las áreas de la DGTI.

No.	Responsable	Responsabilidad
	Responsable de la Seguridad a la Información	Dar seguimiento a la conformación del MGS, así como a su implementación y al cumplimiento de los controles mínimos de seguridad. Presentar al Titular de la UAF y al Titular de la Secretaría, un informe sobre la integración del MGSI. Dar aviso inmediato a la CEDN sobre los incidentes de seguridad de la información que se presenten. Asegurar el cumplimiento del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos. Implementar un programa de evaluaciones, que contemple al menos, una evaluación trimestral del MGSI para verificar el desempeño de los controles de seguridad y determinar acciones de mejora; Hacer del conocimiento del Órgano Interno de Control en la Secretaría, las irregularidades u omisiones en cumplimiento del MGSI, o delitos relacionados con la seguridad de la información en que incurran las personas servidoras públicas, y en su caso los proveedores y su personal, obligados a su observancia Mantener un proceso de mejora continua del MGSI para cumplir con las disposiciones aplicables.

	Dirección de Área 2 (Dirección de Seguridad a la Información)	Promover, aplicar y cumplir lo señalado en este documento. Proponer cambios en el ámbito de sus responsabilidades para su mejora y/o actualización. Elaborar propuestas de modificaciones y mejora a las presentes políticas. Coordinar la revisión y actualización del presente documento.
	Dirección de Red y Telecomunicaciones:	Promover, aplicar y cumplir lo señalado en este documento. Proponer cambios en el ámbito de sus responsabilidades para su mejora y/o actualización. Garantizar la seguridad de la información en: - Equipo de Cómputo - Red local e Internet - Servicio de Seguridad Perimetral - Seguridad de voz por IP
	Dirección de Área 1 (Dirección de Sistemas e Infraestructura)	Promover, aplicar y cumplir lo señalado en este documento. Proponer cambios en el ámbito de sus responsabilidades para su mejora y/o actualización. Garantizar la seguridad de la información en: - Servicios de Centro de Datos. - Correo Electrónico Institucional. - Gestión Documental. - Servicio de Videoconferencias. - Portales y páginas alojadas en la infraestructura de la Secretaría.
	Subdirección de Control de Gestión	- Apoyar a las áreas técnicas de la DGTI para la aplicación y observancia de las presentes Políticas. - Coadyuvar en la revisión de las presentes Políticas para su mejora y/o actualización, en apego a las disposiciones normativas aplicables.

VI. INSTANCIA DE AUTORIZACIÓN

Las presentes Políticas son autorizadas por el Responsable de la Seguridad de la Información quien da conocimiento al Grupo de Trabajo, el cual tiene las siguientes funciones:

1. Definir, implementar y evaluar el MGSI-SSA.
2. Revisar y proponer al Responsable de la Seguridad de la Información, para su consideración y posterior aprobación, las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información que fuera convenientes y apropiadas para la Secretaría de Salud.
3. Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la Secretaría de Salud, frente a posibles amenazas, sean internas o externas.
4. Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de la Secretaría de Salud.
5. Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada unidad administrativa u órgano administrativo desconcentrado de la Secretaría de Salud, así como acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información
6. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de la Secretaría de Salud, sean preexistente o nuevos.
7. Promover la difusión y apoyo a la seguridad de la información dentro de la Secretaría de Salud, como así, coordinar el proceso de administración de la continuidad de las actividades.

VII. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las presentes policías de seguridad de la información, tiene como prioridad:

a) Proteger los recursos de información de la Secretaría de Salud y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

b) Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos, procesos y áreas.

c) Mantener la Política de Seguridad de la Información, actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

1. Seguridad física y ambiental

Propósito: Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la Secretaría de Salud.

Alcance: Infraestructura tecnológica que gestiona y administra la DGTI.

a) Proteger el equipamiento de procesamiento de información crítica de la Secretaría de Salud, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

b) Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la Secretaría de Salud.

c) Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco de sus labores habituales.

d) Proporcionar protección acorde a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la Secretaría, instalaciones, equipamiento, cableado, medios de almacenamiento, etc.

El Responsable de la Seguridad de la Información definirá junto con el Enlace Informático y los Propietarios de Información de cada una de las UA/OAD, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos. El Responsable de la Seguridad de la Información dará seguimiento a su implementación.

Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente.

El Enlace Informático asistirá al Enlace de Seguridad de la Información en la definición de las medidas de seguridad a implementar en áreas protegidas, y dará seguimiento a su implementación. Asimismo, coordinará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de la DGTI, tanto dentro como fuera de las instalaciones de la Secretaría.

El Enlace de Seguridad de la Información definirá los niveles de acceso físico del personal a las áreas restringidas.

En caso de que se requiera que la información salga de la red institucional o se acceda a ésta desde puntos externos a dicha red, el Propietario de la Información deberá autorizar formalmente dichos accesos y extracción de la información siendo explícito en las restricciones correspondientes. Tanto los requerimientos como las autorizaciones o restricciones deberán ser comunicadas por el Enlace Informático correspondiente al Enlace de Seguridad de la Información, a fin de que éste último las valide o ratifique según lo considere.

Todo el personal de la Secretaría es responsable del cumplimiento en el manejo de la imagen institucional en los equipos de cómputo que operen en las institucionales (fondos

de pantallas institucionales) y no facilitar el acceso a información sensible tanto en los equipos informáticos como en los espacios físicos de trabajo (acciones conocidas como "escritorio limpio"), para la protección de la información relativa al trabajo diario en las oficinas.

a) **Controles de acceso físico.** Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados en conjunto por el Enlace de Seguridad de la Información y el Coordinador Administrativo de cada Unidad Administrativa u Órgano Administrativo Desconcentrado, a fin de permitir el acceso sólo al personal autorizado.

b) **Protección de Oficinas, Recintos e Instalaciones.** Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, esta tarea, estará a cargo de cada responsable de la Unidad Administrativa u Órgano Administrativo Desconcentrado.

c) Suministro de Energía. El equipamiento (equipo de cómputo, cableado, almacenamientos, etc.) estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

d) Seguridad del Cableado. El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe estar protegido contra intercepción o daño, la DGTI establecerá los estándares y requerimientos mínimos de seguridad para este rubro.

2. Uso de Equipo de Cómputo

Propósito: Definir el uso adecuado de los equipos de cómputo.

Alcance: A cada usuario se les asigna un equipo de cómputo con características específicas acorde a las necesidades que el Enlace Informático reporta como mínimas para desempeñar sus funciones.

a) Toda la información que se almacene en cualquier equipo de cómputo institucional, o bien se procese en éste, así como el resultado que se obtenga, se considera información institucional.

b) Ante cualquier falla que presente el equipo de cómputo o periférico o bien cualquier nueva necesidad relacionada, el usuario final de cada Unidad Administrativa u Órgano Administrativo Desconcentrado, notificará al Enlace Informático para que

éste a su vez informe esta necesidad a la Dirección de Red y Telecomunicaciones, a través de los mecanismos establecidos por la DGTI.

c) Con la finalidad de evitar o mitigar interrupciones o fallas en los equipos, se deberán realizar mantenimientos preventivos periódicos a fin de garantizar el óptimo funcionamiento de éstos.

   Para el caso de intervenciones correctivas se deberá proceder de acuerdo al inciso a).

d) El uso de dispositivos de almacenamiento externo como: Memorias USB, Teléfonos Celulares, Discos Duros, etcétera, son responsabilidad exclusiva de la Unidad Administrativa u Órgano Administrativo Desconcentrado, por lo que el usuario final que recurra a estos dispositivos deberá contar con autorización expresa de su Unidad Administrativa u Órgano Administrativo Desconcentrado. En caso de que use estos dispositivos sin la autorización mencionada y la información involucrada lo amerite de acuerdo a los criterios de la Unidad Administrativa u Órgano Administrativo Desconcentrado, ésta(éste) actuará conforme a la Ley General de Responsabilidades Administrativas.

e) Es responsabilidad de cada Enlace Informático, mantener actualizado y vigente el inventario de equipo de cómputo y periféricos asignados a su Unidad Administrativa u Órgano Administrativo Desconcentrado, así como los resguardos correspondientes.

   En caso de que exista algún movimiento o reasignación, se deberá generar el resguardo correspondiente y dicha actualización se le hará llegar a la Dirección de Red y Telecomunicaciones, dentro de los primeros cinco días hábiles a partir del movimiento correspondiente.

f) Es responsabilidad del usuario final la información que se almacena en el equipo de cómputo, y podrá solicitar apoyo del Enlace Informático de su unidad, para el respaldo de información cuando se realice algún cambio de equipo o reparación del mismo.

g) En caso de llevarse a cabo un procedimiento de borrado seguro de la información de cualquier equipo de cómputo institucional, éste deberá contar con el visto bueno del jefe inmediato o Titular de Unidad Administrativa u Órgano Administrativo Desconcentrado.

h) La contraseña del equipo de cómputo es asignada al usuario final a la entrega del mismo, está vinculada al listado de usuarios institucionales, y es su responsabilidad su uso; el usuario final deberá actualizar dicha contraseña periódicamente, a través del portal del correo electrónico (https://owa.salud.gob.mx). En caso de requerir una recuperación de contraseña deberá ser a través de su Enlace Informático, conforme al proceso que establezca la DGTI.

i) Si el usuario final del equipo de cómputo requiere la instalación de algún software que no esté previamente instalado en su equipo, deberá notificar a su Enlace

Informático para que a su vez se informe a la Dirección de Red y Telecomunicaciones, para su autorización.

j) El usuario final no podrá hacer modificaciones a nivel de sistema operativo del equipo de cómputo institucional.

k) Queda prohibido instalar y distribuir a través de los equipos de cómputo, programas maliciosos, por ejemplo, virus, troyanos, malware, etc.

l) Queda prohibido el almacenamiento, procesamiento o uso del equipo de cómputo asignado, para actividades de índole personal, así como almacenar información (archivos de datos, imágenes, videos, audios o en cualquier otro formato) que se pueda considerar hostil u ofensiva.

m) Queda prohibido deshabilitar o desinstalar herramientas de monitoreo, software antivirus, corta fuegos del sistema operativo (firewall), así como cualquier otro elemento de seguridad que el equipo requiera para su correcta administración y seguridad.

3. Red Local e Internet

Propósito: Establecer la condiciones y responsabilidades para el uso de la red local e internet.

Alcance: En la Secretaría de Salud, en sus UA/OAD, que están conectas a la red local (LAN) y que a su vez tiene acceso al servicio de Internet (WAN), se establecen las condiciones para el uso correcto de los estos servicios.

a) Corresponde a la DGTI, a través del Administrador del Servicio de red local e internet, el monitoreo de ambos servicios en aras de la correcta operación y garantizar la disponibilidad del servicio.

b) La DGTI podrá bloquear o limitar el acceso a sitios o páginas que se consideren de riesgo la seguridad de la información de la Secretaría de Salud, así como bloquear el acceso a los equipos de cómputo en los que se detecte tráfico de datos de manera inusual.

c) La DGTI por seguridad, podrá restringir accesos a determinados segmentos de red local.

d) El usuario final tendrá acceso a los servicios de red local e internet conforme al perfil que se les asigne, con características de acceso, privilegios y restricciones específicas sobre la red local y el servicio de internet con acceso controlado a Internet, que no representen riesgo a los equipos y sistemas informáticos, la productividad y/o disponibilidad de la red.

e) Es responsabilidad del usuario final reportar cualquier situación respecto a la baja calidad de los servicios de red local e internet, dicho reporte se hará a través del Enlace Informático de su Unidad Administrativa u Órgano Administrativo Desconcentrado, quien a su vez informará al Administrador del Servicio en la DGTI.

f) El usuario final podrá hacer uso de sus cuentas personales externas de correo electrónico (Outlook, Gmail, Yahoo, etc.). El intercambio de información que se realice a través de estas cuentas desde los equipos institucionales, será responsabilidad exclusiva del usuario final.

g) El intercambio de información que se realice a través de mensajería instantánea, tanto en la red local o internet, desde los equipos institucionales, será responsabilidad exclusiva del usuario final.

h) Para los casos en que los usuarios finales requieran el acceso a sitios o páginas de Internet, que se encuentren bloqueadas, el Titular de la Unidad Administrativa será el responsable de hacer la solicitud por escrito al Administrador del Servicio de la DGTI, justificando los motivos por los cuales requiere dicho acceso.

i) Es responsabilidad del usuario final el acceso a sitios o páginas en las que se les solicite un registro, así como el compartir contraseñas y datos personales; asimismo, queda bajo su responsabilidad el acceso a portales de bancos, servicios financieros, de paquetería, etc. La DGTI no realizará procesos de recuperación de datos o trazabilidad de eventos relacionados.

j) Queda restringido el uso de herramientas de gestión remota en todos los equipos de cómputo. En casos extraordinarios el Enlace Informático, con el visto bueno del Coordinador Administrativo solicitará a la Dirección de Red y Telecomunicaciones el servicio correspondiente, para su análisis previo y en su caso autorización.

k) A consideración de la DGTI, queda restringida la ejecución de herramientas de monitoreo de red que implique la intersección, manipulación o alteración de datos, así como monitoreo de puertos o de vulnerabilidades informáticas al interior de la red de la Secretaría de Salud.

l) A consideración de la DGTI, queda restringido usar cualquier tipo de programa, comandos o enviar mensajes de cualquier tipo, con la intensión de interferir, deshabilitar los equipos de cómputo o comunicaciones, a través de la red local o internet.

m) El Enlace Informático, con el visto bueno del Coordinador Administrativo, deberá reportar al Administrador del Servicio, el uso de trasferencia de información utilizando mecanismo de autentificación y protocolos de cifrado o seguros como FTPs, HTTPs, SSL o TLS.

4. Servicio de Seguridad perimetral

Propósito: Establecer servicios que evalúan y actúan sobre la continuidad y calidad de entrega de los servicios de la tecnología tales como el monitoreo, seguridad y atención y respuesta a incidentes.

Alcance: Garantizar la seguridad de la información para la Secretaría de Salud en todas sus plataformas tecnológicas, mismo que coadyuven a la continuidad operativa y protección de la información de los ciudadanos y la entidad. Así como contar con las capacidades de respuesta humana e insumos para el soporte y mantenimiento de las plataformas de comunicaciones y seguridad de la información con las que cuente la La Secretaría de Salud.

a) La DGTI por seguridad, podrá restringir, bloquear o limitar accesos a determinadas Direcciones Ip o Mac Adrees que vulnere la seguridad de la información de la Secretaria de Salud.

b) El usuario final a través del Enlace Informático y con el visto bueno del Coordinador Administrativo, solicitará al Administrador del servicio, permisos específicos de navegación en función de sus actividades.

c) Es responsabilidad del usuario final reportar anomalías respecto a los permisos de navegación, a través del Enlace Informático de su Unidad Administrativa u Órgano Administrativo Desconcentrado, a fin de que éste último reporte al Administrador del Servicio.

5. Seguridad de voz por IP

Propósito: Establecer los lineamientos de seguridad para el uso de equipos de telefonía IP, a fin de proporcionar a las UA/OAD las herramientas tecnológicas en materia de telefonía IP que permitan la interconexión para los servicios de voz y datos, bajo el protocolo IP.

Alcance: Usuarios finales de las UA/OAD a los que se les asignan equipos de telefonía IP para desempeñar sus funciones.

a) La DGTI podrá restringir, bloquear o limitar accesos a determinadas marcaciones que vulneren la red de la Secretaría de Salud.

b) El usuario final a través del Enlace Informático y con el visto bueno del Coordinador Administrativo, solicitará al Administrador del servicio. permisos específicos de marcado en función de sus actividades.

c) Es responsabilidad del usuario final reportar anomalías respecto a los permisos específicos de marcado, a través del Enlace Informático de su Unicad Administrativa u Órgano Administrativo Desconcentrado, a fin de que éste último reporte al Administrador del Servicio.

6. Implementación del Centro de Datos

Propósito: Definir los requisitos mínimos necesarios de seguridad, para la implementación del Centro de Datos para la Secretaría de Salud, a través de un prestador de servicio.

Alcance: El Centro de Datos con el que cuenta la Secretaría de Salud es a través de la contratación de un servicio integral que es proveído por un tercero, quien deberá cumplir con los requerimientos mínimos de seguridad.

a) El centro de datos deberá estar ubicado en región geológica zona A (bajo), B o C (moderado) de peligro sísmico de acuerdo con la clasificación de regionalización sísmica publicada por el CENAPRED.

b) La ubicación del centro de datos deberá estar definida dentro del territorio nacional.

c) El prestador del Servicio, deberá ser dueño del centro de datos propuesto.

d) El espacio designado para el servicio del Centro de Datos deberá ser exclusivo para la Secretaría de Salud y confinado en modalidad de Jaula Privada.

e) Deberá contar con gabinetes o racks que almacenen el equipo designado, éstos deberán contar con cerradura electrónica controlada de manera remota.

f) Deberá contar con personal de vigilancia con cobertura 7x24x365 que registre todo acceso a las instalaciones administrativas y en especial, los accesos al área asignada a la Secretaría de Salud en el Centro de Datos.

g) El centro de datos, previsto para el servicio, deberá contar como mínimo las siguientes certificaciones, con las cuales se acreditará que cuenta con todos los elementos de seguridad:
   - Uptime Institute TIER III o ICREA IV o superior
   - ISO 27001:2013 Seguridad de la Información
   - ISO/IEC 20000-1:2011 Gestión de Servicios de TI
   - ISO 9001:2015 Gestión de Calidad
   - ISO 22301:2012 Gestión de Continuidad de Negocio

h) Los accesos físicos a la Jaula Privada donde se aloje el servicio integral de Centro de Datos para la Secretaría de Salud, así como todas las acciones que se realicen dentro del mismo, serán autorizados por la DGTI y deberán estar registrados en bitácoras, tanto por ésta como por el prestador del servicio. Las bitácoras serán cotejadas por lo menos una vez al mes.

i) La DGTI verificará en todo momento el cumplimiento y observancia de las políticas señaladas en este apartado.

7. Servicios de Centro de Datos

Propósito: Establecer las condiciones adecuadas para el uso y aprovechamiento de los recursos del Centro de Datos.

Alcance: Servicios de cómputo centralizado para el alojamiento de sistemas de propósito específico, almacenamiento y procesamiento de información, los cuales se prestan a través de máquinas virtuales (servidores) y carpetas o directorios compartidos.

Responsabilidades y restricciones:

a) Corresponde a la DGTI, a través del Administrador del Servicio de Centro de Datos, la gestión, monitoreo y control de los recursos, así como establecer los lineamientos para su correcta operación.

b) El requerimiento de una máquina virtual deberá ser solicitado por el Titular o el Coordinador Administrativo de la UA/OAD, a través del formato denominado **Formato de Solicitud Alta de Máquina Virtual** que que se integra en este documento como **APÉNDICE "A"**.

c) Las credenciales de acceso serán proporcionadas únicamente al administrador de la máquina virtual que se especifique en el formato de solicitud de la UA/OAD y éste será el responsable de su correcto uso.

d) La DGTI es responsable del respaldo de las máquinas virtuales alojadas en el Centro de Datos, conforme a las políticas de respaldo establecidas

e) La UA/OAD podrá solicitar la restauración del respaldo de una máquina virtual o la de una versión previa, en función de las políticas de respaldo.

f) Toda la información en aplicativos, sistemas, bases de datos, repositorios, directorios, es responsabilidad de la UA/OAD, a través del administrador de la máquina virtual.

g) Cualquier cambio requerido en sus características, recursos y capacidades deberá ser solicitado por el administrador de la máquina virtual vía correo electrónico al Administrador del Servicio de la DGTI del Centro de Datos, quien autorizará dichos cambios.

h) La navegación a internet, desde la máquina virtual, quedará restringida a un perfil de accesos mínimos por lo que cualquier requerimiento de navegación deberá ser solicitado al Administrador del Servicio justificando la necesidad, ésta será evaluada y, en consideración de las medidas de seguridad, se autorizará.

i) Queda prohibido utilizar una máquina virtual como proxy o conducto de navegación hacia internet que no corresponda al propósito de los servicios que se alojan en dicha máquina virtual.

j) El acceso a la máquina virtual, para su administración será a través de la Red Local de la Secretaría de Salud y, previa justificación podrá acceder vía VPN, desde una red externa, siguiendo las políticas de seguridad para el uso de VPN's.

8. Uso de cuentas VPN's

Propósito: Definir el uso adecuado de las VPN (Red Privada Virtual).

Alcance: A los usuarios finales se les asigna una cuenta VPN (usuario y contraseña), las cuales les va a permitir mantener una conexión directa a la red local de la Secretaría de Salud o en su Centro de Datos, según el propósito.

a) La cuenta VPN para acceso a la red local será asignada únicamente a las personas servidoras públicas de la Secretaría, que justifiquen la necesidad de conexión a la red local. Dicha solicitud deberá realizarse al Administrador del Servicio de la Red Local, por parte del Coordinador Administrativo o el Titular de la Unidad Administrativa u Órgano Administrativo Desconcentrado.

b) La cuenta VPN para acceso a servidores del Centro de Datos será asignada únicamente a las personas servidoras públicas de la Secretaría, que sean administradores del o los servidores a los que desean acceder. Dicha solicitud deberá realizarse al Administrador del Servicio de Centro de Datos, por parte del Coordinador Administrativo o el Titular de la Unidad Administrativa u Órgano Administrativo Desconcentrado.

c) Cualquier cuenta VPN tendrá una vigencia de máximo 30 días y en caso de requerirse otro periodo tendrá que solicitarse nuevamente una vez que concluya el plazo indicado.

d) Toda solicitud solicitud de VPN (ya sea para Red Local o Servidores), deberá indicar si el acceso estará restringido a una IP específica de origen, a credenciales de acceso específicas y a un periodo de inactividad determinado, siempre y cuando éste último no exceda lo indicado en el inciso anterior.

e) En cualquier momento la DGTI podrá restringir el uso de las cuentas VPN's, cuando detecte alguna anomalía en su uso o se vulnere la seguridad de la infraestructura de cómputo y comunicaciones de la Secretaría.

f) El usuario final es responsable del uso de la cuenta VPN, en caso de que se le dé un uso diferente al solicitado, la DGTI cancelará permanentemente la cuenta y notificará al Coordinador Administrativo al respecto.

9. Correo electrónico

Propósito: Establecer las condiciones para el uso adecuado del correo Institucional de la Secretaría de Salud.

Alcance: A los usuarios finales se les asigna una cuenta de correo institucional con características específicas para el envío y recepción de mensajes de correo electrónico de manera local y externo.

a) La DGTI implementará los controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, considerando:

- La vulnerabilidad de los mensajes, el acceso o modificación no autorizados, o a la negación de servicio.
- La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
- La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
- Lo que de acuerdo al RISS faculta a la DGTI para contar con prueba de origen, envío, entrega y aceptación.
- Las implicaciones de la publicación externa de listados de personal, accesibles al público.
- El acceso de usuarios remotos a las cuentas de correo electrónico.
- El uso inadecuado por parte del personal.

b) El uso del correo electrónico institucional debe observar las conductas éticas y profesionales constituidas por la Secretaría de Salud.

c) El Coordinador Administrativo o el Titular de la Unidad Administrativa u Órgano Administrativo Desconcentrado designará a sus Enlaces para gestión de los servicios de Correo Electrónico.

d) Los Enlaces para Correo Electrónico de cada una de las UA/OAD son los facultados para solicitar el Alta, Cambio o Baja de cuentas de correo institucionales, para lo cual deberá requisitarse el formato denominado **Formato de Servicio de Correo Electrónico y Directorio Activo** que se anexa a las presentes Políticas como **APÉNDICE "B"**, éste formato deberá enviarse a través del ticket de la mesa de ayudad de la DGTI para su atención.

e) La cuenta de correo electrónico es personal e intransferible. El usuario final se compromete a hacer un uso responsable de la cuenta y a mantener su contraseña en secreto. Asimismo, el usuario final se compromete a notificar al Enlace para Correo Electrónico de manera inmediata la pérdida de su contraseña o el acceso no

autorizado por parte de terceros a su cuenta, quien a su vez notificará al Administrador del Servicio de Correo Electrónico Institucional.

f) Los usuarios finales en primera instancia, deberán identificar correos que consideren sospechosos, que pudieran representar situaciones de posible fraude, con contenido o aspecto distinto a lo habitual (logotipo, pie de firma, correo sustituto, etc.), el mensaje contiene una llamada a la acción (urge, invita o solicita, hacer algo no habitual, da clic en la siguiente liga, actualiza tu contraseña), en este caso se deberá notificar a su Enlace para Correo Electrónico quien a su vez notificará al Administrador del Servicio de Correo Electrónico Institucional.

g) No podrán enviarse mensajes cuyo contenido sea nocivo o que atente contra las buenas costumbres, la moral y las leyes de derecho de autor (pornografía, obscenos, raciales, juegos, chistes, videos, audios, etc.), así como cualquier otro que no tenga relación con las actividades laborales encomendadas al usuario final.

h) La DGTI cuidará la disponibilidad y continuidad del servicio en general, por lo que en casos particulares en los que se requiera la revisión de una cuenta de correo electrónico en específico, el Enlace para Correo Electrónico de la UA/OAD deberá solicitarlo por oficio al Administrador del Servicio de Correo Electrónico Institucional.

i) Por razones de seguridad del servicio, la DGTI podrá limitar total o parcialmente el acceso a la cuenta de correo de usuarios específicos, así como cancelar, suspender bloquear, respaldar o eliminar cuentas, si tuviese conocimiento efectivo de que la actividad o la información almacenada es ilícita o lesiona bienes o derechos.

j) Es responsabilidad del usuario final realizar respaldos locales (.pst) periódicos de sus mensajes, carpetas de correo y agenda de direcciones electrónicas y mantenerlas bajo su resguardo, y en caso de que así lo requiera el usuario final, el Enlace para C Correo Electrónico apoyará a éste en la realización de su archivo de respaldo.

k) Los usuarios finales de las cuentas de correo electrónico no podrán usar y fomentar las denominadas cadenas, sin importar que tan plausible parezca su propósito.

l) Los usuarios finales no podrán utilizar este servicio de comunicación electrónica para insultar, agredir, intimidar, acosar o interferir en sus funciones a los demás usuarios del servicio.

m) Los usuarios finales deberán borrar, sin abrir, todos los correos electrónicos que procedan de cuentas de correo que les sean desconocidas o cuyo "asunto" pueda relacionarse con publicidad o virus (SPAM).

10. Portales y páginas alojadas en la infraestructura de la Secretaría

Propósito: Proporcionar información para la definición de las reglas y normas de seguridad, para la protección en los sitios web del dominio salud.gob.mx.

Alcance: Administradores encargados de mantener los contenidos de los portales y páginas web de las UA/OAD.

a) Corresponde a la DGTI crear el sitio web con base en las plantillas autorizadas por Comunicación Social y entregar, para su resguardo, a los administradores encargados de mantener los contenidos, las credenciales de acceso a la plataforma de administración de contenidos (CMS).

b) El Coordinador Administrativo o el Titular de la Unidad Administrativa u Órgano Administrativo Desconcentrado designará a los administradores encargados de mantener los contenidos de sus sitios web.

c) Es responsabilidad del usuario administrador del sitio web designado por la Unidad Administrativa u Órgano Administrativo Desconcentrado, hacer uso correcto de las credenciales de acceso, así como de su actualización periódica.

d) Es responsabilidad del usuario administrador del sitio web, el contenido del mismo, así como obtener las autorizaciones y validaciones por parte de área de Comunicación Social sobre cualquier variante de su plantilla, imágenes y texto que ahí se publique.

e) Corresponde a la DGTI ejecutar las actividades que mitiguen cualquier riesgo en materia de ciberseguridad como "actividades que atentan contra la integridad, la disponibilidad y la confidencialidad de los portales y sitios web de la Secretaría de Salud", a fin de establecer estrategias para limitar o contener el impacto de un eventual ataque cibernético.

11. Desarrollo de software

Propósito: Garantizar la seguridad en los nuevos desarrollos de software que se realicen en la Secretaría de Salud, así como en los existentes, en cualquiera de las UA u OAD.

Alcance: Implementación de mecanismos de seguridad para salvaguardar los datos que se procesan, almacenan y se generan en nuevos desarrollos de software, o en su caso del mantenimiento o adecuaciones a software ya existente en la Secretaría de Salud.

a) Contar con ambientes de desarrollo, pruebas y producción, éstos deben ser independientes. Estos ambientes deben ser equivalentes y con los mismos controles de seguridad, a efectos de prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores en el ambiente de pruebas y producción.

b) Los desarrolladores deben realizar su trabajo exclusivamente en ambiente de desarrollo y una vez probados, integrarlos en el ambiente de pruebas o en el de producción.

c) Los nombres de dominio para los ambientes de desarrollo, pruebas y producción deben ser diferentes a efecto de evitar confusión durante la ejecución.

d) Las UA y OAD que desarrollen software son responsables de la administración de las bases de datos, en sus diferentes ambientes, así como únicos responsables de la gestión de cuentas de usuarios y administrativas, así como de la operación de la aplicación.

e) Incluir réplicas de todos los componentes con los cuales el software tendrá interoperación en producción incluyendo: otras aplicaciones cliente servidor, bases de datos relacionales y no relacionales, componentes middleware, interfaces, demonios (daemons), procesos personalizados, utilidades FTP y otros.

f) Se deberán implementar protocolos seguros, a través de certificados de seguridad (SSL), para todos los proyectos que se publiquen por la web (https)

g) Para todo nuevo desarrollo de software que implemente envió de correo electrónico, deberá notificar a la DGTI, para que se identifique el servidor desde el cual se envían, para garantizar que la cuenta o los correos no sean bloqueados por el antispam, además de proporcionar las credenciales correspondientes.

h) Los estándares o arquitecturas de seguridad que se implementen en los nuevos desarrollos deberán ser documentados por parte de la UA o OAD, a fin de contar con la base de conocimiento e identificar posibles riesgos, tales como.

- Guías de hardening para aplicaciones en producción en los siguientes niveles:
  - Sistema operativo
  - Servidor de aplicaciones
  - Servidor web
  - Bases de datos

- Seguridad del acceso de las aplicaciones hacia:
  - Bases de datos
  - Sistemas de archivos
  - Administración de herramientas y servidores de despliegue
  - Las contraseñas deben estar encriptadas en base de dato

- Todos los accesos deben ser mediante las credenciales definidas explícitamente, no abiertos o con las credenciales por default de la herramienta.

- Tomar como referencia el top 10 de riesgos de seguridad más críticos para las aplicaciones web (https://owasp.org):

- Tuning de performance de:
  - Aplicación
  - Servidor de aplicaciones
  - Servidor web
  - Base de datos
  - Sistema operativo

- Bitácora de:
  - Accesos
  - Operaciones a nivel aplicación

- Registro y monitoreo de los logs de:
  - Aplicación (garantizar que la aplicación registre fallas, alarmas, accesos no autorizados, etc., en el log correspondiente)
  - Servidor de aplicaciones
  - Servidor web
  - Base de datos

i) Todos los nuevos desarrollos, previo a su salida a producción, deberán contar con pruebas de seguridad, vulnerabilidad y estrés, una vez que se alojen en el Centro de Datos.

j) A fin de reforzar los mecanismos y controles para garantizar que los datos e información contenida en los sistemas, plataformas, aplicativos y bases de datos utilizados, sean exactos, completos, pertinentes, actualizados y correctos, con la finalidad de que no se altere la veracidad e integridad de la información y así mitigar los riesgos que pudieran afectar las operaciones, las UA/OAD deberán instrumentar lo siguiente:

- Revisar periódicamente la base de datos para validar la información, de acuerdo al proceso que automatiza, mediante datos de control, catálogos y reportes de validación.
- Establecer alertas de calidad, a nivel de base de datos, para identificar potenciales problemas.
- Establecer protocolos para descubrir e identificar posibles desviaciones.
- Establecer controles de acceso al servidor de bases de datos, mediante revisión de logs de auditoria del motor de base de datos.
- Establecer controles para asegurar que no sea alterada por ingresos no autorizados.
- Instalar herramientas de monitoreo.
- Realizar regularmente revisiones y actualizaciones al motor de base de datos.

k) Para nuevos desarrollos de software las UA/OAD, deberán verificar el cumplimiento de la normatividad que resulte aplicable en cada caso en particular.

l) Para la gestión y validación de usuarios y contraseñas de los sistemas y bases de datos, así como los aspectos de identificación y documentación requerida para la operación y funcionamiento de las bases de datos, las UA/OAD dueños de dichos sistemas o bases de datos, deberán remitir a la DGTI debidamente requisitado, el formato denominado "**Formato de información de identificación y documentación para operación de la base de datos**", que se integra en este documento como **APÉNDICE "C"**, para solicitar el acceso correspondiente.

12. Protección de datos personales

Propósito: Cumplir con las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Alcance: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

a) Todo dato personal debe ser tratado como confidencial de conformidad con las disposiciones legales y normativas aplicables en materia de protección de datos personales, y se deberá cumplir con lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

b) Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, corresponderá a cada UA/OAD, en su ámbito de competencia, establecer mecanismos que garanticen de manera particular la confidencialidad de los datos personales, en las actividades que realicen con motivo de sus propias funciones.

13. Respaldo y borrado seguro de información.

Propósito: Validar que, al retirar los servidores del Centro de Datos y Equipo de Cómputo Personal, éstos no lleven registro de algún dato que pueda ser recuperado a fin de garantizar la seguridad de la información.

Alcance: Garantizar el borrado seguro de los datos que se resguardan en medios de almacenamiento, cuando los dispositivos se reemplacen o cambien por situaciones de mantenimiento, sustitución o retiro.

a) En caso de llevarse a cabo un procedimiento de borrado seguro de la información de cualquier Servidor del Centro de Datos, Equipo de Cómputo Personal y demás equipos que interfieran en las actividades de la Secretaría, éste deberá contar con el visto bueno del jefe inmediato o Titular de Unidad Administrativa u Órgano Administrativo Desconcentrado.

b) Los respaldos de datos en el Centro de Datos serán administrados y gestionados por la DGTI.

c) Los respaldos de datos se deberán realizar con base a las políticas de Respaldos de Servidores que sean diseñadas e implementadas por la DGTI.

d) Las políticas de respaldos de los Servidores del Centro de Datos deberán contener de manera clara y precisa la periodicidad de ejecución, así como los tiempos específicos de retención, y se darán a conocer a las UA y OAD que tienen servicios tecnológicos en el Centro de Datos.

e) Se deberá establecer un lugar seguro para la ubicación de las cintas de respaldos, tanto de las cintas en tránsito (productivas) como las históricas.

f) Para el retiro de alguna unidad de almacenamiento o resguardo del Centro de Datos, se deberá realizar un proceso de borrado seguro, garantizando que no es posible realizar un proceso de recuperación de información.

g) La DGTI será la responsable de establecer el procedimiento de borrado seguro en los Servidores del Centro de Datos, Equipo de Cómputo Personal y demás equipos que interfieran en las actividades de la Secretaría, estableciendo los parámetros y estándares mínimos requeridos.

h) Garantizar que todos los dispositivos de almacenamiento de Equipo de Cómputo Personal, sean borrados de forma segura al momento de ser retirados.

i) Las actividades de borrado de los dispositivos de almacenamiento de Equipo de Cómputo Personal, serán programadas y supervisadas por la DGTI con el apoyo de los Enlaces Informáticos.

VIII. CUMPLIMIENTO

El cumplimiento del presente documento tiene como finalidad:

a) Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a los servidores públicos que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

b) Garantizar que los sistemas de información, infraestructura tecnológica y resguardo de datos, cumplan con las políticas, normas y procedimientos de seguridad.

c) Revisar la seguridad de los sistemas de información, infraestructura tecnológica y resguardo de datos, periódicamente, a fin de garantizar la adecuada aplicación de las políticas, normas y procedimientos de seguridad.

d) Garantizar la existencia de controles que coadyuven al uso adecuado y protección de los bienes informáticos, así como el resguardo y seguridad de la información.

e) Las presentes Políticas de Seguridad de la Información podrán ser modificadas o actualizadas, según lo determine la DGTI.

IX. SANCIONES

Se sancionará administrativamente a todo aquel que viole lo dispuesto en las presentes Políticas de Seguridad, conforme a lo dispuesto por las normas estatutarias aplicables a la Secretaría de Salud, así como la Ley General de Responsabilidades Administrativas, sin perjuicio de las demás acciones legales y administrativas a que hubiere lugar para la Secretaría, en cada caso.

X. INTERPRETACIÓN

La interpretación de las presentes Políticas de la Seguridad de la Información de la Secretaría de Salud, para efectos administrativos, corresponderá a la Dirección General de Tecnologías de la Información.

XI. TRANSITORIOS.

ÚNICO. Las presentes Políticas entrarán en vigor al día hábil siguiente de su difusión en la página de la DGTI.

Las presentes Políticas se aprobaron el día 29 de junio de 2023.

César Vélez Andrade
Director General de Tecnologías de la Información

Gerardo Antonio Alipi Mena
Director de Red y Telecomunicaciones

Isaías Ortiz Castillo
Dirección de Sistemas e Infraestructura

Jesús Agustín Ibáñez Calvo
Dirección de Seguridad a la Información

Angélica Cortés Sánchez
Subdirectora de Control de Gestión

APÉNDICES

APÉNDICE "A"

Formato de Solicitud Alta de Máquina Virtual

Guía de Uso

- ***Tomar como referencia principal (no limitativa) de llenado del documento el texto en azul, el cual es una guía incluida en cada sección, eliminar dicho texto e incluir el contenido final del documento en color negro, incluyendo la eliminación de esta sección de guía de uso***
- *Si una sección no puede ser llenada debido a las características del proyecto, indicar* ***No Aplica***
- ***Conservar*** *el tipo de letra, así como para contenido de tablas, todo el texto en color negro*
- *Los datos del formato sombreados en gris, no los proporciona el usuario sino Ingeniería en Sitio dedicada a virtualización*

Fecha de Solicitud: *dd/mm/aaaa*

I. DATOS DEL USUARIO SOLICITANTE

Unidad Administrativa / Órgano Administrativo Desconcentrado	**Siglas**
<Anote la unidad administrativa u órgano administrativo desconcentrado al que pertenece el usuario solicitante>	*<Anote las siglas de la unidad administrativa u órgano administrativo desconcentrado al que pertenece el usuario solicitante>*
Nombre completo del responsable de la solicitud	**Cargo**
<Anote el nombre completo del usuario solicitante>	*<Anote el cargo del usuario solicitante>*
Teléfono interno (SSA) y extensión	**Correo electrónico institucional**
<Anote el teléfono interno (SSA) y extensión del usuario solicitante del servicio>	*<Anote el correo electrónico institucional del usuario solicitante>*

II. DATOS DEL ADMINISTRADOR DEL SISTEMA OPERATIVO DE LA MÁQUINA VIRTUAL

Unidad Administrativa / Órgano Administrativo Desconcentrado	**Siglas**
<Anote la unidad administrativa u órgano administrativo desconcentrado al que pertenece el usuario solicitante>	*<Anote las siglas de la unidad administrativa u órgano administrativo desconcentrado al que pertenece el usuario solicitante>*
Nombre completo del responsable de la solicitud	**Cargo**
<Anote el nombre completo del usuario solicitante>	*<Anote el cargo del usuario solicitante>*
Teléfono interno (SSA) y extensión	**Correo electrónico institucional**
<Anote el teléfono interno (SSA) y extensión del usuario solicitante del servicio>	*<Anote el correo electrónico institucional del usuario solicitante>*

III. ESPECIFICACIONES TÉCNICAS (Hw y Sw)

Número de vcpu's (cores)	**Memoria RAM (GB)**	**Arquitectura**
<Anote el número de vCPU's (cores) solicitados para la máquina virtual a ser creada>	*<Anote la memoria RAM solicitada para la máquina virtual a ser creada>*	*<Anote "x32" o "x64" según sea la arquitectura del sistema operativo que se instalará en la máquina virtual a ser creada>*
Sistema operativo		**Idioma**
<Anote el sistema operativo solicitado para la máquina virtual a ser creada, CentOS, Ubuntu, FEDORA, OpenSUSE, Mint, Debian>		*<Anote "Inglés" o "Español" para especificar el idioma del sistema operativo que se instalará en la máquina virtual a ser creada>*

Nota*: Los datos sombreados en gris son proporcionados por el Proveedor del Servicio.*

IV. PARA SISTEMA OPERATIVO LINUX o UNIX

Configuración por default (marcar opción): | X |

IV.1 Discos

Punto de Montaje	Almacenamiento (GB)	Sistema de archivo	Comentarios
<Anote el nombre del punto de montaje>	*<Anote el espacio en GB del disco 1>*	*<Anote el tipo de sistema de archivo1>*	*<Anote comentarios adicionales sobre la partición 1>*

IV.2. Particiones

Slice	Partición	Almacenamiento (MB)
<Anote el nombre del slice 1>	*<Anote el nombre de la partición 1>*	*<Anote el espacio en Mb de la partición 1>*
<Anote el nombre del slice 1>		

V. PARA SISTEMA OPERATIVO WINDOWS

Unidad	Almacenamiento (GB)	Etiqueta	Comentarios
<Anote el nombre la Unidad>	*<Anote el espacio en GB de la disco 1>*	*<Anote el tipo de sistema de archivo1>*	*<Anote comentarios adicionales sobre la partición 1>*
<Anote el nombre del punto de montaje>	*<Anote el espacio en GB de la disco n>*	*<Anote el tipo de sistema de archivo1>*	*<Anote comentarios adicionales sobre la partición n>*

VI. CLASIFICACIÓN DE LA MÁQUINA VIRTUAL

Ambiente de la Máquina Virtual	Criticidad	Uso de la Máquina Virtual
<Anote si la máquina virtual solicitada será para el ambiente de desarrollo, pruebas o producción>	*<Anote "Alta", "Media", "Baja" según sea la criticidad de la máquina virtual a ser creada>*	*<Anote si la máquina virtual será usada para aplicación local, aplicación Web, página Web, bases de datos, Web, correo electrónico, directorio activo u otro (especificar)>*

VII. MÁQUINAS VIRTUALES PARA APLICACIONES (LOCAL Y WEB) Y PÁGINAS WEB

Nombre de la aplicación	Acrónimo	Descripción detallada
<Anote el nombre de la aplicación 1 que se instalará en la máquina virtual a ser creada>	*<Anote el acrónimo de la aplicación 1>*	*<Anotar una descripción detallada y concisa del servicio o función de la aplicación 1>*

VIII. MÁQUINAS VIRTUALES PARA BASES DE DATOS

Nombre del RDBMS de la BD	Nombre de la BD	Descripción detallada
<Anote el nombre del sistema de gestión de bases de datos relacionales que instalará en la máquina virtual a ser creada, el cual puede ser SQL Server, MySQL o PostreSQL>	*<Anote el nombre de la base de datos 1>*	*<Anotar una descripción detallada y concisa del servicio o función de la base de datos 1>*

Control de Versiones

Versión	Fecha	Descripción	Autor	Revisó y Aprobó
1.0	20-Abril-2021	Creación del formato	Alejandro Saucedo Vidals	Isaías Ortiz Castillo

APÉNDICE "B"
Formato de Servicio de Correo Electrónico y Directorio Activo

Guía de Uso

- ***Tomar como referencia principal (no limitativa) de llenado del documento el texto en azul, el cual es una guía incluida en cada sección, eliminar dicho texto e incluir el contenido final del documento en color negro, incluyendo la eliminación de esta sección de guía de uso***
- *Si una sección no puede ser llenada debido a las características del proyecto, indicar* ***No Aplica***
- ***Conservar*** *el tipo de letra Montserrat 8, así como para contenido de tablas, todo el texto en color negro*
- *El formato se llena para solicitar uno y sólo uno de los servicios de correo electrónico*
- *Los campos marcados con asterisco (*) rojo son de carácter obligatorio*

Fecha de Solicitud: *dd/mm/aaaa*

DATOS DEL USUARIO SOLICITANTE

***Unidad Administrativa / Órgano Administrativo Desconcentrado**	***Siglas**
<Anote la unidad administrativa u órgano administrativo desconcentrado al que pertenece el usuario solicitante>	*<Anote las siglas de la unidad administrativa u órgano administrativo desconcentrado al que pertenece el usuario solicitante>*
***Nombre completo del responsable de la solicitud**	***Cargo**
<Anote el nombre completo del usuario solicitante>	*<Anote el cargo del usuario solicitante>*
***Teléfono interno (SSA) y extensión**	***Correo electrónico institucional**
<Anote el teléfono interno (SSA) y extensión del usuario solicitante del servicio>	*<Anote el correo electrónico institucional del usuario solicitante>*

*Tipo de Cuenta (Marcar una Opción con una **X**):	Institucional:	Servicio:

I. ALTA DE CUENTA DE CORREO ELECTRÓNICO

***Nombre del Usuario / Responsable**	***Domicilio Completo**	***Teléfono y/o Cisco**
<Anote el nombre del usuario al que pertenecerá la cuenta>	*<Anote el domicilio del usuario al que pertenecerá la cuenta>*	*<Anote el teléfono del usuario al que pertenecerá la cuenta>*
***Departamento**	***Cargo / Puesto**	***Clave - Unidad Administrativa**
<Anote el departamento del usuario al que pertenecerá la cuenta>	*<Anote el cargo o puesto que desempeña el usuario al que pertenecerá la cuenta >*	*<Anote la clave de la unidad administrativa del usuario al que pertenecerá la cuenta > - <Anote la unidad administrativa del usuario solicitante del servicio>*
CURP	**Numero De Empleado**	**Requerimiento Especial**
<Anote la CURP del usuario al que pertenecerá la cuenta ; Para uso interno y exclusivo de la secretaria de Salud>	*<Anote el número de empleado del usuario al que pertenecerá la cuenta: Para uso interno y exclusivo de la secretaria de Salud >*	*<Anote en caso de requerir algún requerimiento especial para esta cuenta>*

II. BAJA DE CUENTA DE CORREO

***Usuario De Cuenta De Correo**	***Cuenta De Correo Electrónico**
<Anote el nombre del usuario cuyo correo electrónico será dada de baja>	*<Anote la cuenta de correo electrónico que será dada de baja>*

III. ACTUALIZACIÓN DE DATOS

*Cuenta de Correo Electrónico	Nombre Del Usuario	Teléfono O Cisco
<Anote el correo electrónico del usuario a cambiar los datos>	*<Anote el nombre del usuario al que pertenecerá la cuenta>*	*<Anote el teléfono del usuario al que pertenecerá la cuenta>*
Domicilio Completo	**Cargo / Puesto**	**Clave - Unidad Administrativa**
<Anote el domicilio del usuario al que pertenecerá la cuenta>	*<Anote el cargo o puesto que desempeña el usuario al que pertenecerá la cuenta >*	*<Anote la clave de la unidad administrativa del usuario al que pertenecerá la cuenta > - <Anote la unidad administrativa del usuario solicitante del servicio>*
Departamento	**CURP**	**Numero De Empleado**
<Anote el departamento del usuario al que pertenecerá la cuenta>	*<Anote la CURP del usuario al que pertenecerá la cuenta ; Para uso interno y exclusivo de la secretaria de Salud>*	*<Anote el número de empleado del usuario al que pertenecerá la cuenta: Para uso interno y exclusivo de la secretaria de Salud >*

Control de Versiones

Versión	Fecha	Descripción	Autor	Revisó
1.0	20-Abril-2021	Creación del formato	Alejandro Saucedo Vidals	Isaias Ortiz Castillo

APÉNDICE "C"

SALUD SECRETARÍA DE SALUD	UNIDAD DE ADMINISTRACIÓN Y FINANZAS DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN	
FORMATO DE INFORMACIÓN DE IDENTIFICACIÓN Y DOCUMENTACIÓN PARA OPERACIÓN DE LA BASE DE DATOS		No. Formato. 01 Fecha de Formato 01/12/2022 Versión: 01

DATOS DE LA BASE DE DATOS			
Nombre de la Base de Datos:			
RESPONSABLES:			
UA / OAD Responsable:		Nombre del Administrador de la BD:	
Nombre del propietario de la Información:		Correo del propietario de la información:	
Nombre del Administrador del Servidor:		Correo del Administrador del Servidor:	
DATOS TÉCNICOS			
Software motor de BD:		Ubicación física:	
IP Interna:		IP pública:	
Sistema Operativo:		Puerto:	
Usuario propietario de la BD:		Esquema:	
DATOS DEL APLICATIVO			
Nombre del aplicativo que utiliza la base de datos:		Tecnologías core del aplicativo:	
Nombre del Administrador del Aplicativo:		Nombre del Responsable del Servidor del Aplicativo:	
IP Interna:		IP Publica:	
URL de Acceso:			
Fecha de llenado del formato:			
Revisó:			
Autorizo:			