



MINISTERIO
DE SALUD

**Lineamientos técnicos para el mantenimiento,
administración y desarrollo de tecnologías de la información
y comunicaciones**

El Salvador 2025



MINISTERIO
DE SALUD

**Lineamientos técnicos para el mantenimiento,
administración y desarrollo de tecnologías de la información
y comunicaciones**

El Salvador, 2025



Atribución-NoComercial-SinDerivadas
4.0 Internacional (CC BY-NC-ND 4.0)

Está permitida la reproducción parcial o total de esta obra por cualquier medio o formato, siempre que se cite la fuente y que no sea para la venta u otro fin de carácter comercial. Debe dar crédito de manera adecuada. Puede hacerlo en cualquier formato razonable, pero no de forma tal que sugiera que usted o su uso tienen apoyo de la licencia.

La documentación oficial del Ministerio de Salud puede consultarse en el Centro Virtual de Documentación Regulatoria en:

<http://asp.salud.gob.sv/regulacion/default.asp>

Ministerio de Salud

Calle Arce n.º 827, San Salvador, San Salvador Centro. Teléfono: 22917311

Página oficial: <http://www.salud.gob.sv>

Ministerio de Salud. Dirección de Regulación. Año 2025.

Autoridades

Dr. Francisco José Alabi Montoya
Ministro de Salud ad honorem

Dr. Carlos Gabriel Alvarenga Cardoza
Viceministro de Gestión y Desarrollo en Salud ad honorem

Dra. Karla Marina Díaz de Naves
Viceministra de Operaciones en Salud ad honorem

Contenido

I. Introducción	4
II. Base legal	4
III. Objetivos	4
Objetivo general	4
IV. Ámbito de aplicación	5
V. Adquisición y renovación de recursos informáticos	5
1. Especificaciones técnicas	5
2. Generalidades para la adquisición de equipos informáticos	5
Garantías	5
Donaciones	6
Compatibilidad	6
3. Adquisición de programas informáticos	6
Compra	6
Donaciones	7
VI. Soporte de equipo informático	7
1. Mantenimiento preventivo	8
2. Mantenimiento correctivo	9
3. Instalación de nuevo equipo de cómputo y periféricos	10
4. Inventario de hardware y software	11
4.1. Herramienta automatizada para recopilación de información de los equipos (tablets, laptops y equipos de escritorio)	11
4.2. Sobre las actualizaciones	12
5. Sobre la evaluación y descarga del inventario de equipo para descarte por obsolescencia	12
6. Sobre la administración del software	12
7. Mantenimiento de las medidas de seguridad contra software malicioso (malware)	13
7.1. Mantenimiento de la herramienta de firewall y antivirus (reglas, objetos, entre otras)	13
Herramienta de firewall	13
Herramienta de antivirus	13
VII. Infraestructura de red	14
1. Conexión a la red local	15
2. Administración de la red interna institucional (intranet)	15
3. Administración del acceso a internet	16
VIII. Servicios de internet e intranet	17
1. Acceso a la web y otros servicios de internet	17
2. Administración de los nombres de dominio y subdominios	18
3. Correo electrónico y plataforma de trabajo colaborativo	18
3.1. Creación de cuenta de correo electrónico institucional:	18
3.2. Eliminación de cuentas de correo electrónico institucional:	18
3.3. Reactivación de cuentas de correo electrónico institucional:	18
3.4. Modificación de cuentas de correo electrónico institucional:	19
4. Servicios de comunicaciones digitales de voz	19

Telefonía móvil	19
Telefonía fija	19
IX. Seguridad de la información	20
1. Autenticación	20
2. Certificados digitales	20
3. Seguridad física y lógica	21
4. Mecanismos de protección contra software malicioso (malware)	21
X. Sistemas de información	22
1. Desarrollo de sistemas de información	22
1.1. Solicitud de desarrollo de nuevas aplicaciones	22
1.2. Análisis y diseño	23
1.3. Desarrollo	24
1.4. Pruebas e implementación	24
2. Solicitud de cambios en sistemas de información existentes	24
3. Generación de información gerencial	24
4. Donaciones y desarrollos externos de software	25
5. Administración de sistemas y bases de datos	25
6. Capacitación y soporte técnico de los sistemas de información	26
7. Administración de sitio web institucional	26
8. Administración de servidores	27
9. Respaldo de información	28
XI. Unidades de informática	28
1. Dependencia jerárquica	29
2. Composición	29
3. Infraestructura y equipamiento	29
4. Funciones y actividades	29
XII. Planes de contingencia	30
XIII. Elaboración y aplicación de normas y otras disposiciones relativas a las TIC	30
XIV. Terminología	31
XV. Disposiciones generales	32
De lo no previsto	32
Obligatoriedad	32
Derogatoria	32
XVI. Vigencia	32



Distrito de San Salvador y Capital de la República, 17 de julio de 2025.-

Acuerdo n.º 1880.-

El Órgano Ejecutivo en el Ramo de Salud,

Considerando:

- I. Que el numeral 4 del artículo 41 del *Código de Salud* establece que el Ministerio de Salud es el responsable de organizar, reglamentar y coordinar el funcionamiento y las atribuciones de los servicios técnicos y administrativos de sus dependencias.
- II. Que los artículos 26 y 57 de la *Ley de la Corte de Cuentas de la República* establecen que cada entidad y organismo público, debe definir su propio sistema de control interno, administrativo y financiero, para garantizar que el activo fijo institucional sea debidamente administrado y controlado, así como los servidores públicos y organismos del sector público, son responsables de la administración de los recursos institucionales, debiendo usar, custodiar y registrar los recursos materiales a su cargo.
- III. Que la *Ley Especial contra los Delitos Informáticos y Conexos* tiene por objeto proteger los bienes jurídicos, en relación a aquellas conductas delictivas cometidas por medio de las tecnologías de la información y la comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los sistemas informáticos, su infraestructura o cualquiera de sus componentes, los datos almacenados, procesados o transferidos; o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a otros bienes jurídicos como el patrimonio, la integridad o identidad sexual, la identidad, intimidad y propia imagen de las personas naturales o jurídicas, y habiéndose generado avances sustanciales de los últimos años en las tecnologías y comunicaciones se vuelve indispensable adecuar la normativa institucional en relación a la Ley Especial contra los Delitos Informáticos y Conexos, a fin de prevenir conductas delictivas a nivel institucional, en relación a las Tecnologías de la Información y Comunicaciones.
- IV. Que es necesario dotar a las dependencias MINSAL y sus responsables de la herramienta adecuada para el manejo de las tecnologías de la información y comunicaciones con los lineamientos institucionales necesarios.
- V. Que mediante Acuerdo n.º 860, de fecha 4 de febrero de 2025, se emitieron los *Lineamientos técnicos para el mantenimiento, administración y desarrollo de tecnologías de información y comunicaciones* los cuales requieren ser actualizados a fin de establecer criterios y responsabilidades para garantizar el buen desempeño y la sostenibilidad de las plataformas de tecnologías de información y comunicaciones (TIC) del MINSAL.

POR TANTO, en uso de las facultades legales, **ACUERDA** emitir los siguientes:

Lineamientos técnicos para el mantenimiento, administración y desarrollo de tecnologías de la información y comunicaciones

I. Introducción

El Ministerio de Salud, en adelante MINSAL, con el propósito de establecer procedimientos generales de la actuación relacionada con las tecnologías de información y comunicaciones institucionales, ha elaborado los presentes Lineamientos técnicos para la administración de dichos elementos, facilitando el ordenamiento de los sistemas de información, el soporte técnico del equipamiento de cómputo, así como los enlaces y servicios de telecomunicaciones.

En este instrumento se detallan los lineamientos para la ejecución de actividades destinadas a mantener la coherencia, crecimiento y sostenibilidad de la plataforma tecnológica; tales como los respaldos de datos, adquisición de equipos y programas de cómputo, el inventario de software y equipos de cómputo, resguardo de licencias de software, sitio web institucional, correos electrónicos, transferencia electrónica de archivos, plan de contingencia y las políticas de gestión de redes.

II. Base legal

- *Ley de Especial contra los Delitos Informáticos y Conexos.*
- *Ley de Propiedad Intelectual.*
- *Reglamento relativo al registro e inventario de las licencias de programas de ordenador.*
- *Reglamento de Normas Técnicas de Control Interno Específicas del Ministerio de Salud.*
- *Manual de organización y funciones de la Dirección de Tecnologías de Información y Comunicaciones.*

III. Objetivos

Objetivo general

Establecer los criterios y responsabilidades necesarias y suficientes para garantizar el buen desempeño y la sostenibilidad de las plataformas de tecnologías de información y comunicaciones (TIC) del MINSAL.

Objetivos específicos

1. Estandarizar los procedimientos de mantenimiento, adquisición y reposición de los equipos de cómputo y otros periféricos, que componen la infraestructura informática de los establecimientos sanitarios y dependencias administrativas del MINSAL.
2. Establecer los procesos para la administración, análisis, diseño, desarrollo, implementación y soporte de los diferentes sistemas de información existentes.
3. Regular el uso de servicios digitales de voz y datos disponibles a las personas usuarias, tanto a través de la red internet como la intranet.

IV. Ámbito de aplicación

Están sujetos a la aplicación y cumplimiento de estos lineamientos técnicos, los funcionarios y empleados de los diferentes niveles de organización del MINSAL.

V. Adquisición y renovación de recursos informáticos

1. Especificaciones técnicas

Previo a la adquisición de equipo informático o aplicativos de software, todo establecimiento del MINSAL, deberá iniciar el proceso, dirigiendo a la DTIC, la justificación de compra correspondiente, solicitando el asesoramiento técnico de la DTIC y la emisión del dictamen.

El dictamen versará sobre la viabilidad de la adquisición, en aspectos como compatibilidad con los sistemas implementados, interoperabilidad, si hay o no versiones libres y gratuitas para el caso del software a adquirir. Lo anterior con la finalidad de elaborar las especificaciones técnicas o términos de referencia del equipo o software que se pretende adquirir.

Se deberá solicitar al oferente que incluya todos los manuales correspondientes (en físico o digital), para que los mismos se ajusten a las especificaciones técnicas y a las necesidades de la instancia solicitante, garantizando la compatibilidad y el adecuado funcionamiento con las TIC, implementadas dentro del MINSAL.

2. Generalidades para la adquisición de equipos informáticos

Cualquier equipo informático que se adquiera, deberá contar con los manuales, controladores, accesorios y periféricos correspondientes, para fácil instalación y óptimo funcionamiento del mismo.

En el caso que los equipos a adquirir, incluyan sistema operativo o cualquier otro software preinstalado, se deberá aplicar lo prescrito en el romano V numeral 3 Adquisición de programas informáticos.

Toda adquisición de equipos deberá incluir todos sus manuales o brindar un enlace para la descarga de los mismos; este requisito deberá mencionarse en los términos de referencia o especificaciones técnicas. Para el caso de archivos controladores incluidos con el equipo, estos deberán contar con la compatibilidad para diversos sistemas operativos, adicionalmente al que pudiera estar preinstalado, esto último figurará como una especificación técnica requerida, si es pertinente al tipo de equipo. Ello principalmente para los casos de sistemas operativos basados en software libre.

Garantías

Los plazos mínimos de garantía deben ser los siguientes:

- Para el caso de equipos de escritorio, portátiles, mini computadoras, tablets, otros dispositivos, así como equipos de cómputo con propósito general (AP, switches,

impresoras, UPS, entre otros), el plazo de garantía no deberá ser menor a un año por defectos de fábrica.

- Para el caso de servidores, estos deberán contar con un plazo no menor a dos años de garantía por defectos de fábrica.

Donaciones

La aceptación de donaciones por cada dependencia, estará supeditada a que cumpla con los requisitos siguientes:

1. En perfecto estado de funcionamiento.
2. Para el caso de los equipos con sistema operativo libre o privativo, que éste cuente con actualizaciones disponibles sobre la misma versión.

El donante deberá presentar un ofrecimiento por escrito dirigido al Titular; en el cual se deberá expresar la descripción del bien que desea donar, marca, características, utilidad, entre otras condiciones técnicas, y precio de este.

Una vez presentado el ofrecimiento escrito al Titular, deberá ser marginado a la DTIC, a fin que exprese si es procedente aceptar la donación, de acuerdo a lo prescrito al inicio de este apartado.

Para los casos de donaciones entre instituciones, serán los titulares, a través de los representantes que estos deleguen, quienes harán los procesos administrativos previos, de acuerdo a las disposiciones del convenio celebrado entre las partes y las disposiciones de ley pertinentes.

Compatibilidad

Cualquier equipo que se adquiera deberá garantizar su interoperabilidad y/o soporte para sistemas operativos de software libre, sin que ello implique un licenciamiento adicional.

Lo anterior con la finalidad de extender la vida útil de los mismos en el mediano y largo plazo, así como facilitar el manejo de los datos y el funcionamiento genérico de los sistemas de información.

Asignación de equipo informático

La asignación de equipo informático abarca todas las dependencias del Nivel Superior, regiones de salud y hospitales nacionales e inicia con la recepción de la solicitud de petición por parte de la dependencia solicitante, a través de los medios de comunicación oficiales, y finaliza con la entrega del equipo informático y/o telecomunicaciones, a través del técnico informático destacado en la Unidad de Soporte Técnico o Redes y Telecomunicaciones.

3. Adquisición de programas informáticos

Compra

Es responsabilidad de la unidad o dependencia que adquiere, proporcionar la justificación de la compra a realizar, explicando las razones por las cuales desea adquirir dicho bien o servicio. Para la adquisición de un aplicativo informático, se deberá previamente, acreditar por escrito a la DTIC, la necesidad de funcionalidades específicas (de no haber sido remitida, es responsabilidad de la DTIC solicitarla a la dependencia).

Es responsabilidad de la unidad o dependencia que adquiere, realizar la solicitud de asesoría técnica a la DTIC para la adquisición de programas informáticos (software); dicha solicitud podrá ser remitida a la DTIC por medio de correo oficial o institucional o memorándum. De acuerdo a lo anterior, tanto la justificación como la solicitud de asesoría técnica, podrán realizarse a través del mismo medio siempre y cuando sea por memorándum.

Será responsabilidad de la DTIC, a través del técnico asignado, emitir la respuesta a la solicitud de asesoría técnica, la cual deberá evaluar diferentes aspectos técnicos de idoneidad y compatibilidad con los sistemas existentes, además de la conveniencia de la adquisición, la falta de opciones libres y gratuitas u opciones libres y gratuitas existentes; además de acreditar la sostenibilidad de los fondos para la adquisición y mantenimiento de la licencia, en caso de ser de renovación periódica.

Será responsabilidad de la DTIC que, toda comunicación y documento, debe quedar en copia digital para registro del encargado de inventario y respaldo de la DTIC. Y que todo documento impreso que dé respuesta a la solicitud, incluyendo la firma del técnico asignado y coordinador del área.

Para los casos en que se adquieran software de uso privativo, estos deberán ser resguardados por los responsables de la unidad solicitante correspondiente y proporcionar la documentación que acredite la actualización de los registros de control interno; resguardando el número y/o certificado de licencia, copia de los medios de instalación y la HKEY que el fabricante proporcione, será la DTIC la que determine el mejor medio de resguardo, según sea el formato de la licencia en cuestión.

Si por alguna razón no se contase con forma alguna de acreditar la posesión del licenciamiento de un software, este deberá ser desinstalado al momento de detectarse la situación por el personal informático correspondiente o en su defecto por la DTIC, según lo prescrito por la *Ley de Propiedad Intelectual*.

Donaciones

Con relación al software que ha de recibirse por donación, deberá seguir el procedimiento descrito en el Romano V numeral 1 referente a las especificaciones técnicas y numeral 2 referente a donaciones del mismo.

VI. Soporte de equipo informático

El mantenimiento preventivo y correctivo de hardware y software de los equipos de cómputo será exclusivo para equipo adquirido por el MINSAL o recibido en calidad de donación, se prohíbe el uso de cualquier equipo o software de uso personal entiéndase: CPU, laptop, tablet, UPS, monitores, teclados, mouse, switch, licencias de ofimática, licencias de lectura de archivos PDF, software de edición, software CAD, etc.; el mantenimiento será abordado de manera conjunta y coordinada por la DTIC, de acuerdo a su área de competencia y con el personal de las Unidades de Informática de las direcciones regionales, hospitales y otras dependencias.

Primeramente, será el personal de informática asignado para el establecimiento, quien abordará la situación emergente; posteriormente y en caso de existir necesidad de una intervención técnica, se derivará la gestión al personal de la Unidad de Soporte Técnico de la DTIC.

Los servicios de soporte ofrecidos por la DTIC son los siguientes:

1. Mantenimiento preventivo. A cargo de la Unidad Soporte Técnico.
2. Mantenimiento correctivo: diagnóstico de fallas y eventual reparación. A cargo de la Unidad Soporte Técnico.
3. Instalación y configuración de nuevo equipo de cómputo y periféricos. A cargo de la Unidad Soporte Técnico.
4. Evaluación y descarga del inventario de equipo de cómputo y periféricos dañados u obsoletos. A cargo de la Unidad Soporte Técnico.
5. Evaluación y descarga del inventario de equipos de redes y telecomunicaciones dañado u obsoletos. A cargo de la Unidad de Redes y Telecomunicaciones.
6. Administración de software (instalación, actualización, desinstalación). A cargo de la Unidad de Soporte Técnico en lo referente a equipos de cómputo (desktop y laptop). Lo anterior no atañe la instalación, actualización o desinstalación de aplicativos desarrollados por la Unidad de Desarrollo, que estaría a cargo de estas herramientas.
7. Mantenimiento de las medidas de seguridad contra malware. A cargo de la Unidad de Seguridad en lo referente a la detección y reporte oportuno de las anomalías detectadas a través de la consola del antivirus, por lo cual dicha coordinación deberá comunicar oportunamente a la coordinación de la Unidad de Soporte Técnico, para que esta atienda el reporte generado por la Unidad de Seguridad, brindando la identificación certera del equipo.
8. La creación, actualización y bajas de correos electrónicos. A cargo de la Unidad de Redes y Telecomunicaciones.

Toda gestión de solicitud de soporte deberá canalizarse a través del Sistema de Información de Soporte automatizado de la DTIC (Sistema de Tickets), accediendo desde cualquier navegador web desde el siguiente link: <https://soporte.salud.gob.sv>. Si al momento de solicitar la asistencia de soporte técnico no se cuenta con conexión de red o esta no estuviera disponible en dicho momento, podrá realizarse dicha solicitud a través de correo electrónico, llamada telefónica, memorándum o nota, con la condición de que dicha solicitud sea formalizada a través del sistema de tickets a la brevedad posible. Sin perjuicio de lo anterior, el personal de informática llevará el registro de las asistencias realizadas y su resultado en la herramienta indicada.

Para poder realizar la solicitud a través del sistema de tickets, todo usuario de un equipo de cómputo del MINSAL debe utilizar su usuario y contraseña o su correo institucional. En caso de no contar con ella, deberá solicitar la creación a la DTIC.

Es de carácter obligatorio que para poder acceder al sistema de ticket se debe hacer uso del correo electrónico institucional o de sus credenciales institucionales. Queda terminante prohibido el uso de correo electrónico personal y de igual manera para el uso de la función de escaneo a través de correo electrónico en los impresores multifuncionales adquiridos por el MINSAL o que estén en la modalidad de contrato de arrendamiento por una empresa privada.

Una vez se haya recibido la solicitud, la DTIC asignará al personal técnico competente y disponible en función de la carga de trabajo que el área tenga al momento de la solicitud y la prioridad que esta representa respecto de otras actividades, proyectos o solicitudes realizadas de manera previa. El personal técnico asignado contactará al personal solicitante para la coordinación de la asistencia técnica presencial o remota.

Finalizada la asistencia técnica, se procederá al cierre de la gestión detallando: tiempo utilizado, acciones realizadas sobre el equipo, insumos necesarios, y demás datos pertinentes a la solución brindada; si y sólo si en esta gestión han sido concluidas las actividades para la resolución del problema.

1. Mantenimiento preventivo

Al menos una vez al año, se realizará mantenimiento preventivo a cada equipo MINSAL, sea este en propiedad o mera tenencia. No obstante, deberá realizarse un monitoreo rutinario por parte del personal informático local correspondiente según el área de competencia o de la DTIC según el caso.

Dicho mantenimiento incluirá la realización de una o todas las acciones que se listan a continuación:

- Limpieza exterior e interior, siempre y cuando ello no violente la garantía vigente del fabricante o pérdida de ésta al abrir el equipo en cuestión.
- Revisión y comprobación de funcionamiento normal.
- Sustitución de piezas cuyo desgaste pudiera estar afectando el rendimiento del equipo.
- Actualización de software, en caso de que el equipo no estuviera conectado a la red o bien éste no estuviera configurado para actualizarse automáticamente.
- Comprobación del funcionamiento de la herramienta de inventario automatizado para hardware y software (descrito en el romano VI numeral 4.1), así como el cliente para la asistencia remota en el caso de equipos de cómputo de escritorio y software antimalware.

Toda actividad de mantenimiento preventivo deberá ser registrada, calendarizada y comunicada efectivamente, con antelación a la jefatura respectiva, por los medios de comunicación oficiales; ello con el objetivo de prever actividades alternas o complementarias a los usuarios durante el periodo que dure el mantenimiento.

La programación de las actividades de mantenimiento preventivo estará sujeta a la disponibilidad del personal técnico, lo anterior en función de proyectos, actividades emergentes o prioridades que se le determinen a esta Dirección por parte de las autoridades.

2. Mantenimiento correctivo

En caso de existir fallo o desperfecto que impida el funcionamiento normal de un equipo de cómputo o periféricos, será responsabilidad de la persona usuaria y/o de la jefatura de la dependencia, informar a la instancia correspondiente, como se indica en los incisos primero y segundo de la descripción general del romano VI.

De estar vigente el periodo de garantía del equipo, deberá seguirse el proceso indicado para hacer efectiva la misma, con la debida previsión de no realizar ninguna acción sobre el equipo que lleve a la pérdida de dicha garantía.

En caso de haber caducado el periodo de garantía del proveedor y/o fabricante, se procederá de acuerdo a las acciones siguientes según sea el caso:

- Revisión y prueba de funcionamiento para diagnóstico y presupuesto tentativo del costo de reparación.
- Sustitución de piezas dañadas o con desgaste por funcionamiento.
- Reinstalación de software, aplicaciones de usuario e inclusive sistemas operativos; y las herramientas de administración de inventario y asistencia remota.

Toda solicitud y actividad de mantenimiento correctivo deberá ser registrada y actualizada en la plataforma automatizada de soporte. El diagnóstico, tiempo de ejecución del proceso de reparación y costos, deben ser notificados a la persona usuaria y su jefatura inmediata. En cuanto al tiempo de ejecución del mantenimiento correctivo del equipo, este estará en función de los recursos técnicos disponibles y repuestos.

En atención a la gravedad de la falla que pudiera suscitarse en un equipo, y considerando que el diagnóstico de la misma, indique su estado de irresoluble o que el costo supere o equipare al de la adquisición de un equipo nuevo; se procederá al reporte del equipo como "dañado sin reparación", para su correspondiente descarga del inventario, de acuerdo a lo prescrito en los *Lineamientos para la Administración del Activo Fijo*.

En general, si las fallas reportadas no fueran corregidas por la unidad de informática de las direcciones regionales, hospitales, y otras dependencias; ello deberá ser escalado con reporte de falla a la Unidad de Soporte de la DTIC, para que en coordinación y a criterio de la jefatura de la Unidad de Soporte DTIC, se defina el abordaje y procedimiento según sea el caso y de acuerdo a la disponibilidad del recurso humano y repuestos disponibles.

A efecto de agilizar cualquier gestión de mantenimiento en cualquier equipo de cómputo, en especial aquellas situaciones que implican funcionamiento imprevisto o erróneo de las aplicaciones informáticas instaladas; se intentará resolver vía escritorio remoto; con la condición de que dicha solicitud sea formalizada a través del sistema de tickets a la brevedad posible; dicho acceso remoto deberá estar aprobado por la persona usuaria previamente, de acuerdo a lo establecido por la *Ley especial contra los delitos informáticos y conexos*, referente al acceso indebido a sistemas informáticos, para quienes intencionalmente y sin autorización o

excediendo la que se le hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las tecnologías de la información o la comunicación, y en pro de la protección de la privacidad y confidencialidad, por lo cual queda absolutamente prohibida la configuración de cualquier aplicación de acceso remoto al escritorio, de tal forma que dicho acceso inadvertido y/o sin autorización previa de la persona usuaria del equipo en cuestión.

3. Instalación de nuevo equipo de cómputo y periféricos

Es responsabilidad de la Unidad de Soporte Técnico, la instalación, configuración, actualización y reinstalación del equipo de cómputo. Como prerequisite para la instalación, los equipos deberán contar con licencia vigente de todo el software que incluya al momento de su instalación; en caso contrario se procederá con la instalación de software libre equivalente, como se establece en el romano VI numeral 6.

La persona usuaria del equipo, estará presente para verificar la prueba del equipo y su entrega a satisfacción o de cualquier petición posterior. De todo lo pertinente y acontecido durante el proceso de instalación se informará a la coordinación de la dependencia o área respectiva.

Se configura el equipo para la realización del inventario automatizado de software y hardware, con la herramienta que la DTIC ha ya destinado para ello, así como la asistencia remota, las actualizaciones periódicas y para sistemas privativos vulnerables, las herramientas de seguridad y protección pertinentes y previstas por MINSAL, a través de la DTIC.

Adicionalmente, como prerequisite el equipo deberá contar previamente con el código de inventario correspondiente a la unidad donde ha de ser asignado, previa gestión de la jefatura de la dependencia con la Unidad de Activo Fijo.

4. Inventario de hardware y software

A todo equipo de cómputo del MINSAL se le deberá inventariar los componentes físicos; para ello DTIC se valdrá de una herramienta que enviará de manera automatizada la información de los componentes al servidor central dispuesto para tal fin.

La conciliación del inventario perteneciente a DTIC, será responsabilidad de la persona asignada para el manejo de inventarios en colaboración directa con cada coordinación de las diferentes unidades de la DTIC.

Sin perjuicio de lo anterior es responsabilidad de cada dependencia o unidad la administración, resguardo, control y conciliación de su inventario con la Unidad de Activo Fijo, de acuerdo a lo previsto en los *Lineamientos Técnicos para la Administración del Activo Fijo*.

4.1. Herramienta automatizada para recopilación de información de los equipos (tablets, laptops y equipos de escritorio)

La herramienta automatizada hardware y software de la DTIC, es un software que recopila la información sobre el hardware y software instalados de equipos que hay en la red, utilizando un programa de cliente a través de una interfaz web.

Características

- Soporte para muchos sistemas operativos entre ellos: Microsoft Windows, Mac OS, Linux, Android.
- La interfaz web muestra el detalle de cada equipo incluyendo:
 - Hardware: CPU, RAM, red, placa madre, video, sonido entre otros.
 - Versión de BIOS.
- Prestaciones:
 - Facilita la detección de software no autorizado.
 - Permite ver una vista centralizada de los equipos informáticos ya sea CPU, laptop, tablets.
 - Provee información sobre las características del equipo para la toma de decisiones referente a la manera de proceder en la renovación de equipos.
 - Es una aplicación diseñada para ayudar a dar seguimiento de la configuración de los equipos y software instalados.

En el caso de que el equipo no esté conectado a la red, el personal técnico tiene igualmente la obligación de instalar la herramienta automatizada y obtener la información para ser remitida a la persona asignada para el manejo del inventario, quien la incorporará al inventario de equipos. En estos equipos se aprovecharán las actividades programadas de mantenimiento preventivo para actualizar la información del inventario.

La DTIC podrá realizar supervisiones periódicas de validación de los datos de inventario de uno o varios equipos de cómputo, para verificar su corrección, lo cual será notificado oportunamente a la jefatura correspondiente de la dependencia a efecto de programar la visita evitando entorpecer las actividades habituales del puesto de trabajo o la dependencia.

En caso de detectarse ausencia de partes o equipos completos, se seguirán los procedimientos previstos para denunciar y deducir responsabilidades del hurto o extravío de un equipo propiedad del MINSAL, de acuerdo a lo prescrito en los *Lineamientos Técnicos para la Administración del Activo Fijo* que estén vigentes a la fecha.

4.2. Sobre las actualizaciones

Con base en lo anterior y con la finalidad estandarizar el procedimiento de actualización de equipos del MINSAL y sus dependencias, deberá seguirse las indicaciones siguientes:

En todas las actualizaciones de equipo de cómputo que se realicen, las áreas solicitantes deberán especificar en sus requisiciones de compra el número de inventario del equipo al que pasarán a formar parte las refacciones, accesorios y licencias (si fuera el caso) que sean adquiridas.

Todas las actualizaciones de equipo informático de las diferentes dependencias del MINSAL, sin excepción, deberán contar con el visto bueno de la DTIC, a fin de garantizar la viabilidad técnica de las mismas y vigilar la vigencia de las licencias de software que se tendrán en el equipo.

5. Sobre la evaluación y descarga del inventario de equipo para descarte por obsolescencia

Un equipo podrá ser descartado, previo diagnóstico y evaluación por el personal técnico de la DTIC. Dicho proceso podrá iniciarse a petición de la jefatura donde se encuentra el equipo informático.

Para el caso de equipos adquiridos con licencia de "Fabricante de Equipo Original" (OEM, Original Equipment Manufacturer), dicha licencia debe descartarse una vez que se le dé de baja al equipo, ya que la licencia se considera como parte del equipo.

Se procurará rescatar partes o piezas que eventualmente puedan servir de repuesto en otros equipos en el mantenimiento correctivo. Dicho proceso de descarte deberá ejecutarse de acuerdo a lo establecido en los Lineamientos Técnicos para la Administración del Activo Fijo, para la eliminación de dichos bienes en el inventario del Activo Fijo MINSAL.

6. Sobre la administración del software

Toda instalación de programas o aplicaciones en equipos informáticos de las diferentes dependencias del MINSAL, deberá ser coordinada por medio de una solicitud o a través de la plataforma automatizada de soporte; para dicho proceso se debe utilizar las credenciales de administración de los equipos de cómputo. Queda prohibido a las personas usuarias de los diferentes equipos informáticos del MINSAL, la instalación o desinstalación de programas o aplicaciones.

En cumplimiento a la Ley de Propiedad Intelectual, ningún equipo del MINSAL deberá tener instalado software privativo sin la debida acreditación de la licencia, en cualquiera de las modalidades actuales para respaldar dicho licenciamiento. Será obligación del personal técnico informático en cuestión la desinstalación del software en situación irregular, y brindar el asesoramiento adecuado a la persona usuaria referente a alternativas de software libre o el licenciamiento correspondiente.

Toda documentación de respaldo que acredite el licenciamiento del software de un equipo del MINSAL, estará bajo la custodia y resguardo de la Unidad de Informática o Unidad de Soporte de la DTIC, según corresponda. Para los licenciamientos que se identifican por medio de una viñeta adhesiva o por un dispositivo llave que se conecta a algún puerto de comunicaciones, será responsabilidad de la persona usuaria el cuidado y buen estado de la viñeta de licenciamiento o llave, por lo cual su daño o pérdida conlleva la desinstalación del software en mención por la falta de medio probatorio de licenciamiento.

Con relación al software de actualizaciones automáticas, deberán ser configuradas oportunamente por el personal técnico informático local o soporte DTIC, según corresponda. En caso contrario o no previsto, será la persona usuaria, con aval de su jefatura inmediata, la que solicite la actualización a una nueva versión que le permita corregir fallos o la ampliación de las características requeridas en su puesto de trabajo, sin perjuicio de la evaluación de las capacidades del equipo para el manejo de las actualizaciones más recientes.

La desinstalación de aplicativos que no son requeridos por la persona usuaria en su puesto de trabajo o mejoramiento del rendimiento o capacidades del equipo, también deberán ser requeridas a través de una solicitud en la plataforma automatizada de soporte.

En los traslados de equipos de cómputo entre dependencias, será responsabilidad de la jefatura de la dependencia receptora, iniciar la solicitud de instalación y desinstalación del software de dicho equipo para adecuarlo a las nuevas necesidades.

7. Mantenimiento de las medidas de seguridad contra software malicioso (malware)

Cualquier equipo informático del MINSAL deberá quedar adecuadamente configurado desde un inicio en lo referente a las actualizaciones periódicas y en el caso de sistemas operativos privativos vulnerables, con las herramientas implementadas institucionalmente para la protección contra programas malignos.

Siempre que sea posible, se procurará aprovechar las actividades de mantenimiento preventivo del hardware para verificar la necesidad de actualizar sistema operativo, software de usuario y las herramientas de seguridad como antivirus y otros. Esto aplica en particular a los dispositivos no conectados a la red, además de los equipos conectados a la red de cualquier establecimiento, entendiéndose en ellos equipos móviles y de desktop o laptop.

7.1. Mantenimiento de la herramienta de firewall y antivirus (reglas, objetos, entre otras)

Herramienta de firewall

Será responsabilidad de la Unidad de Seguridad realizar una revisión detallada de los módulos de protección y capa 3 en el dispositivo de seguridad perimetral de Nivel Superior y hospitales, a fin de garantizar un óptimo uso de los equipos y minimizando de esa forma el índice de riesgo a través de la depuración de VPN, permisos, objetos y reglas de firewall.

Herramienta de antivirus

El área de seguridad deberá realizar cada fin de semana, un análisis del estado actual de la solución de antivirus, con el objetivo de generar un reporte de las principales detecciones que han ocurrido y con ello informar mediante los medios oficiales a los directores e informáticos, se deberá llevar a cabo una auditoría de los equipos que llevan más de un mes sin conexión hacia la plataforma, estos equipos deberán ser reportados hacia las unidades de informática de cada establecimiento, en caso de que el equipo no sea ubicado en menos de 24 horas, pasará a su eliminación.

Se deberá generar un reporte mensual ejecutivo destinado para la dirección donde se detallan planes de mejora, puntos de impacto que han tenido las soluciones de antivirus.

En caso de suscitarse un ataque específico a uno o varios equipos del MINSAL, el personal de la unidad de informática del establecimiento o en su defecto, la Unidad de Soporte Técnico de la DTIC, junto a la Unidad de Seguridad de la DTIC; actuará de oficio y con la inmediatez requerida en la eliminación o contención de la amenaza. Toda actuación, en el marco de la resolución de la problemática, deberán ser comunicadas a la jefatura inmediata y a la persona usuaria, oportunamente, además de elaborar un documento del incidente ocurrido para futuras acciones o registros de la unidad, dicho informe deberá ser compartido a la jefatura inmediata, director en funciones y a la jefatura de la unidad o dependencia donde se originó el incidente.

Todos los equipos deben quedar adecuadamente configurados desde su instalación para las actualizaciones periódicas y, en el caso de sistemas operativos privativos vulnerables, con las herramientas de protección contra malware previstas institucionalmente.

Se aprovecharán las actividades de mantenimiento preventivo del hardware para comprobar, ajustar y, en caso de ser necesario, actualizar manualmente el sistema operativo, software de usuario y las herramientas de seguridad como antivirus y otros. Esto aplica en particular a los equipos no conectados a la red.

En caso de detectarse algún tipo de problemática de ataque específica con uno o varios equipos de cómputo, el personal técnico de la DTIC y/o de la unidad de informática correspondiente, podrá actuar por iniciativa propia y a la mayor brevedad posible, para eliminar o contener la problemática. Las actuaciones necesarias para su resolución, ya sea ésta inmediata o no, serán oportunamente comunicadas a la persona usuaria del equipo afectado y a la jefatura correspondiente.

VI. Infraestructura de red

Será responsabilidad de la unidad de informática de las direcciones regionales de salud, hospitales, y otras dependencias y de la Unidad de Redes y Telecomunicaciones de la DTIC ofrecer sus servicios en pro de mantener la red institucional y los servicios de comunicación informáticos de forma operativa, además de proteger la confidencialidad de la información.

Será responsabilidad del personal de informática asignado para hospitales y regiones de salud, el mantenimiento de red, y en caso de ser necesaria la intervención técnica de la DTIC, será transferida a la Unidad Instalaciones de la DTIC. Ambas trabajarán de forma coordinada en la resolución de inconvenientes relacionados a los servicios de comunicación informáticos. A continuación, se listan los servicios de infraestructura de red ofrecidos:

- Conexión a la red local.
- Administración de la red interna (intranet) y los enlaces de comunicación que la componen.
- Administración del acceso a internet.
- Administración de los nombres de dominio y subdominios. (unidad de servidores).

Las unidades informáticas respectivas y la Unidad de Redes y Telecomunicaciones de la DTIC gestionarán las solicitudes a través del correo institucional. En caso que la persona usuaria no cuente con conexión de red podrá hacer su solicitud vía llamada telefónica en función de la criticidad del caso, remitiendo dicha solicitud por correo institucional a la brevedad posible. Será responsabilidad del personal informático llevar el registro de las actuaciones realizadas y su resultado a través de informe técnico para el control interno de esta Dirección.

Para realizar la solicitud a través del sistema de información automatizado, la persona usuaria deberá ingresar con su nombre de usuario y contraseña institucional; de no contar con ello deberá solicitarlo a la DTIC, a través de una gestión con la Unidad de Recursos Humanos, ellos para acreditar el vínculo laboral y vigencia del mismo.

Recibida la solicitud, se le asignará al personal técnico disponible con base a la carga de trabajo y criterio de idoneidad para la resolución del problema técnico del que se trate. El personal asignado para la solicitud se pondrá en contacto con la persona solicitante, procurando la eficiencia en el servicio, evaluando si la solicitud es posible resolverla vía asistencia remota, y de no ser posible coordinando la visita técnica.

Se deberá registrar toda actuación sobre el equipo en informe técnico y de manera asociada a la solicitud realizada, ello comprenderá actuaciones realizadas, materiales necesarios, tiempo de ejecución para la resolución, entre otros. Solo se podrá cerrar la solicitud realizada cuando hayan concluido las actividades correctivas derivadas de la solicitud.

1. Conexión a la red local

Con base en las funciones de cada puesto de trabajo y las necesidades de interconexión que se soliciten derivadas de dichas funciones, la DTIC a través de las unidades de seguridad o redes y telecomunicaciones (según competencia), en su defecto, la unidad de informática de la dependencia deberá proporcionar el acceso a la persona usuaria, procurando que este tenga un nivel de seguridad o derechos de red acordes al desempeño de sus funciones, no importando el medio de conexión con el que se accede a la red de acuerdo a lo prescrito en los presentes Lineamientos Técnicos de la DTIC y demás normas de control interno MINSAL.

Será responsabilidad de la Unidad de Instalaciones de la DTIC, el cableado estructurado y la interconexión de comunicaciones, desde los equipos activos hacia y desde los equipos finales, independiente del medio de conexión (física o inalámbrica). Sin perjuicio de lo anterior, podrá solicitarse apoyo del personal informático o mantenimiento y servicios de cada establecimiento o dependencia, para la instalación técnica de los distintos elementos físicos de la red, con la finalidad de agilizar el proceso.

Excepcionalmente, podrá contratarse el servicio de instalación de redes locales, ello cuando dicha instalación requiera especialización, experiencia y pericia especial o particular con el que no se cuente, la magnitud de la obra, o la disponibilidad del recurso personal técnico debido a otras actividades de MINSAL.

2. Administración de la red interna institucional (intranet)

Será responsabilidad de la Unidad de Redes y Telecomunicaciones, mantener una red interna a nivel nacional (intranet) que conecte todos los establecimientos de salud y dependencias del MINSAL, en función del desarrollo de la Agenda Digital y las asignaciones presupuestarias que ello conlleve.

La red será propiedad del MINSAL, en lo referente al equipamiento y administración; no obstante, los medios de transmisión e infraestructura física podrán ser arrendados, o bien adscribirse a una

iniciativa gubernamental de cobertura y alcance similar o equivalente, previo convenio que respalde dicha adscripción. Dicha red deberá estar construida de acuerdo a las necesidades actuales del MINSAL, de acuerdo a los resultados y metas planteadas por la Agenda Digital en cuanto a su extensión y calidad, ofreciendo redundancia en los enlaces propios. Podrá contratarse el servicio de intranet con proveedores privados según prescriba la Ley de Compras Públicas y lineamientos técnicos de la DINAC, a efecto de las contrataciones públicas.

Será responsabilidad de la Unidad de Redes y Telecomunicaciones garantizar que la transmisión sea bidireccional, rápida, confiable y estable y será responsabilidad de la Unidad de Seguridad, garantizar la seguridad de la información; lo anterior mediante las actividades de monitoreo y administración de enlaces y reparación de fallas de la red, tomando acciones preventivas y correctivas en coordinación con el área correspondiente, unidades de informática de cada región de salud, hospital o soporte técnico además de los proveedores si los existiese.

La Unidad de Seguridad recibirá las peticiones de autorización, revocatoria o revisión de los permisos de acceso a la red del MINSAL en lo referente a los servicios o aplicativos internos; asimismo, la publicación de servicios en la intranet de equipos servidores. Esto de publicación se lleva a cabo de la mano con el equipo de servidores y ellos deben notificar junto al equipo de desarrollo el sistema a publicar para realizar las pruebas de vulnerabilidad pertinentes.

La Unidad de Redes Telecomunicación en coordinación con la Unidad de Seguridad, según sea el caso, a través de la unidad informática del establecimiento o dependencia solicitante, asignará y revisará la configuración de red más idónea a cada equipo que haya de estar conectado a la red MINSAL, procurando así, que cada equipo pueda ser identificado de forma inequívoca en la red y garantizando la detección de situaciones anormales o fuera de las normas específicas en lo referente a la administración de la red como los lineamientos técnicos de la DTIC y/o normas de control interno específicas de MINSAL además de colaborar para el buen funcionamiento de la seguridad de la información mediante la implementación de las herramientas de seguridad y medidas que sea dictada por la Unidad de Seguridad.

3. Administración del acceso a internet

Será responsabilidad de la Unidad de Redes y Telecomunicaciones de la DTIC, la habilitación del acceso a internet para todos los establecimientos y dependencias del MINSAL, se procurará que haya un único acceso a nivel institucional con el objetivo de unificar los costos y mejorar control del acceso al servicio de internet, economizando en contraposición a conexiones múltiples particulares y optimizando la aplicación de la política de administración general de los enlaces y siguiendo los lineamientos emitidos por el Órgano Ejecutivo y armonía el organismo contralor del Estado.

Por lo anterior, se procurará que ningún establecimiento o dependencia del MINSAL tenga conexión diferente de acceso a internet; sino a través de la correspondiente solicitud a la DTIC para acceder a través de la Intranet MINSAL.

Queda totalmente prohibido el uso de dispositivos personales como router, modem o repetidores de señal inalámbrica dentro de los establecimientos de salud

En caso de que una dependencia necesite ampliar el ancho de banda de conexión a internet y cuente con presupuesto o financiamiento externo para ello, deberá apoyar con dicho

financiamiento la adquisición de un enlace común a internet de mayor capacidad y proporcionalmente la mejora en las líneas de comunicación de la red interna que sean necesarias para ofrecer dicha mejora de conexión.

Si fuera el caso en que un establecimiento o dependencia del MINSAL necesitare una ampliación en las prestaciones de su acceso a internet; deberá: contar con presupuesto aprobado o financiamiento externo; además de realizar la justificación pertinente, a efecto de su trámite en la UCP y de acuerdo a todo lo prescrito en la *Ley de Compras Públicas* para el proceso de adquisición. Esta justificación deberá ser valedera y poner de manifiesto la mayor capacidad a contratar, asimismo la mejora que reflejaría en los servicios y líneas de comunicación de la red interna MINSAL.

Para la conexión autónoma a internet, necesarias para algunos puestos de trabajo por su movilidad o lugares con difícil acceso para las tecnologías de conexión; podrá arrendarse, de acuerdo a lo prescrito por la Ley de Compras Públicas, equipos módems de tecnología celular, los cuales serán igualmente administrados por la Unidad de Redes y Telecomunicaciones y la Unidad de Seguridad, en lo que le competa, para efectos de unificar las solicitudes en una sola contratación anual, que permita obtener una mejor relación costo beneficio en dichas contrataciones.

Para servicios o sistemas de información que deben ser publicados en internet, para acceso público o dependencias que no cuenten con la conexión a la intranet, será la Unidad de Desarrollo de la DTIC, la responsable en coordinación directa con la unidad de informática del establecimiento o dependencia del MINSAL, de solicitar dicha publicación a través de la plataforma de soporte, poniendo de común acuerdo las direcciones de red, números de puerto y protocolos con la Unidad de Redes y Telecomunicaciones.

VII. Servicios de internet e intranet

Será responsabilidad de la Unidad de Servidores y Bases de Datos de la DTIC, la renovación de los dominios principales del MINSAL, ante las entidades de registro competentes a nivel nacional o internacional que a su vez definirán la afinidad, función, nombre, abreviatura, siglas y acrónimos de la institución; se procurará que sean reconocibles y asociables a la entidad para una adecuada difusión mediática de los mismos.

Se deberá administrar en dos equipos servidores DNS o servidor de nombres de dominios y subdominios. Estos servidores deberán ser localizados en diferentes puntos de la red nacional. Toda solicitud de subdominio deberá ser realizada a través de la plataforma de soporte. Adicionalmente, se deberá establecer el ámbito de publicación de cada dominio y subdominio, es decir intranet, internet o ambos.

Será responsabilidad de la Unidad de Servidores y Bases de Datos de la DTIC, notificar de la publicación de un nuevo sitio o sistema del MINSAL para la realización de los análisis y pruebas de vulnerabilidades a fin de identificar vulnerabilidades que deban ser corregidas previo a su publicación.

1. Acceso a la web y otros servicios de internet

La aplicación de normas relativas al control del servicio de acceso a internet, particularmente en lo que respecta a navegación, uso de servicios de mensajería, audio y videoconferencia, entre otros, será responsabilidad de la Unidad de Seguridad de la DTIC, que deberá contar con el equipo y recursos humanos necesarios para realizar dicha labor.

El propósito de la aplicación de reglas de filtrado para el uso de los servicios de internet es garantizar el acceso a dichos servicios, evitando el abuso o mala utilización de tales privilegios, en perjuicio de las personas usuarias, así como de su rendimiento laboral.

La Unidad de Seguridad de la DTIC aplicará este tipo de mecanismos de regulación del servicio de internet en general, no obstante, se tomarán en cuenta las diferentes necesidades y funciones de cada usuario o dependencia, quien deberá solicitar a través de correo institucional y remisión del memorándum correspondiente, la configuración específica y además, deberá obtener una autorización por escrito de la jefatura superior antes de que la Unidad de Seguridad proceda a su aplicación.

En el caso de que las solicitudes sean desde hospitales, unidades de salud y regiones, deberá contar con el visto bueno del encargado informático del sitio y director del establecimiento, mediante un memorándum.

2. Administración de los nombres de dominio y subdominios

Será responsabilidad de la Unidad de Servidores y Bases de Datos de la DTIC, la renovación de los dominios principales del MINSAL, ante las entidades de registro competentes a nivel nacional o internacional que a su vez definirán la afinidad, función, nombre, abreviatura, siglas y acrónimos de la institución, tomando en cuenta los tiempos de vigencia y renovación, de acuerdo a las normas internacionales o nacionales; se procurará que sean reconocibles y asociables a la entidad para una adecuada difusión mediática de los mismos.

Se deberá administrar en dos servidores los nombres de dominios y subdominios. Estos servidores deberán ser localizados en diferentes puntos de la red nacional a fin de garantizar el acceso a los sitios web. Toda solicitud de subdominio deberá ser realizada a través de un correo electrónico dirigido a la Unidad con copia al director de Tecnologías de Información y Comunicaciones, con el fin de validar su disponibilidad. Adicionalmente se deberá establecer el ámbito de publicación de cada dominio y subdominio, es decir intranet, internet o ambos a manera de definir su alcance; todo nuevo dominio a publicar en internet e intranet, deberá ser notificado al equipo de seguridad, para realizar su respectivo análisis de vulnerabilidades, además de contar con software o herramientas para la protección del mismo.

3. Correo electrónico y plataforma de trabajo colaborativo

Será responsabilidad de la Unidad de Redes y Telecomunicaciones de la DTIC configurar y administrar el servicio de correo electrónico y la plataforma de trabajo colaborativo para el personal usuario del MINSAL. El acceso a estos servicios se realizará por medio de los mecanismos de autenticación para empleados, descritos en el romano IX numeral 1.

Toda solicitud para este servicio deberá apegarse a las siguientes disposiciones:

3.1. Creación de cuenta de correo electrónico institucional:

En hospitales nacionales y regiones de salud a nivel nacional; las solicitudes de creación de cuenta de correo electrónico institucional serán canalizadas a través del personal informático en sitio designado a cada establecimiento, e ingresarán las peticiones por medio de un formulario designado por la Unidad de Redes y Telecomunicaciones.

En el Nivel Superior, las solicitudes de creación de cuenta de correo electrónico deberán realizarse a través del correo electrónico: gestiondecorreos@salud.gob.sv y conectividad.dtic@salud.gob.sv, por medio de la Dirección de Recursos Humanos o jefaturas correspondientes, de acuerdo a la contratación.

3.2. Eliminación de cuentas de correo electrónico institucional:

Las eliminaciones de las cuentas de correo electrónico institucional deberán ser reportadas por la Dirección de Recursos Humanos, indicando el nombre completo, fecha de salida del recurso de la institución y correo electrónico institucional.

3.3. Reactivación de cuentas de correo electrónico institucional:

La reactivación de una cuenta de correo electrónico post eliminación, deberá ser solicitada a través del correo electrónico: dtic.conectividad@salud.gob.sv y gestiondecorreos@salud.gob.sv con el visto bueno del jefe inmediato, donde justifique el uso del correo electrónico institucional.

3.4. Modificación de cuentas de correo electrónico institucional:

La modificación de una cuenta de correo electrónico institucional deberá ser solicitada a los correos electrónicos: dtic.conectividad@salud.gob.sv y gestiondecorreos@salud.gob.sv.

La cantidad de espacio de almacenamiento asignado para cada cuenta, se realizará en función de las posibilidades de equipamiento servidor disponible y las diferentes necesidades, de acuerdo al cargo nominal y/o funcional, pudiendo solicitarse un ajuste de dicha cantidad por medio de la plataforma de soporte con la oportuna justificación.

La Unidad de Seguridad de la DTIC deberá contar con las medidas de control para contrarrestar el spam en las cuentas de correo, así como los medios disponibles para garantizar el doble factor de autenticación, con ello agregando una medida óptima para garantizar la integridad de las cuentas de los distintos usuarios.

4. Servicios de comunicaciones digitales de voz

Telefonía móvil

Previo visto bueno del Titular; la DTIC autorizará la asignación de equipos celulares, con el levantamiento de acta de entrega del equipo firmada por el usuario receptor del equipo.

Las solicitudes de nuevas líneas, reprogramación de SIM, cambio de línea o equipo; se deberá realizar al correo electrónico dtic.conectividad@salud.gob.sv de la Unidad de Redes y Telecomunicaciones.

Telefonía fija

En función de la disponibilidad de equipamiento, paulatinamente la comunicación de voz tradicional (telefonía analógica), se transformará en comunicación digital de voz para todos los establecimientos de salud, siendo responsabilidad de la Unidad de Redes y Telecomunicaciones, la administración de los diferentes servidores, así como la configuración de los equipos clientes, ya sean aplicaciones físicas como de software que realice este tipo de servicio instalado en un equipo de cómputo de usuario (softphones).

Para la instalación, revisión y mantenimiento de los equipos relacionados a la comunicación de voz se contará con el apoyo de la Unidad de Soporte de la DTIC, así como del personal de las unidades de informática de las diferentes dependencias y establecimientos del MINSAL, quienes canalizarán todas las solicitudes por medio del correo electrónico asignado al área de redes y telecomunicaciones dtic.conectividad@salud.gob.sv

El manejo básico de los servidores de comunicación digital de voz de los diferentes establecimientos y dependencias, corresponderá al personal informático encargado en cada establecimiento. Dicho personal será oportunamente capacitado por la Unidad de Redes y Telecomunicaciones.

Será responsabilidad de la Unidad de Redes y Telecomunicaciones, gestionar la auditoría de las configuraciones y copias de respaldo a la Unidad de Seguridad, para el caso de auditorías y Unidad de Servidores, en el caso de necesitar espacio para el almacenamiento de copias de respaldo.

VIII. Seguridad de la información

Todos los equipos de cómputo y los datos que estos contienen, corren el riesgo de tener accesos no deseados o bien sufrir mal funcionamiento, debido a vulnerabilidades inherentes a las aplicaciones, al sistema operativo o incluso por descuido o exceso de confianza de los propios usuarios.

La Unidad de Seguridad tiene como uno de sus propósitos principales, evitar en lo posible el suceso de cualquiera de las antedichas problemáticas, implementando para ello políticas y mecanismos tecnológicos, que protejan preventivamente la información de los equipos de cómputo, así como su funcionamiento normal, libre de amenazas externas e internas, hasta el punto en que esto sea razonablemente posible.

Adicionalmente, la Unidad Seguridad será la responsable de investigar a posteriori, cualquier problema de seguridad en TIC sucedido y a tal fin, informar a las autoridades respecto de la vulnerabilidad detectada y las medidas correctivas que impedirán la repetición del acontecimiento.

1. Autenticación

Será responsabilidad de la Unidad de Seguridad implementar, paulatinamente, un mecanismo de autenticación único basado en un servicio de directorio de identidades, el cual estará preferiblemente distribuido, para evitar que un problema de comunicación en la intranet afecte al funcionamiento del servicio.

El acceso a cualquier equipo de cómputo propiedad del MINSAL, así como a los diferentes servicios y sistemas de información disponibles, deberá estar validado contra este servicio, por lo que será obligatoria la asignación de un usuario y clave a todos los empleados del MINSAL, independientemente de su tipo de contratación. Dicho acceso será cesado a la mayor brevedad posible cuando la persona deje de tener un vínculo laboral con el MINSAL, por lo que se deberá intentar automatizar la creación y cierre de cuentas, con la información proveniente de los sistemas de información de administración de recursos humanos. Si dicha información no fuera accesible de forma automática por algún motivo, la Dirección de Recursos Humanos deberá suministrar mensualmente la planilla de empleados, en el formato que la Unidad de Seguridad determine. Un empleado también podrá presentar documentación que acredite su vínculo laboral con el MINSAL, para que su cuenta pueda ser creada en un plazo más corto.

Además de la validación de identidad del usuario, paulatinamente se utilizará el servicio de directorio de identidades, para la obtención de nivel de acceso y rol de dicho usuario en los diferentes sistemas de información institucionales y/o módulos del Sistema Único de Información en Salud.

2. Certificados digitales

Con el fin de garantizar la seguridad, privacidad e identidad en el acceso a los diferentes sistemas de información y servicios ofrecidos por la DTIC, dichos servicios serán encriptados, utilizando certificados digitales válidos, emitidos a favor del MINSAL. En caso de que el Estado de El Salvador carezca de una autoridad certificadora propia, será responsabilidad de la Unidad de Servidores y Bases de Datos, la gestión para la adquisición e implementación de los certificados digitales raíz del MINSAL. Los cuáles serán seleccionados en proceso de licitación pública, a fin de garantizar la sana competencia de tal manera que los certificados sean los idóneos en base a las especificaciones técnicas y cumplan con los estándares actuales encriptación de datos

Adicionalmente, dichos certificados podrán considerarse válidos para la implementación de la firma digital de documentos y actos que actualmente requieren la identificación de la persona autorizada para realizarlos. Ello será posible siempre y cuando existan los mecanismos tecnológicos suficientes para garantizar con suficiente certeza que la persona firmante vía digital es en efecto el usuario de su propia firma digital. Los actos firmados digitalmente en los sistemas de información del MINSAL serán equivalentes a la firma y sello manual para efectos de autenticación inmediata y auditorías posteriores.

3. Seguridad física y lógica

Todos los equipos de cómputo deberán contar con las suficientes medidas de seguridad física, que la infraestructura del edificio que los contiene permita, siendo responsabilidad de la Unidad de Seguridad, asesorar a las autoridades de los diferentes establecimientos y dependencias, sobre defectos de seguridad física, para su corrección a la brevedad posible.

En el caso de equipos de cómputo de usuario, tal como se define en el romano VI numeral 3, la administración de los equipos y por tanto la seguridad lógica, corresponde a la Unidad de Soporte y Bases de Datos, quien, en coordinación con la Unidad de Seguridad, definirán la configuración y medidas necesarias para garantizar que el uso de las aplicaciones y sistema operativo sea seguro.

En lo que respecta a la utilización del bloqueo automático de las sesiones de escritorio, tras la ausencia de actividad del usuario con fines de seguridad (además del consecuente ahorro de energía), será definido por la jefatura o autoridad de cada dependencia, el tiempo óptimo para la activación de dicho mecanismo de protección, según la presencia de personal ajeno al área y necesidades particulares de confidencialidad, en función de las labores y privacidad de los datos de dicha dependencia.

En cuanto al equipo servidor, la responsabilidad de implementación de las medidas de seguridad lógica necesarias a nivel de servidor, contra intentos de acceso indebido o ataques de denegación de servicio, será de la Sección de Administración de la Unidad de Servidores y Base de Datos de la DTIC.

En cualquier caso, la Unidad de Seguridad deberá disponer del equipamiento y recursos humanos necesarios y suficientes para implementar medidas preventivas de protección contra estas problemáticas a nivel de toda la red del MINSAL, tanto en la intranet como en el acceso desde internet.

4. Mecanismos de protección contra software malicioso (malware)

Es responsabilidad de la Unidad de Seguridad, disponer de los mecanismos de protección contra programas de cómputo de propósito maligno o inconveniente (virus, programas espía, publicidad no solicitada en navegación y correo electrónico, entre otros).

En función de los diferentes grados de vulnerabilidad de los sistemas operativos y aplicaciones existentes en las computadoras del MINSAL, se aplicarán diferentes medidas de protección, siendo en cualquier caso indispensable, la configuración de las actualizaciones automáticas del sistema operativo y otro software. En caso de computadoras aisladas de la red, estas actualizaciones se realizarán en las actividades de mantenimiento preventivo definidas en el romano VI literal 1.

En los casos de sistemas operativos vulnerables a programas malignos, que necesiten de herramientas de protección adicionales, la Unidad de Seguridad de la DTIC, preverá la adquisición de estas herramientas de protección (antivirus y otras), para toda la institución y sus dependencias. Dichas herramientas deberán ser configuradas para su actualización periódica a través de la red con la mayor frecuencia posible. Anualmente se evaluarán las diferentes

opciones de herramientas de protección contra programas malignos libres y privativas, escogiendo la más idónea, tomando en cuenta el presupuesto disponible y las estrategias de desarrollo tecnológico de la DTIC, para así garantizar el mejor desempeño de los equipos de cómputo del MINSAL.

La instalación y configuración de las herramientas descritas anteriormente es responsabilidad de los técnicos informáticos de la instancia correspondiente, bien la Unidad de Soporte de la DTIC o la unidad de informática local, comunicándose con la Unidad de Seguridad de la DTIC, para cualquier necesidad específica o eventualidad al respecto de estas aplicaciones.

Es de especial importancia, remarcar que dentro de las actividades de mantenimiento preventivo de todos los equipos, deben revisarse la actualización de todos los componentes de software del equipo informático, así como el buen funcionamiento y actualización de las aplicaciones contra programas malignos.

IX. Sistemas de información

La Unidad de Desarrollo de la DTIC, será la responsable de analizar, diseñar, desarrollar, mantener e implementar el sistema de información del MINSAL en toda su extensión, el cual deberá responder a la estructura organizativa, procedimientos y las políticas que emita el Ministerio. Además será su exclusiva responsabilidad la evaluación de idoneidad sobre el uso y desarrollo de cualquier aplicación informática y su correspondiente aceptación para implantación, con excepción de las aplicaciones relacionadas con el ámbito de los servicios de salud, los programas sanitarios y la vigilancia sanitaria, que serán una responsabilidad compartida con la dependencia responsable de dichos sistemas y con la Unidad de Estadística e Información en Salud de la Dirección de Epidemiología, así como la Dirección de Monitoreo Estratégico, ya que es esta quién valida la mayor parte de lo referente al ámbito clínico; como a quien evaluará su adecuación en cuanto a la administración, captura y utilización de la información de dichas aplicaciones.

1. Desarrollo de sistemas de información

1.1. Solicitud de desarrollo de nuevas aplicaciones

Las dependencias del MINSAL que requieran el desarrollo de nuevos sistemas, deberán enviar a la Unidad de Desarrollo de la DTIC, solicitud de desarrollo, a la que se adjuntará un anteproyecto en forma digital bajo estándar Oasis OpenDocument, en el que se defina el perfil general del sistema a desarrollar y su alcance, ello con el fin de evaluar la factibilidad del proyecto. Este documento se elaborará en conjunto con la Unidad de Desarrollo.

El anteproyecto será conformado de las siguientes partes:

- Introducción.
- Antecedentes.
- Justificación.
- Objetivos.
- Alcances.

- Descripción del sistema.
- Estudio de factibilidad: económica y operativa. (Cuando ello aplique según el usuario final).
- Responsables del proyecto.
- Licencia del sistema. (Definido por DTIC)

La Unidad de Desarrollo evaluará la factibilidad del proyecto, junto con las dependencias involucradas en el proceso a desarrollar, a las cuales se les denominará dependencias usuarias o participantes, y notificará la resolución de ésta a la dependencia solicitante. Si la resolución es favorable se nombrará un comité técnico responsable de la gestión del proyecto desde la fase de análisis hasta su implementación.

Dicho comité estará formado por personal representante de la Unidad de Desarrollo de la DTIC, personal de la dependencia solicitante o responsable y personal representante de las dependencias usuarias. Si la resolución no es favorable se comunicará a la dependencia solicitante para realizar una revisión del anteproyecto o bien para archivar la solicitud.

En cuanto a la licencia de los sistemas de información y aplicaciones desarrolladas por la DTIC, ésta deberá ser bajo licencia GNU/GPL en su versión 3 (o posteriores) o compatible con ella, que permita a otras personas físicas o jurídicas estudiar, utilizar y adaptar la herramienta a sus necesidades, así como la publicación de estas modificaciones bajo los mismos términos libres con los que tales instancias obtuvieron la herramienta.

1.2. Análisis y diseño

El propósito de esta etapa es conocer exactamente cómo trabaja el sistema actual (manual o mecanizado), determinar y documentar qué debe hacer el nuevo sistema y recomendar las posibles soluciones.

La Unidad de Desarrollo de la DTIC será la responsable de proponer la solución informática, para la solicitud requerida por la dependencia solicitante, cuyo primer elemento, consistirá un documento de análisis que recopile los requerimientos de información de las dependencias solicitante y participante, en el cual definirá la solución propuesta. Este documento de análisis contendrá los siguientes apartados:

- Descripción de la problemática a resolver y propuesta de solución.
- Alcance detallado del sistema.
- Requerimientos de software y hardware (lado cliente y servidor).
- Diagramas UML, especialmente:
 - Historias de usuario.
 - Diagramas de caso de uso.
 - Descripción de casos de uso.
 - Product Backlog.
 - Sprint Backlog.
 - Estándar de diseño, fuentes, colores, iconografía.
 - Diagrama de procesos BPMN.
 - Acta de aceptación de prototipo.
 - Cambios al prototipo por el usuario.
 - Acta Validación interna de DTIC.

- Acta de aceptación de producto funcional implementado o en pilotaje.
- Cronograma estimado de entregas.
- Estimación de necesidades para la sostenibilidad del sistema (recursos humanos y otros).

Se deberá determinar qué requerimientos de tecnología de información (hardware, software, redes) y de recursos humanos serán indispensables para que el sistema opere correctamente.

En cuanto al software requerido para desarrollar el sistema y su posterior puesta en producción, éste necesariamente deberá ser software bajo licenciamiento libre y gratuito, exceptuando el caso de sistemas de información anteriores a la aprobación de los presentes Lineamientos técnicos y/o circunstancias muy específicas que requieran de funcionalidades no existentes, ni en todo ni en parte, en plataformas libres y gratuitas, las cuales deberán justificarse oportunamente en el documento de análisis.

Independientemente de la plataforma elegida para el desarrollo y puesta en producción del sistema de información, se deberá garantizar un funcionamiento óptimo de cara a la persona usuaria sobre plataformas completamente basadas en software libre y gratuito, no obstante, se procurará también un adecuado rendimiento sobre plataformas basadas en software privativo, sin embargo, esto último no es obligatorio.

1.3. Desarrollo

La Unidad de Desarrollo de la DTIC, será la responsable del desarrollo del software basado en el documento de análisis, y entregará la documentación técnica del sistema desarrollado, comprendiendo:

- Esquema de la base de datos o tablas nuevas si ya existiera sistema
- Diccionario de datos

El sistema deberá incluir módulo de seguridad, controles, niveles de acceso, bitácora de eventos y las medidas necesarias para conservar la integridad de la información. En cuanto a la validación de acceso y niveles de privilegios, se utilizará preferentemente el servicio de autenticación, basado en el directorio de identidades definido en el romano IX literal 1.

Previo aprobación de QA puede pasar a mostrarse al comité técnico. Los diferentes avances en el desarrollo del sistema para su aprobación y seguimiento.

1.4. Pruebas e implementación

Se realizarán pruebas en cada dependencia participante, para verificar que el sistema de información cumpla y cubra lo especificado en el documento de análisis. También se llevarán a cabo pruebas integrales, donde se verificará el sistema en su totalidad, las cuales deberán quedar debidamente documentadas y validadas.

La implementación del sistema será responsabilidad del comité técnico y la DTIC. En el caso de implementarse el sistema en los establecimientos de salud se nombrará un comité técnico que

apoyará el proceso. Cada dependencia participante operará los módulos del Sistema que le correspondan.

La Unidad de Desarrollo elaborará los manuales técnicos y de usuario necesarios y suficientes, para la administración técnica y la utilización de los sistemas de información en producción.

2. Solicitud de cambios en sistemas de información existentes

Cualquier solicitud de nuevos módulos, funcionalidades o modificaciones al sistema por parte de las dependencias responsables, deberá solicitarse a la DTIC, quien notificará al comité técnico, para su conocimiento y validación.

La dependencia responsable notificará a los usuarios de las dependencias participantes de las nuevas funcionalidades del sistema.

3. Generación de información gerencial

Es responsabilidad de la Unidad de Ciencia de Datos, generar información gerencial, de forma oportuna y confiable, para facilitar la toma de decisiones en los diferentes niveles organizativos, especialmente en el nivel estratégico o gerencial del Ministerio de Salud. Normalmente, la información gerencial debe ser visible por medio de tableros de mando.

Las dependencias del MINSAL que requieran el desarrollo de nuevos tableros de mando, deberán tener gobernanza sobre los datos del sistema de información que será la fuente de datos y además realizar una solicitud de desarrollo, dirigida a la Unidad de Ciencia de Datos y a la Unidad de Requerimientos y QA de la DTIC. En dicha solicitud se deberán detallar la información que requieren visualizar en el tablero de mando, cual sistema de información será la fuente de datos determinando campos y/o variables a utilizarse.

Para generar la información gerencial, la Unidad de Ciencia de Datos debe desarrollar herramientas que sean efectivas, eficientes y eficaz para realizar lo siguiente:

- Extraer los datos de los sistemas de información que están en producción.
- Realizar una limpieza, depuración y transformación de la información extraída de los sistemas de información.
- Efectuar el almacenamiento centralizado de la información que fue limpiada, depurada y transformada.
- Facilitar la visualización de la información en medios digitales (generalmente por medio de tableros de mando).

Es responsabilidad de la Unidad de Ciencia de Datos investigar, probar e implementar nuevos softwares de análisis de datos (con preferencia en software libre), con el objetivo de innovar y optimizar las herramientas que permiten generar la información gerencial.

Para generar la información gerencial, la Unidad de Ciencia de Datos trabaja en coordinación con las Unidades de Desarrollo de Sistemas de Información, de Redes y Telecomunicaciones, de Seguridad, de Servidores, de Requerimientos y QA.

4. Donaciones y desarrollos externos de software

Los sistemas informáticos donados y/o desarrollados por terceros a las dependencias o establecimientos del MINSAL, deben ser aprobados por la DTIC y la dependencia beneficiaria para garantizar que cumple con las necesidades de requerimientos de información, compatibilidad con la estructura tecnológica del Ministerio y su sostenibilidad.

La institución donante y/o desarrolladora entregará a la DTIC:

- Un documento que autorice e indique los términos de licenciamiento y uso. Si no se conceden explícitamente todos los derechos patrimoniales o económicos de autor al MINSAL, al menos debe licenciarse el software bajo una licencia libre, preferiblemente GNU/GPL v3 o subsecuente.
- Código fuente.
- Manual técnico de análisis y diseño del sistema.
- Manual de usuario.
- Manual de instalación, configuración y administración.

5. Administración de sistemas y bases de datos

La dependencia responsable del sistema será la responsable de su administración, salvo en los casos que se determine otra fórmula por acuerdo del comité técnico.

La dependencia responsable será la encargada de la administración de uso del sistema, por medio del cual podrá autorizar a todas las dependencias participantes, el acceso a la información y módulos que en el proceso requiera para su operación.

La custodia y administración técnica de las aplicaciones que componen los diferentes sistemas de información en producción del MINSAL serán responsabilidad exclusiva del área de Administración de la Unidad de Desarrollo de la DTIC.

La custodia y administración de las bases de datos de los diferentes sistemas de información en producción del MINSAL, serán responsabilidad exclusiva del área de administración de la Unidad de Servidores y Bases de Datos de la DTIC.

Este procedimiento abarca a las áreas de Desarrollo de Software y Ciencias de Datos de la DTIC del MINSAL; quienes iniciarán con la remisión de la solicitud de acceso proveniente de la jefatura y finalizará con la autorización del acceso.

6. Capacitación y soporte técnico de los sistemas de información

La dependencia responsable dará soporte técnico directo a los usuarios de las dependencias participantes donde los sistemas de información se instalen. Adicionalmente, en coordinación con las Unidades de Sistemas de Información y de Soporte (sección de atención a usuarios y formación) de la DTIC, se proveerán de las capacitaciones necesarias para el uso de los sistemas de información.

En caso de mal funcionamiento o comportamiento imprevisto de los sistemas, la persona usuaria que detectó el inconveniente es la responsable de abrir el caso en la plataforma de soporte, comunicando oportunamente a la dependencia responsable si el problema no tiene solución a corto plazo. La Unidad de Desarrollo podrá convocar al comité técnico para evaluar el caso, cuando éste requiera un esfuerzo excepcional o sea en la práctica un nuevo requerimiento que deba ser analizado con la atención debida.

Es de carácter obligatorio que para poder acceder a los diferentes sistemas de información del MINSAL se debe hacer uso del correo electrónico institucional o de sus credenciales institucionales, con el objetivo que el técnico responsable pueda atender las solicitudes oportunamente.

Toda solicitud de accesos y/o permisos a sistemas deberá realizarse a través de correo electrónico, memorándum o nota. Las solicitudes para la creación de usuarios deberán incluir los siguientes requisitos mínimos: nombre completo, dependencia solicitante y correo electrónico en el caso que fuese requerido.

Será responsabilidad de la Unidad de Soporte, a través del Soporte Técnico de Sistemas de Información, la coordinación de las capacitaciones que se imparten a los usuarios de los sistemas y asimismo, de la elaboración de los manuales de usuario para cada sistema.

7. Administración de sitio web institucional

Será responsabilidad de toda dependencia o establecimiento del MINSAL, previo a la publicación de la información en el sitio web institucional, dar cumplimiento a lo siguiente:

- Designar al técnico, encargado, jefatura o autoridad responsable de revisar adecuadamente la información, que será publicada en el sitio web institucional. Los archivos que serán enviados para dicha publicación deben ser de los siguientes tipos: html, Oasis OpenDocument - ISO/IEC 26300:2006 y subsecuentes (odt, ods, odp), Office Open XML - ISO/IEC 29500:2008 y subsecuentes (docx, xlsx, pptx), PDF - ISO/IEC 32000-1:2008 y subsecuentes, gráficos (svg, jpg, gif, png), multimedia (mp4, mp3, ogg, avi, mpg, ogv). La publicación final de documentos se realizará en formato PDF, para garantizar una fiel visualización e impresión de los mismos, bajo cualquier plataforma y, en caso de ser oportuna la publicación de algún documento en formato fuente, deberá ser autorizado por la dependencia solicitante y será publicado al menos bajo estándar Oasis OpenDocument.
- Cuando ello aplique, los documentos remitidos, independientemente de su formato, deberán establecer los términos de licenciamiento de su contenido bajo una licencia Creative Commons que garantice al menos la obligatoria mención de autoría y redistribución libre de los documentos publicados.
- Cualquier publicación eventualmente podrá necesitar ser consultada con las instancias responsables de edición y relaciones públicas (Unidad Editorial, Dirección de Comunicación Social e Institucional, Oficina de Relaciones Internacionales y Cooperación en Salud, entre otros) o incluso al Despacho Ministerial, lo cual será oportunamente advertido a la dependencia solicitante. Las dependencias del MINSAL deberán contactarse con la Dirección de Comunicación Social e Institucional, para su revisión y avalen la publicación de la información, podrá hacer observaciones pertinentes a lo que haya de ser publicado.

- Las dependencias o establecimientos del MINSAL serán responsables de revisar periódicamente la información publicada en el sitio web institucional, con el objeto de mantener el sitio actualizado; delegando a una persona de la dependencia que supervise los contenidos de los documentos que les competan en comunicación directa con la jefatura correspondiente.
- Previo visto bueno de la jefatura de la dependencia, será posible delegar la autorización de publicación al personal técnico de las dependencias y establecimientos, lo cual implica que dicha dependencia seguirá los lineamientos establecidos para emitir cualquier comunicado, tanto interna como externamente.
- En el caso de que la información publicada se necesite modificar o eliminar, esta solicitud deberá hacerse únicamente a través de la plataforma de soporte técnico e informando vía correo electrónico a la dirección del administrador web, para realizar las acciones respectivas.

8. Administración de servidores

Es responsabilidad de la Sección de Administración de la Unidad de Servidores y Bases de Datos, así como del personal técnico de las unidades de informática de los establecimientos y dependencias, mantener adecuadamente los equipos al servicio de los diferentes sistemas de información y recursos de red.

Se aplicará la misma política de mantenimiento preventivo general descrito en el romano VI numeral 1 y, además, todos los servidores deben contar con un monitoreo permanente al menos en los siguientes aspectos:

- Espacio en disco.
- Actualizaciones de software y de sistema operativo.
- Intentos de violación a la seguridad.
- Uso de CPU y memoria RAM.C
- Conectividad a la red.
- Rendimiento del equipo, aplicaciones y base de datos.
- Disponibilidad.
- Eventos de sistema operativo.

En ningún caso se permitirá el acceso remoto directo con privilegios de administración, y es obligatoria la disposición de medidas para el bloqueo de la conexión ante intentos de entrada no autorizados, tal como se indica en el romano IX literal 3.

Todos los servidores deben ser respaldados periódicamente en sus datos, aplicaciones y configuración. Este punto se detalla en el literal 9 a continuación.

9. Respaldo de información

La información a respaldar en los servidores de los sistemas de información administrados por la Unidad de Servidores y Bases de Datos, en conjunto a la Unidad de Seguridad, comprende los siguientes elementos:

- Archivos de aplicación y/o código fuente.
- Base de datos y/o archivos de datos.
- Configuración del sistema operativo, sistemas de información y aplicaciones accesorias.
- Alojamiento de archivos documentales, multimedia y herramientas de carácter institucional.
- Configuración de equipos de infraestructura (Dispositivos de capa 2, capa 3) y seguridad (Firewall, soluciones de antivirus, entre otros).
- Configuración y datos de herramientas de monitoreo.

Todos los respaldos de la información se mantendrán en los propios servidores y además deberán transferirse automáticamente a un depósito principal situado en la sala de servidores de la DTIC, el cual deberá tener al menos un espejo en otra ubicación fuera del área metropolitana con el fin de garantizar la disponibilidad de la información.

Las rutinas de respaldo se realizarán de forma automática o programada y deberán ser monitorizadas permanentemente a través de bitácoras. Dichas rutinas, en función de un uso óptimo del espacio de almacenamiento, capacidad total de almacenamiento del ancho de banda que interconecte los servidores con el depósito principal, resguardando respaldos completos e incrementales según sea oportuno, así como la frecuencia de ejecución y limpieza de archivos de respaldo obsoletos.

X. Unidades de informática

En aquellas dependencias o establecimientos que tengan un volumen considerable de equipos de cómputo, y por tanto un vínculo directo del buen funcionamiento de estos para las labores normales, en caso de no existir, debe crearse una unidad de informática con suficientes recursos humanos cualificados para dar soporte a la infraestructura de TIC's existente y venidera.

En la actualidad, y sin menoscabo de la asunción compartida de esta responsabilidad por parte de la DTIC, la contratación de recursos humanos de la unidad de informática deberá ser por cuenta del establecimiento o dependencia. Aplican en este sentido las siguientes consideraciones:

- Un cálculo del número y funciones de las personas integrantes de la unidad de informática puede ser solicitado a la DTIC, evaluando la cantidad de equipo y necesidades específicas del establecimiento.
- La DTIC formará parte del comité evaluador para colaborar en la selección del personal idóneo, que compondrá la unidad de informática.
- Debe evitarse la contratación por servicios profesionales y/o tiempos incompletos, siempre que sea posible y se ubicará al personal en la plaza más adecuada, según las funciones asignadas. .
- Las personas que formen parte de la unidad de informática estarán en permanente contacto con la DTIC, para realizar un ejercicio coordinado de sus funciones, pues el desarrollo, seguridad y soporte de las TIC's del MINSAL, será una labor armonizada entre la DTIC y las unidades de informática de las respectivas dependencias y establecimientos.

1. Dependencia jerárquica

Debido a la relevancia, transversalidad y rol estratégico de las labores de la unidad de informática, ésta dependerá preferiblemente de la Dirección o, como mínimo, de la administración del establecimiento.

En el caso de que existan recursos humanos responsables de las labores informáticas del establecimiento, y éstos dependan de otras unidades operativas, como la Unidad Financiera Institucional, Estadística, entre otros, se debe proceder a la brevedad posible con la creación de la unidad de informática y la ejecución del correspondiente traslado.

2. Composición

La unidad de informática tendrá una jefatura, y la persona que ostente tal cargo deberá participar en reuniones con la DTIC, donde contará con voz y voto para la toma de decisiones que afecten al funcionamiento general del desarrollo tecnológico de la Institución. Igualmente será responsable del conocimiento y ejecución de dichas decisiones al interior del establecimiento que represente, así como otros lineamientos específicos emitidos por el MINSAL.

Además de la jefatura, la unidad de informática podrá contar con otros recursos humanos de soporte técnico y administración, análisis y programación de sistemas de información según sea la complejidad y necesidades del establecimiento.

3. Infraestructura y equipamiento

La unidad de informática debe contar con un área para el trabajo administrativo de su personal. Cada persona integrante de la unidad debe contar con el mobiliario básico de oficina, un equipo de cómputo fijo o portátil actualizado con conexión a intranet e Internet y las herramientas necesarias (hardware y software), para brindar los servicios de soporte y/o desarrollo, según sea el caso.

Además del área administrativa de la unidad de informática, debe asignarse un área independiente para que se instale el centro de datos principal, en el que las personas responsables de la unidad de informática realizarán labores de instalación, revisión y mantenimiento de los equipos de red y de los servidores que contienen los sistemas que su establecimiento utilice. Dicha área debe cumplir con las siguientes características:

- Fácil acceso: Para que las personas asignadas de la Unidad de Informática o de la DTIC, si fuera necesario, puedan llegar oportunamente y sin ningún tipo de contratiempo, a la hora que sea necesario.
- Seguro: Debe brindar la seguridad necesaria para que los equipos instalados no puedan ser accesibles a personas no autorizadas, así como para evitar que sean sustraídos.
- Ambientación adecuada: Este lugar debe evitar que los equipos no sufran daños ante las inclemencias del tiempo, tales como la lluvia, polvo, entre otros, y eventualmente estará dotado de aire acondicionado, el cual trabajará las veinticuatro horas del día, según el tipo de equipamiento contenido.

4. Funciones y actividades

Será función de la unidad de informática hacer del conocimiento del personal de su establecimiento o dependencia las normativas, lineamientos, acuerdos específicos y estrategias de tecnologías de información y comunicaciones dispuestos por la DTIC, así como de su consecuente y puntual ejecución. También será responsable de las siguientes actividades en su dependencia o establecimiento, todo ello en coordinación y bajo los lineamientos y estrategias emitidos por la DTIC:

- Analizar y dar el visto bueno técnico de las compras de equipos informáticos, accesorios relacionados y software de la dependencia o establecimiento a la que la unidad pertenece. El análisis y visto bueno de las compras de equipos informáticos, accesorios relacionados y software de las dependencias del Nivel Superior, corresponde únicamente a la DTIC.
- Ofrecer el soporte técnico del equipo, aplicaciones informáticas y módulos del Sistema Único de Información en Salud.
- Colaborar con la administración de la infraestructura de comunicaciones.
- Colaborar con la implementación y funcionamiento de la seguridad informática en sus establecimientos.
- Asignar el correcto nombre al equipo, así como tener la responsabilidad de mantener sus equipos actualizados, minimizando las vulnerabilidades que pueda ocasionar.
- Coordinar las actividades de capacitación a los usuarios en el uso de equipos informáticos, aplicaciones y sistemas de información.
- Evaluar y sugerir la incorporación de nuevas tecnologías a la DTIC y sus autoridades, así como proponer políticas y estrategias adecuadas para el desarrollo de planes y actividades de la Unidad.

XI. Planes de contingencia

La DTIC y las unidades de informática de los establecimientos o dependencias del MINSAL, con el objeto de minimizar las situaciones que pongan en peligro los recursos informáticos, así como el normal funcionamiento de las redes de cómputo, deben elaborar en función de posibilidades presupuestarias realistas un plan de contingencia que contenga entre otros aspectos los siguientes componentes:

- Identificar los factores de riesgo que afecten las instalaciones informáticas que se están analizando.
- Efectuar una valoración de riesgos de las instalaciones donde se encuentran los equipos informáticos.
- Identificar las medidas necesarias para el tratamiento, reducción o disminución de los factores de riesgo resultantes de la valoración de riesgo.
- Elaborar el plan de contingencia que incluya las etapas del antes, durante y después del evento.
- Divulgar el plan de contingencia a los técnicos informáticos para que conozcan las actividades a realizar en caso de un evento.
- Revisar, una vez al año, el plan de contingencia para su actualización.

- Las unidades deberán realizar, una vez al año, las pruebas de funcionamiento de los planes de contingencia, en sus diferentes facetas.
- Elaborar listado del personal de turno en casos fortuitos, detallando personal interno y personal externo (Proveedores).

XII. Elaboración y aplicación de normas y otras disposiciones relativas a las TIC

La Dirección de Tecnologías de Información y Comunicaciones, es la única instancia autorizada para elaborar y revisar cualquier disposición o normativa relacionada con el mantenimiento, administración y desarrollo de tecnologías de información y comunicaciones en el MINSAL, coordinando esta labor oportunamente con la Dirección de Regulación.

Las jefaturas de las unidades y el personal de sus diferentes áreas, tendrán la responsabilidad de llevar a cabo la labor de desarrollo y revisión de estas disposiciones, así como de dar el oportuno seguimiento para garantizar su cumplimiento puntual por parte de la propia DTIC, así como por parte de las personas usuarias de equipamiento de cómputo y los diferentes sistemas de información, realizando periódicamente evaluaciones a tal efecto.

Cualquier consulta, observación, reclamación o solicitud de modificación relativa a las normativas aplicables a las TIC, serán dirigidas a la unidad correspondiente, quien convocará al director de la DTIC y otras personas de las unidades de la DTIC responsables de la aplicación del aspecto concreto consultado para su revisión y eventual modificación.

XIII. Terminología

- Datos informáticos: es cualquier representación de hechos, información o conceptos en un formato digital o análogos, que puedan ser almacenados, procesados o transmitidos en un sistema informático, cualquiera que sea su ubicación, así como las características y especificaciones que permiten describir, identificar, descubrir, valorar y administrar los datos.
- Datos personales sensibles: son los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral, familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la propia imagen, a la intimidad personal y familiar.
- Delito informático: se considerará la comisión de este delito, cuando se haga uso de las tecnologías de la información y la comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información.
- Dispositivo: es cualquier mecanismo, instrumento, aparato, medio que se utiliza o puede ser utilizado para ejecutar cualquier función de la tecnología de la información y la comunicación.
- Firma digital o electrónica: esquema matemático que sirve para demostrar la autenticidad y/o integridad de un mensaje digital o de un documento electrónico, dando

al destinatario seguridad en que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión.

- Hardware: corresponde a todas las partes tangibles de una computadora, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos y cualquier otro elemento físico involucrado.
- Licencia libre: Licencia de software aceptada por la Fundación del Software Libre (en inglés Free Software Foundation) y/o compatible con la GNU/GPL.
- Malware: Programas de tipo vírico, espías, publicidad no deseada, entre otros.
- Medio de almacenamiento de datos informáticos: es cualquier dispositivo a partir del cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin la ayuda de cualquier otro medio idóneo.
- Programa informático: es la rutina o secuencia de instrucciones en un lenguaje informático determinado que se ejecuta en un sistema informático, pudiendo ser éste un ordenador, servidor o cualquier dispositivo, con el propósito que realice el procesamiento y comunicación de los datos informáticos.
- Sistema informático: es un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información.
- Software: conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación.
- Tecnologías de la información y la comunicación: es el conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros.

XIV. Disposiciones generales

De lo no previsto

Todo lo que no esté previsto en los presentes Lineamientos técnicos, se debe resolver a petición de parte por medio de escrito dirigido al Titular de esta Cartera de Estado, fundamentando la razón de lo no previsto, técnica y jurídicamente.

Obligatoriedad

Es responsabilidad del personal que utiliza elementos de tecnologías de información y comunicaciones en el MINSAL darle cumplimiento a los presentes Lineamientos técnicos, en caso contrario se aplicarán las sanciones establecidas en la legislación administrativa respectiva.

Derogatoria

Déjese sin efecto el Acuerdo n.º 860, del 4 de febrero de 2025, que contiene los "Lineamientos Técnicos para el Mantenimiento, Administración y Desarrollo de Tecnologías de Información y Comunicaciones".

XV. Vigencia

Los presentes Lineamientos técnicos entrarán en vigor a partir de la fecha de oficialización por parte del Titular.

A handwritten signature in blue ink is positioned to the left of a circular official seal. The seal features the national coat of arms of El Salvador and is surrounded by the text "MINISTERIO DE SALUD" at the top and "REP. DE EL SALVADOR, C.A." at the bottom.

Dr. Francisco José Alabi Montoya
Ministro de Salud ad honorem