INS03-25-0003

INSTRUCTIVO DE USO ACEPTABLE DE INTERNET

Sistema de Gobernanza de Tecnologías de la Información – Hospital de Tomé

Versión Oficial Actual 1 – Diciembre 2025

Responsable		Fecha	Firma
Elaborado	César Cáceres Urrutia Jefe Área Tecnologías de la Información	16/12/2025	

CONTENIDO

1 PROPÓSITO.

Establecer las directrices y condiciones para el uso aceptable, seguro y responsable del servicio de acceso a Internet provisto por la Institución, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información institucional, prevenir incidentes de seguridad de la información, asegurar el cumplimiento de la normativa vigente y resguardar la continuidad operativa de los procesos asistenciales y administrativos.

Este instructivo busca además concientizar a los usuarios sobre sus responsabilidades en el uso del acceso a Internet como activo de información, promoviendo prácticas alineadas con el Sistema de Gestión de Seguridad de la Información (SGSI) y reduciendo los riesgos asociados a accesos no autorizados, software malicioso, fuga de información y uso indebido de los recursos tecnológicos institucionales.

2 ALCANCE.

El presente instructivo aplica a todas las personas que utilicen el servicio de acceso a Internet provisto por la organización, independientemente de la modalidad de su vínculo contractual o funcional.

En particular, este instructivo es de cumplimiento obligatorio para:

- Funcionarios de planta y a contrata.
- Personal a honorarios, compras de servicios y otros prestadores individuales.
- Estudiantes, internos, becarios y pasantes que utilicen recursos tecnológicos institucionales.
- Proveedores, consultores y terceros que, en el marco de sus funciones o contratos, accedan a Internet mediante infraestructura, redes o dispositivos de la organización.

El alcance de este instructivo comprende el uso del acceso a Internet realizado a través de:

- Redes cableadas y redes inalámbricas (Wi-Fi) institucionales.
- Dispositivos institucionales tales como computadores de escritorio, notebooks, terminales clínicas y otros equipos conectados a la red.
- Accesos remotos autorizados, incluyendo VPN u otros mecanismos habilitados por la organización.

Las disposiciones aquí establecidas son aplicables tanto dentro de las dependencias físicas de la organización como en modalidades de trabajo remoto o fuera de las instalaciones, cuando se utilicen recursos tecnológicos institucionales o se acceda a información de la organización.

Quedan excluidos del alcance de este instructivo los accesos a Internet realizados mediante redes o dispositivos personales, ajenos a la infraestructura institucional, salvo en aquellos casos en que exista una autorización expresa y regulada por normativa interna específica.

3 TERMINOLOGÍA.

Con el fin de facilitar la comprensión del presente instructivo y asegurar una interpretación homogénea de sus disposiciones, a continuación se definen los principales conceptos y términos técnicos utilizados, los cuales deben ser entendidos en el contexto del uso de los recursos tecnológicos institucionales y del Sistema de Gestión de Seguridad de la Información (SGSI).

Las definiciones aquí contenidas tienen carácter referencial y buscan apoyar a los usuarios en el cumplimiento de sus responsabilidades, sin perjuicio de las definiciones establecidas en la normativa legal o institucional vigente.

Activo de información

- Cualquier elemento que tenga valor para la organización y que contenga, procese o permita el acceso a información, incluyendo servicios, sistemas, dispositivos, redes y datos.

Acceso a Internet

- Servicio tecnológico provisto por la organización que permite la conexión a redes externas, incluyendo la red pública de Internet, a través de su infraestructura de comunicaciones.

Usuario

- Persona autorizada para utilizar los recursos tecnológicos de la organización, independientemente de su vínculo contractual o funcional, incluyendo funcionarios, honorarios, estudiantes, proveedores y terceros.

Red institucional

- Conjunto de infraestructuras de comunicaciones, cableadas o inalámbricas, administradas por la organización y destinadas a la operación de sus procesos asistenciales y administrativos.

Dispositivo institucional

- Equipo tecnológico propiedad de la organización o asignado formalmente por esta, utilizado para el desempeño de funciones laborales o académicas, tales como computadores de escritorio, notebooks, terminales clínicas, impresoras u otros dispositivos conectados a la red.

Acceso remoto

- Mecanismo autorizado que permite a un usuario conectarse a la red institucional desde una ubicación externa, utilizando tecnologías como VPN u otros sistemas definidos por la organización.

VPN (Red Privada Virtual)

- Tecnología que permite establecer una conexión segura y cifrada entre un dispositivo externo y la red institucional, garantizando la confidencialidad e integridad de la información transmitida.

Información institucional

- Toda información generada, procesada, almacenada o transmitida en el marco de las funciones de la organización, independientemente de su formato o medio, incluyendo información administrativa, clínica, financiera y de gestión.

Incidente de seguridad de la información

- Evento o situación que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información o de los activos que la soportan.

Software malicioso (malware)

- Programa o código diseñado para causar daño, acceder de forma no autorizada, interrumpir el funcionamiento de sistemas o comprometer información, incluyendo virus, troyanos, ransomware, spyware, entre otros.

Filtrado de contenidos

- Conjunto de controles técnicos implementados por la organización para restringir o supervisar el acceso a determinados sitios web, servicios o tipos de contenido en Internet, de acuerdo con criterios de seguridad y uso aceptable.

Uso aceptable

- Conjunto de prácticas permitidas y esperadas en el uso de los activos de información, orientadas al cumplimiento de las funciones institucionales, la seguridad de la información y la normativa vigente.

SGSI (Sistema de Gestión de Seguridad de la Información)

- Marco de gestión basado en ISO/IEC 27001:2022 que establece políticas, procesos, roles y controles para proteger la información de la organización.

4 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS.

El presente instructivo se enmarca dentro de la normativa vigente de la organización y de la legislación aplicable, y su cumplimiento es obligatorio para todos los usuarios del servicio de acceso a Internet institucional. Su finalidad es asegurar que el uso de este recurso se realice de manera segura, responsable y alineada con los objetivos de protección de la información y continuidad operativa.

4.1 Referencias Internacionales y Estándares

- **ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información (SGSI)**
    - **Cláusula 5.9, 5.10 y 5.11**: Gestión de activos, uso aceptable de activos de información y devolución de activos.
    - **Control A.5.10 – Uso aceptable de la información y otros activos asociados**: Establece normas para el uso apropiado de los activos de información por parte de los usuarios.
    - **Control A.6.3 – Concienciación, educación y formación**: Obliga a la organización a capacitar a los usuarios sobre el uso seguro de los recursos de información.
    - **Control A.6.7 – Teletrabajo y acceso remoto seguro**: Define requisitos para accesos externos a la red institucional, incluyendo VPN y dispositivos autorizados.
    - **Control A.8.20 – Seguridad de redes**: Normas para proteger la infraestructura de comunicaciones, incluyendo filtrado de tráfico y control de acceso a Internet.

4.2 Políticas y Procedimientos Internos

- **Manual de Gestión de Activos**:
    - Define los lineamientos generales para el ciclo de vida de los activos de información de la organización.
    - El presente instructivo constituye un anexo operativo de dicho manual, detallando los usos permitidos y prohibidos del acceso a Internet.
- **Política General de Seguridad de la Información**:
    - Contiene directrices generales asociado a la Seguridad de la Información institucional.

- **Estatuto Administrativo y Normativa Interna Vigente (DFL 29/1984 y modificatorias)**:
    - Regula las responsabilidades y obligaciones de los funcionarios, personal a honorarios y terceros.
    - Incluye disposiciones sobre sanciones por uso indebido de recursos tecnológicos institucionales.

4.3 Otras referencias aplicables

- **Ley 19.628 sobre Protección de la Vida Privada**: Manejo de datos personales y confidenciales en entornos electrónicos.
- **Política de Continuidad Operativa y Gestión de Incidentes de TI**: Normas que garantizan la disponibilidad y resiliencia de los servicios de información, incluyendo Internet.

5 DESCRIPCIÓN DEL ACTIVO – INTERNET INSTITUCIONAL

El acceso a Internet en el Hospital de Tomé constituye un activo de información crítico, dado que habilita la conectividad necesaria para la gestión administrativa, clínica, educativa y de investigación, así como el acceso a sistemas externos requeridos para la operación de la institución. Este servicio se provee a través de la Red de Conectividad del Estado (RCE), una infraestructura privada del Estado destinada a la gestión del ejercicio público, aunque internamente se conoce simplemente como "Internet institucional" para evitar confusión con el Registro Clínico Electrónico (RCE).

Características principales:

- **Ancho de banda y enlaces:** La institución dispone de un enlace principal de 100 Mbps provisto por Entel, con un enlace redundante también de Entel, un tercer enlace de Movistar y enlaces dedicados para sistemas críticos como imagenología (con redundancia Starlink). Esta arquitectura permite continuidad operativa y alta disponibilidad de los servicios.
- **Control y monitoreo:** Toda la conectividad pasa por un **Firewall Fortigate**, que gestiona políticas de acceso, filtrado de contenidos y monitoreo de tráfico. Existen reglas de ruteo que priorizan aplicaciones críticas sobre otras, asegurando disponibilidad para procesos esenciales.
- **Acceso y rutas:** Los usuarios institucionales pueden acceder tanto a recursos internos de la RCE como a Internet público. La resolución de nombres y la salida a Internet público se realiza a través de DNS ministeriales y la MPLS del Estado, mientras que el acceso exclusivo a otros recursos internos se realiza por la LAN interna de la RCE.
- **Dispositivos conectados:** Todo dispositivo institucional autorizado puede conectarse, incluyendo computadores de escritorio, notebooks, terminales clínicas, tablets, impresoras multifunción y otros equipos conectados a la red. (Solo IP Fija)
- **Tipos de usuarios y restricciones:** Existen tres perfiles principales:
    1. **Funcionario estándar:** Uso general según los procesos administrativos y clínicos autorizados.

2. **Usuario periodista:** Accesos temporales y discretos para funciones educativas o de capacitación; algunas restricciones de contenido se flexibilizan de forma controlada.
3. **Administrador (TI):** Acceso completo para gestión y operación de la red y servicios asociados; sujeto a controles estrictos y monitoreo constante.

Valor y riesgos asociados:

- La conectividad a Internet institucional es **vital para la continuidad operativa**, la atención clínica segura y la administración eficiente del hospital.
- Riesgos asociados incluyen: acceso no autorizado, fuga de información, interrupción del servicio, exposición a malware y ataques externos.
- La gestión del activo se complementa con políticas de uso aceptable, filtrado de contenidos, monitoreo continuo y segregación de perfiles de usuario, asegurando un **equilibrio entre disponibilidad, confidencialidad e integridad de la información**.

6 DIRECTRICES DEL INSTRUCTIVOS.

6.1 Directrices Generales

Los permisos para el uso de internet estarán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada usuario.

El servicio de internet se encuentra disponible para todos los usuarios que prestan servicios a la institución, su uso es según el perfil asignado.

La asignación de perfiles es realizada por el Área de Tecnologías de la Información y Comunicaciones a través de las IPs asignadas a los equipos.

6.2 Uso aceptable de internet

- Los usuarios del Hospital de Tomé deben utilizar como primera opción los medios de conexión a Internet dispuestos por la Institución.
- En caso de falla se deben ejecutar los procedimientos de contingencia (Unidad Operaciones TI)
- En caso de fallas de las redundancias o la no existencia de las mismas, se permite el uso de canales alternativos de proveedores externos de Internet, siempre que se implementen **medidas de seguridad obligatorias**, tales como:
  - Firewall entre la institución y la salida a Internet.
  - Equipos con antivirus y antimalware actualizados.
  - Aplicación de todos los parches de seguridad disponibles.
  - Firewall activo en cada equipo de usuario.
- El uso de Internet para fines personales será **ocasional y eventual**, únicamente cuando no interfiera con las funciones laborales ni afecte la continuidad de la actividad institucional.
- No se permitirá el acceso a **redes sociales** a menos que el Comité de Comunicaciones así lo indique a personas individualizada y justificada.

- Las soluciones inalámbricas para visitantes deberán utilizar **portales cautivos**, garantizando que el acceso sea controlado y que la red de trabajo institucional permanezca aislada y protegida.
- Está prohibido **almacenar contraseñas o credenciales en los navegadores**, así como compartir información de acceso con terceros no autorizados.

6.3 Restricciones en el uso de Internet

- **Material ilegal o no autorizado:** No está permitido descargar, almacenar o distribuir material que infrinja el Ordenamiento Jurídico Nacional, el Reglamento Interno, el Código de Ética o cualquier normativa institucional vigente.
- **Redes sociales y servicios de entretenimiento:** El uso de redes sociales, servicios de streaming, chats, foros, blogs o sitios de entretenimiento requiere autorización formal de la Jefatura, del Jefe de TIC y del Encargado de Seguridad de la Información.
- **Contenido inapropiado:** Queda estrictamente prohibido acceder a páginas web con contenido pornográfico o cualquier otro contenido ilegal, inapropiado o que atente contra la seguridad y ética institucional.
- **Fines comerciales o políticos:** La conexión a Internet proporcionada por la institución no puede ser utilizada con fines comerciales, políticos o de lucro personal.
- **Propiedad intelectual y software:** No se permite transgredir la propiedad intelectual, secretos comerciales, patentes, regulaciones u otra propiedad protegida, incluyendo la instalación o distribución de software sin la licencia adecuada para el uso institucional.
- **Interferencia con servicios informáticos:** Los usuarios no deben interferir, denegar, alterar o afectar el funcionamiento de cualquier servicio informático o recurso de la institución mediante programas, scripts, comandos o cualquier otro método, ya sea interno o externo.
- **Sitios inseguros o de hacking:** Los usuarios sin autorización explícita no pueden acceder a sitios de hacking, vulnerables o reconocidos como inseguros, que puedan comprometer la confidencialidad, integridad o disponibilidad de la información institucional.
- **Divulgación de información institucional:** Está prohibido publicar información perteneciente a la institución en sitios personales o externos sin la autorización expresa del propietario de la información.
- **Introducción de software malicioso:** No se permite introducir virus, troyanos, malware, ransomware u otros programas que puedan afectar la seguridad de la red, servidores o dispositivos institucionales.

6.4 Conductas Prohibidas y Restricciones Específicas

Los usuarios de Internet institucional deben abstenerse de realizar las siguientes acciones:

1. **Daño a los servicios o redes:** Causar cualquier daño grave o inmediato que afecte la calidad, disponibilidad o estabilidad de los servicios informáticos, redes o recursos tecnológicos de la institución.

2. **Transgresión de derechos de terceros:** Violentar los derechos de cualquier persona o entidad protegida por copyright, secretos comerciales, patentes, regulaciones u otra propiedad intelectual, incluyendo la instalación, distribución o uso de software sin licencia válida para la institución.
3. **Exportación ilegal:** Exportar software, información técnica, tecnología, software de encriptación u otros activos que contravengan la legislación nacional o internacional sobre control de exportaciones.
4. **Uso para fines ilícitos:** Utilizar los activos informáticos para actividades ilegales, ilícitas o que contravengan la normativa institucional o nacional.
5. **Introducción de software malicioso:** Introducir virus, troyanos, malware, ransomware u otros programas maliciosos en la red, servidores o dispositivos institucionales.
6. **Fraude y estafas:** Realizar ofertas fraudulentas de productos o servicios utilizando recursos institucionales.
7. **Infracciones de seguridad e interrupciones de servicio:** Acceder, modificar, interrumpir o denegar servicios, servidores, cuentas o información sin autorización expresa. Esto incluye, entre otros:
    - Inspección de tráfico no autorizada.
    - Inundación de red (ping flood).
    - Falsificación de paquetes de red o información de ruteo.
    - Denegación de servicios (DoS) o cualquier acción maliciosa que comprometa la infraestructura.
8. **Monitoreo o escaneo no autorizado:** Realizar escaneos de seguridad o monitoreo de redes sin notificación previa a la unidad de seguridad o sin formar parte de sus funciones laborales autorizadas.
9. **Elusión de controles:** Evadir mecanismos de autenticación, firewall, filtrado de contenidos o cualquier medida de seguridad institucional.
10. **Divulgación no autorizada:** Proveer o compartir información institucional con terceros sin autorización formal del propietario de los datos o del Encargado de Seguridad de la Información.
11. **Acceso a contenido ilegal:** Ingresar, almacenar, distribuir o acceder a cualquier contenido con naturaleza ilegal, incluyendo terrorismo, piratería, documentos electrónicos que infrinjan derechos de autor, pornografía infantil, estafas u otros actos delictivos.
12. **Acceso no autorizado a la red:** Todo acceso a la red del estado debe estar administrado y controlado por la Unidad de Operaciones TI.
13. **Uso de otras redes:** Esta Prohibido el uso de redes alternativas como 2g a 5g o cualquier red móvil que no cumpla con el punto 6.2

6.5 Monitoreo

Toda información entrante o saliente a Internet será monitoreada y registrada, por lo que podría ser revisada y auditada sin previo aviso, si las autoridades lo consideran necesario o existen indicios justificados de brechas de seguridad.

6.6 Filtro de contenido

A fin de establecer un adecuado acceso a sitios Web, se establecerán grupos de acceso de acuerdo con perfiles de los usuarios, estos grupos corresponderán a diferentes tipos de categorías de acuerdo a una definición estándar de la industria. A modo de ejemplo y con el propósito de establecer una definición formal al respecto utilizaremos, referencialmente, la definición de filtros WSA (Web Security Appliance) que estarán permitidas en nuestros servicios de navegación.

6.6.1 Tipos de Filtros

Para todos los usuarios conectados a la red Ministerial con acceso a Internet se establecen tres niveles de acceso:

- Acceso Completo (Filtro Ético)
- Acceso General
- Acceso Restringido

La definición de los usuarios por cada uno de los filtros definidos deberá ser asignada por el Encargado de Seguridad de la Información, sin embargo, el Filtro Ético será la mínima asignación posible, esto significa que nadie en la organización podrá tener acceso a las paginas definidas en este filtro.

6.6.2 Filtro de Acceso Completo

Los usuarios que por su perfil hayan sido clasificados en el grupo de acceso Completo sólo tendrán las restricciones de navegación que corresponden al filtro Ético de la Red de Conectividad del Estado no tendrán otras restricciones, las restricciones del Filtro Ético y Completo serán las que se muestran a continuación:

Grupo	**Grupo**	**Acceso Completo**	
Categoría WSA	**Descripción Bloqueo**	**Bloqueo**	**Monitoreo**
Adult	Contenido para Adultos	X	
Child Abuse Content	Contenido de Abuso Infantil	X	
Dating	Sitio de Citas	X	
Extreme	Contenido Extremo	X	
Filter Avoidance	Sitios que utilizan protocolo Proxy para saltarse medidas de seguridad	X	
Freeware and Shareware	Sitios de descarga ilegal de software	X	
Gambling	Sitios de Casinos y apuestas en Línea	X	
Games	Sitios de juegos en Línea	X	
Hacking	Contenido de Hacking	X	
Illegal Activities	Contenido de Actividades Ilegales	X	
Illegal Downloads	Contenido de Descargas Ilegales	X	
Illegal Drugs	Contenido de Drogas Ilegales	X	
Parked Domains	Sitios que venden dominios web con problemas	X	
Pornography	Contenido de Pornografía	X	
Weapons	Sitios relacionados con armas	X	

6.6.3 Filtro de Acceso General

Los usuarios que por su perfil hayan sido clasificados en el gripo de acceso general tendrán las restricciones del filtro Ético más algunos sitios adicionales que se detallan a continuación:

Grupo	Grupo	Acceso Completo	
Categoría WSA	**Descripción Bloqueo**	**Bloqueo**	**Monitoreo**
Advertisements	Anuncios Comerciales	X	
Alcohol	Sitios de elaboración y distribución de bebidas alcohólicas	X	
Astrology	Sitios de Astrología (horóscopo, tarot, otros)	X	
Dynamic and Residential	Acceso a redes domesticas de cada residenciales	X	
Entertainment	Sitios de Entretenimiento (películas, videos, musicales, entre otros)	X	
Internet Telephony	Sitios utilizados para servicios de telefonía por internet	X	
Lingerie and Swimsuits	Sitios utilizados para compra de lencería y trajes de baño	X	
Non-Sexual Nudity	Sitios de desnudos de cuerpos humanos NO con carácter sexual	X	
Peer File Transfer	Sitios para transferencias de archivos	X	
SaaS and B2B	Sitios de servicios de reuniones y ventas en línea	X	
Safe for Kids	Sitios de educación y animación en línea para niños	X	
Sex Education	Sitios relacionados con educación sexual, embarazos	X	
Software Update	Sitios relacionados con parches Informáticos	X	
Web Hostings	Sitio web con Entrega de Información de nuestro sitio Web	X	
Uncategorized	Sitios que no estén categorizados dentro de estos 78 grupos	X	

6.6.4 Filtro de Acceso Restringido

Los usuarios que por su perfil hayan sido clasificados en el grupo de acceso Restringido tendrán las restricciones del filtro Ético más Restricción de Acceso General y algunos sitios adiciones que se detallan a continuación:

Grupo	Grupo	Acceso Completo	
Categoría WSA	**Descripción Bloqueo**	**Bloqueo**	**Monitoreo**
Chat and Instant Messaging	Sitios que permitan servicios Chat's y mensajería Instantanea	X	
Online Communities	Sitios que entregan información de grupos de interés y sociedades	X	
Online Storage and Backup	Sitios que permitan almacenar contenido de información en la Nube	X	
Social Networking	Sitios que prestan servicios de redes sociales en línea	X	
Streaming Audio	Sitios que permiten transmisión de audio en vivo (radios)	X	
Streaming Video	Sitios que permiten transmisión de video en vivo (TV y Youtube)	X	

6.6.5 Acceso a sitios web sin restricciones

Las siguientes categorías de sitios web no estarán sujetas a restricciones.

Grupo Categoría WSA	Grupo Descripción	Acceso Restringido		Acceso General		Acceso Completo	
		Block	Monit.	Block	Monit.	Block	Monit.
Real Estate	Sitios de búsqueda de arriendos, ventas, remates de propiedades		X		X		X
Sports and Recreation	Sitios de deportes, reglas, normas y estadísticas		X		X		X
Digital Postcards	Sitios que permiten enviar servicios de tarjetas y saludos digitales		X		X		X
Arts	Sitios que entregan contenido de arte, museos, galerías, etc.		X		X		X
Auctions	Sitios de subastas en línea		X		X		X
Business and Industry	Sitios de marketing, comercio, negocios, etc.		X		X		X
Cheating and Plagiarism	Sitios de trabajos escritos, plagio de documentos		X		X		X
Computer Security	Sitios de ofrecimiento de servicios de seguridad tecnológica		X		X		X
Computers and Internet	Sitios con información técnica (software y hardware)		X		X		X
Dining and Drinking	Sitios con información de restaurantes y bares		X		X		X
Education	Sitios con información de educación		X		X		X
Fashion	Sitios con información de confección y moda		X		X		X
File Transfer Services	Sitios con información para transmisión de datos		X		X		X
Finance	Sitios con información financiera		X		X		X
Government and Law	Sitios con información legal		X		X		X
Hate Speech	Sitios con discursos mal intencionados		X		X		X
Health and Nutrition	Sitios con información de nutrición y salud		X		X		X
Humor	Sitios de humor		X		X		X
Infrastructure and Content Delivery Net.	Sitios con información de infraestructura y redes de tecnología		X		X		X
Job Search	Sitios con información de trabajos		X		X		X
Lotteries	Sitios de juegos de azar		X		X		X
Mobile Phones	Sitios con información de compañías de telefonía celular		X		X		X
Nature	Sitios con información de naturaleza		X		X		X
News	Sitios con información de noticias		X		X		X
Non-governmental Organizations	Sitios con información de organizaciones no gubernamentales		X		X		X
Online Trading	Sitios con información de venta en línea (eBay)		X		X		X
Organizational Email	Sitios con información de organizaciones no gubernamentales		X		X		X
Personal Sites	Sitios con información personal		X		X		X
Photo Search and Images	Sitios con información y búsqueda de fotografía e imágenes		X		X		X
Politics	Sitios con información de carácter político		X		X		X

Professional Networking	Sitios con conformación de profesionales de redes		X		X		X
Reference	Sitios con información de referencias		X		X		X
Religion	Sitios con información religiosa		X		X		X
Science and Technology	Sitios con información de ciencia y tecnología		X		X		X
Search Engines and Portals	Sitios con información de motores de búsqueda y portales web		X		X		X
Shopping	Sitios con información de compras		X		X		X
Social Science	Sitios con información de ciencias sociales		X		X		X
Society and Culture	Sitios con información de sociedades y cultura		X		X		X
Tobacco	Sitios con información de tabaco		X		X		X
Transportation	Sitios con información de transporte		X		X		X
Travel	Sitios con información de viajes		X		X		X
Web Page Translation	Sitios con información de traducción		X		X		X
Web-based Email	Sitios con información de correos basados en la web		X		X		X

6.6.6 Incidentes de Seguridad

Los usuarios del Hospital de Tomé que identifiquen o perciban o sospechen de algún problema de seguridad se deben contactar inmediatamente Encargado de Seguridad de Información de la Institución.

A través del Procedimiento de Gestión de Incidentes de Seguridad PROC03-25-0002 bajo resolución exenta N° 2122.

7 DIFUSION:

La comunicación del presente instructivo se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Portal Mesa de Servicio TI, sección Centro de Servicio TI.
- Correo informativo.

8 PERÍODO DE REVISIÓN.

El presente instructivo deberá ser revisado cada dos años o cuando ocurran cambios significativos para garantizar que:

- Sigue siendo adecuado para su propósito y preciso.
- Refleja los cambios en las tecnologías.
- Está alineado con la legislación vigente, los estándares internacionales y las mejores prácticas.