6-1-2024

Manual del Sistema de Gestión de Tecnologías y Seguridad de la Información

JOVANNY ANDRES ARBOLEDA ARBOLEDA
ESE HOSPITAL SAN LORENZO DE LIBORINA
TECNICO EN SOPORTE Y MANTENIMIENTO DE SISTEMAS

INDICE

1. INTRODUCCIÓN

Los grandes cambios en el contexto internacional plantean a los hospitales un sinnúmero de retos relacionados entre otras cosas, con los estilos de gestión dentro de un nuevo orden económico mundial, en el que sin duda alguna destaca el modelo técnico-productivo, derivado del vertiginoso avance de la ciencia y la tecnología; lo cual obliga a los hospitales a implementar las mejores prácticas normativas nacionales e internacionales que permitan oportunamente asumir nuevos enfoques estratégicos en la materia. Reconociendo que las tecnologías de la información y la comunicación (TIC) han creado nuevos horizontes y han propiciado importantes cambios en la concepción del proceso enseñanza-aprendizaje, y que el uso de nuevos modelos de asistencia, como las consultas asistidas por computadora, la educación virtual, la videoconferencia interactiva o la multimedia, han modificado la forma de operación de los hospitales. Pero además, las TIC se han convertido en un importante instrumento para hacer más eficientes los procesos administrativos, aumentar la cobertura, reducir costos, optimizar tiempos y, sobre todo, para que los médicos, y asistenciales estén conectados con el mundo en tiempo real y tengan acceso a la infinidad de información disponible en el ciberespacio.

En sustento a estas premisas, la Secretaría de Administración por conducto de la Dirección de Tecnologías de la Información establece el Sistema de Gestión de Tecnologías y Seguridad de la Información (SIGETSI), derivado de la necesidades que se tienen en la Universidad de mejorar las funciones y los procesos de tecnologías de la información considerando las experiencias que se han tenido en las organizaciones donde han implementado mejores prácticas2, y normas nacionales e internacionales, tales como:

- ISO/IEC 9001-2008 (Sistemas de Gestión de Calidad).
- COBIT 5 (Objetivos de Control para la Información y Tecnologías Relacionadas).
- NMX-I-38500-NYCE-2009 (Tecnologías de la Información - Gobierno Corporativo de Tecnologías de la Información).
- BSC (Cuadro de Mando Integral – Balanced Scorecard).
- NMX-I-20000-1-NYCE-2012 (Tecnología de la Información - Gestión del servicio Parte 1: Requisitos del Sistema de Gestión del Servicio).
- ITIL versión 3 (Biblioteca de Infraestructura de Tecnologías de la Información).

• NMX-I-27001-NYCE-2009 (Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información – Requisitos).

• PMBOK 5 (Fundamentos para la Dirección de Proyectos).

Además de contribuir en la gestión y mejora continua de los procesos académicos, de investigación y administrativos de la Universidad con base en los principios de:

- Responsabilidad.- Establecer los roles y responsabilidades de cada individuo o grupo de personas de la Universidad en relación de las TI.
- Estrategia.- Diseñar la estrategia tecnológica de la Universidad que deberá tomar en cuenta el potencial de las TI.
- Adquisición.- Equilibrar el costo-beneficio, riesgo a mediano y largo plazo en las adquisiciones de TI
- Desempeño.- Las TI deberán proporcionar el soporte a la Universidad, ofreciendo servicios con los niveles y la calidad requeridos.
- Cumplimiento.- Las TI cumplirán con el marco normativo. Las políticas y los procedimientos internos estarán claramente definidos, implementados y apoyados.
- Componente humano.- Las políticas y procedimientos establecidos deberán considerar al factor humano en todos los procesos de gestión: competencia individual, formación, trabajo en grupo, comunicación, etc.

2. OBJETIVOS

2.1. General

Estandarizar y efcientar la gestión de los servicios de Tecnologías de la Información que se prestan en la ESE HOSPITAL SAN LORENZO DE LIBORINA a fin de propiciar una cultura de servicio con enfoque a la mejora continua y consolidar las áreas que los gestionan, haciendo énfasis en la calidad y seguridad de la información.

2.2. Específicos

- Establecer una cultura orientada a procesos, usuarios y resultados
- Implementar un modelo de control interno en TI.
- Formalizar y estandarizar los procedimientos de trabajo en materia de TI.
- Establecer una estrategia para impulsar la innovación tecnológica a través de administrar el rumbo y los dominios tecnológicos.
- Entregar consistentemente servicios de TI con los “niveles de servicios” establecidos.
- Efcientar la transición de la operación de las soluciones tecnológicas y componentes de Ti

3. ALCANCE

Todas las áreas del hospital san Lorenzo de Liborina que gestionan Tecnologías de la Información

4. DIRECTRICES EN TECNOLOGÍAS DE LA INFORMACIÓN

4.1. Directrices Generales

4.1.1. La DTI en coordinación y con el apoyo de las dependencias, deberá:

I. Establecer la innovación, accesibilidad y calidad en la entrega de Servicios Tecnológicos;
II. Optimizar la correspondencia entre las necesidades de los procesos asistenciales y administrativos con la directriz tecnológica.
III. Procurar el fortalecimiento al uso de las tecnologías en el hospital.

4.1.2. La DTI y las dependencias deberán establecer y tomar en cuenta para la optimización interna de sus trámites y servicios, debiendo utilizar los lineamientos, las reglas, las guías, manuales y documentos técnicos de interoperabilidad que para este efecto emita la DTI. Asimismo, deberán establecer un Esquema de Interoperabilidad y Datos Abiertos para la integración de los procesos relacionados con servicios digitales, así como para compartir y reutilizar plataformas y sistemas de información, a fin de incrementar la efciencia operativa en la gestión institucional y su relación con el hospital y la sociedad, considerando el desarrollo de acciones para, asegurar la:

I. Gobernanza de la Interoperabilidad;
II. Interoperabilidad organizacional;
III. Interoperabilidad semántica, e
IV. Interoperabilidad técnica.

4.1.3. Se deberá incentivar el uso de herramientas de TI y el desarrollo de sistemas informáticos para optimizar, modernizar y automatizar los procesos, trámites y servicios.

4.1.4. Se deberán compartir recursos de infraestructura, bienes y servicios en todos los dominios tecnológicos utilizando soluciones tecnológicas comunes a nivel dependencia, conforme a las directrices y lineamientos que emita la DTI, tomando en cuenta la seguridad de la información.

4.2. Planeación Estratégica de Tecnologías de la Información

4.2.1. La Planeación Estratégica de TI que elabore la DTI, deberá atender las metas, estrategias, objetivos y líneas de acción establecidos en el Plan de Desarrollo Institucional (PDI).

4.2.2. El Plan Estratégico de Tecnologías de la Información (PETI) se integrará con las Iniciativas y Proyectos de TI que determinen las dependencias, sujetándose al punto anterior, para lo cual atenderán lo siguiente:

I. Favorecer el uso del cómputo en la nube: privada, pública o hibrido para el aprovechamiento de la economía de escala, efciencia en la gestión y estandarización de las TI, considerando la seguridad de la información;

II. Promover la implementación de Tecnologías sustentables;

III. Establecer un registro detallado para cada una de las Iniciativas y Proyectos de TI;

IV. Identificar Iniciativas y Proyectos de TI que aporten mayores beneficios a la comunidad hospitalaria y cuenten con alto impacto en el cumplimiento de los objetivos institucionales, y del PDI, identificándolos como estratégicos;

V. Relacionar las características, especificaciones y estándares generales de los principales componentes por cada dominio tecnológico;

VI. Establecer estrategias de interoperabilidad para los aplicativos de cómputo al interior de las dependencias y que requieran compartir datos que obren en su posesión; puedan o no formar parte de un mismo proceso.

VII. Determinar Iniciativas y Proyectos de TI para la digitalización de los trámites y servicios, considerando las estrategias de interoperabilidad con aplicativos de cómputo de otras dependencias que resulten necesarios para la prestación de esos trámites y servicios.

4.2.3. Una vez elaborado el PETI, conforme al proceso de Planeación Estratégica que se establece en el SIGETSI, las dependencias presentarán si así lo determinan, por lo menos una Iniciativa o Proyecto al Comité de TI; considerando como criterio preferentemente para su identificación, que aporten mayores beneficios al hospital o cuenten con alto impacto en el cumplimiento de los objetivos institucionales del PDI. La DTI dará seguimiento, conforme a los procesos de Administración del Portafolio de Proyectos de TI, y de Administración de Proyectos de TI que se establecen en el SIGETSI (Sistema de Gestión de Tecnologías y Seguridad de la Información)

4.3. Adquisiciones, Arrendamientos de Bienes Muebles y Prestación de Servicios de Tecnologías de la Información

4.3.1. Para las adquisiciones, arrendamientos de bienes y de prestación de servicios, en materia de TI, la DTI y las dependencias deberán sujetarse a lo establecido en los procedimientos de adquisiciones y demás disposiciones aplicables en la materia, además de observar lo siguiente:

I. En la planeación de las contrataciones, se sujetarán a las disposiciones establecidas en los procedimientos de adquisiciones, arrendamientos de bienes muebles y prestación de servicios del hospital;

II. Las dependencias deberán observar los lineamientos, las reglas, las guías, manuales y documentos técnicos para que la materia, ponga a disposición la DTI

III. En aquellos proyectos de infraestructura tecnológica que no se cuente con lineamiento, corresponderá a la Secretaría de Administración (SA) a través de la Dirección de Tecnologías de la Información (DTI) establecer las especificaciones y directrices conforme a las necesidades de la dependencia requirente;

IV. Elaborar la investigación de mercado

V. En el procedimiento para la contratación de prestación de servicios, en materia de TI, complementariamente se deberá presentar un desglose de los componentes que integren el servicio a prestar,

VI. Prever, en su caso, acciones por parte del proveedor para el adiestramiento formal especializado, para quienes resulte pertinente, de acuerdo al dominio tecnológico objeto de la contratación.

4.3.2. La DTI y las dependencias deberán realizar un estudio de factibilidad a efecto de determinar la conveniencia de adquirir o arrendar bienes, o bien contratar servicios cuando impacte directamente en el cumplimiento de los objetivos estratégicos e indicadores del hospital; lo anterior, conforme a lo señalado en los procedimientos de adquisiciones, al proceso de Apoyo Técnico para la Contratación de Soluciones Tecnológicas que se establece en el SIGETSI y demás disposiciones aplicables en la materia.

El estudio de factibilidad deberá comprender, entre otros, los elementos siguientes:

I. El análisis de las contrataciones vigentes y, en su caso, la determinación de la procedencia de su renovación;
II. La pertinencia de realizar contrataciones consolidadas
III. Los costos de puesta en marcha, mantenimiento, operación y soporte que impliquen la contratación, vinculados con el factor de temporalidad más adecuado para determinar la conveniencia de adquirir, arrendar, renovar o contratar servicios.

4.3.3. En las contrataciones relacionadas a las redes de telecomunicaciones, la DTI como sujeto obligado deberá sujetarse a lo establecido en los procedimientos de adquisiciones, en el SIGETSI y demás disposiciones aplicables en la materia, además de observar lo siguiente

I. Los lineamientos, las reglas, las guías, manuales y documentos técnicos de interoperabilidad que para este efecto ponga a disposición la propia DTI
II. Establecer un dominio o segmento virtual en el uso compartido de redes de telecomunicaciones, lo cual deberá realizar para todas las dependencias;
III. Contar con mecanismos estándares de cifrado de datos, considerando la criticidad de los datos en sus etapas de tratamiento, especialmente en su transmisión a través de redes de telecomunicaciones

IV. Incluir mecanismos que soporten y habiliten servicios de multidifusión en redes privadas o locales, así como en redes de área amplia, para soportar el envío de información, voz, datos y video, así como los beneficios en reducción de costos operativos, capacitación, agilidad en la gestión universitaria y experiencia al universitario.

4.3.6. En las contrataciones relacionadas con los servicios de Internet, la DTI como sujeto obligado deberá sujetarse a lo establecido en los procedimientos de adquisiciones, en el SIGETSI y demás disposiciones aplicables en la materia, así como observar lo siguiente:

I. Los lineamientos, las reglas, las guías, manuales y documentos técnicos de interoperabilidad que para este efecto ponga a disposición la propia DTI
II. Mecanismos de protección a ataques de denegación de servicios, desde la propia red del proveedor e independientemente de los controles de seguridad de la información que implemente el hospital, debiendo atenderse mediante las actividades que se señalan en el SIGETSI para el establecimiento de controles de seguridad de la información
III. En caso de ser necesario, la distribución y balanceo del tráfico para más de un enlace de Internet, considerando disponibilidad, confidencialidad, criticidad y redundancia.

4.4. Servicios de Infraestructura Tecnológica

4.4.1. En el caso de los servicios de correo electrónico del hospital, la DTI como sujeto obligado deberá sujetarse a lo establecido en los procedimientos de adquisiciones, en el SIGETSI y demás disposiciones aplicables en la materia, además de observar lo siguiente

I. Los lineamientos, las reglas, las guías, manuales y documentos técnicos de interoperabilidad que para este efecto ponga a disposición la propia DTI,

II. El servicio deberá comprender soluciones de filtrado para correo no deseado o no solicitado, antivirus y de suplantación de identidad que protejan el envío y recepción de correos.

4.4.2. Con respecto a sistemas de comunicaciones unificadas de telefonía y video, la DTI como sujeto obligado deberá sujetarse a lo establecido en los procedimientos de adquisiciones, en el SIGETSI y demás disposiciones aplicables en la materia, además de observar lo siguiente.

I. Los lineamientos, las reglas, las guías, manuales y documentos técnicos de interoperabilidad que para este efecto ponga a disposición la propia DTI,

II. Utilizar tecnología basada en protocolo de internet y mecanismos de cifrado estándar en las comunicaciones de voz y video, tanto en la media como en la señalización según aplique;

III. Utilizar marcación unificada, considerando en el diseño de por lo menos cuatro dígitos y la integración de las dependencias de la Universidad;

IV. Establecer interconexión de sistemas de telefonía entre dependencias, ciudades, regiones y/o centros universitarios, que disminuya costos e incremente la seguridad de las conversaciones, mediante la implementación de sistemas de seguridad de frontera específicos para comunicaciones de voz y video, y se asegure el soporte de trans-codifcación de señalización entre diferentes formatos de comunicación;

V. Prever la infraestructura que quedará a favor de la Universidad al término del contrato, en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas, adjudicación directa o las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, en el caso de contrataciones de servicios que requieran algún tipo de infraestructura de soporte para su prestación;

VI. Utilizar tecnologías de mensajería instantánea, presencia y movilidad, a fin de incrementar la productividad del personal y un mayor uso de éstas, teniendo en consideración la seguridad de la información;

VII. Utilizar esquemas de consulta y acceso a directorio para el control de accesos y usuarios en las unificaciones entre dependencias, conforme a lo establecido en el punto 6.4.3 fracción VI del presente documento;

VIII. Privilegiar el uso de teléfonos de bajo consumo de energía;

IX. Utilizar tecnologías de gestión y monitoreo a fin de facilitar la implementación, operación y planeación de la capacidad instalada de telefonía y video,

X. Prever en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas, adjudicación directa o las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, como parte del servicio la elaboración y ejecución conjunta de un plan de adopción tecnológica para maximizar el uso de los sistemas de voz, de video o de ambos

4.4.3. En el caso de los servicios de Centros de Datos, la DTI y las dependencias deberán observar los lineamientos, las reglas, las guías, manuales y documentos técnicos de interoperabilidad que para este efecto ponga a disposición la DT, además observar lo siguiente

I. Identificar la infraestructura de Centro de Datos con la que cuentan y la utilización de ésta, así como espacio físico, energía eléctrica, aire acondicionado, capacidad de procesamiento y almacenamiento;

II. En caso de haber identificado que tienen capacidad no utilizada deberán comunicarlo a la DTI para su aprovechamiento;

III. Analizar el alojamiento de su infraestructura de operación crítica en el Centro de Datos Central, bajo un modelo de cómputo en la nube o dispositivo externo;

IV. Almacenar y administrar en los Centros de Datos que se encuentren en las instalaciones de las dependencias, los datos considerados información reservada y confidencial, conforme a la normatividad aplicable;

V. Mantener en la infraestructura de los Centros de Datos una arquitectura que permita la portabilidad, de forma tal que las aplicaciones de cómputo puedan migrar entre distintos Centros de Datos y sean interoperables, dicha infraestructura deberá ser compatible con el uso de máquinas virtuales.

VI. Establecer la infraestructura y administración de la seguridad de la información en zonas de seguridad física y lógica, considerando identidad, perfiles y privilegios, incluyendo en éstas las necesarias para el personal involucrado, conforme a los controles de seguridad de la información que se definan, atendiendo a lo previsto en el SIGETSI

5 .seguridad

Objetivo:

Establecer y vigilar los mecanismos que permitan la administración de la Seguridad de la Información hospital, así como disminuir el impacto de eventos adversos que potencialmente podrían afectar el logro de los objetivos de la DTI.

Consejos para la Protección de la Computadora Hoy en día, utilizamos computadoras para todo. ¿PERO…..que pasa cuando su computadora se hackea? A continuación, se indican algunos pasos sencillos pero muy importantes que puede seguir para evitar que los hackers accedan su computadora e información personal.

• Haz un respaldo de su información con frecuencia. Usted puede copiar sus datos a un CD, DVD, dispositivo USB o a un disco duro externo. De esta forma, si su computadora se cuelga o es hackeada, no perderá toda su información.

• Nunca le dé a alguien acceso remoto a su computadora. Si usted recibe una llamada de alguien reclamando ser de Microsoft o cualquier otra empresa diciendo que tiene un virus o que pueden arreglar otros problemas con su computadora, cuelgue inmediatamente. Estafadores intentarán a convencerle a pagar para servicios no necesarios y conseguir acceso a su computadora para obtener información personal o instalar software malicioso.

• Actualice su sistema operativo regularmente. Sistemas operativos de computadora se actualizan periódicamente para mantenerse al día con los requisitos tecnológicos y para arreglar puntos débiles que pueden ser atacados por los hackers. Asegúrese de instalar las actualizaciones para estar seguro de que su computadora tiene la última versión. A menudo hay configuraciones en su sistema operativo para hacer estas actualizaciones automáticas.

• Utilice contraseñas fuertes y cámbielas con frecuencia. No utilice la misma contraseña para cuentas múltiples. Utilice contraseñas que contienen letras minúsculas y mayúsculas, números, y puntuación. Cambie su contraseña cada tres meses y no reúse las contraseñas. Esto es especialmente cierto para contraseñas que se utilizan para acceder su correo electrónico y cuentas bancarias.

• No haga clic en ventanas emergentes. Ventanas emergentes en el internet son herramientas de publicidad rápida, pero ten cuidado con las ofertas "demasiado buenas para ser verdad". Estas ventanas emergentes no solo pueden reducir la velocidad de su computadora e internet, sino que al hacer clic en estos puede accidentalmente registrarse para servicios no autorizados. Establezca la barra de información en su navegadora no permitir ventanas emergentes.

• Tenga cuidado con lo que descarga. Unos de los virus más destructivos se han ocultado en programas del internet y aplicaciones o adjuntos de correos electrónicos. Esté seguro de solo descargar de una fuente confiable. En cuanto a los correos electrónicos, nunca haga clic en enlaces o archivos adjuntos si no reconoce al remitente. Incluso si conoce el remitente, ¡cuidado! Porque es posible que su computadora fue hackeada y está enviando correos electrónicos infectados. Esos correos electrónicos también podrían ser muy bien disfrazados para parecer a instituciones financieras bien conocidas o sitios web minoristas, enviado para conseguir su información personal.

• No envíe información confidencial o personal a través de correo electrónico. El correo electrónico no suele ser cifrado, o en otras palabras no en un “código secreto,” y puede ser interceptado y leído por hackers.

• Utilice software antivirus y configúrelo para actualizarse a diario. Hay muchos productos comerciales que pueden ayudarle a proteger su computadora de los virus maliciosos. La mayoría de protección de software tiene una característica que escaneará archivos descargados automáticamente y algunos incluso escanearán correos electrónicos entrantes por defecto.

• Evite instalar software innecesario, desconocido o no probado. Esto incluiría juegos, barras de herramientas o salvapantallas que podría dejar su computadora vulnerable a ataques. A menudo se instalan spyware y los virus al descargar programas desconocidos. Compruebe para asegurarse de que cuando usted instale el software que quiere, que el programa no está incluyendo otras barras de herramientas o software en la instalación. Busque casillas automáticamente marcadas en la página del acuerdo dando su permiso para instalar estos otros artículos.

• Utilice un cortafuego personal. Un cortafuego actúa como una barrera entre usted y el internet. Ayuda a mantener los hackers fuera y ayuda a prevenir que el software malicioso envíe su información personal a criminales. Hay versiones minoristas y gratuitas disponibles y los cortafuegos pueden venir en la forma de software y hardware.

• Tenga cuidado con redes inalámbricas. Para su red doméstica, asegúrese de que su enrutador está protegido por contraseña. Para acceso a redes públicos (tal como restaurantes, bibliotecas o cafés), este consciente si la red no es segura. Criminales cibernéticos aprovechan estas redes inseguras para hackear su computadora y acceder a sus datos personales.

• Apague su computadora cuando no esté en uso. Dejando su computadora prendida y desatendido podría dejarla abierta a un ataque por hackers. Proteja su computadora, y ahorre energía apagando su computadora cuando no la está usando.

• Deseche su computadora seguramente. Asegúrese de que todos los datos personales se eliminan mediante el borrado o destrucción físico del disco duro de su computadora. Si su computadora ha sido hackeada y usted siente que su seguridad está en peligro, o piensa que el hacker es alguien que usted conoce, debe llamar a la policía local. Póngase en contacto con un profesional de la informática local confiable para remover cualquier software malicioso que pudiera haber sido instalado. La tecnología continúa cambiando y evolucionando. Es posible que no pueda evitar todo el hacking, pero puede ayudar a equiparse con las herramientas y el conocimiento para proteger su computadora de los delincuentes cibernéticos.

Según INVISUS, una compañía de seguridad de computadoras, todas las computadoras conectadas a Internet poseen una dirección IP no asegurada que los hackers pueden encontrar en cualquier lugar del mundo (a menos que dicha computadora tenga un firewall instalado y activado). Cada PC tiene más de 65.000 puertos de datos integrados, que se abren y se cierran y que son utilizados por varias aplicaciones de la computadora para mantener la comunicación con otros sistemas en red.

Los hackers suelen obtener acceso a las computadoras distribuyendo software malicioso como virus, troyano o gusanos. Los usuarios distraídos suelen instalar este tipo de malware cuando abren archivos adjuntos de email, descargan archivos de una red que los comparte e incluso cuando guardan archivos de grupos de noticias públicos también los puertos vulnerables que están expuestos en redes sociales y plataformas como YouTube spotify muchos canales de emisoras entre otros. Un ejemplo es el SDbot, un tipo de troyano que se instala solo en la computadora, abre una “puerta trasera” y usa un canal de Internet Relay Chat (IRC) para buscar contraseñas en la computadora deseada. Según la Comisión Federal de Negocios (FTC en inglés), a veces simplemente basta con ingresar a un sitio web para que una computadora descargue un software malicioso que le permita el acceso a los hackers.

¿Cómo prevenir un ataque?

1. Asegúrate de instalar **software adquirido de forma legal**, así sabrás que está libre de troyanos o virus.

2. **Instala antivirus** con las reglas de configuración y de los sistemas adecuadamente definidos.

3. **Adquiere hardware y software cortafuegos** para bloquear usuarios no autorizados y evitar que accedan a tus equipos de cómputo.

4. **Usa contraseñas grandes y complejas** que contengan letras y números; esto ayuda a que los hackers no puedan descifrarlas fácilmente.

5. Cuidado con social media. **Mediante las redes sociales los ciberdelincuentes tratan de obtener información** para posibles ataques.

6. **Encripta tu información importante** para mantenerla segura y secreta.

En caso de ataque:

I. Solicitar los datos del usuario (cuenta de correo, número telefónico, ubicación de oficina, entre otros).
II. Recabar información para identificar la solicitud del usuario, realizando un análisis de la misma.
III. Registrar la información en herramienta correspondiente.
IV. Generar un identificador de caso

Clasificación y Soporte Inicial

I. Analizar la información de mayor prioridad y su posible solución.
II. Determinar el tipo de solicitud de servicio
III. Categorizar el caso (Operación o producto).
IV. Determinar el impacto de la solicitud.
V. Determinar la urgencia de la solicitud
VI. Priorizar la solicitud de acuerdo al impacto y la urgencia.
VII. Si requiere escalacion de 2Q nivel, se deberá canalizar la solicitud al área correspondiente.
VIII. Si no requiere escalacion, se realiza el procedimiento investigación y diagnóstico.

Apoyo Técnico para la Contratación de Soluciones Tecnológicas (ATC)

Objetivo:

Apoyar en la definición de los requerimientos de las Soluciones Tecnológicas que integran componentes de Tecnologías de la Información, dictaminar, participar técnicamente para su contratación, mediante acciones coordinadas con la Dirección de Adquisiciones responsable de realizar los procedimientos de contratación del hospital, los responsables de la Implantación Técnica de dichas soluciones en las TI y en su caso, con las áreas solicitantes.

Documentos de Entrada:

Estudio de Factibilidad. (ATC)
Investigación de Mercado. (ED)
Paquete de Diseño del Servicio de TI. (DSTI)
Políticas y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de la Universidad Autónoma de Tamaulipas. (SA)

6. GLOSARIO

6.1. Definiciones

Activos de TI:

Los aplicativos de cómputo, infraestructura tecnológica, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.

Acuerdo de nivel de servicio:

El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar una solución tecnológica o servicio de TI.

Aplicativo de Cómputo:

El software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Borrado Seguro:

El proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.

SIGETSI:

(Sistema de Gestión de Tecnologías y Seguridad de la Información)

Cómputo en la Nube:

Al modelo de prestación de servicios digitales que permite a las dependencias acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios.

E.S.E. Hospital San Lorenzo
Al servicio de la vida