UNIVERSIDAD NACIONAL

Sistema de Estudio de Posgrados

Maestría en Administración de Tecnología de la Información (MATI)

Énfasis en Desarrollo de Productos y Servicios de TI

Gestión de Procesos Preventivos en Servicios de TI del Hospital México

Presentado por: Bryan Valverde Piedra

Heredia, Costa Rica, 18 de Abril 2016

Agradecimientos

Agradecer en principio a Dios por darme la inteligencia, sabiduría, paciencia, entendimiento y la capacidad para desarrollar este proyecto.

A mis padres por todo su apoyo, comprensión y confianza en toda mi vida y principalmente, en mi vida profesional.

A todos los profesores a lo largo del desarrollo de esta Maestría, en especial a doña Xenia Guerrero por su guía y apoyo con el último y más importante esfuerzo de la Maestría, que es este proyecto de graduación.

A los colaboradores del Departamento de TI del Hospital México de Costa Rica, en especial a doña Danelia Ramírez, Adrián Badilla y Harold Morales, quienes depositaron la confianza y concedieron parte de su tiempo para el desarrollo de este proyecto en su institución.

Por último y no menos importante, al MICIT y CONICIT por su gran apoyo financiero en la Maestría, que me ha permitido a mí y muchos otros profesionales en Costa Rica un desarrollo en las carreras.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

Resumen Ejecutivo

El Hospital México es uno de los hospitales más importantes de Costa Rica, el cual utiliza las Tecnologías de Información (TI) como un gran apoyo para brindar sus servicios diariamente. TI se pueden convertir en el mejor aliado, pero también pueden convertirse en el peor enemigo si no se gestionan de forma adecuada.

En el Departamento de TI del hospital siempre se busca mejorar en su operación, por tanto, se observó que han ocurrido incidentes asociados a la infraestructura de TI, algunos de gran impacto y a pesar de que se pudo resolver la situación, no es parte de la administración de TI procesos o labores preventivas para disminuir o evitar completamente el impacto de esos incidentes.

De aquí nace este proyecto, con el objetivo principal de diseñar procesos para la gestión preventivos que buscan prevenir y disminuir el impacto de los incidentes, para esto de manera específica la identificación de los principales incidentes que afectan la infraestructura de TI, definición de procesos asociados a esos principales incidentes, desarrollo de propuesta asociado a esos procesos y desarrollar un plan piloto de la propuesta.

Para definir en qué enfocarse en este proyecto, la metodología usada es a través de un estudio de la situación actual con colaboradores del Departamento de TI a quienes se les hacen consultas que afecta más la infraestructura de TI, además, de que consideraban importante desarrollar que no se ha tenido la oportunidad de trabajar.

Se decide trabajar la gestión preventiva con procesos de gestión de eventos y gestión de seguridad de red. El primer proceso involucra revisar cambios significativos en equipos de infraestructura y tomar acciones sobre ellos, eventos que pueden anunciar un incidente, inclusive antes que se presente. Con la gestión de seguridad se trabaja en vulnerabilidades las cuales se han visto que pueden llegar a comprometer la disponibilidad, confidencialidad e integridad de equipos e información a través de la infraestructura de TI.

A la propuesta se le da forma con base en marcos de referencia asociados a los procesos, investigación y juicio experto, las recomendaciones propias de la propuesta, ante todo un estudio de campo y consultas a colaboradores sobre cómo se gestiona actualmente la infraestructura.

Adicionalmente se desarrollan las bases de uno de los procesos como plan piloto, que sirva de trabajo inicial y a partir de este esfuerzo se pueda seguir desarrollando toda la propuesta.

Se concluye que fue necesaria la indagación con los colaboradores, donde el identificar y categorizar los principales incidentes ayudó a definir los procesos a seguir, definir un marco de referencia, investigación, juicio experto y estudio de campo, colaboraron para que la propuesta pueda ser más realista y no se quede solo en el papel, sino que llegue a ser implementada.

Como recomendaciones revisar la propuesta y de ser necesario corregir o adicionar, no pretender implementar todo a la vez y se recomiendan otros procesos preventivos por tomar en cuenta a futuro

1 CAPÍTULO I: EL PROBLEMA Y SU IMPORTANCIA

1.1 Antecedentes

El Hospital México es uno de los principales y más grandes hospitales públicos de Costa Rica, pertenece a la Caja Costarricense del Seguro Social (CCSS), la cual es una institución autónoma del Estado costarricense, encargada de servicios públicos de salud y seguridad social del país.

Este hospital puede llegar a atender diariamente hasta 5 mil personas según estimación de Harold Morales, colaborador del Departamento de TI, lo cual muestra la importancia de los servicios que brinda este hospital. Se atienden inclusive padecimientos críticos y de alto riesgo con la salud.

El hospital cuenta con una planilla de colaboradores directos e indirectos de alrededor de 3600, los cuales distribuyen sus jornadas de trabajo entre las 24 horas del día, al estar la mayoría de este personal laborando entre al 7 a.m. y 4 p.m. El Departamento de TI brinda servicio normal de lunes a viernes entre 6 a.m. a 4 p.m.; después de las 4p.m. y hasta las 7 p.m. entre semana y durante el día fines de semana se brinda soporte limitado de pocos colaboradores a través de horas extra que se les asigna en un horario establecido, una modalidad similar a roles de guardia de trabajo.

Como todo hospital y en realidad, una institución de gran tamaño en la actualidad, casi todos los empleados requieren del uso de las tecnologías de información y comunicación (TIC) para realizar sus labores, estas se presentan como diferentes servicios que brinda y facilita el Departamento de Gestión de TIC, los cuales se vuelven estratégicos y hasta esenciales para las operaciones del hospital.

Los servicios de TIC permiten gestionar información de pacientes, transmitir imágenes médicas, controlar inventarios y entregas de medicamentos, se accede a sistemas institucionales de la CCSS, además, otros servicios de TIC generales como correo electrónico o acceso a Internet.

Para que los servicios de TIC sean utilizados de forma apropiada por los usuarios, debe haber una infraestructura tecnológica que los soporte. En el hospital, como parte de la infraestructura de TIC, se cuenta con elementos activos como computadoras personales, equipos de red de datos y de telefonía, de almacenamiento de datos y servidores;

adicionalmente con elementos pasivos, principalmente asociados con el cableado para transmisión de datos y voz por cobre o fibra óptica.

Hay un equipo de trabajo interno encargado de brindar soporte a toda esa infraestructura, sin embargo, mucho del soporte brindado es de tipo correctivo, ante incidentes y problemas que se presentan. También se realizan labores preventivas, como mantenimiento de equipos.

El Departamento de TI tiene contratos de soporte con proveedores de servicios de consultoría tecnológica externos, para casos de soporte muy especializados o de alta complejidad. Se cuenta con 3 proveedores recurrentes por el momento asociados a la infraestructura de TIC, uno para servidores y equipos de red, otro para telefonía y el último para enlaces inalámbricos.

Este Departamento de TI está integrado por 15 colaboradores que se clasifican, según los siguientes puestos asociados a la CCSS:

- Siete técnicos.
- Seis analistas de sistemas.
- Una asistente de TIC
- Un Jefe de TIC

La organización del departamento es en una sección de soporte de usuario final (telefonía y computadoras), una sección de soporte de infraestructura (servidores, almacenamiento de datos y redes) y una sección de analistas de sistemas de software. Se define un líder en cada área por organización interna, sin embargo, mantienen los mismos puestos asociados a la CCSS.

Actualmente no se tienen definidos acuerdos de nivel de servicio con personal interno y se está trabajando en la definición de acuerdos de servicios con los proveedores.

Como todo Departamento de TI y en este caso específico, el equipo de soporte de Infraestructura tecnológica, tienen como objetivo primordial que esta infraestructura se encuentre disponible lo más cercano a un 100% del tiempo, además, deben procurar que sea redundante, escalable y segura. La importancia de este objetivo está en que al hablar de un hospital, se está hablando de vidas humanas que requieren atención médica, los

servicios de TI colaboran para que esa atención sea más rápida y precisa. Por ejemplo: para obtener resultados de exámenes a través de consultas de red, sin tener que ir físicamente al equipo que da los resultados, o en farmacia, donde se consultan perfiles de pacientes para ver si son alérgicos a uno u otro componente químico.

1.2 Descripción y delimitación del problema

Como se indicó en los antecedentes, el principal objetivo del Departamento de TI del Hospital México es mantener la disponibilidad de los servicios de TIC, para esta función existe un equipo de soporte interno para trabajar en incidentes o situaciones que atenten contra esa disponibilidad de los servicios de TIC.

Sin embargo, el personal del Departamento de TI es consciente que podrían evitarse muchos incidentes y problemas asociados a la infraestructura tecnológica que afecten los servicios de TIC, por ejemplo: si se implementaran prácticas de gestión preventiva sobre la infraestructura tecnológica.

Cuando se habla de incidentes se refiere a esas fallas que afectan o degradan un servicio, por ejemplo: fallo en la conectividad por saturación de un dispositivo de red o ataque de seguridad al mismo. Esto afecta la continuidad del servicio de todos los usuarios conectados a ese dispositivo de red y ese usuario no va a poder realizar sus funciones dependientes del servicio de TI.

La infraestructura tecnológica permite el acceso a los servicios de TIC que gestionan la información requerida por los diferentes colaboradores del hospital. Como ejemplo de una vulnerabilidad de esta infraestructura, si un servidor comienza a saturarse en memoria o uso de CPU, puede llegar a apagarse de forma inadvertida, lo cual sin una redundancia adecuada, afecta el acceso al sistema que tiene corriendo ese servidor.

Actualmente no existen elementos que permitan prevenir este tipo de situaciones del ejemplo comentado, solo hasta el momento que se presente el incidente, se puede trabajar en la corrección del mismo.

En el momento que se presenta un incidente o problema, es posible que la solución no sea compleja, sin embargo, hay un tiempo en el cual se tiene que entender qué es lo que está

pasando y llevar a cabo esa solución. Ese tiempo para el hospital puede marcar mucha diferencia sobre la atención eficiente de un paciente.

Los incidentes de TIC en el Hospital México pueden llegar a afectar la atención rápida y precisa de pacientes, por ejemplo: servicios como registro de visitantes y pacientes, entrega de medicamentos, pago de servicios y atención de pacientes a través de acceso a sus registros informáticos, incluyendo resultados de exámenes médicos que se consultan por red.

Lo que se busca con este proyecto es una gestión preventiva, como su nombre lo indica, es prevenir que ocurran incidentes y/o problemas, es decir, implementar prácticas proactivas de forma tal que antes de que se manifieste un incidente o problema, se puede trabajar en el mismo y evitar que se dé alguna afectación en la infraestructura de TI.

A través de consultas al personal de TI y observaciones realizadas durante visitas en las que se ha consultado sobre la infraestructura de TIC del hospital, se han detectado aspectos que podrían contribuir a la gestión preventiva de incidentes y problemas que no se aprovechan en el hospital, entre ellos:

- Sistemas de gestión de eventos, como monitoreo.
- Implementación de seguridad informática basado en alguna buena práctica para la gestión de equipos.
- Gestión de incidentes de Infraestructura tecnológica.
- Gestión de conocimiento de información asociada a infraestructura de TIC
- Diseño y documentación sobre redundancia de servidores y red.

Con este proyecto se pretende aprovechar aún más los recursos con los que actualmente cuenta el Departamento de TI, tanto recursos tecnológicos como recurso humanos y de proveedores, por lo que lo primordial es brindar una propuesta alineada a esto. Se pueden recomendar opciones que impliquen uso de presupuesto para una nueva inversión económica, sin embargo, la prioridad es aprovechar los recursos existentes.

En conclusión, el problema en concreto está en que se han dado y se siguen dando incidentes y problemas asociados a la infraestructura de TIC que generan un impacto negativo directo sobre los servicios de TIC, como se mencionó antes afecta los servicios que

brinda el hospital, además, este problema se hace aún mayor al no tener forma dentro del hospital de prevenir muchos de esos incidentes.

1.3 Justificación

Basado en el marco de referencia de ITIL se define como incidente "una interrupción no planificada de un Servicio de TI o una reducción de la Calidad de un Servicio de TI" (IT Process Wiki, 2013). El hecho que se dé en forma constante un incidente, o que un único incidente sea de gran impacto, genera lo que se conoce como un problema.

Una solicitud de servicio no está asociado a lo que se pretende en este proyecto, no se genera afectación del servicio. Según ITIL una solicitud de servicio es:

> Generada por un usuario que busca información o consejo, o que desea solicitar un cambio menor o que se le conceda acceso a algún servicio de TI. Esta solicitud puede ser de cambio de contraseña, o de que se le provean servicios comunes de TI a otro usuario (IT Process Wiki, 2013).

Hoy las empresas que basan sus servicios en sistemas informáticos deberían hacerse la consulta sobre qué están haciendo sus departamentos de TI para anticipar esos incidentes, que a la larga se pueden convertir en problemas.

Existen múltiples causas de incidentes de TI, algunas asociadas a diseños no apropiados, vulnerabilidades de seguridad informática, falta de monitoreo de infraestructura tecnológica e inclusive errores de los propios usuarios. De hecho, la empresa de seguridad informática Kaspersky a través de un estudio indica que "El 80% de los incidentes de seguridad TI de las compañías españolas los causaron los mismos empleados" (Sala de Prensa de Kaspersky Lab España, 2014).

Más allá de la causa de los incidentes, su impacto puede llegar a generar inconvenientes en el servicio que brinda el hospital y esto con la consecuencia principal de afectar la imagen de la institución, que es un servicio de salud público, el cual los asegurados de la CCSS tienen derecho a recibir y el hospital debe brindar sin inconvenientes.

Riegos de que ocurran incidentes informáticos siempre van a existir, sin embargo, el cómo mitigarlos es lo que hace la diferencia de si estos riesgos se manifiestan, y la labor más importante al gestionar estos riesgos es la que se realiza para evitar que llegue a afectar.

En este punto se denota que una gestión preventiva de TI evita a minimizar el impacto asociado a los riesgos de TI. Para el caso de este proyecto se asocia a la infraestructura de TI, que permite el acceso a los servicios de TIC.

El no contar con una gestión preventiva de infraestructura de TI no permite anticipar o evitar incidentes informáticos y en caso de que se presenten, se va a tener un tiempo de respuesta en el cual se afecta el servicio y dependiendo la hora y elemento de infraestructura impactado, puede ser fatal dentro de las operaciones del hospital.

El impacto e importancia de procesos de gestión preventiva como lo que se plantea en este proyecto, no es solo de un punto de vista técnico, sino estratégico, el Departamento de TI con su objetivo estratégico principal de mantener la disponibilidad de los servicios de TIC, llega a encontrar con esta gestión preventiva un medio para tener más control sobre la infraestructura que se está administrando y generar buenas prácticas para alcanzar ese objetivo.

1.4 Objetivo General

Diseñar procesos estratégicos para la gestión preventiva de Infraestructura Tecnológica en procura de reducir la cantidad y el impacto de los principales incidentes que afectan la calidad de los servicios de TIC del Hospital México.

1.5 Objetivos Específicos

1. Identificar tipos de incidentes y/o vulnerabilidades que más afectan o podrían afectar la infraestructura tecnológica asociada a servicios de TIC del hospital, a través de indagación con colaboradores del Departamento de TI, para basar en estos la propuesta.
2. Definir los procesos preventivos por diseñar basado en principales incidentes y/o vulnerabilidades identificados, de manera que sirvan de guía para los diseños de la solución propuesta.
3. Diseñar procesos establecidos en el objetivo anterior, por medio de investigación de buenas prácticas asociadas relacionadas con los procesos, juicio experto y uso de elementos existentes en el hospital, de esta forma apoyar a la gestión preventiva que se pretende.
4. Desarrollar un prototipo de un proceso preventivo, lo cual involucra puesta en marcha de herramientas asociadas y validación de resultados iniciales, para obtener primeros resultados de la propuesta brindada.

1.6 Alcances y beneficios del proyecto

El proyecto va a generar un impacto positivo directo asociado a la disponibilidad de los servicios de TIC, debido a que tiene como objetivo principal que a través de procesos preventivos se pueda reducir incidentes y problemas que afectan de forma negativa los servicios de TIC.

El marco de referencia de ITIL habla de incidentes, problemas y solicitudes de servicio. Lo que se pretende con la gestión preventiva de la infraestructura de TIC está asociada únicamente a incidentes y problemas.

Los incidentes y problemas que no estén asociados a la infraestructura de TIC y solicitudes de servicio en general direccionadas al Departamento de TIC estarían fuera del alcance de este proyecto.

No se puede evitar al 100% que haya afectación de los servicios de TIC y con esto los servicios que brinda el hospital, pero al menos se puede mejorar la gestión de la infraestructura de TI y prevenir incidencias. El funcionamiento de los elementos de infraestructura de TIC debe ser medido con el mismo fin de evitar fallas.

El alcance de este proyecto está en definir una propuesta de procesos preventivos asociado a principales incidentes que se han presentado y que más han afectado, basado en una indagación con las personas que brindan soporte a esa infraestructura de TIC y Jefe de TI, quienes son los únicos que pueden dar el detalle técnico y a la vez impacto de los incidentes.

Parte del alcance del proyecto es implementar un plan piloto de un proceso asociado a la gestión preventiva, como esfuerzo inicial para que luego siga siendo desarrollado por el personal del hospital y de ser necesario con colaboración de sus proveedores.

El beneficio personal estará asociado a la implementación de procesos desde una perspectiva estratégica, además, tener a disposición recurso humano para que se faciliten las labores asociadas a los procesos y los mismos llegan a brindar medidas para que sean llevadas a cabo en mejora del soporte y servicio de TI brindado al hospital.

A nivel de la maestría, se desarrolla un proyecto estratégico enfocado en un tema de combinación de Administración del Servicio de TI, pero enfocada a la gestión de infraestructura de TI, tomando en cuenta varios elementos de los diferentes cursos vistos a

lo largo de la maestría, pero principalmente enfocándose en la puesta en marcha de cursos tales como gestión de servicio TIC y gestión de infraestructura.

2 CAPÍTULO II: MARCO CONCEPTUAL

Este proyecto involucra varios temas asociados a la gestión de servicios de TI, además, la calidad en estos servicios, que por sí solo representa temas por desarrollar de forma teórica. Además, directamente asociado al proyecto, es importante desarrollar de forma teórica sobre buenas prácticas y recomendaciones asociadas una gestión preventiva de TI, para mejora en la calidad de los servicios brindados.

2.1 Gestión de servicios de TI

Un servicio es un medio o una actividad que es utilizada por un cliente por el valor que le genera, pero además, este cliente no está asumiendo los costes que su uso le genera, los cuales lo asume quien se lo provee.

A nivel de servicios de tecnología de información o TI, aplica el mismo concepto de servicio, solo que estos servicios están asociados a herramientas informáticas que para el cliente final le generan valor dentro de sus operaciones y proyectos. Estos clientes pueden ser internos, es decir, dentro de la misma compañía, o clientes externos a la compañía en la que provee los servicios.

La gestión de servicios de TI "refiere al conjunto de actividades, dirigidas por políticas, procesos organizados y estructurados y procedimientos de apoyo, que son ejecutadas por una organización o parte de ella para planear, entregar, operar y controlar servicios de TI ofrecidos a los clientes" (Wikipedia Foundation, 2015). Esta gestión de servicios de TI involucra personas, procesos y las propias tecnologías de información y se encarga de la calidad de esos servicios de TI.

La gestión de servicios de TI se relaciona mucho con el conjunto de buenas prácticas que representa el marco de trabajo de ITIL, el cual se basa en la definición de diferentes procesos estratégicos, de diseño, de transición, de operación y mejora continua como parte de un ciclo de vida de la gestión de servicios de TI. Adicionalmente existen otros marcos de trabajo relacionados:

- Business Process Framework (eTOM): marco de trabajo para proveedores de servicios de telecomunicaciones.
- COBIT: es un marco de gobernanza de TI que especifica los objetivos de control, métricas y modelos de madurez.

- FitSM: es un estándar para la gestión del servicio más ligero. Contiene varias partes, incluyendo, por ejemplo: requisitos auditables y plantillas de documentos, que se publican bajo licencias *Creative Commons* (licencias de uso público).
- ISO/IEC 20000: es un estándar internacional para la gestión y entrega de servicios de TI.
- MOF (Microsoft Operations Framework): además, de un marco general de las funciones de gestión de servicios, está orientado a la gestión de los servicios basados en tecnologías de Microsoft. (Wikipedia Foundation, 2015)

Como se indicó, la gestión de servicios de TI debe buscar una calidad, este último concepto definido bastante bien por Horacio Lago, que define la calidad como "característica de un producto, servicio o proceso para proporcionar su propio valor y cumplir con determinados requisitos" (Lago, 2010).

Para saber si se tiene calidad deben implementarse mecanismos, que permitan medir la misma, lo cual estará involucrado en este proyecto ya que a través de medidas y procesos preventivos se pretende mejorar la calidad de servicios que actualmente se proveen.

2.2 Estrategia de gestión de servicios de TI

El Departamento de TI de cualquier compañía, como proveedor de servicios técnicos internos, debe generar valor al negocio de esa empresa, de otra forma no representa más que un gasto.

Para generar valor a una empresa, se deben alinear los esfuerzos a los objetivos estratégicos de la misma. El Departamento de servicios de TI debe tener objetivos propios que busquen alinearse a los objetivos globales de la empresa, para conseguir estos objetivos se debe desarrollar un plan, es lo que se reconoce como una estrategia, en este caso una estrategia en la gestión de servicios de TI.

La multinacional europea especialista en servicios de TI OSIATIS define puntos que deben estar presentes dentro de la estrategia de servicios de TI, algunos de estos son los siguientes:

- Servir de guía a la hora de establecer y priorizar objetivos y oportunidades.
- Proponer servicios diferenciados que aporten valor añadido al cliente.

- Alinear los servicios ofrecidos con la estrategia de negocio.
- Elaborar planes que permitan un crecimiento sostenible.
- Crear casos de negocio para justificar inversiones estratégicas (OSIATIS S.A., 2015).
- En Costa Rica la CCSS es una institución estatal autónoma que tiene como parte de su estrategia mejorar la prevención y atención de problemas que atenten la salud de los asociados, todos los centros médicos que administra funcionan bajo esta estrategia.

El Hospital México debe brindar servicios muy especializados de salud y las tecnologías de información deben estar disponibles para soportar esos servicios de salud, por tanto, la estrategia del Departamento de TI debe estar alineada a brindar disponibilidad y calidad de servicios tecnológicos, que van a colaborar con la estrategia global del hospital y su institución madre, la CCSS.

2.3 Gestión preventiva de servicios de TI

La gestión preventiva por sí sola es un concepto general que no solo se aplica a los servicios de TI, se busca evitar hechos indeseados como malas prácticas, errores, repeticiones de trabajo, afectación de calidad y/o disponibilidad, que se asocian a riesgos de diferente tipos en diferentes campos, como riesgos de salud, laborales, comerciales y más asociado a este proyecto de tecnología de información.

A nivel de tecnologías de información y comunicación, hay riesgos que siempre van a estar presentes, debido a que hardware, software y las personas que lo administran no son cien por ciento infalibles y todos presentan vulnerabilidades.

Como otros modelos de gestión, la gestión preventiva se desarrolla a través de un ciclo, tal y como lo muestra en su documento de modelo de gestión preventiva la Fundación INVATE, reflejado en la siguiente ilustración:

Ilustración 1: Ciclo de vida de gestión Fuente: Fundación INVATE, 2011

En el documento la fundación propone un modelo para la prevención principalmente asociado a accidentes laborales, pero bien puede aplicarse a nivel de servicios de TI ya que el objetivo de prevenir hechos inesperados es el mismo. Para cada fase se define lo siguiente:

1. Planificación: prever anticipadamente lo que debe hacerse, conciliando recursos disponibles con los objetivos y oportunidades de la empresa.
2. Organización: definir y atribuir con claridad las tareas de cada uno, de modo que todos sepan exactamente lo que se espera como resultado.
3. Ejecución: llevar a cabo las tareas necesarias para la consecución de lo planificado.
4. Control: medir el desempeño de lo ejecutado, comparándolo con los objetivos y metas fijados; detectar las desviaciones y proponer las medidas necesarias para corregirlas. (Fundación INVATE, 2011)

Si se llevan estas fases al ambiente de gestión de servicios de TI, se trata en esencia de lo mismo:

1. En un principio se planifica lo que se quiere con la gestión preventiva, se definen objetivos y se analiza que se oportunidades y recursos presenta actualmente el Departamento de TI para llevar a cabo esta gestión.
2. Asociado a la organización, se definen los procesos, con entradas y salidas de los mismos, donde se definen roles y funciones asociadas dentro de la gestión de los servicios que proporciona el Departamento de TI.
3. Como parte de la ejecución, se implementan los procesos previamente diseñados, involucrando personas, procesos y recursos tecnológicos disponibles.
4. Como control se analizan métricas definidas.

En este proyecto se va a trabajar sobre todo en la definición de procesos, lo cual involucra en parte la planificación que ya se ha comentado previamente con objetivos que se han propuesto. De manera adicional se va a realizar una ejecución inicial de algún sub proceso de gestión preventiva y se van a definir mecanismos de control de los mismos.

2.4 Gestión de infraestructura tecnológica

Este proyecto está limitado a gestionar elementos de infraestructura tecnológica, que el concepto de infraestructura de TI se asocia con "equipos, programas, recursos de red y servicios compuestos necesarios para la existencia, el funcionamiento y la gestión de un entorno de TI de la empresa." (Janalta Interactive Inc). La anterior se resume en:

- Hardware: servidores, computadoras, equipos de red, equipos de gestión de datos. Incluyendo sus sistemas operativos.
- Programas: software de aplicación a nivel empresarial, como ERP (Enterprise resource planning), CRM (customer relationship management).
- Instalaciones físicas como centros de datos, interconexiones de equipos.

Para el caso del Hospital México la infraestructura más importante es la de Hardware ya que no utilizan software programas de software asociados a la infraestructura de TI y las instalaciones físicas dependen mucho del Hardware que se gestiona.

La gestión de la infraestructura de TIC es una de las funciones bajo la gestión de servicios de TI. Se trata de la gestión de políticas, procesos, equipos, datos, recursos humanos y otros recursos internos y externos asociados a la infraestructura de TI.

Cuando se gestiona infraestructura, por lo general se dividen el esfuerzo de soporte en gestión de sistemas (servidores), gestión de red y gestión de almacenamiento de datos. La gestión de infraestructura en el Hospital México está asociada principalmente a equipos y software de fabricantes como Cisco (equipos de red), Hewlett-Packard (servidores y almacenamiento de datos) y Microsoft (sistemas operativos).

2.5 Gestión de eventos

Un evento se refiere a un cambio relevante de estado de un elemento o servicio de TIC. La gestión de estos eventos involucra definir cuáles son relevantes y cómo se van a monitorear, qué alertas se van a generar ante los cambios de estado, y qué hacer ante estas alertas. Todo esto con el fin de anticiparse a incidentes, e inclusive resolverlos y prevenir su impacto.

El marco de referencia de ITIL define tres tipos de eventos:

- Informacional: un evento básicamente informativo, no requiere ninguna acción y no representa una amenaza. Como ejemplo: la notificación que un respaldo se realizó de forma correcta o indicar que se efectuó una autenticación correcta a una aplicación.
- Warning: es una advertencia, que se manifiesta como una notificación generada cuando un dispositivo o servicio se aproxima a un límite que comprometa su buen funcionamiento. Como ejemplo: elevación de CPU de un dispositivo más allá de lo normal de su utilización o intentos de ingresos a un sistema con credenciales incorrectas.
- Excepción: es un evento de que un dispositivo o servicio no está funcionando de manera adecuada. Como ejemplo: el porcentaje de uso de memoria de un dispositivo llega a un 95% de su disponible o una transacción está tomando un tiempo considerable mayor al normal.

En primera instancia se deben identificar los elementos por monitorear, también conocidos como ítems de configuración (CI:Configration Items), para este proyecto, se trata

principalmente de servidores y equipos de red, aunque podría tomarse en cuenta otros aspectos como temperaturas de espacios físicos o tiempos de vida de licencias.

Otra forma de categorizar los eventos de un CI es basado en la capacidad de detalle o profundidad en la cual se quiera monitorear un elemento, mostrado en la siguiente pirámide, donde la base muestra lo más básico por monitorear que es la disponibilidad el CI y en lo más alto, eventos más complejos de monitorear, pero que permiten tener más información del funcionamiento del CI.

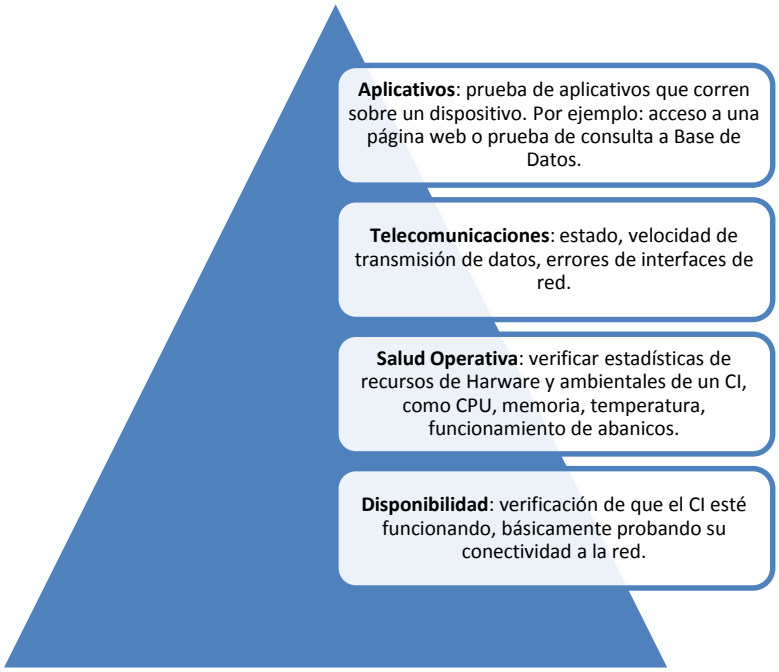


Ilustración 2: Categorización de eventos basado en información que brinda

Estas categorías de eventos pueden extraerse de varios CI de infraestructura de TI, todo depende de la capacidad del fabricante del equipo que habilita la lectura de estadísticas respectivas a lo que se desee monitorear, que en algunos casos por propias limitaciones del equipo, no se van a poder gestionar eventos en todas las categorías.

2.5.1 Herramientas de monitoreo

Para gestionar los eventos, se requiere de un software que utilice diferentes herramientas para monitoreo y procesamiento de estos eventos, que verifica el estado de los elementos de TIC y su disponibilidad, en caso de detectar una cambio de estado que comprometa el funcionamiento de un dispositivo o servicio, generar la alerta respectiva.

Se tienen herramientas de monitoreo que trabajan de forma activa, donde a cada elemento por monitorear se valida el estado y disponibilidad, en caso de detectar algún evento relevante, generar la alerta. Algunos ejemplos de herramientas utilizadas para el monitoreo activo son:

- PING: en una herramienta que se compone de mensajes de solicitud y respuesta a una dirección IP de un equipo, de esta forma se puede determinar si el equipo está activo y el tiempo de respuesta, entre otros valores. Un servidor de monitoreo enviaría un mensaje de solicitud, esperando que el equipo por monitorear lo responda y así determinar si el equipo tiene conectividad de red. La siguiente imagen muestra un ejemplo de un PING donde se valida la correcta conexión al equipo con la dirección IP 8.8.8.8.

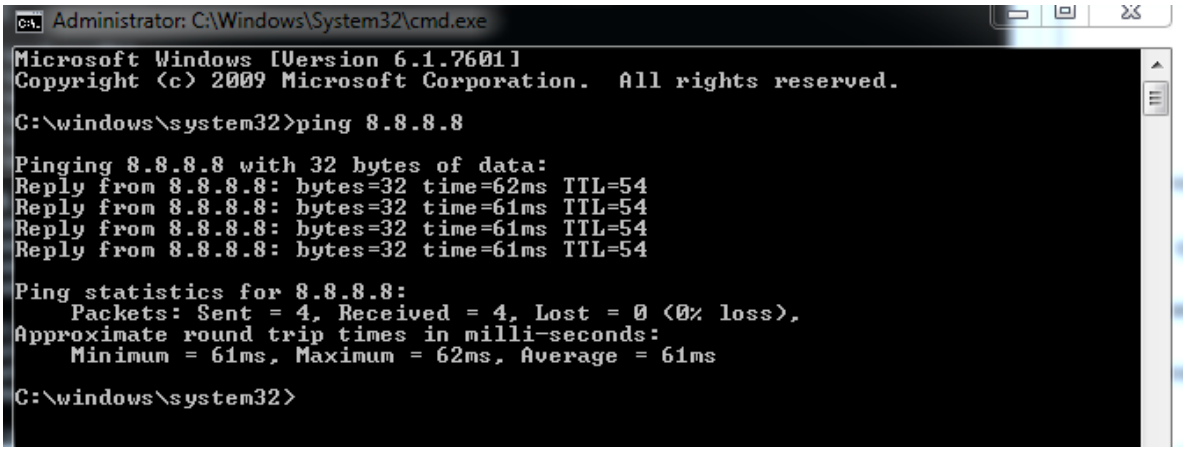


Ilustración 3: Ejemplo de PING

- Traceroute: Herramienta utilizada para reconocer el camino a través de la red que se utiliza para conectarse a un destino. Funciona bajo un protocolo similar al PING, de manera que va indicándose el rastro desde el origen hasta una dirección IP destino y en tiempo que toma en cada salto. La siguiente imagen muestra un ejemplo de un Traceroute

Ilustración 4: Ejemplo de uso de Traceroute

- Colector SNMP: SNMP viene de sus siglas en inglés (Simple Network Management Protocol) y como su nombre lo indica, es un protocolo para gestión de la red. Un colector de SNMP constituye un equipo que establece una sesión con otro, a este último a través de una autenticación por SNMP le puede extraer estadísticas del equipo, tales como porcentaje de uso de CPU, memoria, temperatura, funcionamiento de hardware como ventiladores, interfaces de red y muchos más.

Existen herramienta que trabajan de forma pasiva y alertan sólo cuando el elemento o CI le informe un evento. Algunas herramientas pasivas son:

- Monitorización de logs: un log se refiere a un mensaje que genera un equipo ante un evento en el mismo. Se puede utilizar este mensaje como herramienta de monitoreo pasiva, de forma tal que cuando un equipo genere un log, lo envíe a la consola de monitoreo y de esta forma se genere una alerta
- Receptores SNMP: funciona bajo el mismo protocolo de SNMP, pero en este caso el equipo es quién genera un mensaje y lo envía hacia el servidor de monitoreo sin que este último lo haya solicitado, este mensajes conocido como trap, permite indicar un evento, por ejemplo: apagado de un interface debido a un ataque de seguridad.

Una herramienta de código abierto para monitoreo se llama NAGIOS, esta combina varias herramientas para monitoreo y notificación de alertas.

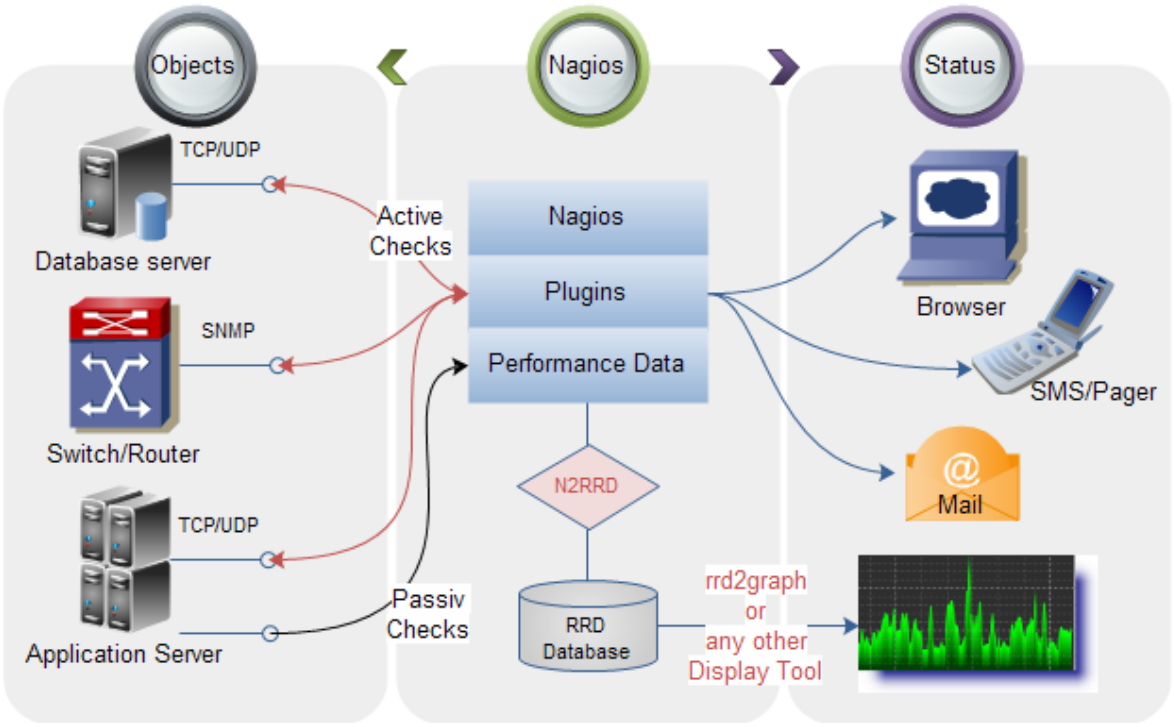


Ilustración 5: Funcionamiento de herramienta de monitoreo NAGIOS Fuente: Fundación Wikimedia, Inc., 2015

Se pueden observar en esta ilustración con líneas rojas herramientas de monitoreo activo usando verificación de puertos TCP/UDP como puerto 80 para web de HTTP, colección de estadísticas por SNMP. Con líneas negras herramientas pasivas, donde es el equipo quien le envía el mensaje a la herramienta de monitoreo.

El término de puertos TCP y UDP se refiere a valores numéricos por los que se establecen sesiones entre equipos, por ejemplo: como se mencionó antes, para ver una página web, se establece una sesión con el servidor por el puerto TCP 80 como un puerto estándar. La diferencia entre puertos TCP y UDP es que las sesiones a través de puertos TCP retransmiten paquetes de datos perdidos, mientras que por UDP no se retransmiten paquetes perdidos, principalmente por el tipo de aplicaciones que no lo requieren, como aplicaciones de telefonía IP.

Se puede observar adicionalmente en la ilustración envío de alertas por correo electrónico y mensajes a teléfonos celulares, y visualización de las alertas por explorador web.

Además el mismo Nagios, tiene una base de datos donde almacena eventos que se han dado, se pueden consultar y los mismos representarlos de manera gráfica a través del mismo explorador web.

Se reconocen principalmente cinco herramientas de monitoreo libres y/o de código abierto, estas son "Nagios, Zabbix, Cacti, Zenoss y Munin" (Auza, 2010), tomado del artículo del sitio web TECHSOURCE.

La versión Nagios Core es la de código abierto, no tiene costo el descargarlo y usarlo, además, cumple con varias características, como las siguientes anunciadas en su sitio web:

- Monitoreo de servicios de red (SMTP, POP3, HTTP, NNTP, PING, etc.).
- Monitoreo de recursos de equipos (carga de procesador, uso de disco, etc.).
- Permite crear a usuarios sus propias formas de monitoreo.
- Notificaciones a contactos cuando problemas de servicios o de equipos ocurren y se resuelven (vía email, mensajes a equipos portátiles, métodos definidos por el usuario).
- Posibilidad de implementación de monitoreo redundantes.
- Interfaz web opcional para ver el estado de eventos actuales de la red, historia de problemas y notificaciones, logs, etc. (Nagios Enterprises, LLC, 2009-2016).

Para instalar Nagios Core se recomienda un servidor con sistema operativo basado en Linux como Ubuntu, Fedora, Debian, además, de tener ciertos elementos instalados como servidor Web apache y PHP 5, este último un código de programación.

Con respecto al hardware requerido en el servidor, se tiene lo siguiente, como mínimo recomendado tomado del sitio web de Nagios Enterprises, LLC, 2009:

- 2 GHz+ CPU
- 1 GB+ RAM
- 2 GB de espacio libre de disco

2.5.2 Enfoques para atender la gestión de eventos

En la línea de libros y documentos Redbooks de IBM, se encuentra un libro denominado "Event Management and Best Practices", que traducido del inglés es un libro para gestión de eventos y mejores prácticas asociadas. Los autores Bhe, Glasmacher, Meckwood, Pereira y Wallace de este libro publicado en 2004, ofrecen en general un enfoque de gestión de eventos aún válido, ya que en concepto en sí ha estado presente desde hace varios años, con la aparición de nuevas tecnologías, pueden traer consigo nuevos eventos por tomar en cuenta, pero la gestión de eventos como tal es la misma que exponen en el libro aplicado a la actualidad.

Este libro, "Event Management and Best Practices", define los siguientes enfoques para desarrollar la gestión de eventos, estos se resumen de la siguiente manera:

- Enviar todos los eventos posibles: Es el más fácil de implementar, simplemente cada dispositivo que se elige a monitorear envía todas las alertas, logs y demás al servidor de monitoreo. Como desventaja, genera más carga a la red, llegan mensajes que realmente no representan mayor relevancia o un problema real, por tanto, muchos mensajes son ignorados.
- Comenzar con notificaciones por defecto y analizarlas de forma reiterativa: Se refiere a monitorear básicamente eventos que el fabricante de un determinado CI define como recomendados. Se confía en el buen juicio del fabricante, no obstante, pueden presentarse eventos que no se comprenden con facilidad, adicionalmente, aplicaciones hechas en casa no podrían ser monitoreadas bajo este enfoque.
- Reportar solo problemas conocidos y agregar eventos adicionales a la lista tan pronto son identificados: se informa de los eventos que indican problemas reales. Cuando se producen nuevos problemas, los técnicos responsables de la resolución determinan si un mensaje de registro se puede extraer o un monitor desplegado para comprobar la condición de error. No genera trabajo extra pues si hay algún evento reportado, es porque realmente está asociado a un problema reconocido, que posiblemente se sabe cómo atenderlo. Con la desventaja de que el problema debe en realidad ocurrir para ser luego reportado, no pudiéndose prevenir la primera vez que se dé.

- Escoger el top X de problemas de cada área: diferentes áreas de soporte indican los principales problemas, como son condiciones que más frecuentemente se dan, o que no se dan tan frecuentes, pero en caso de materializarse, generarían un gran impacto. A diferencia del anterior, no solo se toma en cuenta los problemas que haya pasado, sino que se involucra eventos que vayan a generar un gran impacto. De igual forma se reciben notificaciones definidas y controladas. Además, de igual forma no se recibirían notificaciones de problemas que no se conocen.
- IBM define una metodología más detallada que denominan Event Management and Monitoring Design (EMMD), que traducido significa básicamente gestión de eventos y diseño de monitoreo. Se definen los siguientes pasos:
    1. Definir alcance: Decidir qué servicios o fuentes de agentes de monitoreo se van a analizar. Principalmente se toman en cuenta elementos críticos al negocio, basándose en servicios brindados.
    2. Determinar políticas de control de eventos: Definir qué acciones tomar ante eventos de forma particular. Miembros clave deben trabajar para desarrollar estas políticas.
    3. Documentación de repertorio de eventos: los eventos enviados por una fuente son recopilados en documentos como hojas de Excel, los cuales son usados para tomar decisiones acerca de los mismos. En caso que una fuente envíe muchos eventos, se pueden limitar basado en filtros, aquellos eventos asociados a cambios de configuración o que no reporte eventos de tipo informacional. Esta lista debe actualizarse y ajustarse en un marco de tiempo definido de dos a cuatro semanas
    4. Selección de monitores y umbrales: revisar el monitoreo existente, en caso de haber, sugerir nuevos monitoreo para asegurar que los eventos son reportados. Además, definir umbrales basados en buenas prácticas.
    5. Documentación de decisiones del control de eventos: expertos en temas asociados a los elementos por monitorear definen qué filtrar, enviar, notificar, y acciones automatizadas para cada evento dentro del repertorio. Se definen severidades de los eventos, prioridades de tiquetes de incidentes, nombres de scripts automatizados.

6. Conducir un análisis de correlación de eventos: definir una correlación de los eventos. Se establece la relación de eventos basado en el significado de varios de los eventos.
7. Revisión de entregables: Política de control de eventos, hojas del repertorio de eventos completo, diagramas de correlación de eventos. Se debe revisar que sea entendido por los responsables de la gestión de eventos y monitoreo.
8. Definición de un plan de implementación: Discutir las formas de implementar el diseño y desarrollar un plan de implementación. El plan incluye orden en el que los eventos deben ser configurados, tareas requeridas para completar la implementación, partes responsables, pruebas y plan para dar marcha atrás a cambios. (págs. 26-31)

2.6 Gestión de seguridad informática

Con la seguridad informática se busca mantener la confidencialidad, integridad y disponibilidad de la información, así como de los elementos de software y hardware que administran y trasmiten esta información.

Un sistema de gestión de seguridad informática (SGSI) se refiera a un conjunto de políticas a seguir, con normas que rigen cómo se realiza el acceso a la información, control de acceso, manejo de credenciales, entre otros aspectos.

Para este proyecto, se enfocará la gestión de la seguridad a generar políticas asociadas a administración de equipos de red y acceso por parte de usuarios a la red.

Debido a que las organizaciones y sus sistemas de información cambian constantemente, las actividades dentro del proceso de gestión de la seguridad deben ser revisados de forma continua, con el fin de mantenerse actualizadas. Con este fin, para orientar estas políticas del proyecto, se va a seguir un enunciado del estándar de gestión de seguridad informática ISO/IEC 27001, este estándar especifica los requisitos necesarios para "establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI)" (Fundación Wikimedia, Inc, 2016), el cual se basa en el ciclo de Deming (Plan-Do-Check-Act) de la siguiente forma como lo expresa Allen, J. H en 2013:

- Plan: Establecer política del SGSI, objetivos, procesos y procedimientos relacionados con el manejo de riesgos y la mejora de la seguridad de información para conseguir resultados de acuerdo con las políticas y objetivos generales de la organización.
- Do: implementar y operar las políticas, controles, procesos y procedimientos del SGSI.
- Check: Evaluar y, en su caso, medir el rendimiento del proceso contra la política del SGSI, objetivos y la experiencia práctica e informar de los resultados a la dirección para su revisión.
- Act: tomar acciones correctivas y preventivas, con base en los resultados de la auditoría y la gestión de revisión interna del SGSI u otra información relevante, para lograr la mejora continua del SGSI.

Cabe aclarar que el hecho que se tome el enunciado asociado al estándar, no quiere decir que se pretende la certificación. Simplemente es una referencia para definir las políticas por desarrollar en el hospital.

2.6.1 Buenas prácticas de seguridad para administración de equipos de red

Para este caso específico, el tema de administración de equipos de red se refiere al acceder al equipo y poder realizar cambios en su configuración de forma lógica principalmente.

Lo que se pretenden con las prácticas de seguridad asociadas a la administración de equipos de red es limitar en lo posible el acceso a sólo usuarios autorizados, evitando prácticas que atentan contra la seguridad de los equipos, como suplantación de identidad, de forma que un usuario maligno ingresa al equipo haciéndose pasar por un usuario autorizado, y dentro del equipo puede comprometer la disponibilidad, integridad y confidencialidad del equipo e información transmitida a través de ellos.

Existen muchas prácticas de seguridad para administración de equipos de red, se enumeran algunas, que además, puedan ser implementadas sin importar los fabricantes de los equipos de red:

1. La administración por puerto de consola requiere conexión física frente al equipo para poder ser realizada. Esta administración permite tener privilegios de administración total del dispositivo. La recomendación es que cualquier equipo de red debe estar protegido con seguridad físicamente en compartimientos de acceso

a sólo usuarios autorizados a través de cerraduras y controles de acceso. Inclusive en centros de datos o donde haya equipos de red muy importantes ubicar cámaras de seguridad para registrar quién o quienes tiene accesos a esos equipos.

2. Administración de equipos de forma remota siempre debe utilizar autenticación, es decir, que solicite credenciales que solo usuarios autorizados a los equipos tengan acceso. Es altamente recomendado que cada usuario tenga sus propias credenciales, inclusive con credenciales manejadas a través de un servidor RADIUS (Remote Authentication Dial-In User Service), este servidor puede asociarse a las credenciales de directorio activo del usuario autorizado, e inclusive registrar horas de ingreso.
3. Utilizar contraseñas que no sean fáciles para descifrar, por ejemplo: combinar letras mayúsculas, minúsculas y números, con una extensión mayor a 6 dígitos. Siempre que se guarden contraseñas como parte de la configuración de los equipos, se deben realizar configuraciones de forma tal que se encripten las mismas contraseñas y no sean descifrables.
4. Una recomendación con respecto a mensajes al ingresar a equipos es la siguiente:

> Cuando los usuarios acceden con éxito un equipo de red, deben ser conscientes de las políticas de acceso y de uso aceptable pertinente a su organización. Debe configurarse mensajes del sistema para que se muestre este tipo de información cuando los usuarios accedan a un equipo de red. La idea es advertir a los usuarios no autorizados (en caso de que tengan acceso) que sus actividades podrían ser penadas o castigadas, o que no son bien recibidos, por lo menos. (Hucaby, 2010, p.385).

5. Es altamente recomendado utilizar métodos de administración segura, donde credenciales no se transmiten en texto claro a través de la red, para esto por ejemplo: en lugar de usar TELNET, se debe usar SSH para la administración por línea de comandos. Por otra parte, si no se requiere administración vía web, deshabilitar la misma, como mínimo sólo utilizar el protocolo HTTPS, en lugar del protocolo HTTPS ya que este último encripta las credenciales a través de la red.
6. Se debe configurar dentro de los equipos que solo ciertos segmentos autorizados de la red puedan realmente administrar los equipos de forma remota, esto a través de un control por listas de acceso que filtren por dirección IP de cada equipo, si

realmente puede ingresar o no ya que esta dirección IP es identificador único dentro de la red para cada equipo.

7. En caso de que el equipo sea monitoreado a través del protocolo SNMP (Simple Network Management Protocol), se debe de igual filtrar su acceso por este protocolo, que sólo ciertos equipos lo puedan monitorear. Además, utilizar credenciales de solo lectura, que no se utilicen credenciales de escritura, que pueden ser mal utilizadas para alterar la configuración del equipo.

2.6.2 Buenas prácticas de seguridad para acceso a la red

Por acceso de red, en este caso, se refiere a como los usuarios pueden acceder a la red, además, qué prácticas se pueden implementar a nivel de medios cableados e inalámbricos, para no comprometer la seguridad y disponibilidad de los equipos de red e información que estos transmiten.

Existen muchas prácticas que pueden realizarse para controlar el acceso a la red, ya sea inalámbrico o cableado. Algunas de ellas son las siguientes:

a. Identificar puertos de red que no estén conectados en switches, principalmente en switches de acceso de usuarios y apagar los mismos, o cómo mínimo asignarlos a una VLAN (red virtual) aislada al resto del tráfico del resto del tráfico del hospital. Esto principalmente para evitar que a través de algún puerto libre cualquier usuario ajeno a usuarios del hospital tenga acceso a la red.
b. Una dirección MAC es un identificador de red que permite reconocer las tarjetas de red de los diferentes equipos, es un identificador único. Los switches de red, como parte de su funcionamiento, aprenden estas direcciones MAC de los equipos que se conectan en la red, estos se almacenan en una tabla interna del equipo, que tiene un máximo de entradas, si se alcanza ese máximo de entradas, se compromete el correcto funcionamiento del equipo. En ambientes donde las computadoras son estacionarias, se debe limitar el número de direcciones MAC aprendidas en un puerto ya que posiblemente solo uno o dos equipos estén normalmente conectados. Esta práctica se da porque existen ataques donde se simula la existencia de muchas direcciones MAC en un puerto de red, esto intentando que se llene la tabla de direcciones MAC aprendidas por un equipo y de esta forma afectar el funcionamiento de ese equipo de red.

c. Los puertos donde se conecta a usuarios finales, deben ser configurados como puertos de acceso, no dejarlos configurados a su funcionamiento por defecto pues si se deja de esta forma, un usuario puede conectar otro switch de red no autorizado y usando diferentes protocolos y mensajes que intercambian entre switches de red, generar afectación a los switches de red autorizados y existentes en la red.
d. Asociada a la recomendación anterior, existen un protocolo estándar para el funcionamiento de switches de red que se conoce como su nombre en inglés, Spanning-Tree Protocol *(STP),* este funciona a través de mensajes que se conocen como BPDU. En puertos de acceso de usuarios no permitir que se reciban estos mensajes de BPDU, para esto se debe habilitar una opción denominada *BPDU* protection*,* es decir, protección de BPDU. Esta recomendación se da por el mismo hecho que switches no autorizados pueden utilizar la conexión de usuarios para enviar estos mensajes e intentar modificar el comportamiento del protocolo de STP de los switches autorizados y existentes en la red.
e. Se puede implementar una práctica de autenticación de las conexiones a los puertos, e inclusive a la red inalámbrica. De forma tal que quien se conecte, debe tener credenciales, certificados, identificador de red como MAC Address o una combinación de ellas que le permitan el acceso a la red. De esta forma identificar un usuario legítimo y en caso que no presente alguno de los elementos que se utiliza para autenticarlo, no se permita el acceso a la red. Para realizar esta labor se utiliza el protocolo estándar 802.1x, y se requiere implementar un servidor RADIUS.
f. DHCP es un protocolo a través del cual se obtiene direccionamiento IP de forma dinámica para poder conectarse a la red, donde un servidor provee ese direccionamiento. Existe un ataque denominado DHCP Spoofing, para este ataque un equipo se hace pasar por el servidor DHCP y brinda direcciones IP de forma no autorizada, esto genera desconexiones e incidentes en equipos de usuarios finales, inclusive un atacante puede brindar el mismo direccionamiento de red existente, pero hacer el tráfico pasa primero por un equipo antes que llegue el destino final, entonces poder ver la información de un usuario en la red. Se debe configurar la funcionalidad de DHCP Spoofing, lo cual permite indicar a través de cuales puertos se van a autorizar respuestas de un servidor DHCP y lo que no se configure como un puerto confiable, no va a poder brindar direccionamiento por DHCP.

g. Algunas recomendaciones básicas para redes inalámbricas son las siguientes:
    i. Utilizar encriptación a través de la red inalámbrica, existen dos opciones, Wi-Fi Protected Access (WPA) y Wired Equivalent Privacy (WEP). Utilizar WPA que es de encriptación más fuerte, inclusive existen equipos que usan la versión WPA 2, si el equipo que se conecta a la red inalámbrica, como el que permite la conexión pueden utilizar esta versión 2, utilizarla.
    ii. No utilizar nombres de redes inalámbricas descriptivos como "Hospital", "Administrativa", "Gerencia" ya que esto permite a un usuario externo conocer el tipo de tráfico de red que va a pasar por esa red. No se debe no dejar el nombre una red inalámbrica privada como su nombre por defecto y además, dejar la red oculta.
    iii. Utilizar contraseñas para acceso a la red inalámbrica que no sean fácilmente descifrables o recordables.
    iv. De forma opcional, usar el filtrado por dirección MAC, de forma que en el equipo de red inalámbrica se especifique exactamente cuáles equipos pueden acceder a la red inalámbrica. Sin embargo, la administración se puede complicar al tratarse de muchos equipos y no tener una administración centralizada.
    v. Utilizar método de Encriptación WPA2, o como mínimo WPA de no estar disponible WPA2, estos son más seguros en comparación al método WEP.

2.7 Cierre de Marco Conceptual

Se presenta en esta sección número 2 inicialmente la definición de conceptos de gestión asociados a la propuesta, que van de lo general como lo que es la gestión de TI como tal, hasta llegar a temas específicos asociados directamente a la propuesta de gestión de procesos preventivos, con la gestión de eventos y la gestión de seguridad de red.

Se revisan diferentes teorías al tener variedad en los conceptos, pero todos los conceptos al final alineados con una mejora en la gestión de servicios de TI, que es parte de lo que se busca con el proyecto.

Los elementos que más favorecen la propuesta están en un principio con los enfoques asociados a la gestión de eventos, que indican cómo realizarla a cabo la misma, con buenas prácticas recomendadas.

Por otra parte, con respecto a la gestión de seguridad, se definen muchas buenas prácticas, principalmente asociadas a juicio experto en el ambiente de redes, las cuales serán posteriormente diagnosticadas con respecto a la situación actual y cuáles se llevan a cabo, para así basado en el ciclo de Deming mostrado, definir como llevar a cabo las que están pendientes.

3 CAPÍTULO III: MARCO METODOLÓGICO

3.1 Naturaleza de la investigación

La investigación propuesta parte de un análisis de datos sin medición numérica, por tanto, esta investigación es de carácter cualitativo, siendo el enfoque relacionado con la definición de conceptos, el descubrimiento de datos o la mejor definición de preguntas de investigación.

En el libro de Metodología de la Investigación se indica que el "Enfoque cualitativo Utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación." (Hernández Sampieri, Fernández Collado, & Baptista Lucio, Meodología de la investigación, 2010, pág. 7)

Una de las características de la investigación cualitativa es su capacidad de variar conforme se analizan los datos, basados en esto se plantea una recolección y análisis de datos simultánea que puede ir arrojando respuestas claras a la investigación, pero también puede definir pequeños virajes o adaptaciones que se deban desarrollar en el transcurso de la misma.

Lo anterior de igual forma que coincide con lo enunciado En el libro de Metodología de la Investigación:

> "El enfoque cualitativo5 también se guía por áreas o temas significativos de investigación. Sin embargo, en lugar de que la claridad sobre las preguntas de investigación e hipótesis preceda a la recolección y el análisis de los datos (como en la mayoría de los estudios cuantitativos), los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos. Con frecuencia, estas actividades sirven, primero, para descubrir cuáles son las preguntas de investigación más importantes, y después, para refinarlas y responderlas." (Hernández Sampieri, Fernández Collado, & Baptista Lucio, Meodología de la investigación, 2010, pág. 7)

Para guiar el proyecto al diseño de procesos asociados a la gestión preventiva de incidentes asociados a la infraestructura que administra en Departamento de TI, primeramente se va obtiene información de las personas inmersas en el ambiente de infraestructura de TIC del hospital, se enfoca en estas personas por que tienen la capacidad de brindar trasfondo

técnico, además, a través del contacto con usuarios finales a quién han soportado, entienden el impacto de los incidentes que se han dado y pueden seguir presentándose.

La información obtenida por parte de ellos marca un camino claro respecto a la dirección de la investigación, pero también puede arrojar nueva información no estipulada al inicio y que presente un grado de importancia tal que daba ser abordado. Parte de esta flexibilidad o capacidad de adaptación es clave en la investigación cualitativa.

La investigación cualitativa permitirá hacer un análisis de campo más profundo y flexible respecto a la problemática planteada, obtener resultados de este y formular hipótesis en el proceso, para lograr así un resultado específico a la problemática, no se pretende desarrollar o identificar una tendencia de gestión preventiva de infraestructura general, sino más bien específica a la realidad del Hospital México.

3.2 Tipo de diseño de Investigación

Se realizará la investigación desde un enfoque no experimental, el cual "se realiza sin la manipulación deliberada de variables y los fenómenos se estudian en su ambiente natural para después analizarlos" (Hernández Sampieri, Fernández Collado, & Baptista Lucio, Metodología de la Investigación, 2010, pág. 149), objetivo de la presente investigación generar hipótesis, más concretamente generar un diseño de procesos de gestión preventiva, basado en lo observado.

Adicionalmente la investigación se realizará en un momento específico para estudiar un fenómeno en particular de la institución, por lo que a la investigación también se le dará un enfoque transversal el cual recolecta datos en un solo momento, en un tiempo único.

3.3 Población de estudio

Para sustentar el objetivo de reconocimiento de la situación actual se debe recolectar esta información de quienes tienen relación con la administración de infraestructura administrada por el Departamento de Servicios de TIC dentro del hospital, a través de un cuestionario.

Involucra una población pequeña, debido a que el personal al que va a dirigirse el cuestionario es el personal de soporte directo la infraestructura de TIC, que en el hospital se trata de 3 personas. No se considera necesario definir un tamaño de la muestra ya que se habla prácticamente de un censo, basado en la cantidad pequeña de la población.

Como se ha indicado previamente, se dirige la recolección de datos a esta población, ya que como personal de soporte de infraestructura y Jefe de TIC, se puede obtener la visión técnica y estratégica sobre los incidentes de TI y su impacto. Además, ellos han tenido mucho contacto de usuarios finales que de igual forma permite que a través de ellos se refleje como afectan los incidentes a los usuarios en sí.

3.4 Instrumentos de recolección de datos

En un principio se recolecta información sobre cómo está siendo gestionada la infraestructura de TIC, a través de un cuestionario con consultas sobre elementos o dispositivos importantes en la red y que se considera debe trabajarse como parte de una gestión preventiva de incidentes asociados a la infraestructura de TIC.

Esta información recolectada sirve de insumo para definir el rumbo a seguir sobre procesos por desarrollar, además, es necesario recolectar documentación de buenas prácticas o recomendaciones asociadas a estos procesos y así adecuarlo a lo que se tiene bajo la gestión de los servicios de TIC del hospital.

Para recolectar esta información se utilizó un cuestionario dirigido al total de la población ya que con una serie de preguntas se puede obtener información básica requerida de la situación actual.

El cuestionario se aplicó a través de consultas por correo electrónico. El mismo semiestructurado, debido a que en algunos casos hay respuestas definidas, pero dependiendo de la respuesta se puede profundizar en algunos temas.

En el anexo 1 se ve un diseño preliminar del cuestionario por realizar, donde se pretendió identificar lo siguiente:

- Entendimiento de una gestión preventiva.
- Reconocimiento de incidentes y vulnerabilidades que pueden acarrear incidentes en la actualidad.
- Reconocimiento de elementos importantes de infraestructura actual de TIC
- Propuestas de labores preventivas por efectuar.

Las respuestas obtenidas están en el anexo 2, respuestas por parte del Jefe de TI y dos analistas de sistemas, uno asociado directo al soporte de infraestructura de red y el otro asociado con el soporte de servidores, respaldos y almacenamiento de datos.

3.5 Procedimiento metodológico por objetivos

En la siguiente tabla se presentan elementos metodológicos asociados a los objetivos de este proyecto.

Tabla 1: Procedimiento metodológico por objetivos

Objetivos de Proyecto	Entregables de Proyecto	Fuentes de información	Herramientas de investigación
Identificar tipos de incidentes y/o vulnerabilidades que más afectan o podrían afectar la infraestructura tecnológica asociada a servicios de TIC del hospital, a través de indagación con colaboradores del Departamento de TI, para basar en estos la propuesta.	Definición documentada de principales incidentes y vulnerabilidades que puedan generar incidentes de TIC	• Colaboradores que trabajan brindando soporte a Infraestructura de TIC	• Cuestionario • Juicio Experto de investigador
Definir los procesos preventivos por diseñar basado principales incidentes y/o vulnerabilidades identificados, de manera que sirvan de guía para los diseños de la solución propuesta.	Definición documentada de los procesos que va a ser diseñados basado en los principales incidentes y/o vulnerabilidades identificadas.	• Colaboradores que trabajan brindando soporte a Infraestructura de TIC	• Cuestionario • Juicio Experto de investigador

Objetivos de Proyecto	Entregables de Proyecto	Fuentes de información	Herramientas de investigación
Diseñar procesos establecidos en el objetivo anterior, por medio de investigación de buenas prácticas asociadas relacionadas con los procesos, juicio experto y uso de elementos existentes en el hospital, de esta forma apoyar a la gestión preventiva que se pretende.	Desarrollo documentado de procesos como parte de la gestión preventiva, basado en marco teórico de buenas prácticas y adaptado a la realidad del Departamento de TI del Hospital México.	• Entregables de objetivos anteriores. • Colaboradores que trabajan brindando soporte a Infraestructura de TIC (apoyo en desarrollo).	• Consultas a colaboradores. • Juicio Experto.
Desarrollar un prototipo de alguno de los procesos definidos, lo cual involucra puesta en marcha de herramientas asociadas y validación de resultados iniciales, para obtener primeros resultados de la propuesta brindada.	Documentación de prototipo desarrollado. Capacitación sobre proceso desarrollado.	• Entregable de objetivos anteriores. • Documentación asociada el proceso a desarrollar el prototipo. • Profesionales relacionados con el prototipo desarrollado.	• Consultas a colaboradores. • Juicio Experto. • Investigación literaria de documentación. • Consultas a profesionales en desarrollo del proceso.

4 CAPÍTULO IV: DIAGNÓSTICO Y ANÁLISIS DE RESULTADOS

4.1 Sobre relevancia del hospital

El Hospital México en Costa Rica, es uno de los hospitales más desarrollados y complejos. Representa para la CCSS un hospital de la mayor instancia, es decir, es el hospital que otros hospitales de menor instancia y/o clínicas deben escalar padecimientos que no han podido resolver, en su defecto, que otros de estas instituciones no tienen los especialistas y deben remitirse los casos a este hospital. Tiene cobertura sobre varios cantones en provincias de San José, Alajuela, Heredia, Puntarenas y Guanacaste.

El Hospital México también refiere casos a otros centros de salud y hospitales más especializados, coma el Hospital Nacional de Niños, Hospital Psiquiátrico, Hospital de las Mujeres, entre otros.

En resumen, basado en las estadísticas de la CCSS para el año 2015, los principales servicios de salud que tiene el Hospital México y su cantidad de atenciones fueron:

Tabla 2: Atenciones en 2015 de principales servicios del Hospital México

Servicios	Cantidad de atenciones
Consultas y horas médicas referidas	318 541
Atenciones de urgencias	89 458
Medicamentos adquiridos o despachados en Farmacia	1 332 633

Para un promedio por los 365 días del año, se observa que diariamente se pueden tener alrededor de 900 consultas médicas programadas, 250 urgencias y 3700 medicamentos despachados. Si se lleva a horas, tomando las 24 horas diarias, sería en promedio 38 consultas médicas, 11 urgencias y 155 medicamentos despachados por hora.

Lo anterior se refiere a valores promedio que no se ajustan a la realidad del todo ya que entre semana se tiene por mucho la mayor cantidad de atenciones y principalmente consultas médicas, estas principalmente en horario de 7 am a 4 pm. Sin embargo, es un hospital que debe operar las 24 horas del día.

Los valores promedio son simplemente una referencia asociada a servicios indicados del hospital, los cuales tienen una dependencia de los servicios de TI, por lo que un incidente que tome afectación de estos servicios por una sola hora, afecta directamente esa gran cantidad de consultas, urgencias y despacho de medicamentos.

4.2 Impacto de incidentes previos en TIC

En la actualidad no se tiene un registro de todos los incidentes que se dan a nivel de infraestructura, simplemente se trabaja en ellos, y si se requiere soporte adicional, se contacta a los proveedores específicos.

Para entender el impacto de los incidentes se toma como ejemplo dos incidentes de alto impacto que ocurrieron fuera de ventanas de cambio, en horas de trabajo normal que generaron un impacto mayor para el servicio del hospital, estas informadas por Adrián Badilla, Jefe de TI en el momento de los incidentes.

- En 2015 en una ocasión se apagaron varios equipos en el Centro de Datos en un día normal de trabajo alrededor de las 10 am, principalmente servidores. Luego que varios usuarios contactaran a personal de TI y ellos se dieran cuenta que no tenían acceso a los sistemas. Se procede a movilizarse al centro de datos dentro del hospital, se observa que los servidores estaban apagados y se debía a un sobrecalentamiento del centro de datos debido a una falla de los equipos de aire acondicionado. El servicio se interrumpió por aproximadamente 4 horas.
- En enero del presente año 2016, hubo otra interrupción del servicio similar donde se apagó todo el centro de datos en horario hábil, pero en esta ocasión se debió a un problema del suministro eléctrico pues las UPS respondieron correctamente. La afectación del servicio fue de aproximadamente 2 horas.

Los dos anteriores ejemplos son una muestra de impactos altos del servicio del hospital, donde los siguientes servicios se vieron afectados:

- Farmacia: revisión de inventario e historial médico de paciente.
- Consulta externa: revisión y actualización de registro médico de atenciones médicas en diferentes especialidades.
- Admisión: registro de internamiento de pacientes dentro del hospital.

- Urgencias: respuesta rápida de resultados de exámenes, registro de hojas de puerta de pacientes.

Los servicios de TI automatizan y agilizan su funcionamiento de estos servicios médicos del hospital, a pesar que pueden funcionar sin TI, su ausencia genera carga de trabajo, colaboradores sin poder realizar parte o totalidad de su trabajo durante caídas del servicio, además, de re-trabajo luego que se restaure el servicio ya que para algunos casos, al no haber acceso a sistemas de TI, se deben hacer registros en papel y que luego se deben pasar registros tan pronto se restablecen los servicios de TI.

4.3 Sobre infraestructura actual del hospital

La infraestructura de equipo activo, sin tomar en cuenta computadoras de usuarios finales, se compone de servidores y equipos de red.

Los servidores están ubicados en un centro de datos, con las condiciones ambientales y eléctricas apropiadas para un centro de datos, tomando en cuenta principalmente aires acondicionados y UPS. Se tienen 31 servidores, de los cuales 15 son físicos y los otros 16 virtualizados.

Por su parte se tiene una variedad de equipos de red, todos del mismo fabricante. Existe un switch de red principal de 13 módulos con función de Core o corazón de la red ubicado en el cuarto del personal de TI, este tiene conexiones de cables de cobre para usuarios, pero más importante, sirve de punto de interconexión central de otros switches de red ubicados a lo largo del hospital que se conectan por fibra óptica en su mayoría. Este switch con fuentes de poder y tarjetas redundantes

Además, hay otros switches de red de 7 módulos con función de distribución de red, es decir, interconexión de una mayor cantidad de equipos al Core, estos distribuidos en diferentes cuartos de comunicaciones del hospital, incluyendo uno en el centro de datos, con fuentes de poder y tarjetas redundantes.

Hay alrededor de 12 switches de red de acceso de usuarios finales de igual forma, pero más pequeños, no son modulares con una sola conexión eléctrica.

4.4 Sobre resultados de encuesta

Tomando como base las respuestas obtenidas mostradas en el anexo 2, se tiene información asociada al primer objetivo, además, información que sirve como insumo para el segundo objetivo.

Como se comentó previamente, el enfoque de la investigación es principalmente cualitativo, basado en opiniones a quienes se les dirigieron las preguntas del cuestionario. Diagramar o graficar una tendencia en las respuestas se torna más complicado, al no tratarse de valores numéricos a respuestas cerradas, más bien se trata de analizar cada una de ellas y encontrar puntos de vista similares.

Para la pregunta número uno sobre si se está familiarizado con la gestión preventiva, se nota que todas las respuestas, a pesar de ser diversas en las palabras utilizadas, demuestran que sí se tiene un entendimiento de lo que trata una gestión preventiva. Concuerdan que son labores que se realizan de análisis de riesgos y esto previo a que se materialice ese riesgo.

En una de las respuestas para la pregunta número uno se comenta de planes de contingencia, lo cual, a pesar de tener claro desde antes que se dé un evento, trata más de un concepto de gestión reactiva, no preventiva.

La idea de la gestión preventiva es que no se tenga que pensar en la ocurrencia del incidente, que se pueda trabajar antes que ocurra, por ejemplo: que de alguna forma se hubiera detectado la alta temperatura del centro de datos y no esperarse hasta que ocurra lo que pasó al apagarse todos los servidores, para así poder ver qué generó el incidente y qué hacer de forma contingente.

Como parte de la pregunta número dos sobre incidentes y vulnerabilidades reconocidas, se resumen en las siguientes categorías asociadas a los mismos, que está principalmente asociado al primer objetivo específico de este proyecto:

Tabla 3: Categorización de incidentes

Categoría o tipo de incidentes	Incidentes
Incidentes de hardware o componentes internos de equipos	• Falla de aire acondicionado, generó aumento de temperatura en el centro de datos, lo que apagó los servidores. • Daños en fuentes de poder de switches de red. • Daños en tarjetas controladores de switches de red. • Daños en discos duros de servidores.
Incidentes de redes de comunicación	• Caídas de servicios de comunicación con oficinas centrales de la CCSS
Vulnerabilidades por falta de implementación de procesos	• No hay herramientas que permitan determinar o generar un seguimiento de incidente ocurridos con anterioridad. Se entiende que no hay una herramienta para anticiparse a incidentes. • Falta de gestión de acceso a administración de equipos de red. Además, falta de control de acceso para quienes se conectan a la red.

Esta categorización permite clasificar los incidentes, de forma tal que se puedan asociar procesos por trabajar basados en categorías y no ver los incidentes de forma individualizada.

Como parte de la pregunta número tres asociadas a acciones preventivas que se dan actualmente, se reconocen las siguientes acciones asociadas a la infraestructura de TI:

- Limpieza física de equipos de red y servidores. Actualización de sistemas operativos de los mismos.
- Dos respuestas mencionan el plan de continuidad, pero como se comentó antes, esto es una labor más reactiva que preventiva.

Se demuestra que no hay muchas prácticas claras de prevención de incidentes. La de limpieza y actualización se sistemas operativos, es prácticamente la única labor preventiva, que en sí se considera como un mantenimiento preventivo de equipos.

Se destaca para la pregunta número cuatro sobre servicios de TI de gran importancia, las respuestas se resumen en los siguientes puntos:

- Conectividad de los siguientes servicios del hospital: Laboratorio Clínico, Farmacia, Admisión y Urgencias.
- Telefonía.
- Cuarto de servidores.

Los anteriores servicios y elementos de infraestructura de TIC son muy importantes para ser tomados en cuenta como parte de la solución del proyecto. Se menciona de forma genérica de servidores y equipos de red, pero esto se sobreentiende que deben estar disponibles y ambos representan un complemento para que cualquier servicio de TIC pueda ser brindado.

Para la pregunta final número 5 donde se consulta sobre posibles procesos preventivos, se destacan los siguientes procesos en orden descendente en cuando a la cantidad de elecciones que tuvo:

1. Gestión de eventos asociados a equipos de red, almacenamiento de datos y servidores (involucra monitoreo) (x3).
2. Gestión de seguridad a través de control de acceso para administración de equipos de red y servidores (x2).
3. Gestión de conocimiento (documentación, actualización y acceso a información sobre elementos actuales de infraestructura de TIC). Esto para futuras referencias en caso de reincidencia de un incidente (x1).

Con este resultado se concluye que es necesario proponer el proceso de gestión de eventos, no solo por el hecho de que fue el proceso al que todos se refirieron, sino que permite prevenir varios de los incidentes que más se presentan, como problemas de hardware de equipos, problemas de comunicación por red y hasta los mismos problemas de cambios de temperatura en un espacio físico ya que inclusive se puede penar en sensores de temperatura a los cuales se les pueda hacer una gestión de los eventos que en él se dan.

Tanto el Jefe de TI como el analista de sistemas encargado de brindar soporte a la infraestructura de red, para la pregunta número cinco sobre procesos por implementar de forma preventiva, definieron de igual forma implementar una gestión de seguridad en la administración de equipos y el acceso a la red. Esta representa una alternativa interesante a tomar en cuenta ya que la continuidad, confidencialidad e integridad de la información a través de los servicios de TIC están muy asociados a las políticas de seguridad que se tengan.

La gestión de conocimiento que indica el analista de sistemas encargado del soporte de servidores, respaldos y almacenamientos de datos, es un proceso importante, sin embargo, basado en los incidentes que se están dando y los servicios de TIC que se desean mantener en funcionamiento, no llega a brindar una solución directa a estos o sus categorías.

Sin embargo, puede asociarse una gestión de conocimiento a los otros procesos enunciados porque deben documentarse y de hecho para el proceso de gestión de eventos, es posible que deba documentarse de cierta forma cómo está la infraestructura actual, para así entender los eventos generados.

Basado en lo anterior y asociado al segundo objetivo específico de este proyecto, se establecen los siguientes procesos asociados a los tipos de incidentes identificados:

Tabla 4: Procesos asociados a categoría de incidentes

Categoría o tipo de incidentes	Incidentes	Procesos asociados
Incidentes de hardware o componentes internos de equipos.	• Falla de aire acondicionado, generó aumento de temperatura en el centro de datos, lo que apagó los servidores. • Daños en fuentes de poder de switches de red. • Daños en tarjetas controladores de switches de red. • Daños en discos duros de servidores.	• Gestión de eventos
Incidentes de redes de comunicación.	• Caídas de servicios de comunicación con oficinas centrales de la CCSS.	• Gestión de eventos
Vulnerabilidades por falta de implementación de procesos.	• No hay herramientas que permitan determinar o generar un seguimiento de incidente ocurridos con anterioridad. Se entiende que no hay una herramienta para anticiparse a incidentes. • Falta de gestión de acceso a administración de equipos de red. Además, falta de control de acceso para quienes se conectan a la red.	• Gestión de eventos. • Gestión de seguridad en la administración de equipos y acceso a la red.

Una propuesta para estos procesos de gestión de seguridad y gestión de eventos va a desarrollarse como parte del proyecto en la propuesta de solución del siguiente capítulo.

Como conclusión se reconoce por medio del personal del Hospital México la importancia de gestionar de forma preventiva la infraestructura de TI, a pesar de que hay muchas prácticas que pueden realizarse, enfocarse en los incidentes y vulnerabilidades más reconocidas permite generar un impacto a corto plazo más significativo, por esto la elección de dos sub procesos, enfocados en la gestión de eventos y seguridad a nivel de red.

4.5 Diagnóstico de situación actual asociado a la gestión de eventos

El Departamento de TI del Hospital México no ha tenido la oportunidad de desarrollar un proceso formal de gestión de eventos, ni monitoreo formal. En algunas ocasiones se han realizado monitoreo aleatorio de algunos equipos de red, sin embargo, este se ha hecho para efectos de un análisis de capacidad de equipos y se removió tan pronto se obtuvieron resultados.

No se tiene implementada una herramienta fija para monitoreo, lo cual funcione como insumo de la gestión de eventos, aunque sí existe infraestructura para instalar la herramienta.

No se tiene un registro de tiquetes de soporte o incidentes asociados a la infraestructura de TI dentro del hospital. Lo único es que el proveedor de soporte sí lleva el control de los incidentes que con ellos se abra, pero esto solo aplica para el hospital en caso que requiera soporte especializado aparte del soporte interno.

Adicional a lo indicado, lo que se tiene a disposición para la gestión de eventos, es la infraestructura actual de correos electrónicos, en caso de manejar alertas. De igual forma el personal de TI para ser tomada en cuenta dentro de la propuesta para roles asociados al proceso.

4.6 Diagnóstico de situación actual asociado a la gestión de seguridad de administración de equipos de red y acceso a la red

Para este diagnóstico se realiza una revisión en el sitio de configuraciones de equipos de red, además, de consultas dirigidas a encargado principal del soporte de la red en el hospital.

Basado en las buenas prácticas definidas en el capítulo número 2.6 del Marco Conceptual, sobre las buenas prácticas de gestión de seguridad, se realizan los siguientes hallazgos en la infraestructura del hospital. En la primera columna se indican los hallazgos y en la segunda columna se resume la buena práctica y entre paréntesis el número que hace referencia a la buena práctica con el identificador de la misma en el propio Marco Conceptual.

Tabla 5: Hallazgos asociados a gestión de seguridad de red

Hallazgos encontrados	Buena práctica asociada
• Se implementa correctamente la seguridad física de acceso a los equipos, no se puede tener acceso a los equipos de red sin llaves o uso de huella digital. Sin embargo, para el caso de los equipos en el área de colaboradores de TI en el piso 1, que a pesar de que para ingresar a esta área se precisa de acceso con huella digital o apertura desde adentro, los equipos están en gabinetes donde no se utiliza llave para cerrarlos y personas ajenas al Departamento de TI, que por alguna razón requieran ingresar a esta área, podrían tener acceso a los equipos, que de hecho se ubica el switch de red principal.	• Administración física de equipos (1)
• No se cuenta con cámaras de seguridad para registrar el acceso a cuartos con equipos principales de red, como lo son el centro de datos y el área de personal de informática en el piso 1.	• Administración física de equipos (1)
• Todos los equipos de red tienen credenciales de un usuario y contraseña robusta (no asociado a palabras de diccionario, nombres o de fácil aprendizaje), pero son credenciales administradas de formas locales y son compartidas para todos los que requieran acceso a estos equipos.	• Credenciales de administración (2) • Contraseñas (3)
• Los equipos de red sí tienen mensajes que indiquen que el acceso a usuarios no autorizados no es permitido.	• Mensaje al intentar autenticarse a los equipos (4)
• La mayoría de equipos son administrados por SSH, solo en los casos que el sistema operativo de pocos equipos, no permiten encriptación de datos y que el fabricante	• Protocolos de administración remota segura (5)

Hallazgos encontrados	Buena práctica asociada
no brinda opciones de actualización, estos mantienen la administración por TELNET. En algunos equipos está habilitado el acceso web (HTTP) y por el momento no está siendo utilizado.	
• No existen filtros por direcciones IP, de forma tal que ciertos usuarios sean los únicos con poder de administrar los equipos de red.	• Filtrado de segmentos de red autorizados para administración remota (6)
• No se están monitoreando los equipos usando el protocolo de SNMP, aunque existen algunos equipos que tienen configuradas comunidades de SNMP.	• Seguridad en el monitoreo de equipos por SNMP (7)
• No se tienen identificados los puertos de red que en definitiva no están en uso.	• Identificación de puertos de red en uso (a)
• No se tiene un filtro para prevenir el ataque de múltiples MAC inyectadas en un puerto de red.	• Limitación de direcciones MAC aprendidas por puerto de red (b)
• Ya tienen como parte de sus políticas configurar todos los puertos como modo acceso.	• Configuración de puertos que conectan a equipos finales como acceso (c)
• No se tiene configurada la función de protección de mensajes BPDU o BPDU Protection.	• Configuración de protección de mensajes BPDU asociados a protocolo STP (d)
• No se tiene configurada ninguna autenticación para ingreso a la red, simplemente con tener acceso físico a un puerto de red y conectarse a este, ya se tiene acceso a la red del hospital.	• Autenticación de usuarios o equipos de usuarios para conectarse a puertos de red (e)

Hallazgos encontrados	Buena práctica asociada
• No se tiene configurada protección contra ataque DHCP Spoofing en todos los switches de red.	• Protección contra ataques asociados a DHCP (f).
• A nivel de redes inalámbricas, se tiene una infraestructura de configuración centralizada, es decir, no se tiene que configurar en cada punto de acceso las funciones de red inalámbrica, sino en un equipo central replica las configuraciones a todos los puntos de acceso. Los nombres que se utilizan para redes inalámbricas son descriptivos al hospital, es una red visible, no se utiliza filtrado por dirección MAC, a pesar de no ser muchos los equipos que se conectan. No se tiene claro el método de encriptación de las redes inalámbricas.	• Medidas de seguridad asociadas a redes inalámbricas (g).

5 CAPÍTULO V: PROPUESTA DE SOLUCIÓN DEL PROBLEMA

Recapitulando el problema, se tiene que en el hospital se han dado incidentes asociados a la infraestructura de TIC que afectan los servicios brindados por el hospital, el problema llega a ser mayor, desde el punto de vista que no se tienen prácticas para prevenir incidentes. Basado en esto la solución del problema, que colaborará en detectar incidentes desde antes que ocurran, e inclusive evitarlos del todo.

Se proponen dos subprocesos asociados a una gestión preventiva, donde el primer proceso es de gestión de eventos, que no se trata simplemente de un monitoreo, sino de darle seguimiento a los eventos, proponiendo niveles de tolerancia asociados a umbrales y definiendo acciones preventivas y correctivas inclusive, para que su identificación genere realmente valor en la gestión de TI. El otro subproceso de seguridad de red, como medida preventiva ante vulnerabilidades encontradas, que representan un riesgo a la integridad, confidencialidad y disponibilidad de la información del hospital, de esta forma evitar cualquier incidente asociado a estas vulnerabilidades.

Las propuestas hacen referencia a enfoques desarrollados en el marco conceptual tanto para el desarrollo de la gestión de eventos, como la gestión de seguridad. Por lo que la propuesta se brinda en función de estos enfoques de diseño de gestión de eventos y monitoreo de IBM y del ciclo de vida de Deming enunciado en el estándar de seguridad ISO 270001.

5.1 Propuesta de solución para implementar gestión de Eventos

Para la propuesta de gestión de eventos se requiere definir un software donde basado en diferentes herramientas se pueda monitorear el estado de equipos y generar eventos asociados a esto, luego de definir un plan para determinar qué elementos monitorear y el seguimiento respectivo de los eventos.

5.1.1 Herramienta de monitoreo

La primera propuesta es la herramienta de monitoreo, esta debe tener la capacidad de realizar como mínimo monitoreo de forma activa, a través de PING y SNMP que permiten visualizar disponibilidad y obtener estadísticas de recursos de equipos (explicado con más detalle en la sección 2.5 del marco conceptual), lo cual permite un monitoreo básico de la infraestructura de TI.

La herramienta de monitoreo debe ser escalable para poder monitorear a futuro servicios por diferentes puertos TCP/UDP (puertos lógicos para establecer sesiones y permitir comunicación entre equipos, por ejemplo: el puerto 80 para tráfico web, explicado con más detalle en la sección 2.5 del marco conceptual), monitorear interfaces de red, acceso a aplicaciones, entre otros. Adicionalmente debe presentar opciones de notificación como vía correo electrónico.

De manera adicional se requiere una herramienta de monitoreo de libre uso, que eventualmente no comprometa a adquirir licenciamiento o equipo adicional, sobre todo porque este proyecto no pretende uso de presupuesto extraordinario si se tienen opciones libres y completas disponibles que se pueden aprovechar.

De estas herramientas de monitoreo libres mencionadas en la sección 2.5 de este documento de Marco Conceptual, se recomienda utilizar Nagios ya que como lo indica el artículo es "una de las más populares, sino la más popular" (Auza, 2010), lo que refleja que es ampliamente aceptada, de confianza de varios administradores de TI. Además, Nagios en su descripción en el artículo indica que incluye los sensores de monitoreo requeridos.

Esta herramienta se puede instalar en un servidor virtual, además, se requiere la configuración de una comunidad de SNMP en los equipos a gestionar eventos, que coincida con la del servidor, lo cual es lo que le permite al servidor obtener las estadísticas del monitoreo.

5.1.2 Definición de Alcance de la gestión de eventos

Para definir el alcance de los elementos o CI a los cuales van a ser gestionados sus eventos, se realiza una decisión de qué servicios o elementos individuales de monitoreo se deben tomar en cuenta.

Si se define trabajar basado en servicio, se elige un servicio de TI que es elemental para el negocio y se descompone en la infraestructura que permite tener ese servicio arriba. Se identifican los equipos de red y servidores involucrados, a los cuales eventos van a ser gestionados.

Lo anterior para servicios críticos del hospital basado en el criterio estratégico que puede ser obtenido del Jefe de TI, quien puede apoyarse en la dirección médica de la institución.

De cada uno de los elementos se debe obtener información como tipo de dispositivo, dirección IP, ubicación del dispositivo, encargado primario de soporte, como información mínima.

Adicionalmente, luego de ser definidos los elementos asociados a los servicios más importantes, se pueden elegir equipos u otros adicionales que haya quedado por fuera, pero la idea no se trata de sobre poblar en un principio con elementos no tan críticos.

5.1.3 Determinar políticas de gestión de eventos

La política de la gestión de eventos debe indicar acciones que se van a tomar con los eventos que se presenten, aspectos tales como filtrado de eventos, notificaciones de eventos, correlación, tiquetes o casos asociados a los eventos, automatizaciones en respuesta a los eventos, entre varias acciones cuando sea posible.

Algunas pautas recomendables a manejar dentro de la política de gestión de eventos inicial como parte de la propuesta de este proyecto son:

- Designar un servidor y proceder con toda la instalación de la herramienta de monitoreo, lo cual involucra habilitar recursos sistema operativo, paquetes de software y cualquier requisito, para luego instalar el software de la herramienta de monitoreo como tal.
- Definir elementos de infraestructura para gestionar sus eventos, principalmente basado en cuales dan soporte a los servicios más importantes para el hospital.
- De cada elemento por monitorear, se van a documentar los eventos que se van a gestionar, en un principio como mínimo disponibilidad y salud operativa (recursos) del elemento.
- Para cada evento seleccionado, definir umbrales que van a estar asociados a la severidad del eventos reportado. Estos umbrales basado en recomendaciones del fabricante.
- Documentar las acciones que se van a tomar para cada evento. Como mínimo definir un medio de notificación del evento.
- Definir encargados de roles de la gestión de eventos. Una persona puede desempeñar más de un rol. Estos roles definidos igualmente en el libro de gestión de eventos de IBM (Bhe et al., 2004, págs. 37-38):

- Encargado del Proceso: lidera el desarrollo de las políticas referidas en esta sección. Tiene la responsabilidad final por el éxito del proceso de gestión de eventos.
- Arquitecto de gestión del sistema: diseña la solución técnica para satisfacer las necesidades de procesamiento de eventos mientras que se adhiere a las políticas y normas apropiadas.
- Implementadores de herramienta: instalar, configurar y apoyar a las herramientas de gestión de sistemas para procesar los eventos a las especificaciones de diseño del arquitecto
- Expertos en diferentes campos: Suministran conocimiento sobre una plataforma o un sistema en particular y determina el procesamiento requerido para los eventos dentro de sus áreas de especialización. Por ejemplo: expertos en servidores, respaldos, redes.
- El personal de apoyo: gestionan incidentes y problemas con las plataformas y sistemas.
- Mesa de ayuda: Proporciona el primer nivel de soporte para los usuarios y dan retroalimentación que es utilizada por los expertos para tomar decisiones de procesamiento de eventos.
- Gerentes: control de cumplimiento de la política por parte del personal, se deben asegurar que los problemas se aborden de forma oportuna.

- Definir una estructura de correlación de eventos, es decir, determinar la relación entre eventos, si existe dependencia entre ellos.

Los anteriores, algunos puntos a ser tomados en cuenta como política asociada a la gestión de eventos. Como parte de esta propuesta, se desarrolla cómo hacer los diferentes puntos de la política.

5.1.4 Documentación de repertorio de eventos (Filtrado de eventos)

De todos los CI, se debe documentar los eventos que se van a estar gestionados, para luego definir acciones para los mismos y llevarlos a operación en la herramienta de monitoreo.

Permitir la gestión de todos los eventos genera mayor complejidad, principalmente porque no todos tienen relevancia o no se tiene conocimiento total de lo que representan. En un

principio se debe filtrar qué eventos se van a gestionar, de forma que se pueda iniciar el proceso con eventos más relevantes y que se conozca realmente su significado.

Para cada CI como mínimo se debe en un principio gestionar la disponibilidad del mismo y validar eventos asociados a recursos del CI que pueden comprometer su disponibilidad, como son los elementos ambientales de CPU, memoria, disco duro, temperatura y componentes de Hardware. De ser sumamente necesario, se puede pensar en gestionar eventos de telecomunicaciones y aplicativos, sin embargo, se recomienda estos para una segunda fase de la gestión de eventos ya que representan eventos más complejos a configurar y gestionar.

La herramienta de monitoreo va a revisar cambios de estado en esos eventos seleccionados. Principalmente se utilizaría herramientas como PING y colección de estadísticas por medio de SNMP, aunque también se pude valer de colección de mensajes de logs.

El experto en el CI respectivo debe participar en la elección de eventos por gestionar pues basado en su experiencia y problemas conocidos se puede poblar con más relevancia la gestión de eventos.

Las siguientes son algunas prácticas a la hora de filtrar eventos, estas recomendadas en el libro de IBM de gestión de eventos (Bhe et al., 2004, págs. 44-45):

- No filtrar o eliminar eventos de limpieza o arreglo de un problema, por ejemplo: si se está monitoreando una interface de red, puede existir un evento para indicar su caída, pero también existe un evento para indicar que levantó, por lo cual no se debería eliminar ese segundo evento.
- No hacer doble monitoreo sobre un mismo CI o elemento ya que esto genera eventos redundantes, que provoca dos alertas diferentes por el mismo evento.

5.1.5 Documentación de atención de los eventos gestionados

Expertos en las diferentes plataformas de infraestructura deben participar en la documentación sobre cómo se va a gestionar cada evento basado en su experiencia y conocimiento, para así definir qué tipo de atención se le dará a los diferentes eventos. Se deben definir como mínimo los siguientes:

- Severidades de eventos.

- Prioridades para trabajar en los eventos.
- De ser posible, asociar a un manejo de tiquetes, definir cómo y cuándo se abrirían tiquetes asociados a los eventos.
- Documentar acciones automáticas por realizar a eventos, en caso que sea posible, por ejemplo: cambios automáticos de configuraciones.

Con severidad y prioridad de atención de eventos, se debe definir qué se va a realizar ante la ocurrencia de un evento, por ejemplo: un evento de tipo advertencia o excepción en el switch de Core de la red debe ser atendido con mayor prioridad que un evento cualquiera en algún otro switch de red.

Basado en el juicio experto de los profesionales en cada área de infraestructura, se va a dar seguimiento a los eventos que se consideren necesarios para ser atendidos y llegar a un cierre del evento, es decir, se va a trabajar en el incidente hasta que se restablezca su condición recomendada.

Se debe llevar un registro de los eventos dados que hayan sido catalogados como advertencia o excepción. Se deben registrar aspectos como fecha y hora en que se dio, tipo de evento, dispositivo afectado, de ser posible, acción ejecutada para restablecer estado de evento. Por ejemplo: si el porcentaje de CPU de un equipo se está elevando todos los días a una hora específica, la única forma de saberlo y trabajar de forma más precisa en el evento es a través de la revisión de estos registros.

Este registro se debe tener en un sistema compartido, de no existir una aplicación para hacer registro de eventos, se podría comenzar con un documento de Excel compartido en un servidor de archivos accesible por red y por ciertos usuarios, que muestre lo siguiente asociado al mismo problema de CPU:

	A	B	C	D	E
1	Clasificación de Evento	Descripción de Evento	Dispositivo	Fecha y hora de eventos	Acción Ejecutada
2	Excepción	Porcentaje de uso de CPU por encima del 90%	Servidor XYZ	22/04/2015 12:00pm	Se ingresa de forma remota al equipo, se revisan procesos que están ejecutando en el momento, se observa un uso inusual del CPU de un proceso asociado al explorador de Internet. Se cierra el proceso y reduce de forma significativa el uso de CPU.
3					

Ilustración 6: Ejemplo de registro de evento

Se proponen asociar eventos a tiquetes de soporte tal y como si fuera un incidente, como mínimo los eventos considerados excepciones, para que se les dé seguimiento y queden documentadas las acciones tomadas y no se dejen como simples notificaciones recibidas.

5.1.6 Correlación de eventos

Correlación de eventos se refiere a la relación que se establece entre un evento y otro, por ejemplo: que si se dan dos o más eventos de forma simultánea, pueden tener un significado en específico, que si se dieran de forma aislada.

Para una correlación, se requiere definir nodos y jerarquías de dispositivos y eventos. Lo que se pretende es atender eventos de forma precisa y entender mejor los incidentes

La siguiente ilustración muestra un ejemplo:

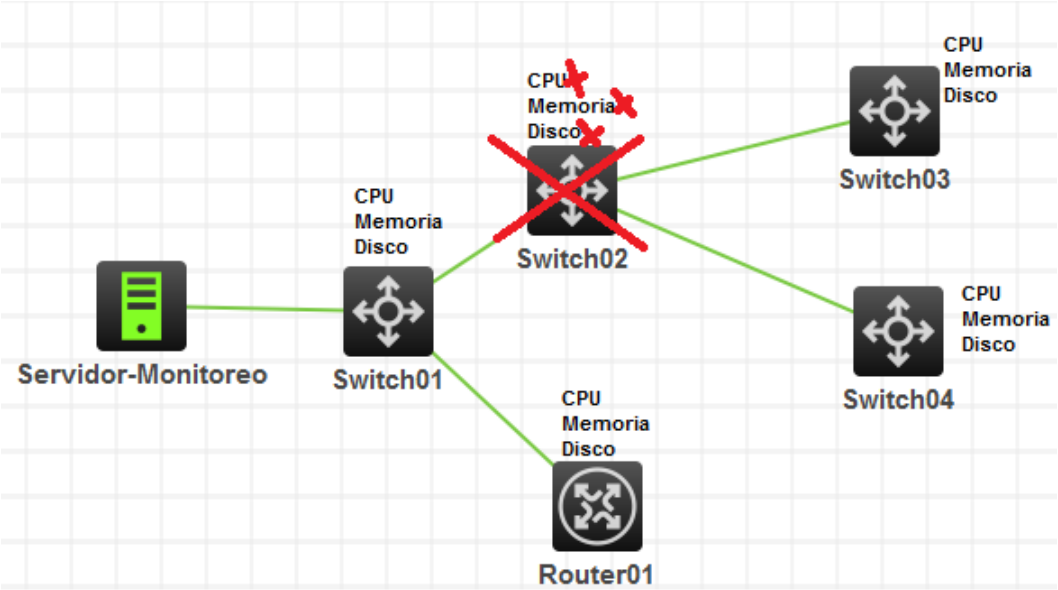


Ilustración 7: Ejemplo de Correlación de eventos

Como ejemplo de correlación, si un dispositivo presenta un evento de elevación de CPU únicamente representa solo una advertencia o excepción de este recurso y se toman acciones basadas en este hecho. Sin embargo, si además, del CPU, se alerta la memoria, disco duro, red y hasta la disponibilidad del equipo, posiblemente se debe a un problema de conectividad total del dispositivo y se tomarán otras medidas.

En el ejemplo anterior, otra correlación es que para el servidor de monitoreo, no solo va a tener eventos del Switch02, sino que posiblemente se reciban eventos asociados al de los Switches03 y 04 ya que a través del 02 es como se comunican con el servidor de monitoreo.

En la documentación de las acciones por tomar, asociadas a los eventos, se deben definir correlaciones y así tomar medidas de acción más precisas, la cuales pueden determinar no prestar atención a ciertos eventos que se den pues un evento de una categoría mayor puede estar generando los eventos de categoría menores.

Algunas propuestas asociadas a la correlación de eventos del libro de gestión de eventos de IBM (Bhe et al., 2004) en las págs. 51 a la 53 son:

- Solo correlacionar eventos que realmente se entiendan, el correlacionar eventos basado en suposiciones puede generar que se dejen de lado eventos que si requieren acción.
- Correlacionar eventos que muestran la peor condición: en ocasiones cuando una situación se intensifica, afecta varios elementos, lo cual genera múltiples eventos. Se debe correlacionar, de forma tal que se prioricé en el primer evento que genera los demás y dejar los otros en lo posible que automáticamente tengan menor prioridad.
- Reportar todos los eventos que requieren acción, no solo los primarios: esto se refiere a que se reporten todos los eventos asociados a una situación específica pues resulta posible que al trabajar en el evento primario, los eventos secundarios se restablezcan, sin embargo, cabe la posibilidad que sigan dándose aunque el evento primario no se siga dando.

5.1.7 Mediciones de gestión de eventos

Para comprobar que la gestión de eventos genera un efecto, ya sea positivo o negativo dentro de la gestión de TI como tal, se deben tener métricas asociadas al proceso, por lo que se debe llevar un registro de al menos las siguientes métricas:

a) Número de eventos total notificados.
b) Numero de eventos que no requirieron atención por ser falsa alarma.
c) Número de eventos atendidos de forma preventiva que no se materializaron en incidentes.

d) Número de eventos que se materializaron en incidentes.
e) Número de eventos que se materializaron en incidentes que requirieron soporte de proveedores externos.

La fuente para las métricas está en el registro que se lleva de eventos y el reporte de incidentes de proveedor externo, que se debería asociar a un evento si aplica.

De las métricas anteriores, se pueden obtener los siguientes Indicadores Clave de Rendimiento o KPI (Key Performance Indicators) relacionadas con la gestión de eventos:

1) Porcentaje de eventos inválidos=(b/a)*100
2) Porcentaje de acciones proactivas tomadas basado en eventos=(c/a)*100
3) Incidentes asociados a eventos reportados=(d/a)*100
4) Incidentes asociados a eventos que requieren soporte especializado=(e/d)*100

Basado en los KPI, se pueden obtener factores claves de éxito de la propuesta como

Tabla 6: Factores clave de éxito de gestión de eventos

Factor clave de éxito	KPI	Resultado esperado
Invalidez de eventos reportados	1	Disminución
Proactividad sobre eventos	2	Aumento
Disminución de incidentes asociados a eventos	3 y 4	Disminución

Como se muestra en esta tabla de factores, clave de éxito de la gestión de eventos. Para que esta gestión sea exitosa va a estar en función de la disminución de eventos inválidas ya que se refiere a un ajuste de los eventos reportados, además, de una disminución en incidentes asociados a los eventos. Por otra parte, si aumentan los eventos atendidos que no generaron incidentes, es un resultado aún mejor, principalmente asociado a la proactividad que se quiere alcanzar con el proyecto.

Se debe medir estos factores clave de éxito cada cierto período, por ejemplo: cada mes.

5.2 Propuesta de solución de políticas a seguir asociadas a seguridad de red

Esta propuesta de políticas de seguridad de red se basa como se indicó anteriormente en el Marco Conceptual, en el enunciado del ISO 27001, donde se habla acerca del ciclo de Deming (Do-Plan-Check-Act).

Se desarrolla en la fase de "Plan", donde se analizaron riesgos de la infraestructura actual de red y basado en esto se definen políticas por implementar.

La sección "Do" refiere a lo que debe implementarse para conseguir la política asociada al "Plan". Se proponen pautas a seguir en la siguiente tabla, pero esto puede variar basado en criterio del personal de TI del hospital, además, si cambian factores como fabricantes de dispositivos de red.

Tabla 7: Pautas de política de gestión de seguridad (Plan) y propuestas de atención (Do)

Plan	Do
1. **Reforzar la seguridad física de acceso a los equipos, de forma tal que para poder tener acceso físico a los mismos, debe haber un mecanismo de seguridad que permita este acceso solo a usuarios autorizados.**	Cerrar con llave el rack de equipos de red en cuarto de colaboradores de TI, principalmente que está el switch de red principal. De ser posible instalar rack en centro de datos, de forma que la infraestructura quede protegida de personal que deba ingresar al centro de datos y no tenga relación con el soporte de infraestructura de TI. Por ejemplo: personal de soporte de aires acondicionados o sistemas de alimentación eléctrica.
2. **Implementar protección física a través de cámaras de seguridad que registren el acceso a principales equipos de red, como mínimo debe implementarse esta medida dentro del centro de datos y área de personal de TI.**	Implementar un sistema de circuito cerrado de cámaras de video para tener registro de acceso en centro de datos y área de equipo en oficina de colaboradores de TI.
3. **Implementar un sistema de autenticación centralizado a equipos de red a través de un servidor, de forma tal que para administrar a cualquier equipo de red dentro de la infraestructura del Hospital México, se deben presentar las credenciales al**	Utilizar los servidores de Active Directory locales en Windows Server, activar los roles de NPS (Network Policy Server) y configurar sobre esta plataforma el servidor de autenticación RADIUS, uno en cada servidor. Configurar en los equipos de red que se autentiquen primero con el servidor RADIUS para poder tener acceso a la administración de los mismos.

Plan	Do
servidor y que esté basado en privilegios definidos, autorice o no al usuario.	
4. En el servidor que autentica, se definirá un grupo de usuarios quienes podrán tener acceso exclusivo a los equipos, estos usuarios son únicamente colaboradores directos del personal de TI del Hospital México. Cualquier otro usuario externo al hospital que requiera acceso a los equipos, se le habilitará un usuario temporal, tan pronto como no se requiera su acceso a los equipos, este usuario se deshabilitará.	Crear en los servidores de Active Directory un grupo de cuentas de usuarios, quienes van a ser los únicos con derecho de administración de los equipos de red. Luego en el NPS crear la política que solo usuarios en ese grupo puedan tener acceso. Para cualquier proveedor externo, se tendrá un usuario que represente a la empresa, este usuario será habilitado únicamente en los momentos que el personal del hospital esté consciente de las actividades que van a ser realizadas, por lo que se habilitará de forma temporal. Es recomendable inclusive llevar un registro de cuál persona exactamente requirió de usar ese usuario de proveedor, con fecha y hora.
5. Todos los equipos de red deben ser administrados de forma remota, utilizando únicamente protocolos de comunicación seguros, como SSH y HTTPS.	Permitir acceso solo por SSH y HTTPS a equipos, este último si realmente se requiera tener acceso a un equipo por web, de otra forma deshabilitar esa administración. Para el caso de equipos que en la actualidad su sistema operativo no permite administración por protocolos que encriptan las credenciales, se deben actualizar a una versión de sistema operativo que lo soporte. En última instancia que no se pueda actualizar, mantener el uso de mecanismos alternativos a los seguros, pero se debe informar a la

Plan	Do
	dirección de TI el riesgo ya que no solo representa un problema de seguridad, sino que además, continuidad del servicio pues un equipo que no se le pueda actualizar la versión de sistema operativo, representa un equipo descontinuado por el fabricante, por tanto, su tiempo de vida útil ha sobrepasado.
6. Definir los segmentos de red desde donde se puede administrar los equipos de red, los cuales deben ser lo más reducido posibles en cantidad de equipos. Luego filtrar en todos los equipos de red que únicamente esos segmentos definidos tengan la posibilidad de administrar de forma remota los equipos.	Crear lista de acceso en todos los equipos de red de forma tal que solo se permita el acceso remoto a las subredes del Hospital México, específicamente a las subredes donde se ubica el personal de TI.
7. Si no se va a implementar monitoreo de los equipos de red, eliminar cualquier comunidad y configuración de monitoreo de SNMP de estos dispositivos. En caso de pretender realizarse un monitoreo de los mismos, configurar comunidades de SNMP de más de seis caracteres, que involucre al menos dos tipos de caracteres entre letras, números o símbolos, que sean únicamente de lectura y que se filtre	Revisar cada equipo de red y verificar cualquier configuración de SNMP, en caso de que no se vaya a realizar monitoreo del equipo usando el protocolo SNMP, remover cualquier configuración asociada. Si se va a utilizar, crear la comunidad como indica la política, además, crear una lista de acceso que permita únicamente al servidor de monitoreo y que pueda monitorearse únicamente de lectura (Read-Only).

Plan	Do
exclusivamente al servidor de monitoreo que pueda obtener estadísticas del equipo a través de SNMP.	
8. Se deben identificar los puertos de red cableada actualmente utilizados en cada uno de los switches de red, apagar y/o asignar a una VLAN aislada todos aquellos puertos que no estén ahora en uso.	Se puede con algunas de las siguientes formas, la combinación sería lo más certero: • Revisar periódicamente logs de los equipos para ver actividad de apagado y encendido de puertos y así ver si un puerto está siendo usado realmente. • Verificar periódicamente el estado operativo de las interfaces de los switches y comparar los diferentes resultados, si luego de varias revisiones en diferentes semanas en diferentes horas se identifica un puerto que nunca haya estado activo, puede significar que nunca está en uso. • Seguir físicamente cableado para validar que en realidad no esté siendo usado. • Crear una VLAN que tenga un direccionamiento el cual no tenga conexión con el resto del hospital, asignar esos puertos que se piense que no están siendo usados a esa VLAN

Plan	Do
9. Configurar que todos los puertos de red que conectan a usuarios finales que puedan aprender un máximo de cinco direcciones MAC, el tráfico adicional a estas direcciones MAC configuradas no debe ser permitido en el puerto. El aprendizaje de las direcciones MAC puede ser de forma dinámica.	Asegurarse que un puerto no va a ser utilizado para conectar otro switch de red, es decir, que van a ser solo usados para usuarios finales. Para esos puertos que van a ser usados únicamente en usuarios finales, se debe configurar seguridad de puerto, de forma tal que permita solo 5 direcciones MAC como máximo aprendidas en un mismo instante en el puerto de forma automática y en caso que se eleve ese uso, se restrinja y no sea permitido ese tráfico, además, poner un tiempo para que se refresque ese aprendizaje, que no deba manualmente borrar las direcciones MAC aprendidas.
10. Configurar protección de mensajes BPDU en cada uno de los puertos de red que conectan a usuarios finales.	Configurar Protección de BPDU de forma global en los dispositivos o de forma individual en cada puerto de red identificado para un usuario final, solo se debe validar si el fabricante del switch de red tiene ambas funcionalidades.
11. Gestionar a través del protocolo 802.1x en acceso a la red a través de autenticación con servidor RADIUS de usuarios que conectan a la red, de forma tal que en cada puerto de usuario final para poner tener conectividad, debe primero autenticarse a través de dirección MAC, credenciales o certificado instalado en la computadora.	Configurar autenticación de puertos usando un servidor RADIUS en los switches de red, se debe configurar en cada puerto el modo de autenticación, de forma tal que lo que se utilice para autenticar al usuario se envíe hacia el servidor RADIUS. Configurar el rol de NPS en los servidores de Active Directory, en este servidor se configuran las políticas de autenticación a través de dirección MAC, credenciales o certificado. Dependiendo el

Plan	Do
	método que se utilice, es posible requerir instalación de certificado o software de autenticación en los usuarios finales.
12. Configurar DHCP Snooping en todos los switches de red que brindan a acceso a usuarios finales y que así lo permite el sistema operativo actual de los equipos de red, de no permitirlo, procurar actualización a una versión que lo permita.	Configurar DHCP snooping en la VLAN respectiva, además, configurar solo los puertos hacia el servidor DHCP y los puertos que interconectan switches como puertos confiables por donde se pueden ubicar a servidores DHCP.
13. Ocultar los nombres de las redes inalámbricas existentes. Adicionalmente al ser muy pocos los equipos que deben conectarse a la red inalámbrica, filtrar el acceso a la misma a través de dirección MAC de los equipos. Usar encriptación de red inalámbrica WPA2.	Configurar en el controlador de red inalámbrica que el SSID (identificador de la red) de forma oculta, levantar un inventario de direcciones MAC y habilitar el filtrado con esas direcciones MAC. Configurar WPA2 como medio de encriptación de la red.

Para continuar con el enunciado del ciclo de Deming, se proponen labores asociadas a "Check" y "Act", que van ya luego de implementadas las pautas enunciadas.

Como parte del "Check" de las medidas de la política de seguridad refiere a validar la real implementación de cada una de las pautas o normas enunciadas en la tabla anterior, llevar registro de limitaciones a la hora de implementarlas. No todas las políticas estaban relacionadas a incidentes que previamente se tenían, en su mayoría las medidas proactivas, aunque sí se tenían reportes de incidentes, como con DHCP.

Adicionalmente, dentro del "Check" involucra validar que en realidad surja efecto la configuración respectiva, para el caso que así lo sea, por ejemplo: conectar a un puerto de usuario un switch de red y verificar que a través de este no se pueda tener siquiera conectividad a la red, inclusive el puerto al cual conecta no debería permitir tráfico.

Como parte del "Check" inclusive, no es de esperarse, pero cuando se trabaja con medidas de seguridad, en ocasiones se generan incidentes debido a la misma medida de seguridad que no se implementa correctamente o más bien bloquea tráfico que no representa una amenaza sin más bien tráfico normal de usuarios, por lo que se debe llevar registro de estos incidencias.

Asociado con el "Act" se debe validar qué ha hecho falta para ejecutar alguna de las medidas de la política y procurar llevarla a cabo. En caso que una medida no dé los resultados esperados o genere incidentes, validar las razones, reajustar y llevarla a cabo.

Se debe asignar un responsable del proceso quien no necesariamente debe ejecutar las acciones propuestas, pero sí debe llevar un registro del proceso y su evolución, de cuántas normas se implementas satisfactoriamente, así como de problemas asociados.

5.2.1 Mediciones de gestión de seguridad de red

Para comprobar que la gestión de seguridad de red genera un efecto, ya sea positivo o negativo dentro de la gestión de TI como tal, se deben tener métricas asociadas al proceso, por lo que se debe llevar un registro de al menos las siguientes métricas:

a) Número normas o pautas de política propuestas.
b) Número normas o pautas de política implementadas.
c) Número de incidentes asociados a implementación de políticas de seguridad.

La métrica con la letra a es de un valor fijo de 13, que son las que se proponen en la tabla anterior, podría variar si por alguna razón se decide en definitiva no implementar una propuesta. La fuente para las métricas está en el registro que se debe llevar del proceso

De las métricas anteriores, se pueden obtener los siguientes Indicadores Clave de Rendimiento o KPI (Key Performance Indicators) relacionadas con la gestión de eventos:

1) Porcentaje normas o pautas implementadas=(b/a)*100
2) Cantidad de incidentes asociados a implementación de políticas de seguridad=c

Basado en los KPI, se pueden obtener factores claves de éxito de la propuesta como los mostrados en la siguiente tabla.

Tabla 8: Factores clave de éxito de gestión de seguridad de red

Factor clave de éxito	KPI	Resultado esperado
Conclusión satisfactoria de implementación de Política de Seguridad propuesta	1	Aumento
Incidentes generados por implementación de política de Seguridad	2	0

La gestión de seguridad de red exitosa va a estar en función del ir completando cada una de las pautas enunciadas de forma satisfactoria. Además, lo deseable, no tener incidentes en la implementación de la política.

Se deben medir estos factores clave de éxito cada cierto período, por ejemplo: cada mes durante su implementación.

5.3 Plan Piloto de Implementación asociado a gestión de eventos

Como implementación inicial se pone a prueba uno de los subprocesos, en conjunto con la jefa de TI y Harold Morales (analista de sistemas encargado de soporte de red), se elige implementar una herramienta de monitoreo como desarrollo inicial del proceso de gestión de eventos.

La principal razón de la decisión del plan piloto es que se considera que al momento del desarrollo de este proyecto, esta solución de gestión de eventos genera más valor al negocio ya que no se ha desarrollado ningún trabajo similar y como se observó previamente en el diagnóstico del proyecto, este proceso responde a una prevención para la mayoría de los incidentes reportados y fue elegido por todos los encuestados para su desarrollo.

Se realiza únicamente un subproceso, además, solo una parte del mismo ya que ambos procesos se pueden medir a través del tiempo, que involucra varias semanas y hasta meses y se tiene esta limitación de tiempo en este proyecto, el cual se basa principalmente en la propuesta, por lo que esta implementación de plan piloto busca dar un esfuerzo inicial, para continuar con el resto de la propuesta a través del tiempo.

Para efecto del plan piloto, se recapitulan los puntos de la presente propuesta de gestión de eventos, específicamente en la sección 5.1.3 de este documento:

1. Determinar políticas.
2. Instalación de herramienta de monitoreo.
3. Definición de alcance de gestión de eventos.
4. Documentación de repertorio de eventos.
5. Documentación de gestión de eventos.
6. Correlación de eventos.

Como primer resultado asociado al plan piloto, es que existe una diferencia de los puntos de la propuesta y estos enunciados del plan piloto, se considera a la hora de poner en marcha la gestión de eventos, que la definición inicial de la política da pautas para seguir el proceso. Por esta razón se tiene como resultado práctico que para una mejor guía, se defina primero la política de gestión de eventos.

En el Anexo 4 se adjunta la aprobación de la bitácora del plan piloto realizado.

5.3.1 Política de gestión de eventos asociada a plan piloto

La política en general refiere a que se definan pautas para la gestión de eventos, que de hecho se basa en toda la propuesta, para el caso del plan piloto en específico se visualizan las siguientes pautas:

- Se instala y pone en marcha la herramienta de monitoreo.

- Se incluye en monitoreo servidores y principales equipos de red (switches de red modulares).
- Para todo equipo como mínimo se debe monitorear disponibilidad del mismo, opcionalmente se pueden gestionar los recursos del equipo.
- Definir umbrales aceptables para los eventos seleccionados, en este caso la disponibilidad.
- En caso que se observe un evento crítico de disponibilidad de un equipo, se maneja como evento de excepción y se debe brindar soporte al equipo que presentó el evento.

Esta política del plan piloto es un resumen de la política general mencionada en la propuesta, se acorta para ajustarse al tiempo reducido del desarrollo del piloto. Sin embargo, se toman en cuenta los aspectos principales que le dan forma a la gestión de eventos que se desarrollan en los siguientes puntos.

5.3.2 Puesta en marcha de Herramienta de Monitoreo

Se procede a instalar en un servidor virtual la herramienta libre de Nagios Core y se agregan equipos de red al monitoreo, para esto se definen equipos que soportan los principales servicios, para lo cual sobresalen servidores y equipos de red.

Unos de los primeros resultados observados es que para la instalación y administración de Nagios Core se requiere conocimiento de la administración de Sistema Operativos Linux, a pesar de que se puede visualizar el monitoreo de forma gráfica, la administración y cambios de configuración se realiza principalmente a través de comandos especializados.

Este primer resultado muestra que a pesar de ser una herramienta de uso libre, sí requiere más horas de implementación al no ser una herramienta sencilla de instalar y poner a trabajar, al menos en comparación de otras herramientas que se realiza una administración gráfica, que puede representar mayor facilidad.

5.3.3 Definición de alcance de plan piloto de gestión de eventos

En la propuesta se indica que se gestione eventos de equipos basado en los que le dan soporte a servicios estratégicos. Pero al momento de poner a trabajar la propuesta, se tiene como resultado que en lugar de dedicarse a definir servicios estratégicos, se considera que todos los servidores y equipos de red tienen una función importante dentro del servicio que

brinda TI al hospital, por lo que se decide gestionar eventos de los servidores y al menos los principales equipos de red.

5.3.4 Repertorio de Eventos por gestionar en Plan Piloto

Se limita este plan piloto a una mínima gestión de eventos de disponibilidad porque lo que se pretende es comenzar a visualizar el proceso de gestión de eventos y el evento mínimo que debe monitorearse en la disponibilidad de cada equipo.

Adicionalmente de forma proactiva se comienzan a monitorear eventos de recursos como CPU, memoria y espacio en disco de Servidores Windows, por la facilidad que Nagios ofrece de una librería interna pre configurada que permite entender las estadísticas de SNMP de estos equipos.

Se encuentra que para los equipos de red, no se tiene una librería interna preconfigurada en Nagios, por lo que se prueba con CPU, memoria y temperatura de unos componentes internos del switch de red principal. Sin embargo, es un trabajo que debe hacerse manual para entender las estadísticas del equipo, por lo que involucra incluso labores de conocimiento de gestión de los equipos de red.

Se comienza a evaluar eventos de disponibilidad usando PING. Para visualizar la administración de recursos de CPU, memoria, disco y temperatura, se habilita SNMP en un servidor y el switch principal de red.

Algunas ilustraciones de la interfaz gráfica donde se observa el monitoreo son las siguientes:

Ilustración 8: Vista de monitoreo de disponibilidad de servidor de Hospital México

En la ilustración se muestra una de las vistas al ingresar a un tipo de monitoreo específico de un equipo, en este caso la disponibilidad del dispositivo que se encuentra en buen funcionamiento según el momento que se captura la ilustración.

Para este ejercicio no se muestra el nombre completo y dirección IP del dispositivo, para mantener la confidencialidad de información de equipos reales del hospital.

La siguiente es una muestra adicional de una gráfica que se obtiene por PING, la gráfica muestra el comportamiento diario y semanal, pero la que para el momento de la captura, es más representativa, constituye la diaria pues no se tenía monitoreo suficiente para tener una vista semanal.

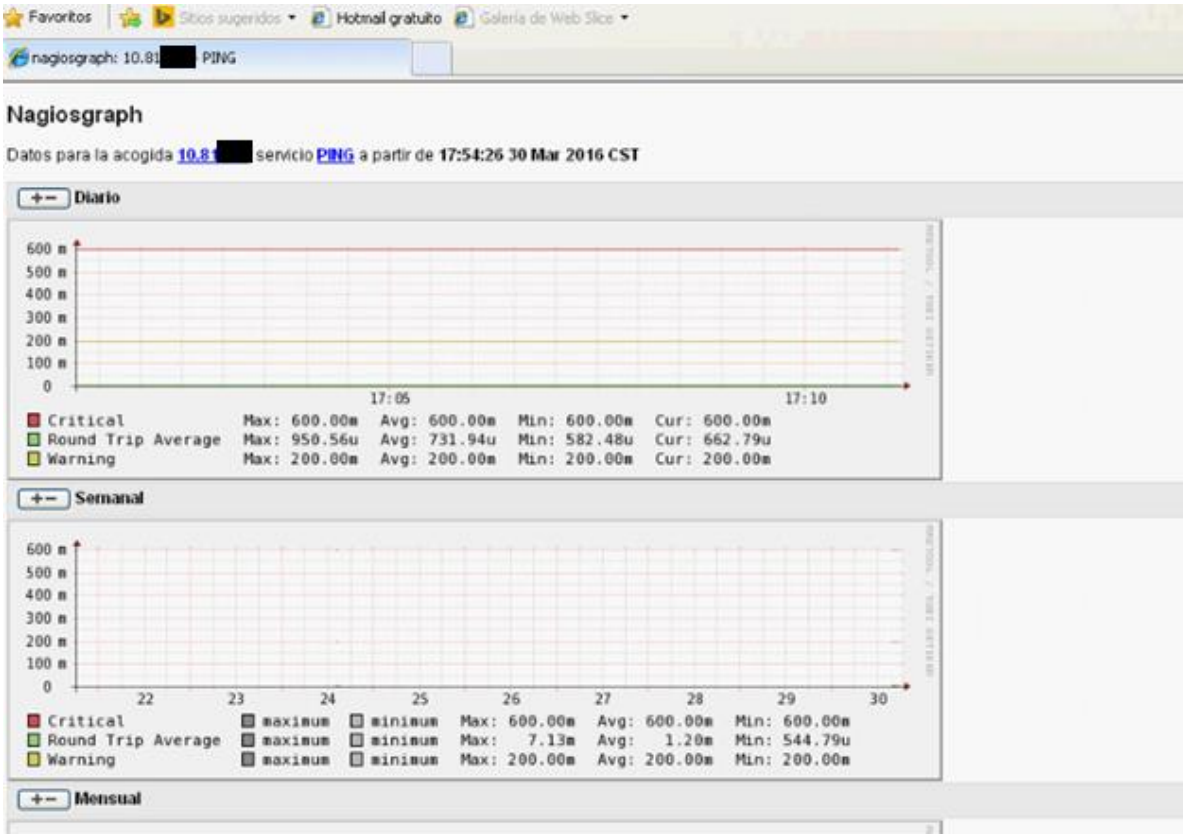


Ilustración 9: Gráfica de PING de Herramienta de Monitoreo en Plan Piloto

Se observa en la gráfica diaria tres líneas, una verde que representa el tiempo promedio de respuesta del PING, una amarilla que indica que tiempos más arriba de esa línea generan una advertencia, y la línea roja que indica que tiempos arriba de ella ya representan una situación crítica.

5.3.5 Definición de umbrales de eventos por monitorear

El umbral principal por tomar en cuenta es el de disponibilidad, se toma en cuenta el PING para valorar la disponibilidad de un equipo.

Como ejemplo, en la última ilustración, los valores de líneas en amarillo y rojo de la gráfica es lo que representa a los umbrales de alertas que deben ser definidos por expertos en el equipo que se está monitoreando. Como parte de los resultados asociados a esta implementación, se observa que los umbrales vienen muy por encima del valor promedio, por lo cual las alertas muy posiblemente no se van a dar, de forma que si se quiere que en realidad se generen alertas de valores más cercanos a los promedios, se deben bajar esos

umbrales. Esto es una recomendación para este caso, que igual aplica para cualquier evento que se quiera monitorear.

Por ejemplo: en este caso, si se reconoce que el valor del PING está normalmente en un valor de 1 ms, se deben ajustar los umbrales a valores más bajos, como ejemplo, 15 ms para advertencia de lentitud y 50 ms para alerta crítica. Esto de igual forma hay que validarlo en el tiempo, y verificar si hay posibilidad de ajustar aún mejor estos umbrales.

Esto último permite extraer un resultado, que se refiere a los valores de umbrales que trae por defecto la herramienta de monitoreo y no necesariamente son los más idóneos.

5.3.6 Atención de eventos de plan piloto

Para este caso, se debe configurar notificación de eventos, principalmente alertar por problemas de disponibilidad de un equipos, se debe reportar a los encargados del soporte del equipos y a la gerente de TI.

En caso que se presente el evento, se deberá validar a través de conexión de red si realmente el equipo no es accesible de forma remota y en caso que no se tenga acceso remoto, dirigirse de manera física al equipo y valorar por qué no está accesible por red, tal y como si fuera un incidente.

Adicionalmente se va a habilitar un documento de Excel para el registro de los eventos, se indicará la descripción del evento, el equipo que se vio afectado, fecha y hora, además, la posible causa y acción tomada al evento.

5.3.7 Resumen de mejoras por hacer a la propuesta luego del piloto

De la implementación del plan piloto, se recapitulan los siguientes resultados, que difieren de la propuesta a la implementación real.

- La propuesta enumeraba primero definir la herramienta y el alcance de a cuales equipos gestionar eventos, luego hablar de la política de la gestión de eventos. Sin embargo, dentro de la implementación, se observó que brinda mejor guía definir en primera instancia las políticas o pautas a seguir.
- En la propuesta se define el software de Nagios Core. A pesar de que es una herramienta muy reconocida y tiene múltiples opciones, su instalación y administración no resultó ser tan sencilla de lo que se pensó y se tuvo que trabajar

en varias sesiones para echar a andar este software. Se podría pensar en investigar no solo las funciones del software, sino además, su facilidad de administración.

- Al definir el alcance de equipos por gestionar eventos, resultó ser más práctico en la implementación, simplemente decir qué equipos quieren que se gestionen eventos, sobre todo basado en la importancia que se considera del equipo. Esto a diferencia de estar revisando que servicios trabaja TI y gestionar los equipos asociados a estos servicios tal y como lo indicaba la propuesta.
- Los umbrales para las alertas no necesariamente deben basarse de forma exclusiva en recomendaciones del fabricante como lo menciona la propuesta ya que no siempre el fabricante define umbrales para todos los eventos que se desean monitorear. Adicionalmente, se puede analizar los resultados iniciales de los eventos que se están gestionando y validar si los umbrales se ajustan a la realidad del equipo y condiciones en las que se desempeña.

La propuesta para la gestión de eventos representa una guía para su implementación, sin embargo, se observó con este plan piloto que se pueden hacer mejoras, las cuales se obtuvieron a la hora de llevar la propuesta al ambiente de producción real.

6 CAPÍTULO VI: ANÁLISIS FINANCIERO

Como se ha indicado en las secciones previas de este proyecto, no se estima invertir dinero para la adquisición de activos asociados a este Proyecto de Gestión Preventiva de Infraestructura de TI, basado en que aprovecharán los recursos existentes en el hospital.

Sin embargo, sí se requiere inversión en horas de trabajo de personal de la Unidad TIC del hospital para obtener los resultados de esta propuesta, que se traduce en dinero invertido. Además, sí se pretende obtener beneficios económicos asociados a ahorro de horas de trabajo en incidentes.

6.1 Inversión Inicial

La inversión inicial, gastos e ingresos de proyecto están asociados a horas de trabajo de personal del hospital y de soporte de consultores especialistas.

Como inversión inicial de personal de TI del hospital de trabajo en forma exclusiva en el proyecto se estiman 5 horas en acompañamiento, colaboración en consultas sobre estado actual de infraestructura y creación de máquina virtual para herramienta asociada a plan piloto de gestión de eventos, la mayor parte del trabajo ha sido por parte de estudiante.

Sin definición exacta del recurso del hospital que va a realizar el acompañamiento, se van a estimar las horas como base de un Analista de Sistemas 2 ya que es la posición de unos de los colaboradores que han soportado el desarrollo de este proyecto. Según el índice salarial de la Caja Costarricense del Seguro Social un Jefe de TIC 2 tiene un salario base para el 2015 de "643 200 colones" (Caja Costarricense de Seguro Social, 2015).

Siendo el salario base mostrado, el cálculo de una hora de trabajo sería el siguiente:

Tabla 9: Cálculo de costo de hora de colaborador

Salario base	₡643.200,00
Horas laboradas semanalmente	40
Semanas laboradas en año	52
Meses laborados en el año	12
Costo de hora de colaborador	₡3.710,77

Para obtener el costo de la hora del colaborador, multiplica el salario por la cantidad de meses laborados, luego este se divide entre la cantidad de semanas laboradas en el año y

eso se divide entre las horas laboradas a la semana, con esto se obtiene que la hora del colaborador tiene un costo de 3.711 colones aproximadamente.

Adicionalmente, el plan piloto deja trabajando la herramienta de monitoreo en una situación estable, sin embargo, se estima que se requiere apoyo adicional del consultor que ahora brinda soporte a servidores, para poner a trabajar la herramienta con mayores detalles, además, de apoyo en la gestión de seguridad de red.

Se estima una inversión adicional de 30 horas, por las cuales el hospital paga 60 USD por hora, siendo alrededor de 32.500 colones por hora, se estima una inversión inicial de especialistas de 520.000 colones.

A estas 30 horas de especialista se le suman 30 horas de acompañamiento de colaborador, que se va a suponer que es el mismo analista de sistemas 2. Por lo que de inversión inicial en horas del colaborador interno es de 35 horas y como se calculó el costo de la hora a 3.711 colones, se tendría una inversión inicial de 129.877 colones aproximadamente.

Tabla 10: Inversión inicial del proyecto

Inversión Inicial basado en horas de funcionario	₡129.876,92
Inversión inicial de especialistas	₡975.000,00
Inversión inicial total	₡1.104.876,92

Con base en las estimaciones anteriores, la inversión inicial total es de 1.104.877 colones aproximadamente.

6.2 Gastos del proyecto

En relación con los gastos del proyecto, se estima que durante la fase de ejecución se destinarán cuatro horas a la semana de un colaborador para que se fije en el cumplimiento de procesos asociados a la gestión preventiva, para lo cual se define el costo por hora según el salario de un colaborador con la categoría de Analista de Sistemas 2.

Para el caso de gastos e ingresos, se van a tomar en cuenta tres periodos de 52 semanas, es decir, un año cada período. El salario del analista se va a aumentar cada año a 1% como

un porcentaje estándar, que es el máximo acordado por el gobierno en 2016 (Jiménez B., 2016).

Con cada periodo de 52 semanas, al multiplicar esas semanas por la cantidad de 4 horas presupuestadas, se tiene un total de 208 horas para cada período, estas horas que van a representar el costo de cada periodo, que va a aumentar basado en el aumento del salario de un 1% comentado.

Tabla 11: Gastos por período del proyecto

	P1	P2	P3
Salario base	₡643.200,00	₡649.632,00	₡656.128,32
Costo de hora de colaborador	₡3.710,77	₡3.747,88	₡3.785,36
Horas invertidas por periodo por colaborador	208	208	208
[redacted]			
Costo de inversión de horas semanales	₡771.840,00	₡779.558,40	₡787.353,98

Como se observa el salario base va a aumentar en un 1% cada año, por lo que si se invierten las mismas horas en cada período, el gasto va a ir aumentando cada período.

6.3 Ingresos asociados al proyecto

El beneficio monetario asociado al proyecto está directamente relacionado con la reducción de tiempos en la atención de incidentes producto de una gestión preventiva de la infraestructura tecnológica en el hospital. En ese sentido, cuando se producen incidentes críticos, se requiere la contratación de especialistas externos.

Con la gestión de procesos preventivos para la infraestructura de TI del Hospital México se pretende disminuir el impacto de los incidentes, inclusive evitarlos completamente. De esta forma, por ejemplo: si se reduce el tiempo de atención de 4 a 3 horas, es una hora menos invertida en ese incidente, es decir, se ahorra una hora de tiempo del colaborador e inclusive del consultor especialista que colabora con el soporte.

Si se logra reducir una hora a la semana de incidentes, se ahorra una hora no solo del especialista, sino que además, del colaborador que lo acompañe, se resumen los ingresos de la siguiente forma.

Con una estimación de ahorro de una hora a la semana, es decir, 52 horas del colaborador y las mismas horas del especialista, se calculan los ingresos asociados al proyecto.

Tabla 12: Ingresos asociados a ahorro de tiempo para atención de incidentes

	P1	P2	P3
Costo por hora de colaborador	₡3.710,77	₡3.747,88	₡3.785,36
Horas reducidas a la semana de colaborador	52	52	52
Costo de hora de especialista	₡32.500,00	₡32.500,00	₡32.500,00
Horas reducidas a la semana de especialista	52	52	52
Ingreso por reducción de horas invertidas en incidentes	₡1.882.960,00	₡1.884.889,60	₡1.886.838,50

Como se aprecia en la tabla anterior, los ingresos van aumentando levemente por el ahorro de la hora del colaborador interno y para el especialista la estimación está fijada al mismo precio por los siguientes periodos.

6.4 Evaluación financiera del proyecto

Los valores de diferencia entre ingresos y costos del período 1, con el cálculo de valor presente neto y la tasa interna de retorno del proyecto se presentan en la siguiente tabla:

Tabla 13: Tabla de factibilidad financiera del proyecto para el período 1

	P0	P1	P2	P3
Costos para periodo		₡771.840,00	₡779.558,40	₡787.353,98
Ingresos para periodo		₡1.882.960,00	₡1.884.889,60	₡1.886.838,50
Utilidad		**₡1.111.120,00**	**₡1.105.331,20**	**₡1.099.484,51**
Inversión Inicial(-)	-₡1.104.876,92			
Valor Presente Neto	₡1.224.923,28			
Tasa Interna de Retorno	84%			

Para evaluar la viabilidad de este proyecto se utiliza el valor presente neto (VPN), que se define desde un punto de vista de administración financiera como una "Técnica más desarrollada de elaboración del presupuesto de capital; se calcula restando la inversión inicial de un proyecto del valor presente de sus flujos de entrada de efectivo descontados a una tasa equivalente al costo de capital de la empresa" (Gitman & Zutter, 2012, pág. 368).

Asociado a la fórmula, "El valor presente neto (VPN) se obtiene restando la inversión inicial de un proyecto (FE0) del valor presente de sus flujos de entrada de efectivo (FEt) descontados a una tasa (k) equivalente al costo de capital de la empresa" (Gitman & Zutter, 2012, pág. 368). Para este proyecto la inversión inicial de 1.104.876,92 colones, todo se trabaja con una tasa de retorno sobre la inversión del 20%.

VPN = Valor presente de las entradas de efectivo - Inversión inicial

$$\text{VPN} = \sum_{t=1}^{n} \frac{FE_t}{(1 + k)^t} - FE_0$$

Ilustración 10: Fórmula para calcular el valor presente neto Fuente: Gitman & Zutter, 2012, pág. 368

Como el valor presente neto es positivo para el cálculo de los tres periodos, hay viabilidad para este proyecto, partiendo del supuesto en el ahorro de tiempos de atención de incidentes anteriormente explicado.

Adicionalmente se presenta la tasa interna de retorno o rendimiento (TIR).

> "La tasa interna de rendimiento (TIR) es la tasa de descuento que iguala el VPN de una oportunidad de inversión con $0 (debido a que el valor presente de las entradas de efectivo es igual a la inversión inicial); es la tasa de rendimiento que ganará la empresa si invierte en el proyecto y recibe las entradas de efectivo esperadas" (Gitman & Zutter, 2012, pág. 372).

Por tanto, con las estimaciones asociadas a este proyecto, la rentabilidad del proyecto en términos porcentuales de acuerdo con la TIR es de 84%, lo cual es bastante alta por las condiciones favorables de flujos estimados de caja.

7 CAPÍTULO VII: CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones

1. Se concluye a través del diagnóstico que los principales incidentes y vulnerabilidades que se reconocieron en la infraestructura de TI del hospital se relacionaron principalmente a problemas de hardware y aspectos ambientales que acarrearon incidentes, además, de falta de control en la seguridad de red que también fue indicado en el diagnóstico.
2. Se concluye que la gestión de eventos y gestión de seguridad de red cumplían con la prevención de los principales incidentes y vulnerabilidades identificados, estos se desarrollan como subprocesos en la propuesta de gestión preventiva de TI.
3. Se brinda una propuesta de solución de diseño de procesos, donde se concluye que es requerido integrar un diagnóstico de la situación actual, definir un marco de referencia para darle forma, además, a través de investigación y juicio experto, definir el contenido de la misma. Involucrando estos aspectos, va a permitir que una propuesta pueda llegar a ser tomada en cuenta más allá del papel y llegue a ser implementada.
4. Se desarrolla el plan piloto de gestión de eventos, se concluye que la implementación de cualquier propuesta va a presentar variables que no salen a la vista durante el diseño de la misma, como en este caso, se debió tomar en cuenta financieramente que iba a requerir más tiempo inicial para instalación y administración inicial de la herramienta de monitoreo ya que tomó más de unas pocas horas estimadas.

7.2 Recomendaciones

Estas recomendaciones van dirigidas a quien tenga la posición de Jefe de TI en el Hospital México, se brindan basadas en el diagnóstico realizado durante el desarrollo del proyecto en las instalaciones del Departamento de TI del Hospital México, desde un juicio experto personal, además, tras la implementación del plan piloto de la propuesta de solución presentada en este proyecto.

1. La propuesta brindada en este proyecto es un tema abierto, se recomienda revisarla y en caso que se quiera corregir o ampliar alguna recomendación o acción por tomar, se puede realizar sin problema, siempre y cuando esté justificado de alguna forma, ya sea a través de investigación o juicio experto.

2. Se recomienda trabajar la propuesta de forma paulatina, no intentar trabajar todos los procesos de una sola vez porque puede existir confusión. Inclusive desarrollarla en pasos y cada vez que se tiene un avance validar su correcto funcionamiento para seguir al siguiente paso.
3. Esta propuesta de gestión de procesos preventivos en el Hospital México representa solo el comienzo de varias labores que se pueden llevar a cabo para mejorar cada día la gestión de TI, por ejemplo: se rescatan algunos procesos y labores que se recomienda estudiar para tener mayor control sobre la tecnología que se administra.

    3.1. Gestión de configuraciones: de forma tal que en un repositorio centralizado se gestionen las configuraciones y cambios de configuraciones de los diferentes dispositivos de infraestructura, de forma tal que sirva como respaldo en caso de algún incidente.
    3.2. Registro de incidentes y soluciones, puede trabajarse como una gestión de conocimiento y gestión de incidentes, de forma tal que las experiencias y conocimiento que se obtiene ante la atención de incidentes por parte del Departamento de TI sea documentado y compartido a otros colaboradores. Además, involucra crear tiquetes de soporte interno en caso de incidentes y hasta eventos que requieran una revisión.

8 CAPÍTULO VIII: ANÁLISIS RETROSPECTIVO

La idea del proyecto se tuvo a raíz de ver una necesidad que se había observado no solo en el hospital, sino de diferentes departamentos de TI donde se reconoce la posibilidad de ocurrencia de incidentes, pero no se ha llegado a un grado de madurez en la gestión de TI que permita tener un control mayor, no solo en la corrección de incidentes, sino con procesos de prevención de los mismos.

El proyecto significó un sacrificio de muchos aspectos de vida personal durante su desarrollo para poder brindar una propuesta suficientemente útil para que en realidad pueda ser llevada a cabo.

Este sacrificio comentado vale la pena desde el punto de vista que se ponen a prueba conocimientos adquiridos a lo largo de la maestría en un ambiente de gestión de productos y servicios de TI como el que brinda la Unidad TIC del Hospital México internamente, que de hecho cuenta con limitaciones, pero el poder desarrollar soluciones sobreponiéndose a esas limitaciones, es donde se genera aún más valor en lo personal como profesional y para el hospital en el aprovechamiento de sus recursos.

El grado de cumplimiento al plan de trabajo inicial no varió mucho, se pretendía desarrollar procesos preventivos y que estos acapararán la mayor cantidad o al menos los incidentes más importantes. Sin embargo, se visualiza que existen múltiples procesos los cuales se pueden desarrollar y también pueden integrarse como parte de una gestión preventiva, que los dos procesos desarrollados en la propuesta generan valor, pero no son suficientes para una gestión preventiva completa.

Inicialmente se quería ser más pretencioso, se quería desarrollar hasta tres procesos, sin embargo, por limitaciones de tiempo asociadas al proyecto, para brindar propuestas completas se consideró que más de dos procesos iban a poner en riesgo la culminación del proyecto.

Los objetivos del proyecto en esencia se cumplen satisfactoriamente ya que en resumen lo que se pretendía era identificar los principales incidentes y vulnerabilidades que afectaban los servicios y a través de diferentes investigaciones, dar una propuesta para prevenir esas situaciones, se presenta como tal en el proyecto.

El proyecto eventualmente no sufrió desviaciones significativas, siempre mantuvo ese horizonte de prevención de incidentes, como un concepto asociado a evitar desastres en TI. Sin embargo, sí existieron cambios como el comentado, de no poder acaparar más procesos preventivos; además, que de desarrollar el proyecto desde una perspectiva más estratégica y de calidad de servicios y que no se vea como una propuesta meramente técnica, al ser un proyecto asociado a infraestructura de TI.

Se considera que la propuesta presentada puede ser desarrollada aún más, lo que se muestra en este proyecto es un inicio de la gestión preventiva con dos subprocesos asociados, como son la gestión de eventos y la gestión de seguridad de red. Estos seguramente con su implementación y a través de una mejora continua, pueden representar un valor mayor a la gestión de TI, no solo del hospital, sino de otras instituciones, donde las propuestas son perfectamente aplicables.

9 REREFENCIAS BIBLIOGRÁFICAS

Allen, J. H. (02 de Julio de 2013). *Carnegie Mellon University*. Recuperado de "Plan, Do, Check, Act": https://buildsecurityin.us-cert.gov/articles/best-practices/deployment-and-operations/plan-do-check-act

Auza, J. (12 de Diciembre de 2010). *TECHSOURCE*. Recuperado de 5 of the Best Free and Open Source Server/Network Monitoring Software: http://www.junauza.com/2010/12/free-server-monitoring-software.html

Bhe, T., Glasmacher, P., Meckwood, J., Pereira, G., & Wallace, M. (2004). *Event Management and Best Practices.* International Business Machines Corporation: http://www.redbooks.ibm.com/abstracts/sg246094.html.

Caja Costarricense de Seguro Social. (01 de Enero de 2015). Recuperado de Índice Salarial: https://rrhh.ccss.sa.cr/?proc=36&sub=23&flw=1&sidchk=6hq245haqm7k400smmd5n07381&nmrchk=g86c136o7752n35287x1699o458x59q1&lnkchk=991942281

Fundación INVATE. (2011). Recuperado de Modelo de Gestión: http://www.invate.es/dmdocuments/Modelo_Gestion_Preventiva.pdf

Fundación Wikimedia, Inc. (14 de Marzo de 2016). *ISO/IEC 27001*. Recuperado de https://es.wikipedia.org/wiki/ISO/IEC_27001

Fundación Wikimedia, Inc. (22 de Noviembre de 2015). *Wikipedia*. Recuperado de Nagios: https://es.wikipedia.org/wiki/Nagios

Gitman, L. J., & Zutter, C. J. (2012). *Principios de Administración Financiera.* México: Pearson Educación de México, S.A. de C.V.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2010). *Metodología de la Investigación.* México D.F.: The McGraw-Hill Companies, Inc.

Hucaby, D. (2010). *CCNP SWITCH 642-813.* Indianápolis, IN USA: Cisco Press.

IT Process Wiki. (4 de Agosto de 2013). *ITIL Gestión de Eventos*. Recuperado de http://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_Eventos

IT Process Wiki. (4 de Agosto de 2013). *Procesos de ITIL*. Obtenido de ITIL Gestión de Incidentes: http://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_Incidentes#Incidente

IT Process Wiki. (4 de Agosto de 2013). *Procesos ITIL*. Obtenido de ITIL Cumplimiento de la Solicitud: http://wiki.es.it-processmaps.com/index.php/ITIL_Cumplimiento_de_la_Solicitud

Janalta Interactive Inc. (s.f.). *Techopedia.* Recuperado de IT Infrastructure: https://www.techopedia.com/definition/29199/it-infrastructure

Jiménez B., E. (11 de Febrero de 2016). Gobierno decreta aumento de 1% para trabajadores del sector público que ganen menos de ¢439.000. *La Nación*. Recuperado de http://www.nacion.com/nacional/trabajo/Gobierno-decreta-aumento-trabajadores-publico_0_1542045874.html

Lago, H. (Septiembre de 2010). *LinkedIn Corporation ©.* Recuperado de Calidad en Gestión de Servicios de TI: mejores prácticas y normas: http://www.slideshare.net/Nbarros/calidad-de-gestin-en-servicios-it

Nagios Enterprises, LLC. (2009). Recuperado de Nagios Core - Features: https://assets.nagios.com/datasheets/nagioscore/Nagios%20Core%20-%20Features.pdf

Nagios Enterprises, LLC. (2009-2016). *Nagos Core*. Recuperado de About Nagios Core: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/about.html#whatis

OSIATIS S.A. (18 de Octubre de 2015). *ITIL Foundation: Gestión de servicios de TI.* Obtenido de Estrategia para los Servicios TI: http://itilv3.osiatis.es/estrategia_servicios_TI.php

Sala de Prensa de Kaspersky Lab España. (28 de Enero de 2014). Obtenido de El 80% de los incidentes de seguridad TI de las compañías españolas los causaron los mismos empleados: http://www.kaspersky.es/about/news/press/2014/El_80_de_los_incidentes_de_seguridad_

Wikipedia Foundation. (1 de Octubre de 2015). Recuperado de IT Service Management: https://en.wikipedia.org/wiki/IT_service_management

10 GLOSARIO

Servidor: computador con recursos mayores a las que un usuario normalmente posee, el servidor corre un servicio el cual es solicitado por diferentes computadoras de usuario en una red.

Dirección IP: identificador de computadoras para entregar paquetes de datos.

TELNET: protocolo de administración por red de equipos a través de línea de comandos, la comunicación, incluyendo las credenciales, viajan en texto plano a través de la red.

Servidor RADIUS: es un acrónimo de palabras en inglés (Remote Authentication Dial-In User Service), este servidor es utilizado para autenticar usuarios que requieren acceso a un equipo o recurso en la red.

Protocolo 802.1x: es una norma de la IEEE (Institute of Electrical and Electronics Engineers) asociado al control de acceso basado en puertos, es decir, se utiliza para autenticar y permitir la conexión de un equipo a un puerto de red.

VLAN: acrónimo de palabras en inglés (Virtual Local Area Network), se refiere a una red virtual de área local, lo cual refiere a una separación lógica de dos subredes, generalmente utilizada para segmentar tráfico de red.

Puerto de consola: puerto físico de administración de equipos, se utiliza para administrar un equipo de forma directa o físicamente presencial al equipo. Es una alternativa a la administración remota por red, por lo general utilizado en la administración inicial de un equipo o cuando se tienen problemas que no permiten la administración por red.

Puertos TCP/UDP: puertos lógicos en equipos que se conectan por red, se utilizan para identificar sesiones en las diferentes aplicaciones, por ejemplo: el puerto TCP 80 se utiliza para establecer sesiones Web por HTTP a servidores.

Active Directory: palabras en inglés que hacen referencia al servidor de directorio activo, es una forma de llamar en la empresa Microsoft al servidor utilizado para crear usuario o grupos de usuarios, basados en estos se puede tener un control de inicios de sesión y elaborar políticas de red.

11 ANEXOS

11.1 Anexo 1: Diseño preliminar de cuestionario

El presente cuestionario se presenta para identificar aspectos relacionados con la gestión de la infraestructura de TIC en el Hospital México, con el objetivo de analizar la situación actual para diseñar una propuesta de procesos preventivos de incidentes que afecten la disponibilidad y/o calidad de servicios de TIC.

Se agradece de antemano la participación. El tiempo estimado para responder el cuestionario no es mayor a 15 minutos.

1. ¿Está familiarizado con la gestión preventiva, favor comentar qué se entiende al respecto?
2. Indique al menos tres incidentes y/o vulnerabilidades asociados a infraestructura de TIC (redes, servidores y conexiones físicas entre ellos) que se presentan comúnmente o que han generado, o pueden generar un impacto significativo en la calidad y/o disponibilidad de los servicios de TIC. Entiéndase por vulnerabilidad puntos débiles de la infraestructura que pueden ser comprometidos y generar un incidente.
3. ¿Considera que en la actualidad dentro de la gestión de servicios de TIC del hospital, se ponen en práctica procesos o prácticas para prevenir incidentes o mitigar vulnerabilidades, que afecten la disponibilidad y/o calidad de servicios de TIC brindados en al hospital? (En caso de ser afirmativo, favor mencionar cuáles)
4. Indique al menos dos servicios de TIC que son de suma importancia y deben estar disponibles en todo momento para un correcto funcionamiento de las operaciones del hospital. Favor indique por qué son de gran importancia
5. Favor indique de las siguientes opciones máximo dos procesos o buenas prácticas que considera que son importantes por desarrollar dentro de la gestión preventiva de infraestructura de TIC del hospital, que además, no se estén desarrollando actualmente (En caso de considerar otro proceso o buena práctica preventiva que no sea parte de los mencionados, favor indicarlo y dar una breve explicación de lo que trata)
    a. Gestión de eventos asociados a equipos de red, almacenamiento de datos y servidores (involucra monitoreo).

b. Gestión de seguridad a través de control de acceso para administración de equipos de red y servidores.
c. Revisión de conexiones redundantes de equipos, rediseño en caso necesario.
d. Gestión de conocimiento (documentación, actualización y acceso a información sobre elementos actuales de infraestructura de TIC). Esto para futuras referencias en caso de reincidencia de incidentes.
e. Gestión de incidentes de infraestructura (seguimiento y documentación de incidentes que se dan asociados a la infraestructura de TIC). Esto para futuras referencias en caso de reincidencia de incidentes
f. Otros (favor explique):

11.2 Anexo 2: Respuesta a cuestionario

11.2.1 Respuestas de Jefe de TI

1. ¿Está familiarizado con la gestión preventiva, favor comentar qué se entiende al respecto?

Está relacionado con los mecanismos que permiten monitorizar la infraestructura, mediante la lectura de variables que permitan determinar el comportamiento estándar de la plataforma, para así identificar cuando se presentan problemas que afecten el rendimiento o calidad de los servicios o que pueda generar una interrupción en la prestación de un servicio específico o un conjunto de los mismos.

Por otra parte es importante un correcto análisis de riesgos, su posible impacto, probabilidad de ocurrencia y asimismo cual evento puede provocar que un posible riesgo se materialice, en caso de que esto ocurra que hacer, como hacerlo y definición de planes alternos de trabajo. Estas tareas son importantes realizarlas de forma previa.

2. Indique al menos tres incidentes y/o vulnerabilidades asociados a infraestructura de TIC (redes, servidores y conexiones físicas entre ellos) que se presentan comúnmente o que han generado, o pueden generar un impacto significativo en la calidad y/o disponibilidad de los servicios de TIC. Entiéndase por vulnerabilidad puntos débiles de la infraestructura que pueden ser comprometidos y generar un incidente.

Actualmente no se cuentan con herramientas que permitan determinar o generar un seguimiento de incidentes ocurridos con anterioridad. Debo aclarar que el Hospital México es un centro que su principal función es la prestación de servicios de salud, no es una empresa que se dedique a brindar servicios de TI, no obstante, dependemos de la tecnología en muchos de los procesos existentes, aunque se han logrado contratos de mantenimiento para equipos críticos, no se cuenta con los recursos o herramientas necesarias para poder obtener información sobre posibles vulnerabilidades o incidentes en tiempo real.

Aunque se cuenta con un análisis de riesgos, es necesario realizar procesos o contar con herramientas preventivas y no sólo reactivas, ya que muchas veces se encuentra un riesgo el mismo ya está materializado.

De los más importantes que recuerde en este momento, se presentó una falla en un aire acondicionado en un cuarto de servidores, el cual aunque cuenta con un aire acondicionado secundario ninguna alarma indico que el aire acondicionado se había apagado y se vio afectado la prestación de los servicios ya que al calentarse los equipos se apagaron de forma automática para proteger su integridad. Aunque se cuenta con un contrato de mantenimiento de aires acondicionados hasta que se presentó el problema se contactó a la compañía para su atención.

Existen algunos otros casos, pero este es el más significativo que recuerdo en este momento.

3. ¿Considera que en la actualidad dentro de la gestión de servicios de TIC del hospital, se ponen en práctica procesos o prácticas para prevenir incidentes o mitigar vulnerabilidades, que afecten la disponibilidad y/o calidad de servicios de TIC brindados en al hospital? (En caso de ser afirmativo, favor mencionar cuáles)

Se realiza limpieza de física de equipos y aplican actualizaciones (sistema operativo, firmwares)

4. ¿Indique al menos dos servicios de TIC que son de suma importancia y deben estar disponibles en todo momento para un correcto funcionamiento de las operaciones del hospital? Favor indique por qué son de gran importancia

Existen muchos servicios, no todos funcionan las 24 horas, entre los servicios más importantes que tienen un impacto directo con el paciente es el Laboratorio Clínico, Farmacia, Admisión y Urgencias. Los cuales cuentan con sistemas de información para registro y toma de decisiones del paciente. Adicionalmente la telefonía es un sistema vital que permite interconectar los servicios y comunicarnos con otros hospitales y clientes externos.

5. ¿Favor indique máximo dos procesos o buenas prácticas considera que son importantes a desarrollar dentro de la gestión de infraestructura de TIC del hospital, que además, no se estén desarrollando actualmente? (En caso de considerar otro

proceso o buena práctica preventiva que no sea parte de los mencionados, favor indicarlo y dar una breve explicación de lo que trata).

- *Gestión de eventos asociados a equipos de red, almacenamiento de datos y servidores (involucra monitoreo).*
- *Gestión de seguridad a través de control de acceso para administración de equipos de red y servidores.*

11.2.2 Respuestas de analista de sistemas asociado a soporte de redes

1. ¿Está familiarizado con la gestión preventiva, favor comentar qué se entiende al respecto?

Toda gestión preventiva está orientada a que de manera proactiva y preventiva los funcionarios de una determinada compañía, empresa u organización realicen mantenimiento a sus equipos, edificaciones u otros disminuyendo el daño por deterioro. De igual manera se brinda y gestiona planes de continuidad ante posibles fallos de estos activos.

2. Indique al menos tres incidentes y/o vulnerabilidades asociados a infraestructura de TIC (redes, servidores y conexiones físicas entre ellos) que se presentan comúnmente o que han generado, o pueden generar un impacto significativo en la calidad y/o disponibilidad de los servicios de TIC. Entiéndase por vulnerabilidad puntos débiles de la infraestructura que pueden ser comprometidos y generar un incidente.

- *Daño en Fuentes de Poder en equipos de comunicación. (Switches de Comunicación).*
- *Daño en Tarjetas Controladoras. (Switches de Comunicación).*
- *Daños en Discos Duros en Servidores.*
- *Vulnerabilidad de equipos de red con respecto a su control de administración, y en sí al control de acceso a la red.*

3. ¿Considera que en la actualidad dentro de la gestión de servicios de TIC del hospital, se ponen en práctica procesos o prácticas para prevenir incidentes o mitigar

vulnerabilidades, que afecten la disponibilidad y/o calidad de servicios de TIC brindados en al hospital? (En caso de ser afirmativo, favor mencionar cuáles)

Existe un Plan de Continuidad, en el mismo se tipifican los riesgos y por cada uno de ellos se trata de mitigar el impacto que puede producirse con el mismo, por otro lado los diferentes departamentos o unidades que conforman el Hospital cuentan con un Plan Alterno de Trabajo, el cual se ejecuta en caso de que por algún incidente.

4. ¿Indique al menos dos servicios de TIC que son de suma importancia y deben estar disponibles en todo momento para un correcto funcionamiento de las operaciones del hospital? Favor indique por qué son de gran importancia

- *Las Redes de Comunicación.*
- *Los Servidores.*

Son vitales estos servicios ya que a través de la red se trasportan los datos que se integrarán en las diferentes Bases de Datos, por otro lado los servidores proveen los diferentes servicios computacionales que se requieren para compartir información y almacenarla en las diferentes DB.

5. ¿Favor indique máximo dos procesos o buenas prácticas considera que son importantes a desarrollar dentro de la gestión de infraestructura de TIC del hospital, que además, no se estén desarrollando actualmente? (En caso de considerar otro proceso o buena práctica preventiva que no sea parte de los mencionados, favor indicarlo y dar una breve explicación de lo que trata)

a. Gestión de eventos asociados a equipos de red, almacenamiento de datos y servidores (involucra monitoreo).

- *Además de mi respuesta anterior deseo aprovechar diciendo que en la actualidad el Hospital requiere una herramienta que le permita brindar monitoreo de una forma integral a todo lo referente a Infraestructura y Comunicación, el mismo debe ser parte de las labores de uno de los colaboradores de la UTIC, para garantizar y atenuar el riesgo de fallos al máximo de lo posible y así mantener los servicios en operación constante.*

- *Esta práctica es excelente, ya que el contar con soporte, mantenimiento y monitoreo nos garantiza la continuidad del Servicio en todo momento, ya que de manera proactiva se puede estar resolviendo incidentes antes de que ocurran.*

b. Gestión de seguridad a través de control de acceso para administración de equipos de red y servidores.

- *En cuanto a este tema es importante indicar que deberíamos aplicar a todos los puertos de red políticas de seguridad, en los cuales podamos apagar los que no estén conectados y aplicar Access List a las Mac asociadas a cada Switch para denegar servicios a equipos que no sean los institucionales.*
- *Nos proporciona confidencialidad y tranquilidad de que las personas que ingresen a la red o a los sistemas son las que deben contar tanto con los permisos como con los accesos a los diferentes sistemas. Es Excelente siempre invertir en la gestión de seguridad por lo que una buena herramienta de gestión colabora en gran manera en cuanto a este tema.*

11.2.3 Respuestas de analista de sistemas asociado a soporte de servidores, respaldo y almacenamiento de datos

1. Está familiarizado con la gestión preventiva, favor comentar, ¿qué se entiende al respecto?

Sí, básicamente es validar la mayoría de acciones/funciones/trabajos y evitarlas que se conviertan en un problema concreto, esto para que la continuidad de las labores del negocio no se afecten. Evitar que un riesgo materialice en problema.

2. Indique al menos tres incidentes y/o vulnerabilidades asociados a infraestructura de TIC (redes, servidores y conexiones físicas entre ellos) que se presentan comúnmente o que han generado, o pueden generar un impacto significativo en la calidad y/o disponibilidad de los servicios de TIC. Entiéndase por vulnerabilidad puntos débiles de la infraestructura que pueden ser comprometidos y generar un incidente.

- *Caídas de líneas de comunicación entre oficinas centrales y nosotros.*
- *Problemas con discos duros de servidores, más que todo por espacio.*
- *Problemas con switch de red.*

3. ¿Considera que en la actualidad dentro de la gestión de servicios de TIC del hospital, se ponen en práctica procesos o prácticas para prevenir incidentes o mitigar vulnerabilidades, que afecten la disponibilidad y/o calidad de servicios de TIC brindados en al hospital? (En caso de ser afirmativo, favor mencionar cuáles)

Existe un plan de continuidad, pero debido al poco personal, a veces es difícil inclusive hasta seguir las mismas resoluciones del mismo. Además, que en su mayoría son por problemas a nivel central.

4. ¿Indique al menos dos servicios de TIC que son de suma importancia y deben estar disponibles en todo momento para un correcto funcionamiento de las operaciones del hospital? Favor indique por qué son de gran importancia

Servidores y redes, porque en ellos reside la utilización de los sistemas, bases de datos, información de los usuarios, telefonía, impresión, etc., existe una interconexión entre ellos que no se puede eliminar y si uno falla se afecta todo.

5. ¿Favor indique máximo dos procesos o buenas prácticas considera que son importantes a desarrollar dentro de la gestión de infraestructura de TIC del hospital, que además, no se estén desarrollando actualmente? (En caso de considerar otro proceso o buena práctica preventiva que no sea parte de los mencionados, favor indicarlo y dar una breve explicación de lo que trata)

a. Gestión de eventos asociados a equipos de red, almacenamiento de datos y servidores (involucra monitoreo)

- *Esta opción es muy necesaria, creo que no se hace en el Hospital como se debiera, seria por medio de sistemas que envíen informes de cómo están funcionando los equipos, si hay algún tipo de incidente o que avise si el equipo tiene manteniendo*

preventivo y para cuando, etc. Este monitoreo ayudaría mucho en la parte preventiva.

d. Gestión de conocimiento (documentación, actualización y acceso a información sobre elementos actuales de infraestructura de TIC). Esto para futuras referencias en caso de reincidencia de incidentes

- *Este proceso me parece muy importante ya que da la oportunidad de tener un mayor control sobre la infraestructura para cuando haya que responder algún tipo de información ya sea a nivel de incidentes o a lo interno, pues la mayoría de información referente a documentación (sobre todo gráficos o parte más visual) de la red debería estar al alcance de la mayoría de TI, sobre todo cuando es tan cambiante como en nuestro caso y que requiere dejar un bitácora de los mismos.*

11.3 Anexo 3: Carta de aceptación para desarrollo de proyecto en institución

10 de setiembre del 2015

Jefe de TI
Lic. Adrián Badilla Muñoz
HOSPITAL MÉXICO

Estimado y Distinguido Adrián:

Me place extenderle un cordial saludo, en ocasión de solicitarle que mi persona **Bryan Valverde Piedra** estudiante de término de la **Maestría en Administración de Tecnologías de Información de la Universidad Nacional de Costa Rica**, pueda tener el debido permiso de usted para realizar el Proyecto de Graduación en su prestigiosa empresa **Hospital México**, específicamente en el **Departamento de Servicios de TI,** que su persona dirige, y tenga acceso a la misma con fines de obtener informaciones que les permitan desarrollar su proyecto de trabajo de grado o fin de carrera.

Dado que en el **Departamento de servicios de TI del Hospital México** se tienen funciones de velar por el correcto funcionamiento de los servicios de TI para el hospital, mi persona ha decidido visitar sus instalaciones para obtener información que les permitan completar su Proyecto de Graduación sobre el tema de investigación relacionado a la **Gestión Preventiva de Servicios de TI en Hospital México**. En adicción consideran oportuno para su empresa, la sociedad y mi persona como estudiante, que se realice este Proyecto de Graduación en su institución, y cuyo Proyecto de Graduación contribuirá e impactara en dicha organización positivamente. **Principalmente tendrá beneficios relacionados a la continuidad de los servicios de TI, de forma que se puedan evitar incidentes de forma proactiva.**

Con saludos cordiales y a tiempo de agradecerle su atención a esta solicitud, aprovecho la oportunidad para reiterarle mi más alta consideración y estima, y el apoyo como Licenciado y estudiante de la Maestría en Administración de TI de la Universidad Nacional de Costa Rica

Atentamente,

BRYAN VALVERDE PIEDRA
Estudiante de Maestría en Administración de TI, UNA
Tel.: 8898 5884, bryanvp1987@gmail.com

Aceptado por

ADRIÁN BADILLA MUÑOZ
Jefe de TI, Hospital México
Tel: 2242-6599, abadillm@ccss.sa.cr

Ilustración 11: Carta de aceptación para comienzo de proyecto en Departamento de TI de Hospital México

11.4 Anexo 4: Bitácora de decisiones asociadas al plan piloto

Bitácora de plan piloto

La siguiente bitácora muestra definiciones asociadas al plan piloto, en la primera definición se tiene participación doña Danelia Ramírez (Jefa de TI) y del encargado del soporte de red don Harold Morales. Para el resto de las definiciones se trabajó solamente con Harold Morales.

Definiciones de Plan Piloto	Resultado	Fechas de acuerdo
Definición de subproceso a trabajar en plan piloto	Se decide realizar plan piloto de implementación de Proceso de Gestión de Eventos	15 de marzo, 2016
Definición de dispositivos a monitorear	Gestionar eventos de servidores y principales equipos de red	19 de Marzo, 2016
Definición de eventos a monitorear	Por el momento sólo disponibilidad de equipos por PING. Se der posible adicionar recursos de equipos para ver ejemplo de cómo se presentan esos eventos	19 de marzo, 2016
Definición de atención de eventos	En caso que se dé una alerta de un equipo inalcanzable, se va a proceder a la atención del evento y al finalizar la atención, registrar el evento y acciones correctivas.	5 de abril, 2016

Bitácora validada el 7 de abril de 2016 por:

Harold Morales Charpantier

Unidad de Tecnologías de Información y Comunicación de Hospital México

Tel: 2242 6599

Ilustración 12: Aceptación de bitácora asociada a plan piloto de proyecto

11.5 Anexo 5: Carta de aceptación final del proyecto y carta de filóloga

San José, Costa Rica
15 de abril de 2016

Señores
Maestría en Administración de Tecnologías de Información
Universidad Nacional de Costa Rica

Estimados señores:

Por medio de la presente me permito saludarlos y además indicar que el señor **Bryan Valverde Piedra** estudiante de su maestría, estuvo desarrollando en conjunto con personal de la Unidad de Tecnologías de Información y Comunicaciones del Hospital México el proyecto titulado, **"Gestión de Procesos Preventivos en Servicios de TI del Hospital México."**

Por otra parte hago constar lo siguiente:

- La propuesta fue compartida al personal de este servicio.
- Se desarrolló satisfactoriamente un plan piloto como parte de la propuesta.
- Se acepta el proyecto, por cuanto se cumplieron los objetivos asociados al mismo y su entregable es aceptado.
- La propuesta genera valor estratégico dentro de la Gestión de Tecnologías de Información del Hospital México, esto por que colabora con nuestra función estratégica de mantener la alta disponibilidad de los servicios de TI.

Se le agradece al señor Valverde el tiempo y colaboración brindada con el desarrollo de este proyecto, deseándole lo mejores éxitos en su carrera profesional.

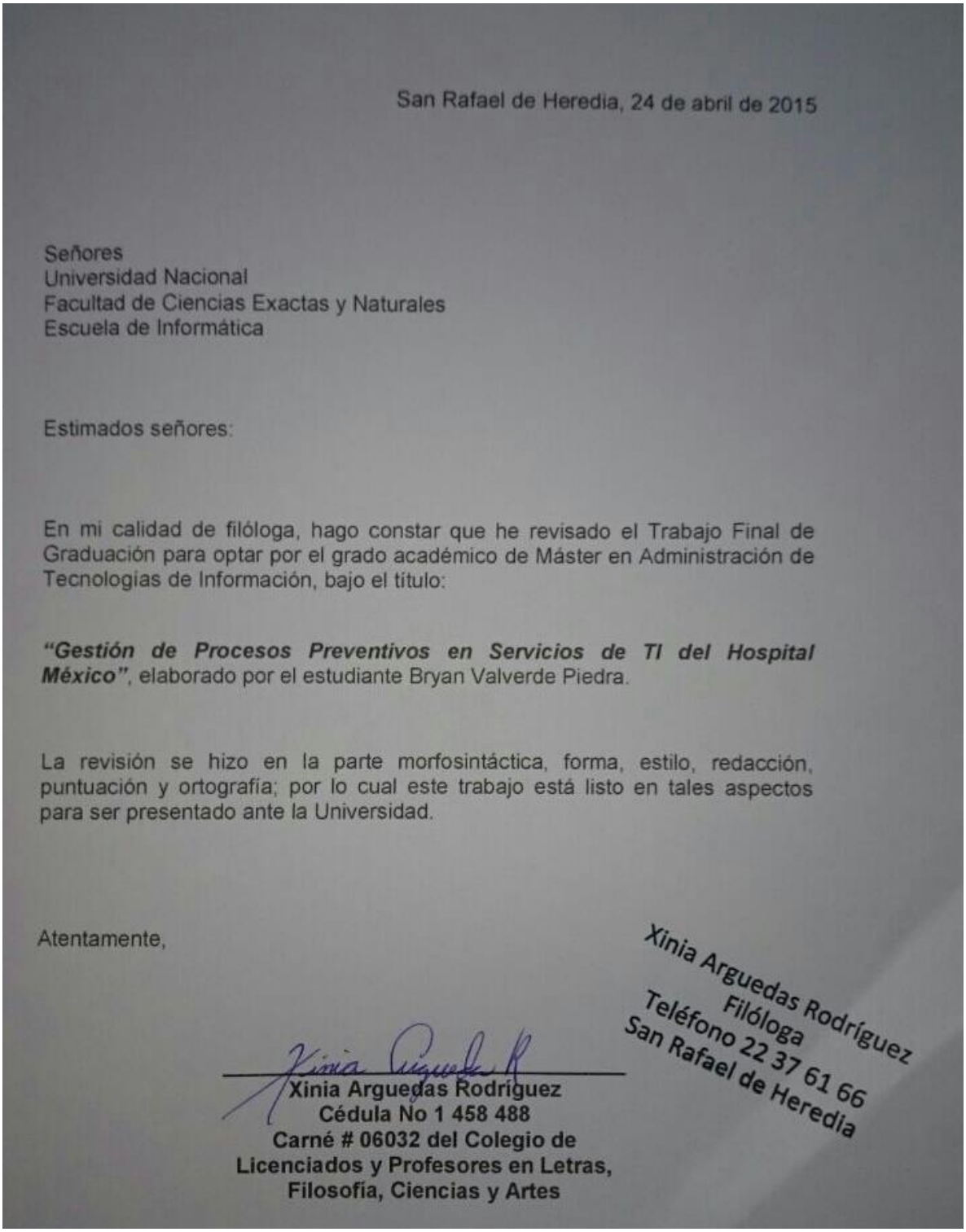
Sin más por el momento me suscribo,

HOSPITAL MEXICO * UNIDAD DE TECNOLOGIAS DE INFORMACION Y COMUNICACIONES * SEGURO SOCIAL COSTA RICA

Mci. Danelia Ramírez Vargas
Jefe Unidad de Tecnologías de Información y Comunicaciones
Hospital México
Tel: 2242-6599, dramirezv@ccss.sa.cr

cc. Archivo

Ilustración 13: Carta de aceptación de proyecto final



San Rafael de Heredia, 24 de abril de 2015

Señores
Universidad Nacional
Facultad de Ciencias Exactas y Naturales
Escuela de Informática

Estimados señores:

En mi calidad de filóloga, hago constar que he revisado el Trabajo Final de Graduación para optar por el grado académico de Máster en Administración de Tecnologías de Información, bajo el título:

"Gestión de Procesos Preventivos en Servicios de TI del Hospital México", elaborado por el estudiante Bryan Valverde Piedra.

La revisión se hizo en la parte morfosintáctica, forma, estilo, redacción, puntuación y ortografía; por lo cual este trabajo está listo en tales aspectos para ser presentado ante la Universidad.

Atentamente,

Xinia Arguedas Rodríguez
Filóloga
Teléfono 22 37 61 66
San Rafael de Heredia

Xinia Arguedas Rodríguez
Cédula No 1 458 488
Carné # 06032 del Colegio de
Licenciados y Profesores en Letras,
Filosofía, Ciencias y Artes

Ilustración 14: Carta de revisión de filóloga