Nombre completo del investigador: Bryan Valverde Piedra

Formación académica:

- Master en Administración de TI, UNA
- Licenciado en TI para la gestión de negocios, Universidad Latina de Costa Rica
- Bachillerato en Ingeniería Telemática, Universidad Latina de Costa Rica
- Profesional en TIC, especializado y con certificaciones profesionales en implementación y diseño de redes inalámbricas y alámbricas, además de seguridad en redes.
- Más de siete años de experiencia en soluciones y soporte de TIC.

Centro de Investigación: Proyecto de graduación para Maestría en Administración de TI (MATI) en Universidad Nacional de Costa Rica (UNA), proyecto diseñado para Hospital México de Costa Rica

Nombre de la Investigación:

"Gestión de Procesos Preventivos en Servicios de TI del Hospital México"

Resumen

Prevención se refiere a actuar antes de que un hecho se materialice y tenga efectos inesperados y/o negativos. Una gestión preventiva por tanto se relaciona con la administración de recursos para que de forma preventiva se pueda evitar en el mayor porcentaje eventos y situaciones que afecten una operación normal.

Como analogía asociada a la gestión preventiva, por lo general, no se espera que ocurra un robo de un vehículo, sin embargo, después que desafortunadamente le ocurre a una persona, saltan preguntas del por qué una acción u otra no se realizó, por ejemplo, el por qué no se pagó el seguro vehicular a tiempo o por qué no se dejó el vehículo estacionado en otro sitio. Todo se resume a que de haberse prevenido mejor, el hecho quizá no hubiera ocurrido o no sería tan nefasto.

En la administración de TIC, resulta similar al párrafo anterior, cuando un incidente tecnológico genera mucha afectación en un negocio, se debe acelerar el paso para trabajar en la solución, que lamentablemente no siempre llega de forma rápida, y luego de que finalmente se soluciona, saltan preguntas de cómo se pudo haber evitado o reducido el impacto de ese incidente.

Basado en estos aspectos mencionados, se desarrolla la investigación de una gestión preventiva, que se fundamente en hechos encontrados en el Hospital México, pero que no escapan a la realidad de otras instituciones y compañías y sus departamentos de gestión de TIC, que tiene un objetivo común de brindar alta disponibilidad de la tecnología para soporte del negocio.

La investigación se resume como un estudio de la gestión de TI dentro del hospital, y mediante buenas prácticas y juicio experto, se brinda una propuesta, principalmente asociada a gestión de eventos de TIC y gestión de seguridad de red.

La gestión de eventos trata de la identificación y monitoreo de cambios relevantes en un elemento o servicio TIC, a partir de esto definir como atenderlos. La gestión de seguridad informática busca mantener confidencialidad, integridad y disponibilidad de la información y de elementos de software y hardware que administran esta información.

Descripción del trabajo realizado

Se realiza una investigación con enfoque cualitativo, donde se realiza una recolección de datos sin medición numérica, sino que más bien se recolecta la información basado en el estudio de respuestas abiertas a personal del departamento de TIC del hospital, que posteriormente fueron interpretadas.

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.

Desarrollo de propuesta de Gestión de Eventos

Lo que se busca con la gestión de eventos, es identificar eventos que puedan representar una situación anómala, inclusive antes de que genere un incidente, como analogía en el campo médico, sería como identificar síntomas en un paciente y tratarlos de forma temprana, antes que eventualmente puedan desatar una enfermedad.

Tomando como referencia documentación de la empresa IBM de gestión de eventos y buenas prácticas, se parte como base para proponer un marco de referencia a seguir en la gestión de eventos de infraestructura de TI del hospital.

Se define utilizar la herramienta de monitoreo llamada NAGIOS, la cual es una herramienta de código abierto, que combina varias funcionalidades para monitoreo y notificación de alertas.

Para la gestión de eventos se tienen los siguientes pasos a seguir:

Pasos a seguir	Descripción
Definición del alcance de la gestión de eventos	Definir los elementos a los cuales eventos van a ser gestionados, esto basado en servicios de TI elementales al negocio
Determinar políticas asociadas a la gestión de eventos	Se indican acciones a realizar basado en lo que los eventos representen, aspectos tales como filtrado de eventos, notificaciones de eventos, tiquetes o casos asociados a los eventos, entre otras acciones
Documentación de repertorio de eventos (filtrado de eventos)	Documentar los eventos que se van a gestionar, definir acciones para los mismos y llevarlos a operación en la herramienta de monitoreo
Documentación de atención de los eventos gestionados	Con severidad y prioridad de atención de eventos identificada, se debe definir qué se va a realizar ante la ocurrencia de un evento
Correlación de eventos	Identificar posible correlación de eventos, es decir, relación que se establece entre un evento y otro, por ejemplo: si se dan dos o más eventos de forma simultánea, pueden tener un significado en específico, que si se dieran estos de forma aislada
Medición del proceso de gestión de eventos	Definición de métricas asociadas a la gestión de eventos, y como parámetro para comprobar el efecto positivo o negativo, e inclusive

Desarrollo de propuesta de Gestión de Seguridad de Red

Esta propuesta de políticas de seguridad de red se fundamenta en un enunciado del estándar de gestión de seguridad informática ISO/IEC 27001, el cual se basa en el ciclo de Deming (Plan-Do-Check-Act).

Adicionalmente se toma en cuenta buenas prácticas de seguridad de red, a juicio experto y otras descritas en publicaciones por fabricante de equipos de red Cisco. Estas buenas prácticas se asocian a hallazgos sobre oportunidades de mejora en seguridad de red que se identifican en el hospital.

Algunas acciones propuestas asociadas a una gestión de Seguridad como parte de una gestión preventiva son las siguientes:

- Implementar mecanismos de seguridad que permita este acceso físico solo a usuarios autorizados
- Cámaras de seguridad para registrar el acceso físico a los principales equipos de red
- Implementar un sistema de autenticación centralizado, es decir, que no sean credenciales locales para cada equipo. Además, que sólo usuarios de TI puedan ingresar, proveedores externos deberán solicitar accesos únicos cuando sea requerido
- Utilización de protocolos seguros para acceso a equipos como SSH y HTTPS, de forma que no se utilicen mecanismos con claves y demás en texto plano.
- Identificar puertos de red cableada que no estén en uso y apagarlos y/o asignarlos a una red aislada a la red de producción.
- Ocultar redes inalámbricas existentes.

Adicionalmente, también se definen métricas para comprobar el efecto y por mejora continua del proceso de gestión de seguridad de red.

Resultados y conclusiones

TI debe comenzar a verse como parte vital de cualquier negocio o institución, y no como un “gasto”. La disponibilidad y buen funcionamiento de servicios de TI debe ser algo a garantizar, por lo que se debe se debe coordinar esfuerzos y recursos para que se gestione TI de una forma preventiva, y que los departamentos encargados de esta función no sean sólo reactivos ante incidentes, que pasen de ser “apaga incendios” a ser personal proactivo que impida que los “incendios” ocurran, comparando el término incendio con incidentes y/o problemas informáticos.

Este tipo de propuestas deben desarrollarse de forma paulatina, no intentar trabajar todos los procesos de una sola vez porque puede existir confusión. Adicionalmente debe ser un compromiso íntegro, donde colaboradores y proveedores del departamento de TI trabajen juntos en el objetivo común, además de seguir el proceso de mediciones para una mejora continua en el tiempo.