INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 2, No. 1, (Enero 2018), 24-30 ISSN 2550-6730

Plan de gestión de incidentes que afectan a los equipos informáticos de la ESPAM MFL.

María Gabriela Cuzme Romero[1], Roxanna Elizabeth Pinargote Anchundia[2], Elizabeth Sabando Loor[3]

[1]Universidad Técnica de Manabí, Manabí, [2]Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López", [3]Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López"
[1]gabys_r92@hotmail.com, [2]roxypinargote@hotmail.com, [3]roxannasabando@hotmail.com

Recibido: 18/10/2017
Aceptado: 19/1/2018

RESUMEN

La presente investigación se realizó con la finalidad de elaborar un plan de gestión de incidentes que afectan a los equipos informáticos de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López (ESPAM – MFL), estableciendo cursos de acción para reducir el impacto y mejorar la productividad de los usuarios.

Para tal efecto, se empleó el apartado gestión de incidentes de la metodología (ITIL), la cual se divide en cuatro fases: registro, que incluyó la determinación de los equipos informáticos, donde se identificaron y clasificaron los riesgos a los que estaban expuestos a través de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT (versión 3.0)).

Lo correspondiente a la fase de clasificación permitió establecer niveles de prioridad para cada incidente de acuerdo a criterios de urgencia e impacto; así mismo el punto de diagnóstico y resolución, en donde se elaboraron el catálogo y acuerdos de servicios tecnológicos disponibles entre el personal encargado de los equipos informáticos y responsables de los departamentos de la ESPAM-MFL.

En base a los resultados obtenidos mediante el plan de gestión de incidentes, se limitó el impacto de tales eventos, con la asignación de un equipo responsable para gestionarlos, situación que se comprueba con los acuerdos de servicios elaborados, por lo que al ejecutar los procedimientos de respuesta a inconveniente se pueden contener y mitigar los mismos; por lo tanto, resulta conveniente adoptar medidas de seguridad eficientes para proteger los activos de información de la institución.

PALABRAS CLAVES: Gestión, Plan de Gestión, Incidentes Informáticos, ITIL, MAGERIT.

ABSTRACT

The present investigation was carried out with the purpose of elaborating an incident management plan that affects the computer equipment of the Higher Polytechnic School of Manabí Manuel Félix López (ESPAM - MFL), establishing courses of action to reduce the impact and improve the Productivity of users.

For this purpose, the Incident Management of the Methodology (ITIL) was used, which is divided into four phases: registration, which included the determination of the computer equipment, where the risks to which they were exposed were identified and classified Through the Methodology of Analysis and Risk Management of Information Systems (MAGERIT (version 3.0)).

The corresponding to the classification phase allowed to establish priority levels for each incident according to criteria of urgency and impact; As well as the point of diagnosis and resolution, where the catalog and agreements of technological services available between the personnel in charge of the computer equipment and responsible of the departments of the ESPAM-MFL were elaborated.

Based on the results obtained through the incident management plan, the impact of such events was limited, with the allocation of a responsible team to manage them, a situation that is verified with the service agreements elaborated, so when executing the procedures Of response to inconvenience can be contained and mitigated; It is therefore appropriate to adopt efficient security measures to protect the institution's information assets.

KEYWORDS: Management, Management Plan, Computer Incident, ITIL, MAGERIT.

1. Introducción

La seguridad informática concierne a la protección de la información, que se encuentra en una computadora o en una red de ellas y también a la protección del acceso a todos los recursos del sistema [1]. Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de análisis, implantar medidas preventivas y correctivas que eliminen los riegos asociados o que los reduzcan hasta niveles manejables [2].

La seguridad debe ser apropiada y proporcionada al valor de los sistemas, al grado de dependencia de la organización a sus servicios y a la probabilidad y dimensión de los daños potenciales. Los requerimientos de seguridad variarán por tanto, dependiendo de cada organización y de cada sistema en particular [3].

Un incidente de seguridad informática se define como cualquier evento que atente contra la confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos [4]. Velasco y Arean (2008) específica a los incidentes informáticos como aquellas situaciones que atentan, vulneran o destruyen información valiosa de la organización, además del impacto psicológico y económico que puede generar en el mercado accionario o en los accionistas cuando se informa sobre intrusiones y pérdidas de información en un ente empresarial.

El objetivo primordial, aunque no único, del Centro de Servicios es servir de punto de contacto entre los usuarios y la Gestión de Servicios TI. Un Centro de Servicios, en su concepción más moderna, debe funcionar como centro neurálgico de todos los procesos de soporte al servicio: registrando y monitorizando incidentes, aplicando soluciones temporales a errores conocidos en colaboración con la Gestión de Problemas, colaborando con la Gestión de Configuraciones para asegurar la actualización de las bases de datos correspondientes y gestionando cambios solicitados por los clientes mediante peticiones de servicio en colaboración con la Gestión de Cambios y Versiones. Pero también debe jugar un papel importante dando soporte al negocio, identificando nuevas oportunidades en sus contactos con usuarios y clientes [5].

La investigación tiene como objetivo elaborar un plan de gestión de incidentes que afectan a los equipos informáticos de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, estableciendo cursos de acción para reducir el impacto de los incidentes y mejorar la productividad de los usuarios.

Desarrollo

Para el desarrollo del trabajo, se utilizó la metodología ITIL, tomando como referencia el apartado gestión de incidentes, la cual establecía conceptos básicos, procesos y actividades sobre la gestión de incidentes, con el objetivo de restaurar el servicio tan pronto como sea posible y minimizar los impactos adversos de las interrupciones generadas. Esta metodología comprendía los siguientes procesos: registro, clasificación, diagnóstico y resolución, mediante los cuales, las autoras ejecutaron el trabajo de investigación.

El uso de ésta metodología permitió incorporar las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la presente investigación y el esquema gubernamental de la seguridad de la información

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 2, No. 1, (Enero 2018), 24-30 ISSN 2550-6730

(EGSI) Versión 1.0, el cual establece en su apartado 9, el procedimiento mediante el cual se gestionan los incidentes de seguridad de la información.

Asimismo la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT-versión 3.0) permitió identificar los riesgos, su origen y posible impacto. Para lo cual se procedió a elaborar un listado de posibles amenazas sobre cada equipo informático según lo establece MAGERIT en su catálogo de elementos correspondiente al tercer libro.

Materiales y Métodos

La ejecución del presente trabajo de investigación se realizó mediante la metodología ITIL, tomando como referencia el apartado gestión de incidentes, la cual establecía conceptos básicos, procesos y actividades sobre la gestión de incidentes de seguridad informática, con el objetivo de restaurar el servicio tan pronto como sea posible y minimizar los impactos adversos de las interrupciones generadas. Esta metodología comprendía las siguientes actividades: registro, clasificación, diagnóstico y resolución, mediante las cuales, las autoras desarrollaron el trabajo de investigación.

Una parte fundamental para la recopilación de la información, estuvo basada en diseñar una ficha de registro, con el propósito de reconocer y detallar los equipos informáticos con los que contaban los departamentos y carreras de la ESPAM – MFL, para lo cual se realizó una encuesta, dirigida a los custodios de los equipos informáticos de cada carrera y departamento de la universidad.

Posteriormente, mediante las visitas realizadas a las instalaciones de la universidad para aplicar las encuestas, se obtuvo información general de las actividades y procesos que manejan cada uno de los departamentos y carreras de la institución, lo cual permitió evaluar el medio en el que se desarrollan cada una de las actividades, logrando identificar los riesgos a los que están expuestos cada uno de los equipos informáticos, para proceder a evaluarlos con el fin de que reciban una especial atención.

Luego de determinar el número de equipos con los que contaba la institución, se procedió a realizar el análisis de riesgo utilización la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT-versión 3.0) que permitió identificar los riesgos, su origen y posible impacto. Para tal efecto, se elaboró un listado de posibles amenazas sobre cada equipo informático según lo establece MAGERIT en el catálogo de elementos correspondiente al tercer libro.

Después de realizar el análisis de riesgo a los equipos informáticos, se hizo la clasificación de los incidentes encontrados, permitiendo a través de esta, establecer los niveles de prioridad en base a la urgencia e impacto que tengan, así como también sus escalados, dependiendo de su función y jerarquía. Posteriormente se procedió a realizar el respectivo diagnóstico de los incidentes informáticos presentados en cada uno de los departamentos y carreras de la ESPAM – MFL.

Una vez obtenido las incidencias con el debido análisis, se continuó con la elaboración del catálogo de servicios y el plan de Gestión de Incidentes informáticos, permitiendo establecer acuerdos y normas entre las autoridades de la Institución, personal a cargo de cada uno de los departamentos y carreras; y el departamento de tecnología encargado de dar mantenimiento y soporte a las instalaciones de la ESPAM – MFL.

Resultados y Discusión

Como resultado en la investigación planteada se pudo determinar los equipos informáticos que existían en la institución, para lo cual, fue necesario establecer, en primera instancia la definición de tales equipos, tal como se muestra a continuación:

Se desarrolló un inventario para detallar cada uno de los equipos informáticos con los que cuenta la ESPAM – MFL, aproximándose a un total de 1442 equipos, según los resultado obtenidos en las encuestas aplicadas a los custodios de las carreras y departamentos.

Una vez finalizada la encuesta, se continuó con el análisis de riesgo por medio de la metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT-versión 3.0) permitiendo identificar los riesgos, su origen y posible impacto. Para tal efecto, se procedió a elaborar un listado de posibles amenazas sobre cada equipo informático, según lo establece MAGERIT en el catálogo de elementos correspondiente a su tercer libro.

Luego, se elaboró un cuestionario de incidencias informáticas permitiendo identificar y clasificar los principales inconvenientes que sucedían en la institución (Figura 1).

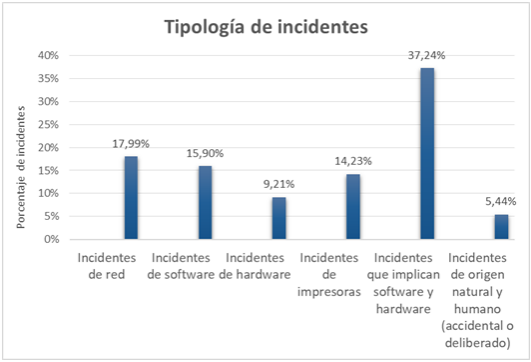

Figura 1: Incidencias informáticas de la ESPAM – MFL

Lo realizado para determinar las incidencias informáticas que transcurren en las instalaciones de la ESPAM-MFL, permitió elaborar una clasificación de los principales inconvenientes ocurridos, estableciendo en número y porcentaje el total de incidentes registrados mediante la aplicación del cuestionario.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 2, No. 1, (Enero 2018), 24-30 ISSN 2550-6730

Tabla 1: Rango de valores de velocidades.

TIPOLOGÍA DE INCIDENTES	N°	%
Incidentes de red	**43**	**17,99** %
Fallo del servicio de comunicación (Problemas con la conexión a internet)	24	10,04 %
Inconvenientes con el servicio de correo electrónico de la institución	19	7,95 %
Incidentes de software	**38**	**15,90** %
Problemas de video (proyectores, pantallas o monitores)	5	2,09 %
Problemas al actualizar programas	9	3,77 %
Problemas al ejecutar programas (abren lentos o no se ejecutan)	12	5,02 %
Alerta por licenciamiento de programas	12	5,02 %
Incidentes de hardware	**22**	9,21 %
Problemas por suministro de componentes a computadoras de escritorio	12	5,02 %
Desperfectos de hardware (componentes internos del CPU)	9	3,77 %
Daños en el hardware de scanner	1	0,42 %
Incidentes de impresoras	34	**14,23** %
Daños en las impresoras multifunción	14	5,86 %
Problemas por cambio de suministro a los equipos de impresión	20	8,37 %
Incidentes que implican software y hardware	**89**	**37,24** %
Reinicio constante de las computadoras	12	5,02 %
Problemas por virus en las computadoras	20	8,37 %
Falta de mantenimiento preventivo	21	8,79 %
Falta de mantenimiento correctivo	25	10,46 %
Denegación del servicio (saturación del sistema informático)	11	4,60 %
Incidentes de origen natural y humano (accidental o deliberado)	**13**	**5,44** %
Problemas con fuego (incendios)	0	0,00 %
Daños en los equipos por agua (escape, fugas e inundaciones)	1	0,42 %
Presencia de desastres industriales (Debido a la actividad humana)	2	0,84 %
Corte de suministro eléctrico	6	2,51 %
Robo de equipos informáticos	4	1,67 %
TOTAL DE INCIDENCIAS	**239**	**100,00** %

Como se observa en el (Tabla 1), las incidencias más relevantes en relación al total de las mismas son aquellas que implican software y hardware, las cuales alcanzan un 37,24 %; mientras que los incidentes de red se encuentran en un 17,99 %. Por consiguiente, las menos relevantes son las de origen natural y humano con un 5.44 %, debido a su probabilidad y frecuencia de ocurrencia.

En base a la información obtenida de las incidencias encontradas, se procedió a realizar el debido proceso que lleva resolver un incidente (Figura 2), desde que se notifica hasta el cierre del mismo, tomando en cuenta niveles de prioridad y escalado.

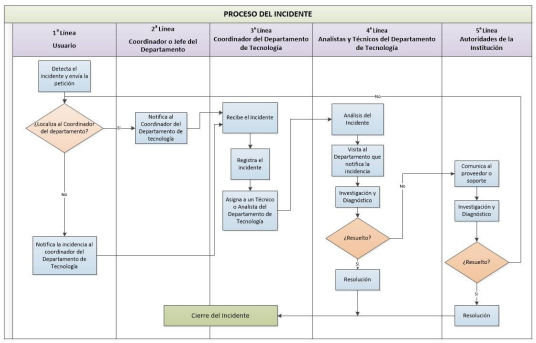

Figura 2: Diagrama del proceso de resolución del incidente

Posteriormente, se realizó el catálogo que define cada uno de los servicios tecnológicos disponibles que brinda la institución, así mismo, se elaboró el Acuerdo de servicios (SLA) y el plan de gestión de incidencias informáticas, permitiendo establecer tiempos de respuesta a cada una de las incidencias que se presentan de manera cotidiana en las instalaciones de la ESPAM – MFL, tomando en cuenta para tal fin, las buenas prácticas de Gestión de Incidentes que proporciona la metodología ITIL.

En comparación con otros trabajos investigativos, con la finalidad de descubrir procedimientos, estructuras y características en común referente a la investigación planteada, se analizaron varias tesis de grado sobre Gestión de Incidentes informáticos, dentro de las cuales se puede mencionar la Implantación de los procesos de gestión de incidentes y gestión de problemas según itil v3.0 en el área de tecnologías de información de una entidad financiera de la Pontificia Universidad Católica del Perú, del autor, Jesús Rafael Gómez Álvarez [6], el cual realizó su investigación utilizando la metodología ITIL para determinar cada una de las actividades y procesos que intervienen en la Gestión de Incidentes y por ende en el proceso de gestión de incidentes de seguridad informática.

Por lo cual, se coincide que es indispensable que las instituciones lleven un control y registro adecuado de los incidentes informáticos, definiendo correctamente cada uno de los procesos. Donde efectuado el análisis, las autoras acuerdan en que la metodología idónea aplicada a Gestión de Incidentes de seguridad informática es ITIL, conjuntamente con su apartado Gestión de Servicios, ya que proporciona, establecer niveles de prioridad al clasificar las incidencias, tomando en cuenta procesos de escalamiento para definir los tiempos de atención.

Adicionalmente, se acuerda que por medio del plan de respuesta a incidentes se detallan todas las políticas y reglamentos que deben ser tomadas en cuenta al momento de notificar un incidente y todo el proceso que lleva desde que sucede hasta el cierre del mismo.

2. Conclusiones

- El uso de la metodología ITIL permitió el desarrollo del Plan de Gestión de Incidentes que afectan a los equipos Informáticos, proporcionando una serie de procedimientos y actividades, a través de los cuales se alcanzaron los objetivos propuestos.
- Por medio de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT-versión 3.0) se consiguió determinar y detallar las amenazas a las que están expuestos los equipos informáticos.
- Mediante la información recolectada con el uso de las encuestas, se alcanzó un mejor análisis de los sucesos que afectan a los equipos informáticos de los departamentos y carreras de la institución.
- La elaboración del catálogo de servicios tecnológicos, permitió establecer acuerdos entre las autoridades y el personal encargado de brindar la asistencia a las incidencias.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 2, No. 1, (Enero 2018), 24-30 ISSN 2550-6730

Referencias

[1] M Baldeon. "Plan maestro de seguridad informática con lineamiento de la norma ISO 27002". En: (2012).

[2] G. Morlanes. "Seguridad Informática, Matanzas, CU". En: *Revista de Arquitectura e Ingeniería* 6.2 (2012), págs. 1-14.

[3] Edgar Valdés Castro. "TENDENCIAS DE LA AUDITORIA INFORMATICA". En: *Ingenium* 4.8 (2009), págs. 69-98.

[4] CAES S.A. *¿Qué es un incidente informático?*

[5] OSIATIS S.A. *ITIL Gestión de Servicios TI: Fundamentos de la Gestión TI.*

[6] Jesús Rafael Gómez Álvarez. "Implantación de los procesos de gestión de incidentes y gestión de problemas según ITIL v3. 0 en el área de tecnologías de la información de una entidad financiera". En: (2012).