ESTRATEGIAS PARA LA CREACION DE UN MODELO DE ATENCION DE INCIDENTES DE SEGURIDAD INFORMATICA PARA EMPRESAS PYMES.

Cesar Augusto Correa Mancilla. Ing. Electrónico [1]

Universidad Pontificia Bolivariana
Bucaramanga, Colombia

Resumen

Este articulo presenta algunas estrategias para la creación de un modelo de atención de incidentes de seguridad de la información y puede servir como guía para las pequeñas y medianas empresas que estén interesadas en este proceso, los temas tratados en este documento son: la descripción y clasificación de algunos incidentes de seguridad, el manejo para cada uno de ellos y se propone la gestión de incidentes como la herramienta principal, para poderlos analizar, manejar, controlar y erradicar. La metodología para el tratamiento de los incidentes se explica con el desarrollo de las fases del ciclo de vida de un incidente. El objetivo principal de esta investigación es mostrar las diferentes herramientas para el tratamiento de incidentes, implementar la clasificación de los activos de la información y dar respuesta de manera controlada a los incidentes de seguridad, mediante la adaptación algunos marcos de trabajo o buenas prácticas internacionales.

Palabras claves

Incidentes, Evento, Gestión de Incidentes, Estrategias, Política de Seguridad, Plan de Sensibilización.

[1] El autor está vinculado a la Universidad Pontificia Bolivariana Seccional Bucaramanga y pertenece al grupo de estudiantes de la Facultad de Ingeniería Informática Especialización en Seguridad Informática Segunda Cohorte.

Abstract

This article presents some strategies for creating a model of incident response information security and can serve as a guide for small and medium enterprises that are interested in this process, the issues raised in this paper are the description and classification of security incidents, the management for each of them and proposed incident management as the primary tool, so that they can analyze, manage, control and eradicate. The methodology for the treatment of incidents is explained in the development of life cycle phases of an incident. The main objective of this research is to show the different tools for incident handling, implement the classification of information assets and responding in a controlled manner to security incidents by adapting some frameworks or best practices.

Keywords:
Incident, Event, Incident Management, Strategy, Security Policy, Awareness Plan.

1. Introducción

En la actualidad, el tema de seguridad de la información ha despertado un gran interés, debido a los diferentes eventos que han ocurrido y que afectan la seguridad de la información, entre ellos están: correo electrónico masivo no deseado "spam", código malicioso, denegación de servicios, intentos de intrusión, la suplantación de identidad y el acceso no autorizado entre otros [1]. Todos estos eventos cada día son más comunes y frecuentes, por este motivo es necesario que en las pequeñas y medianas empresas (PYMES), se cuente con personal capacitado y entrenado para enfrentar estas amenazas y así proteger uno de los bienes más importantes en las empresas "la información", en este orden de ideas surge la necesidad de crear un modelo de atención de incidentes de seguridad de la información que nos ayude en esta labor, es primordial el trabajo de todos los miembros de cada PYMES, desde los directivos hasta las personas encargadas de los oficios varios, porque todos ellos hacen parte del proceso de negocio y cada uno tiene acceso a diferentes activos de información, por este motivo se tiene que empezar a realizar campañas de concientización y sensibilización en este tema, para comprender, afrontar y gestionar los riesgos en seguridad de la información.

Este articulo plantea algunas estrategias para la gestión de atención de incidentes, que se pueden implementar en las PYMES como: conseguir el apoyo de la gerencia en este proyecto, realizar un plan de sensibilización y capacitación y la revisión de las metodologías que existen como ejemplo lo planteado por "ITIL"[2] que describe las mejores prácticas en la administración de servicios de tecnologías de la Información; implementar estas buenas prácticas en las organizaciones con el fin de mejorar el nivel de servicio y por ende mejorar la satisfacción del cliente.

2. Planteamiento del problema.

2.1 Incidentes de Seguridad: Son todos los eventos adversos en un entorno informático, que comprometen la confidencialidad, la disponibilidad y la integridad de la información [2]. Define

[2] ITIL. Biblioteca de Infraestructura de Tecnologías de la Información, Desarrollada a finales de 1980.

los tres principales elementos de la información, que es conocida como CID; Según la siguiente definición: "la confidencialidad: los recursos del sistema solo pueden ser accedidos por los elementos autorizados, Integridad: los recursos del sistema solo pueden ser modificados o alterados por los elementos autorizados, Disponibilidad: Los recursos del sistema deben permanecer accesibles a los elementos autorizados."[3] La anterior definición nos dimensiona el significado de un incidente en el área de seguridad de la información, que es todo aquel que compromete los tres pilares de la información: CID, si se llega a incumplir alguno de los tres, nos indica que la información no es segura y que el sistema se encuentra comprometido.

Otra definición de un incidente es: una violación o amenaza de violación de una política de seguridad de la información, política aceptable de uso o mejores prácticas de seguridad [2]. Si una política de seguridad es quebrantada, significa que el sistema de seguridad se encuentra vulnerable a cualquier amenaza y por consiguiente se deben aplicar controles para reducir el riesgo. Las políticas se elaboran con el fin de tener aplicación a largo o mediano plazo y guíen el desarrollo de reglas y criterios específicos. [3].

2.2 Evento: Es toda ocurrencia observable en un entorno informático, cualquier suceso o acontecimiento que se puede ver en una red o en un sistema [2]. Esta definición se relaciona con lo que sucede en los procesos de funcionamiento de un sistema de información y que afectan su curso normal, algunos de estos eventos se pueden presentar esporádicamente o en algunas ocasiones con mayor frecuencia, lo importante es establecer parámetros de medidas e identificación de cada uno de ellos, porque proveen información valiosa de lo que está sucediendo en el sistema de información, para ello se puede realizar un análisis de estos eventos y tomar las medidas de control respectivas, este proceso hace parte de la gestión de incidentes que se tratara a continuación.

3. Gestión de Incidentes.

Existen diferentes definiciones para gestión: las actividades encaminadas a la obtención de un objetivo específico, o las labores de administrar, orientadas a la solución de un proyecto. Se puede formular que es el resultado de actividades como: planear, organizar, dirigir, evaluar y controlar [4]. También se define como el conjunto de diligencias que se realizan para desarrollar un proceso o para lograr un producto determinado. La gestión de incidentes comprende actividades desarrolladas para erradicar los incidentes de seguridad de la información, uno de los objetivos de la gestión de incidentes es: restablecer la normalidad de los servicios en el menor tiempo posible y minimizar el impacto en el negocio [5].

El objetivo del anterior enunciado es impedir pérdidas para la organización, para ello el tiempo juega un papel fundamental, por esta razón es un proceso que requiere organización, trabajo en equipo y entrenamiento. La gestión de incidentes indica las medidas a tomar respecto a los incidentes de seguridad de la información, estas pueden ser: preventivas, de detección y correctivas, entre las medidas preventivas están: contraseñas, políticas, actualizaciones,

[3] Armando Carvajal R, Msc Seguridad Informática, está vinculado a la Universidad Pontificia Bolivariana Seccional Bucaramanga, pertenece al cuerpo de docentes de la Facultad de Ingeniería Informática Especialización en Seguridad Informática.

firewall, etc. De detección: auditorias, revisiones de seguridad, logs de registro. Correctivas: sistema de detección de incidentes, planes de recuperación de desastres, etc. [2].

En resumen la gestión de incidentes consiste en la asignación oportuna de los recursos necesarios y su uso adecuado, con el objeto de prevenir, detectar y corregir incidentes que afectan la seguridad de la información. Cuando en una organización se tiene definido un sistema de gestión de incidentes, se logran importantes beneficios, por ejemplo; dar respuesta en forma sistemática, es decir, tan pronto ha ocurrido un evento que afecte la seguridad de la información en la organización, inmediatamente las personas encargadas toman las medidas necesarias para atender el incidente que ocurrió, otro beneficio es prevenir la ocurrencia reiterada de incidentes mediante el aprendizaje, cómo se logra este objetivo por medio de los registros, de la documentación por parte del grupo de respuesta a incidentes; de lo contrario, puede presentar fuga de información y la empresa ve afectado su correcto funcionamiento llevando a una inestabilidad económica. [2].

Después de la investigación de algunos modelos de atención de incidentes, se selecciona como referencia uno de ellos para la realización de este artículo, esta metodología, entrega una visión clara del trabajo a realizar para la creación de un modelo de atención de incidentes de seguridad de la información donde se realiza una clasificación por fases de dicho modelo [2].

Fases de la gestión de incidentes de seguridad.

- Preparación y Prevención
- Detección y Notificación
- Análisis Preliminar
- Contención, Erradicación y Recuperación
- Investigación

Cada fase forma el conjunto de actividades a desarrollar para realizar un sistema de gestión de incidentes seguridad de la información, se define como el ciclo de vida de un incidente.

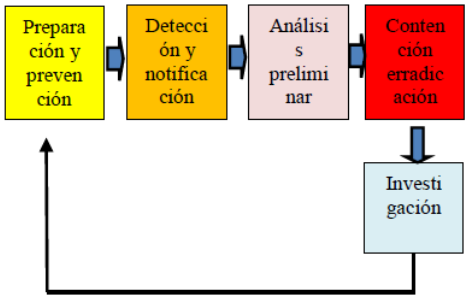

Fig.1 "Ciclo de Vida de un Incidente."[2]

Preparación y prevención: Esta fase realiza una clasificación de los incidentes de seguridad, también brinda información sobre el tiempo de respuesta a cada uno de ellos; por ejemplo: denegación de servicios, código malicioso, acceso no autorizado, etc. La clasificación ayuda a enfrentar los incidentes, midiendo el daño que han causado a cada empresa y los recursos que

ha afectado, se define el tiempo máximo para atender un incidente, un ejemplo de ello se muestra en la siguiente tabla:

Tabla 1 "Tiempo de respuesta a cada incidente." [2]

Clasificación del Incidente	Tiempo de Respuesta
Incidente muy grave	15 Min.
Incidente grave	25 Min.
Incidente de nivel medio	2 Horas.
Incidente de nivel bajo	3 Horas.

La información de la tabla 1, permite establecer un patrón de medida para cada incidente, en el cual cada empresa, puede considerar, si es un tiempo justo para evitar daños o consecuencias de mayor nivel a cada una de ellas.

Detección y Notificación de Incidentes: Esta fase indica el medio en el cual la empresa, toma sus propias decisiones sobre los incidentes y la manera en que están organizadas y preparadas para enfrentarlos, se puede seleccionar algunas de las siguientes medidas:

- Implementar software de detección de intrusiones.
- Implementar software antivirus
- Analizar logs del sistema.
- Implementar controles internos, el uso de contraseñas seguras, etc.

Incluye la notificación del incidente, el trabajo involucra por primera vez al grupo de atención de incidentes, que es el mayor responsable y se encuentra en el medio gestionando todo este proceso.

Análisis Preliminar: Realiza el análisis inicial del incidente, se pueden tener en cuenta alguna de las siguientes recomendaciones para facilitar esta labor: efectuar labores de revisión de toda la red, verificar el uso del ancho de banda y tener un promedio de los recursos que se consumen para encontrar cualquier anormalidad en el sistema, establecer un uso centralizado de login y crear políticas de logs, para definir el tiempo en que se debe mantener esta información, que ayuda en las tareas de reconocimiento de identificación de incidentes [2].

Contención, Erradicación y Recuperación.

- Contención. Evitar que el incidente siga produciendo daños.
- Erradicación. Eliminar la causa del Incidente y todo rastro de daños.
- Recuperación. Volver el entorno afectado a su estado original.

Investigación: En esta etapa se trabaja lo relacionado a la recolección de datos, se aplican diferentes técnicas y herramientas para esta labor, entre algunas de ellas se pueden mencionar aquellas que permitan recolectar los datos de los host como la fecha y hora de los relojes del sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en los puertos y el estado general de la red. [2].

4. Estrategias para la creación de un modelo de atención de incidentes.

Las estrategias que se van a desarrollar a continuación van dirigidas principalmente a las PYMES en Colombia, por las siguientes razones: representan un porcentaje superior del total de empresas, son grandes generadoras de empleos, pertenecen a la mayoría de los sectores de la economía en nuestro país, su estructura organizacional se adaptan a la totalidad de sectores de la economía y obtener información sobre ellas es una labor sencilla, comparándola con las grandes compañías de este país. Una definición de PYMES; se entiende por pequeña y mediana empresa (Artículo 2, Ley 905 de 2004), toda unidad de explotación económica, realizada por persona natural o jurídica, en actividades empresariales, agropecuarias, industriales, comerciales o de servicios, rural o urbana, que responda a dos (2) de los parámetros presentados en la tabla 2 [6].

Tabla 2. "Clasificación de la empresas colombianas" [6].

Tipo de Empresa	Planta de Personal	Activos Totales (SMVL[1])
Micro	1-10	menos 501
Pequeña	11-50	501 y 5000
Mediana	51-200	5001 a 30000
Grande	201 o más	más de 30000

Existen diferentes definiciones de estrategias para el sector corporativo, por ejemplo son las decisiones que se toman en una organización que determina los objetivos y metas a alcanzar [6].
Lo anterior indica que las estrategias representan el conjunto de métodos, reglas, planes que se llevan a cabo con el fin de alcanzar los objetivos esperados. En este orden de ideas es fundamental esclarecer que definir una estrategia en una PYMES, requiere de un orden, análisis y un estudio a fondo de lo que se quiere obtener, para este caso en concreto: "Un modelo de atención de incidentes de seguridad de la información", teniendo claro el concepto de estrategia y junto con el desarrollo del tema anterior: gestión de incidentes, se puede complementar la definición de estrategia de seguridad de la información: es un patrón frente al cual una organización toma sus decisiones de protección de la información con base en sus objetivos, el propósito de toma de decisiones requiere de la definición de una política y de un plan de acción para alcanzar los objetivos de seguridad [6].

Otra definición de estrategia de seguridad de la información es la siguiente; poder pasar del estado actual a un estado deseado, es el conjunto de objetivos de seguridad de la información,

junto con procesos, métodos y herramientas que proporcionan los medios para elaborar una estrategia de seguridad [7].

Teniendo en cuenta que las estrategias de seguridad, buscan apoyar el logro de los objetivos del negocio, representa un punto de referencia en la creación de estrategias de seguridad, pueden tomarse de base para definir las estrategias para la creación de un modelo de atención de incidentes de seguridad de la información, el proceso estándar que se utiliza para formular cualquier planeación estratégica, se resumen en el desarrollo de las siguientes preguntas: ¿Dónde estamos?, ¿Adónde vamos? y ¿Cómo llegamos?. El primer interrogante, se trata de la situación actual de la PYMES, esta etapa define los objetivos y estrategias del negocio, se analiza la situación actual de la seguridad de la información y se establecen los requerimientos de seguridad del negocio. El segundo es la situación futura, se define la situación deseada, se plantea un valor de medida o porcentaje que defina la brecha frente a la situación actual de la PYMES referente a la seguridad de la información. El tercero, se trata del plan de acción, donde se desarrollan tareas como: acciones inmediatas, proyectos a desarrollar, como: programas de concientización, educación y entrenamiento, desarrollando estas tares se obtiene el objetivo deseado y la diferencia entre la brecha de seguridad se reduce significativamente. Para este trabajo se puede remitir a diferentes marcos de trabajo, o estándares internacionales, como por ejemplo; ITIL, ISO 27000, COBIT, etc. [7].

Un marco de trabajo que se puede adoptar como referencia es la norma ISO 27001, la cual contempla la gestión de incidentes como una de las mejores prácticas a considerar en la seguridad de la información, razón por la cual contiene el décimo tercer dominio llamado: Gestión de los incidentes de Seguridad de la Información. En este dominio se establecen los objetivos de control enfocados al reporte de incidentes y la gestión y aprendizaje de los mismos, la propuesta de esta norma busca, no sólo que sean reportados los eventos de seguridad y las debilidades de sistemas de información, también que se tomen las acciones emprendidas ante estos reportes, mantener una base de aprendizaje y experiencias vividas en pro de mejorar la respuesta ante incidentes y conocer el plan de acción basado en hechos ocurridos anteriormente [7].

Para la mayoría de las organizaciones y en este caso particular las PYMES, que están pensando en cómo combatir o proteger sus activos de información contra los diferentes tipos de incidentes de seguridad informática, que en los últimos años se han incrementado, es por esta razón que las organización están pensando en una estrategia para la protección de incidentes, no existe un plan único o una guía metodológica para esta tarea, y surgen diferentes interrogantes como los siguientes: cuales son los requerimientos para implementar un modelo de atención de incidentes en las PYMES, cuanto costara el modelo de incidentes, con qué recursos se sostendrá, cuales son los pasos iniciales para su creación, entre otros, es por eso que no hay un conjunto estándar de respuestas a estas preguntas cada PYMES tiene que crear su propia estrategia de atención de incidentes, y estos son únicos como las organizaciones, no existe un modelo igual al otro y que opere de la misma manera.[8]

La primera estrategia planteada para la creación de un modelo de atención de incidentes para las PYMES es: “obtener apoyo de la gerencia”. Aunque las estrategias planteadas, cada una tiene su nivel de importancia, esta estrategia es de las principales, debido a que sin el apoyo de la alta gerencia, el proyecto no prosperaría, se deben conseguir los recursos, en este orden de ideas lo primero que se debe plantear es como vender el proyecto a la gerencia, es

demostrarles que el objetivo del modelo de atención de incidentes está alineado con los objetivos del negocio y su objetivo principal es proveer a la organización la continuidad del negocio, es una herramienta para que el negocio permanezca, eliminar la idea que tienen los gerentes, que creen que todas las implementaciones de TI son un gasto y no una inversión, que pueda mejorar los procesos del negocio. También es importante el compromiso de la gerencia para el sostenimiento del mismo y garantizar las operaciones a largo plazo. [8].

La segunda estrategia planteada está dividida en tres secciones:

- Crear una política para el manejo de incidentes de seguridad de la información.
- Desarrollar un plan de acción para el manejo de la política.
- Implementar un grupo interdisciplinario para el manejo de incidentes.

La primera sección: "*establecer una política para el manejo de incidentes de seguridad de la información***".** Esta política se define en términos de las características del negocio, la organización, sus activos y tecnología, también contiene las declaraciones, intenciones y expectativas de la gerencia, con un nivel alto de seguridad y los controles establecidos. [ISO 27001:2005] Además se debe tener en cuenta los requisitos del negocio, como los legales y reglamentarios (circulares, normatividad, etc.). La política para el manejo de incidentes de seguridad de la información establece un objetivo, alcance y responsabilidad, también debe garantizar el conocimiento de esta y el cumplimiento por parte de todos los miembros de la organización. [9].

El objetivo de la política es el proteger los recursos de información de la organización y la tecnología utilizada para su procesamiento, frente a las diferentes amenazas mencionadas anteriormente, con el fin de cumplir con la confidencialidad, integridad y disponibilidad de la información. Asegurar los recursos necesarios para su implementación y mantener la política actualizada con el fin de asegurar su vigencia. [9]

El alcance de esta política es poder aplicarla a todos los sectores del negocio a sus recursos y a la totalidad de los procesos ya sean internos o externos. [9]

Los principales responsables de la implementación y cumplimiento de la política, son todos los miembros de la organización desde el gerente, personal administrativo, comercial, departamento técnico, etc. La política tiene una aplicación obligatoria para todo el personal de la organización. [9].

Otro de los aspectos generales en la implementación de la política para el manejo de incidentes de seguridad de la información es: la clasificación y control de activos. Este aspecto es fundamental el saber con qué activos cuenta la organización, realizar un inventario y clasificación de los mismos, para poderlos medir y controlar, entre los activos tenemos; recursos de información: (bases de datos, documentación de sistemas, procedimientos operativos, etc.), recursos de software: (aplicaciones, sistemas operativos, etc.), activos físicos: (equipos informáticos, de comunicaciones, medios magnéticos, unidades de almacenamiento, etc.). Esta clasificación se debe realizar de acuerdo al nivel de sensibilidad y criticidad de la información que contengan y deben tenerse en cuenta el periodo de tiempo en cual la información es crítica es decir cuando pasa de ser privada o pública, como un ejemplo una noticia para un diario o canal de noticias deja de ser critica cuando esta información es divulgada, este procedimiento

debe ser muy claro para aplicar un adecuado manejo de la información y clasificación de los activos.[10]

La segunda sección: "*Desarrollar un plan de acción para el manejo de la política*". Este plan de acción incluye un cronograma de actividades, con el desarrollo de objetivos a mediano y largo plazo, indicar tareas concretas a realizar para cada uno de los objetivos y los tiempos para realizar cada una de ellas, para este propósito se hace necesario responder los siguientes interrogantes ¿Qué quieres hacer? es el propósito u objetivo general ¿Hasta dónde quieres llegar? la meta a alcanzar, ¿Para qué lo quieres hacer? Objetivos específicos, ¿Cómo lo vas a hacer? tareas, ¿Cuándo y dónde lo vas a hacer?: cronograma de actividades y ¿Con quién lo vas a hacer? Recursos, estos pueden ser tangibles como intangibles, con los cuales la organización cuenta.[9]

Las respuestas a estas preguntas, nos indica, el estado actual de la PYMES frente al manejo de atención de incidentes de seguridad de la información y son un indicador de los problemas que se tienen que resolver, para alcanzar los objetivos deseados. Todo lo anterior difícilmente se puede lograr si no se tiene una planeación. También es importante establecer prioridades y tomar decisiones, es como si el plan de acción de subdividiera en varios planes como: anuales, semestrales, trimestrales, mensuales, etc., se puede realizar cada día una tarea que gradualmente nos aproxime al objetivo final. [9].

La tercera sección: "*Implementar un grupo interdisciplinario para el manejo de incidentes*". La creación de un grupo de respuesta incidentes dentro de la organización, es necesario para lograr el objetivo que se ambiciona: la creación de un modelo de atención de incidentes, el grupo debe tener características multidisciplinarias y que pertenezcan a diferentes áreas como: seguridad informática, sistemas, auditoría, recursos humanos y legales, donde estén comprometidos todos los miembros de la organización y se tomen las medidas adecuadas, también se requiere del trabajo de cada uno de ellos, donde la responsabilidad sea compartida y no sectorizada. [11]

La tercer estrategia planteada es: "*Realizar un plan de sensibilización y capacitación*" Esta estrategia es fundamental para la creación de un modelo de atención de incidentes, tiene como objetivo el de captar la atención de todos los miembros de la organización en este caso la PYMES, es necesario comenzar al interior de la organización, se puede empezar desde las áreas gerenciales, administrativas, operativas, etc., e ir escalando y si fuera necesario incluir a los demás personas u organizaciones que tiene relación directa o indirecta, es decir en caso de los outsourcing, contratistas, temporales, etc. [12].

El plan de sensibilización debe estar acompañado por una campaña y el objetivo principal es alinear los objetivos de la empresa con los objetivos de seguridad de la información, este plan se debe elaborar teniendo en cuenta los marcos de trabajo y estándares internacionales con respecto a la seguridad de la información como la norma ISO 27001, ITIL, COBIT, etc. Para el desarrollo de este medio de divulgación es necesario realizar las siguientes labores; utilizar medios impresos como: afiches, folletos, donde se resuma los objetivos principales del modelo de atención de incidentes, la normatividad al respecto, la responsabilidad que cada miembro de la organización tiene con el modelo de atención de incidentes, también realizar autoevaluaciones de seguridad y dar pautas para el tratamiento de los incidentes de seguridad, y algunos casos de estudio. También podemos utilizar las tecnologías de información para este

trabajo, a través de internet se pueden realizar campañas de sensibilización, con todos los miembros de la organización, debido a que es el medio más utilizado hoy en día en la mayoría de las PYMES, una herramienta efectiva para llegar a cada miembro es con él envió de correos electrónicos, donde se describan diagramas de seguridad, los modelos de seguridad, etc. Por último se puede incorporar un plan de capacitación de cada usuario de la organización, realizándolo por áreas o departamentos, siendo muy claros y sencillos en la terminología y en los ejemplos que se van a utilizar para no incomodar o llegar a irritar a los participantes, con metodologías complejas que no puedan comprender. Estas campañas se deben realizar con especial cuidado dependiendo del cargo que cada miembro desempaña en la organización, para preparar cada una de estas capacitaciones, se pueden organizar de forma periódica y no darlas todas de una vez, para que las personas vayan asimilando esta nueva información, si es posible se pueden invitar a participantes de otras organizaciones o empresas proveedoras de servicios de seguridad informática, los cuales tienen personal altamente entrenado para este tipo de charlas.[12]

La cuarta estrategia planteada es: "*la adaptación de buenas prácticas o marcos de trabajo internacionales como: La Biblioteca de Infraestructura de tecnologías de Información ITIL.*" Como ya es conocida la implementación de buenas prácticas en las organizaciones que garanticen la prestación de un mejor servicio, esa interacción entre la organización el cliente y el servicio. ITIL, nace como un código de buenas prácticas, para alcanzar las metas del negocio, como lo logra, mediante un enfoque sistemático del servicio TI, centrado en procesos y procedimientos, establece estrategias para la gestión operativa de la infraestructura TI. El propósito de ITIL es demostrar a la organización que cada vez se necesita de la informática, para alcanzar sus objetivos corporativos, esta dependencia aumenta la necesidad de crear servicios informáticos de calidad y que estén alineados con los objetivos del negocio. [13]

ITIL v3 estructura la gestión de los servicios TI, sobre el concepto del ciclo de vida de los servicios. El ciclo de vida del servicio consta de cinco fases que corresponden con los libros de ITIL: estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio. [14]

- Estrategia del servicio: trata la gestión no solo como una capacidad sino como un activo estratégico.
- Diseño del servicio: cubre los principios y métodos necesarios para transformar los objetivos en portafolios de servicios y activos.
- Transición del servicio: cubre el proceso de transición para la implementación de nuevos servicios o su mejora.
- Operación del servicio: cubre las mejores prácticas, para la gestión del día a día en la operación del servicio.
- Mejora continua del servicio: proporciona una guía para la creación y mantenimiento del valor ofrecido a los clientes a perfiles de un diseño, transición y operación del servicio optimizado. [14]

Estos cinco libros ofrecen una guía práctica sobre como estructurar la gestión de servicios de TI de forma que estos estén correctamente alineados con los procesos de negocio.

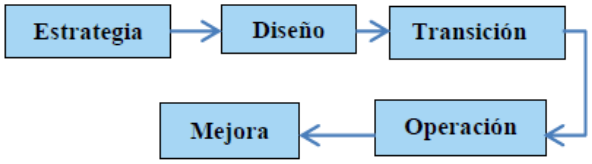

Fig.2 "Ciclo de Vida de un servicio."[14]

La figura No.2, muestra todas las fases del ciclo de vida de un servicio, se analizara la fase de operación del servicio, esta fase es sin duda la más crítica de todas, porque en ella tenemos la percepción del cliente y los usuarios de la calidad del servicio, depende de una correcta organización y coordinación, los objetivos principales de esta fase son en su orden; coordinar e implementar todos los procesos, dar soporte a todos los usuarios del servicio y gestionar la infraestructura para la prestación del servicio. [14].

Uno de los procesos asociados a la fase de operación del servicio es la gestión de incidencias, este proceso es el responsable de registrar todas las incidencias que afecten la calidad del servicio y restaurarlo a los niveles acordados de calidad del servicio en el plazo más breve posible. [14]. El objetivo principal de la gestión de incidencias es detectar cualquier alteración de servicios de TI, registrar y clasificar estas alteraciones y asignar el personal encargado de restaurar el servicio según se define en los acuerdos de nivel de servicios SLA correspondiente. Los principales beneficios de una correcta gestión de incidencias son:

- Mejorar la productividad del usuario
- Cumplimiento de los acuerdos de niveles de servicio
- Optimización de los recursos disponibles
- Una base de datos del conocimiento más precisa donde se registran los incidentes.
- Por ultimo mejora la satisfacción general de los clientes y usuarios. [14]

5. Conclusiones

Para el desarrollo de un modelo de atención de incidentes, una de las tareas principales en la gestión de incidentes, es realizar una clasificación de los activos de la información, esta permite la priorización de los mismos, entender cuáles son los más críticos para la organización y que deban atenderse con urgencia, para aplicarle los controles respectivos. Cuando se presente algún incidente de seguridad, hay que mantener la calma, realizar el procedimiento propuesto para la gestión de incidentes de seguridad de la información, ver figura No.1, este momento es clave para demostrarle a la gerencia, que se deben invertir los recursos necesarios para la implementación y sostenimiento del modelo de atención de incidentes de seguridad de la información y que el modelo está alineado con los objetivos del negocio y su objetivo principal es lograr la continuidad del negocio.

El objetivo real de la gestión de incidencias no es tener un proceso documentado e implementado, es detectar y contener los incidentes de seguridad, analizarlos y tomar las medidas para que estos incidentes no vuelvan a ocurrir, se pueden presentar errores e

incidencias, pero es importante aprender de ellos y tomar las decisiones para que no se vuelva a presentar, es inaceptable que se presenten la ocurrencia de incidentes; como por ejemplo, la caída de la red o un servidor que dejo sin servicio el sistema por uno o varios días y dentro de un par de meses se vuelva a presentar la misma situación la caída del sistema con el argumento, que se trataba de otro tipo de virus, es en este punto donde se realizan las valoraciones, donde se toman las decisiones y las medias para contrarrestar esos incidentes, y donde se evalúa si el modelo está trabajando y está dando los resultados esperado para las PYMES. [15]

El objetivo principal del plan de sensibilización y capacitación no es el de llegar a todos los miembros, es decir que tenga una cobertura total, de eso no se trata, se trata que los miembros de la organización que recibieron la información y capacitaciones, realmente tomen conciencia de la seguridad de la información, no es una inversión que la gerencia realiza por un periodo y que con el tiempo se olvide y no se vuelva a hablar sobre el tema, esta plan debe ser permanente y realizar evaluaciones del mismo, no con exámenes sino con prácticas y pruebas donde se evalúen las medias de seguridad que tiene cada usuario con respecto al modelo de atención de incidentes de seguridad de la información.

El trabajo futuro después de realizar esta investigación es continuar con el diseño e implementación del modelo de atención de incidentes de seguridad informática, se cuenta con diferentes herramientas para este propósito que se presentaron en el desarrollo de este artículo. Tener presente que el trabajo de la gestión de incidentes no termina con la implementación del modelo, es un proceso que continua y está en constante cambio, se puede adoptar para esta labor el ciclo PHVA, planear, hacer, verificar y actuar. Se propone la revisión e investigación de trabajos desarrollados al respecto como los que propone el siguiente artículo de investigación: “La evolución de la gestión de eventos de seguridad de la información SIEM”. [16].

Este artículo presenta una panorámica de un modelo para la gestión de eventos de seguridad de la información, donde se dan pautas para la detección de anomalías de red y amenazas, disminuir los falsos positivos, establecer un análisis antes, durante y después del ataque y una correlación avanzada y profunda de eventos, en conclusión es una plataforma de inteligencia de la seguridad.

6. Referencias Bibliográficas

[1] Experiencias en el Manejo de Incidentes de Seguridad. Julio Cesar Ardita. [En línea]. Disponible en WWW: http://www.criptored.upm.es/guiateoria/gt_m241f.htm.

[2] Lorena B. Ferreyro. Gestión y Tratamiento de Incidentes de Seguridad de la Información. [En linea]. [Julio 2008] Disponible en WWW: http://es.scribd.com/doc/89153312/Gestion-de-Incidentes-Parte1-2009.

[3] Guía para la elaboración de políticas de seguridad. [En línea]. [julio 2010]. Disponible en WWW: http://www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf.

[4] El Concepto y Alcance de la Gestión Tecnológica. Guillermo Restrepo González [En línea]. [junio 2010] Disponible en WWW: http://es.scribd.com/doc/9759936/Resumen-1-Gestion-de-Tecnologia

[5] ITIL como apoyo a la seguridad de la información. [En línea]. [Agosto 2010] Disponible en WWW: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/04-ITILSoporteSGSIBasadoISO27001.pdf

[6] Guía para la apropiación de buenas prácticas de ITIL V3 en PYMES. Caso de estudio Laboratorios Merey. Daniel Armando Diaz, Olga lucia Giraldo. [En línea]. Disponible en WWW: http://www.faccamp.br/ojs/index.php/mesfaccamp/article/viewArticle/100

[7] Definición de Estrategias de Seguridad de la Información. Wilmar Arturo Castellanos. [En línea]. Disponible en WWW: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/16-PlaneacionEstrategicaSeguridad.pdf

[8] Creando un Grupo de Respuesta a Incidentes Proceso para iniciar la Implementación. ArCERT. [Octubre 2004]. [En Linea]. Disponible en WWW: http://www.arcert.gov.ar/webs/csirt_creacion.html

[9] Modelo de política de seguridad de la información para organismos de la administración pública nacional. Documento público. [En línea]. [Julio 2005]. Disponible en WWW: http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

[10] La eficacia de las estrategias de comunicación del gobierno de España (2004:2008) ante el terrorismo: análisis comparado de discursos y “frames” mediáticos desde la teoría dramatistica de keneth burke. Tesis doctoral. Mario García Gurrionero. [En línea]. [2009]. Disponible en WWW: http://eprints.ucm.es/11083/1/T32071.pdf

[11] Como crear un CSIRT paso a paso. Enisa. [En línea]. [2006]. http://www.enisa.europa.eu/

[12] Capitulo 1 Curso preparación CISM. Diplomado en Auditoría y Gestión de la Seguridad de la Información Gerencia de la seguridad de la información Auditoría interna de la norma ISO/IEC 27001:2005. Universidad Pontificia Bolivariana. [2009].

[13] Gobierno de TI a la práctica. Pedro Rozo. [En línea]. Disponible en WWW: www.acis.org.co/fileadmin/Conferencias/DeGobiernoTIPractica.pdf

[14] ITIL V3. Gestión de servicios de TI. Osiatis. [En línea]. Disponible en WWW: http://itilv3.osiatis.es/estrategia_servicios_TI.php

[15] Alineación Estratégica de Modelos de Seguridad de la Información. Richard García Rondon. XII Jornada Nacional de Seguridad Informática. [Acis] [Junio 2012]. Disponible en WWW: http://www.acis.org.co/

[16] La evolución de los Sistemas SIEM frente a la correlación de eventos de seguridad de la información. Armando Carvajal. XII Jornada Nacional de Seguridad Informática. [Acis] [Junio 2012]. Disponible en WWW: http://www.acis.org.co/

Biografía

Cesar Augusto Correa Mancilla, Nació en Bucaramanga, Ingeniero Electrónico de la Universidad Manuela Beltrán seccional Bucaramanga, candidato a Especialista de Seguridad Informática de la Universidad Pontificia Bolivariana, Auditor Interno ISO 27001:2005, miembro activo de ISACA capitulo Bogotá. Actualmente se desempeña como consultor independiente y asesor tecnológico para empresas del sector privado.