Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta - CSIRT

Gonzalo Diego Vargas Ramos
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz – Bolivia
gonzalo.vargas.ramos@gmail.com

***Resumen*—El análisis que se realizará en el presente artículo se enfoca en el desarrollo de un modelo de Gestión de Incidentes Informáticos para un adecuado tratamiento de las amenazas cibernéticas presentes en la actualidad como incidentes y vulnerabilidades que son detectados en aplicaciones, software y servicios informáticos, el alcance se encuentra desde el reporte del incidente hasta la mitigación o solución del problema informático, para lo cual se ha basado en la guía de gestión de incidentes de seguridad de la información de los lineamientos para la elaboración e implementación de los planes institucionales de seguridad de la información de las entidades del sector público y el estándar ISO 27035, diseñado específicamente para equipos de respuesta ante incidentes cibernéticos, con el objetivo de mejorar la atención de incidentes dentro de una organización o conjunto de organizaciones, mediante la colaboración y mejora continua, el modelo puede ser aplicado en las distintas entidades públicas para un adecuado tratamiento de estos problemas de seguridad informática.**

Palabras clave—CSIRT, ciberseguridad, gestión de incidentes, equipos de respuesta, incidentes informáticos

I. INTRODUCCIÓN

Los sistemas de información son desarrollados por personas, y las personas no son perfectas tienen debilidades que dependen de su psicología, por tanto, las aplicaciones informáticas desarrolladas tienen debilidades o vulnerabilidades que aún no son detectadas y quedan ocultas el código de cada software desarrollado e implementado [1].

El Centro de Gestión de Incidentes Informáticos – CGII, es la unidad dependiente de la AGETIC encargada de tratar con los incidentes informáticos ocurridos en las entidades públicas del Estado Plurinacional de Bolivia [2]. Es así que comienza sus operaciones de la atención de incidentes de seguridad informática en agosto 2016 y todos los reportes son dirigidos al mismo.

El Centro de Gestión de Incidentes Informáticos – CGII es considerado el CSIRT Nacional, encargado de la atención de Incidentes de seguridad informática, ocurrido en el Estado Plurinacional de Bolivia [3].

La atención de incidentes implica una tarea de coordinación con distintas instituciones y personas, luego de las coordinaciones viene las tareas técnicas relacionadas a la resolución del problema, tomando en cuenta distintas adversidades con dispositivos informáticos a tratar [4]. Es por tanto que un adecuado flujo de trabajo en el equipo de respuesta conlleva un resultado óptimo en la mitigación de los problemas de seguridad informática.

Así mismo, un enfoque orientado a buenas prácticas de la seguridad de la información, da lugar a que existan controles de detección y corrección destinadas a reducir los impactos desfavorables y aprender las lecciones aprendidas [5]. Es por tanto lo que da lugar a la necesidad de aplicar esas buenas prácticas mediante un modelo de gestión orientado a los equipos de respuesta.

A. Planteamiento del Problema

La necesidad de implementar cada vez más sistemas de información genera un problema para los administradores de sistemas de las entidades públicas, el cual hace que descuiden las configuraciones de seguridad de las aplicaciones, servicios e infraestructuras informáticas, lo que provoca que sean vulnerables a ataques cibernéticos por parte de cibercriminales.

Es en este contexto que los *Computer Security Incident Response Teams - CSIRT* (Equipos de Respuesta a Incidentes de Seguridad Informática) llevan la tarea de mitigar estos problemas de seguridad cibernética y colaborar en su resolución, pero debido a la gran cantidad de reportes de incidentes recibidos y detectados hace necesario una adecuada gestión de incidentes informáticos.

Formulación del problema

¿Cómo se puede mejorar la gestión de incidentes informáticos en un Equipo de Respuesta a Incidentes – CSIRT?

Objetivo General

Desarrollar un modelo de gestión de incidentes de seguridad informática para mejorar la atención de incidentes para equipos de respuesta – CSIRT.

Objetivos Específicos

Diseñar un flujo de trabajo para lograr la coordinación de las personas en el equipo de respuesta de forma más efectiva.

Probar el rendimiento del modelo respecto a la atención de incidentes de incidentes informáticos.

Planteamiento de Hipótesis

El modelo de gestión de incidentes informáticos, mejorará la atención de incidentes gestionados por el equipo de respuesta.

Para referenciar este artículo (IEEE):

[N] G. Vargas, «Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta - CSIRT», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 82-85, 2020.

TABLA I. OPERACIONALIZACIÓN DE VARIABLES

Variables	Definición conceptual	Dimensiones	Indicadores
Independiente Modelo de gestión de incidentes informáticos	Forma de trabajo donde las personas del equipo interactúan para mejorar la atención de incidentes.	Resolución de casos	* Tiempo de atención * Cantidad de incidentes gestionados
Dependiente Incidente gestionado	Amenazas a la seguridad de un sistema de información que fueron gestionadas por el equipo de respuesta	Incidentes informáticos y vulnerabilidades detectadas	* Cantidad de reportes * Equipo de respuesta

Fuente: Elaboración propia

B. Marco Teórico

1) Ámbito Internacional

a) Un Modelo de Gestión de Incidentes de TI aplicando Gestión del Conocimiento, de Karin Díaz Millones, en el artículo se propone un modelo de gestión de incidentes aplicando gestión de conocimiento para ello se explica el modelo propuesto, se indica cómo se implementa y adapta el modelo aplicando gestión del conocimiento, además se resuelve casos de estudio donde se comprueba la efectividad del modelo [6].

b) Sistema de Gestión de Incidentes de Seguridad Informática para Corbeta, de Lyda Durley Mona Cardona & Andrés Esteban Uribe Serna, en el cual describe que la información en las organizaciones es el activo más preciado, estas invierten grandes cantidades en dinero, tiempo y recursos para proteger sus activos tanto de amenazas externas como internas, hace unos años las organizaciones manejaban toda la información en un solo lugar, eran dueños de la infraestructura, los equipos de cómputo, la red informática, pero el aumento de servicios en la nube, el uso de dispositivos móviles, las redes sociales, genero un aumento del riesgo de fuga de información. Poder detectar, gestionar, clasificar, atender, medir y solucionar los distintos incidentes que pueden suceder en la empresa, es de gran importancia pues los sucesos fortuitos acarrean pérdidas económicas que ninguna organización está dispuesta a pagar [7].

c) Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT), de Heltton Emmanuel Ramírez Luna & Jezreel Mejía Miranda, en este artículo se describe una propuesta creada para proteger la información y la infraestructura de un equipo de respuestas ante incidentes de seguridad (CSIRT), el cual es una organización dedicada a dar respuesta a incidencias de seguridad en tecnologías de la información. Un CSIRT está conformado por un grupo de expertos en seguridad de la información la cual provee de servicios como alertas y advertencias, tratamiento de incidentes, observatorio de tecnología, auditorías de seguridad, cómputo forense, entre otros. Por lo tanto, se hace uso de información sensible como datos de usuarios y de empresas que deberá tener fuertes métodos de seguridad. En este artículo se aborda una propuesta de los aspectos de seguridad que debe tener un CSIRT abarcando las áreas de Telecomunicaciones, Equipo hardware y Sistemas SIEM (Security Information and Event Management). Esta propuesta no toma en consideración la tipología en la que un CSIRT puede establecerse [8].

2) Ámbito Nacional

La Guía para la Gestión de Incidentes de Seguridad de la Información, elaborado en la Mesa de Seguridad - CTIC (Comité de Tecnología de Información y Comunicación), el cual indica las acciones a responder ante incidentes que afecten la seguridad de la información. Toma a la gestión de incidentes como un control más en la seguridad de la información, siendo una guía basada en la ISO/IEC 27035 [9].

C. Referencia Teórica o Conceptual

1) Modelo

Un modelo es una abstracción teórica del mundo real que permite reducir la complejidad y realizar predicciones concretas que se puede realizar mediante experimentos u observaciones. Dicho de otra forma, el modelo no intenta representar la realidad como tal, sino solo aquellos aspectos o variables más importantes y significativos [10].

2) Tipos de modelos

Los modelos pueden dividirse en [11]:

a) Modelos físicos: este tipo de modelo se identifica por la representación de un elemento determinado, proporcionando la oportunidad de exponerlo a acontecimientos de diversa índole. La escala puede variar de acuerdo al modelo realizado.

b) Modelos matemáticos: los modelos matemáticos tienen como finalidad la representación de distintos fenómenos, o los vínculos existentes entre ellos, por medio de una fórmula de carácter matemático. Se pueden clasificar en:

- Modelos Deterministas
- Modelos Numéricos
- Modelos Estocástico.
- Modelos Gráficos.

c) Modelos conceptuales: hace referencia a cuadros conceptuales en donde se relacionan un conjunto de elementos determinados, conteniendo además postulaciones sobre la naturaleza de los fenómenos representados a través de dichos conceptos. Los modelos conceptuales se caracterizan por un grado elevado de abstracción.

3) Gestión de Incidentes

El principal objetivo de la gestión de incidentes es recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo el daño negativo posible en la organización de forma que la calidad del servicio y la disponibilidad se mantengan. Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio. El objetivo de ITIL es reiniciar el funcionamiento normal tan rápido como sea posible con el menor impacto para el negocio y el usuario con el menor coste posible [4].

4) Etapas del proceso de la atención de incidentes

De acuerdo a la ISO 27035, la estructura de la atención de incidentes presenta 5 etapas [5]:

a) Planificación y preparación: establecer una política de gestión de incidentes de seguridad de la información, formar un equipo de respuesta incidente, etc.

b) Detección y reporte: alguien tiene que detectar y reportar "eventos" que podrían ser o convertirse en incidentes;

c) Evaluación y decisión: alguien debe evaluar la situación para determinar si en realidad es un incidente;

d) Respuesta: contener, erradicar, recuperar y realizar el análisis forense el incidente, cuando corresponda;

e) Lecciones aprendidas: realizar mejoras sistemáticas en la gestión de riesgos de información de la organización como consecuencia de los incidentes experimentados.

5) Marco Legal o institucional

Decreto Supremo 2514 de 2015, artículo 8.- Centro de Gestión de Incidentes Informáticos, en cual describe la creación del CGII como parte de la estructura técnico operativa de la AGETIC [2], y sus funciones.

II. MÉTODOS

La presente investigación se basará en el enfoque cuantitativo, debido a que se recogerán y analizarán datos numéricos o estadísticos, con el objetivo de probar la hipótesis planteada, en base a mediciones y el análisis estadístico.

Para realizar la presente investigación se utilizará el tipo "no experimental", el cual implica observar los fenómenos tal como se suceden, mediante la recolección y análisis de información sin manipulación de variables. Adicionalmente el tipo de investigación será "correlacional" porque describe relaciones entre variables y se pretende realizar el análisis de información que se genere.

A. *Fases Metodológicas*

Para cumplir con los objetivos planteados se tiene las siguientes fases metodológicas:

Fase 1: Recopilación y análisis de información
- Identificar estándares nacionales e internacionales de gestión de incidentes;
- Analizar referencias de gestión de incidentes;
- Esquematizar la forma de trabajo actual en el equipo.

Fase 2: Diseño y desarrollo del modelo
- Elaborar bosquejos de formas de trabajo en equipo mediante diagramas de flujo;
- Plantear casos de prueba

Fase 3: Pruebas del modelo
- Implementar el modelo en una herramienta informática;
- Realizar pruebas automáticas del modelo

Fase 4: Análisis de datos y conclusiones
- Analizar los resultados obtenidos;
- Comparar los resultados con datos históricos.

B. *Técnicas de investigación*

Observación: una técnica que permite entender el funcionamiento de los flujos de trabajo que se realiza, así como el uso de la experiencia.

C. *Universo o Población de Referencia*

El universo o población de referencia para el cual está dirigido esta investigación es el Centro de Gestión de Incidentes Informáticos (AGETIC) y los datos de incidentes publicados que ocurren en las entidades públicas.

La muestra o población de estudio está enfocada en la información recabada de los incidentes reportados al CGII, que se constituye en el CSIRT más grande con alcance nacional.

D. *Delimitación Geográfica*

El presente trabajo de investigación se delimitará geográficamente al Estado Plurinacional de Bolivia.

E. *Delimitación Temporal*

El estudio del presente trabajo tomará en cuenta la información histórica del periodo 2019.

III. RESULTADOS

A. *Modelo de Gestión de Incidentes Informáticos*

De acuerdo al análisis realizado de la forma de trabajo de un equipo de respuesta y de las buenas prácticas de seguridad de la información respecto a la ISO 27035, se presente el modelo propuesto bajo el siguiente esquema:

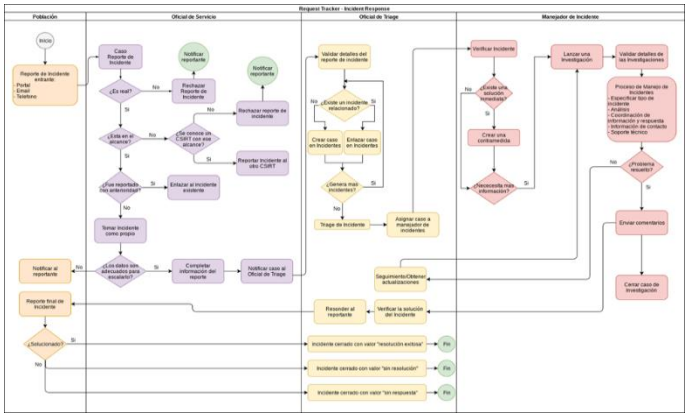

Fig. 1. Modelo de Gestión de Incidentes Informáticos
Fuente: Elaboración propia

En el cuadro se observa la distribución de funciones de acuerdo a los actores que interactúan con el problema de seguridad informática. De acuerdo al siguiente detalle:

Población	Respondedor	Gestor	Manejador	Manejador
	Reportes	Incidentes	Investigaciones	Contramedidas
Reportantes	Reporte a partir de mensaje de correo, portal, o creado manualmente (teléfono, fax).	Creado después de verificar los hechos y obtener todos los detalles del reporte.	Creado mientras se realiza las investigaciones y esta vinculado al incidente.	Creado para aplicar acciones inmediatas o posibles soluciones.
				

Fig. 2. Roles y actores del modelo
Fuente: Elaboración propia

Se ha definido 4 actores a interactuar sobre resolución del incidente de seguridad informática, debido a que se cumple con el manejo de incidente:

- Detección: Reportes y detección
- Triage: Evaluar, categorizar, priorizar
- Análisis: Investigación, qué sucedió y quien está afectado
- Respuesta a incidente: Acciones para resolver el incidente

B. *Herramienta de gestión de incidentes*

Se ha determinado el uso de la herramienta *Request Tracker* para el manejo de incidentes de seguridad informática, bajo las colas (listas de casos) de trabajo siguientes:

*a) Incident Reports (*Reportes*)*
Nuevos reportes, bandeja de entrada
b) Incidents (Incidentes)
Reportes validados se convierten en incidentes.
Detalles del incidente
c) Investigations (Investigaciones)
Análisis o investigación sobre el caso reportado
Canal de comunicación
d) Countermeasures (Contramedidas)
Acciones inmediatas para mitigar los incidentes
Soluciones temporales y rápidas

C. Roles y responsabilidades

a) Oficial de servicio o guardia (Respondedor)
A cargo de las solicitudes entrantes
Actividades periódicas
b) Oficial de triage (Gestor)
Trata reportes y decide si es un incidente, cuando manejarlo, quien de acuerdo al proceso de triage.
Controla y monitorea todo el incidente.
c) Manejador de incidente (Analista)
Analizar datos, crear soluciones, resolver el incidente.
Comunicar el progreso al oficial de triage y población.

D. Herramienta de gestión de incidentes

El modelo en su concepto básico se viene aplicando desde marzo y abril del presente año:

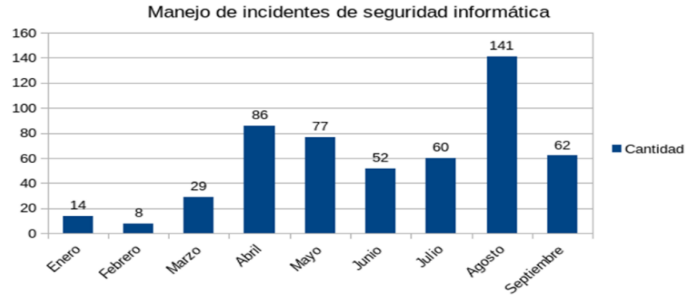

Fig. 3. Cantidad de incidentes tratados por meses
Fuente: Implementación de sistema Request Tracker con el modelo

En el gráfico se puede observar que la cantidad de incidentes gestionado va subiendo de acuerdo a aplicación del modelo en el equipo de trabajo. Los fueron obtenidos del uso de la herramienta informática en el equipo de respuesta CGII.

IV. Conclusiones

Desde la implementación del modelo en el equipo de respuesta se puede observar que el tratamiento de incidentes de seguridad informática va creciendo.

El equipo de respuesta pasa de un manejo independiente a una atención de incidentes colaborativo, donde cada miembro cumple ciertas funciones de la resolución de incidentes.

En los meses de abril de y agosto es donde se tiene mayor índice de incidentes resueltos o rechazados, esto se debe a que la cantidad de reportes ingresados al flujo de trabajo fueron bastantes.

Se puede determinar que el equipo de respuesta a medida que va aceptando los parámetros de trabajo del modelo la gestión de incidentes se hace más eficiente.

Recomendaciones. De acuerdo a la implementación del modelo en el equipo de trabajo, este va ajustándose a las necesidades de la resolución de incidentes, por ello se recomienda automatizarlas con Request Tracker para hacer más eficiente el trabajo del equipo.

Referencias

[1] Mitnick, K. D. & Simon W. L. (2007). El Arte de la Intrusión. México, México.

[2] Decreto Supremo 2514. (2015). Creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC. La Paz. Bolivia.

[3] Centro de Gestión de Incidentes Informáticos – CGII. (2019). RFC 2350. Obtenido de: https://www.cgii.gob.bo/es/rfc-2350. Fecha de consulta: agosto de 2019.

[4] Axelos. (2019). ITIL Foundation, ITIL 4 edition. Obtenido de: https://www.tsoshop.co.uk/Business-and-Management/AXELOS-Global-Best-Practice/ITIL-4/?DI=650015. Fecha de consulta: agosto de 2019.

[5] ISO 27035. (2016). Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management. Geneva, Switzerland.

[6] Diaz Millones, K. (2009). Un Modelo de Gestión de Incidentes de TI aplicando Gestión del Conocimiento. Lima. Perú.

[7] Mona Cardona, L. D. & Uribe Serna, A. E. (2015). Sistema de Gestión de Incidentes de Seguridad Informática para Corbeta. Medellín. Colombia.

[8] Ramírez Luna, H. E. & Mejía Miranda, J. (2015). Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). Zacatecas. México.

[9] CTIC – AGETIC. (2017). Guía para la Gestión de Incidentes de Seguridad de la Información. Obtenido de: https://www.ctic.gob.bo/wp-content/uploads/bsk-pdf-manager/ANEXO_C._Guia_para_la_gestion_de_incidentes_de_seguridad_de_la_informacion_197.pdf. Fecha de consulta: agosto de 2019.

[10] Carvajal Villaplana, Á. (2002). Teorías y modelos: formas de representación de la realidad. Cartago. Costa Rica.

[11] Enciclopedia de clasificaciones (2019). Tipos de modelos (científicos). Obtenido de: https://www.tiposde.org/ciencias-exactas/415-tipos-de-modelos-cientificos/. Fecha de consulta: agosto de 2019.

Breve CV del autor

Gonzalo Diego Vargas Ramos es Ingeniero de Sistemas por la Universidad de Aquino Bolivia (2013). Actualmente realiza la Maestría en Alta Gerencia de Tecnologías de la Información y las Comunicaciones e Innovación MAG-TIC (2015-2016), en el Postgrado en Informática de la UMSA.
Ejerce profesionalmente como analista forense del Centro de Gestión de Incidentes Informáticos de la AGETIC. Anteriormente trabajo en el Área de Desarrollo del Ministerio de Economía y Finanzas Públicas.
Sus intereses investigativos se centran en el software libre, machine learning, herramientas de pentesting, gestión de incidentes informáticos y ciber inteligencia. Email: gonzalo.vargas.ramos@gmail.com.