Desarrollo de un Sistema de Información Web para la Gestión de Incidentes de TI En Correcol S.A.

Efraín Díaz Mejía
Germán Barreto Reyes
Universidad Piloto de Colombia
Bogotá D.C., Colombia

Resumen- En el presente artículo se dan a conocer los resultados del proyecto en el cual se llevó a cabo el desarrollo de un sistema de información Web para el proceso de gestión de incidentes de TI en la empresa CORRECOL S.A., mediante un modelo metodológico enfocado a las buenas prácticas en el desarrollo de software, con el fin de disponer de un mecanismo facilitador a través del cual la compañía logre alcanzar los niveles de eficiencia establecidos en sus procesos y garantice la seguridad de sus activos.

Palabras claves: sistemas de información, gestión de incidentes TI, seguridad informática, aplicativo web.

Abstract - In this article, the results of the project in which the development of a Web information system for the process of management of IT incidents in the company CORRECOL SA, through a methodological model focused on the good practices in software development, in order to have a facilitating mechanism through which the company achieves the levels of efficiency established in its processes and guarantees the security of its assets.

Keywords: information systems, IT incident management, computer security, web application.

1. INTRODUCCIÓN

Actualmente los sistemas de información son cada vez más complejos y las empresas dependen más de servicios tecnológicos para su gestión, por lo que la caída o la interrupción de la operación pueden llegar a tener importantes consecuencias tanto en la obtención de los objetivos como en problemas legales, razón por la cual es crucial que las empresas sean capaces de identificar y resolver fallos que se presenten en los servicios, además que sean resueltos en el lapso más corto posible.

En este sentido, la gestión de incidentes en tecnologías de información es un aspecto clave para el mejoramiento continuo de los procesos de las compañías, sin embargo, ante actividades de alta complejidad por sucesos no habituales que requieren de soluciones inmediatas, es necesario un manejo oportuno que evite inconvenientes de interrupción de los mismos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad en las actividades diarias empresariales; por lo que el propósito de la gestión de incidentes de TI es identificar el incidente, categorizarlo y priorizarlo, diseñar una solución, restaurar las operaciones, cerrar y monitorear el incidente con la calidad deseada, el tiempo de resolución más corto y con el mínimo impacto en el negocio en general [1].

Dado lo anterior, se escogió la CORRECOL S.A. que presta servicios de intermediación de seguros para personas naturales y jurídicas, teniendo como principal componente el aseguramiento de la satisfacción de sus clientes, para desarrollar un aplicativo que web para la gestión de incidentes TI, ya que hoy en día las acciones preventivas, correctivas y de mejora que se han implementado para mejorar la gestión de incidentes, han ocasionado inconvenientes tales como gastos innecesarios en los procedimientos de acuerdo a la afectación en los activos de la organización y múltiples quejas por parte del área usuaria al momento del diagnóstico y restablecimiento del servicio ante una eventualidad, dando como resultado la afectación en la disponibilidad, integridad y confidencialidad en los activos de la organización; surgiendo de este modo la necesidad de desarrollar un sistema de información capaz de mejorar la gestión de

incidentes de TI en CORRECOL S.A, buscando el mejoramiento en tiempos de respuesta y adaptando un modelo metodológico, capaz de aumentar la productividad, además de optimizar los recursos disponibles y mejorar el nivel de satisfacción de los clientes.

2. REFERENTES TEÓRICOS

A. SISTEMAS DE INFORMACION EMPRESARIAL

Un sistema de información empresarial comprende el análisis y la organización de la información a través de la aplicación de tecnología. Como tal, combina los conceptos básicos de administración, operaciones y teoría de sistemas de información con métodos y tecnologías de ingeniería informática para administrar los datos de una organización.

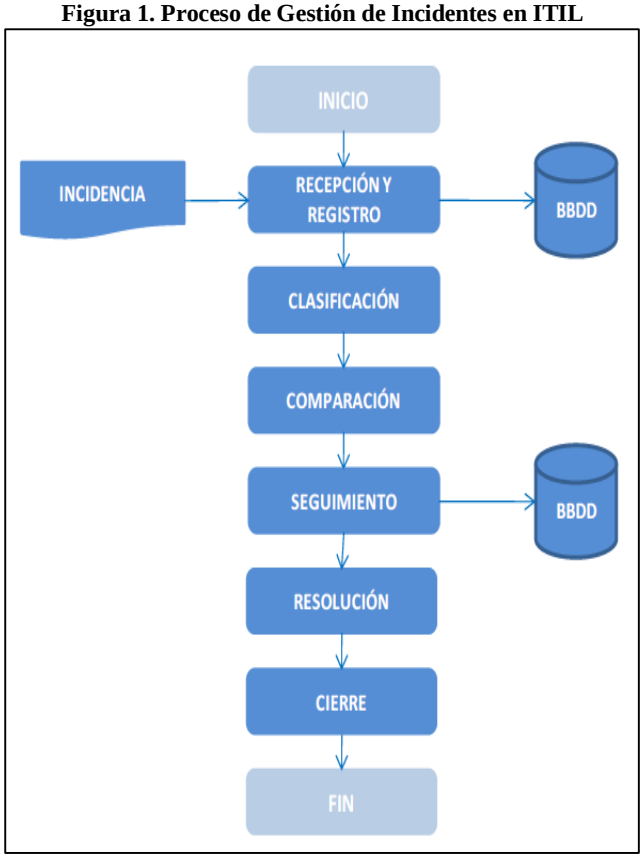
Así mismo, los sistemas de información están sujetos a la dinámica del entorno empresarial y deben ser lo suficientemente flexibles para absorber los cambios inevitables en las necesidades de información de las empresas, por lo que deben ser eficientes anticipar los cambios en las necesidades de información de los usuarios y, en consecuencia, adaptarse a sus necesidades [2].

B. GESTIÓN DE INCIDENTES ITIL V3

La gestión de incidentes en ITIL tiene como objetivo principal manejar el ciclo de vida de todos los incidentes y restablecer el servicio de TI a los usuarios lo más pronto posible, de esta manera poder minimizar el impacto negativo en las operaciones de negocio [3]. Para ello se debe detectar cualquier alteración en los servicios de TI La gestión de incidentes de hace comúnmente a través de un centro de servicio Service Desk, ya que a gran mayoría de estas incidencias provendrán de los usuarios utilizan el servicio, por lo tanto, la gestión de incidentes es una labor reactiva [4].

Una correcta gestión de incidentes, al igual que la gestión de problemas, brinda grandes beneficios a la organización, por tanto, se debe seguir un proceso adecuado, como se muestra en la Figura 1.

Figura 1. Proceso de Gestión de Incidentes en ITIL



Fuente. Ríos Huércano (2014, p. 80)

Una correcta gestión de incidentes, al igual que la gestión de problemas, brinda grandes beneficios a la organización, como los siguientes:

- Las personas más organizadas y concienciadas hacia la consecución de los objetivos del proceso.
- Mayor satisfacción para los clientes.
- Generación de mayor conocimiento y mejora del rendimiento del servicio para la organización.

3. RESULTADOS DE LA INVESTIGACIÓN

A. METODOLOGIA

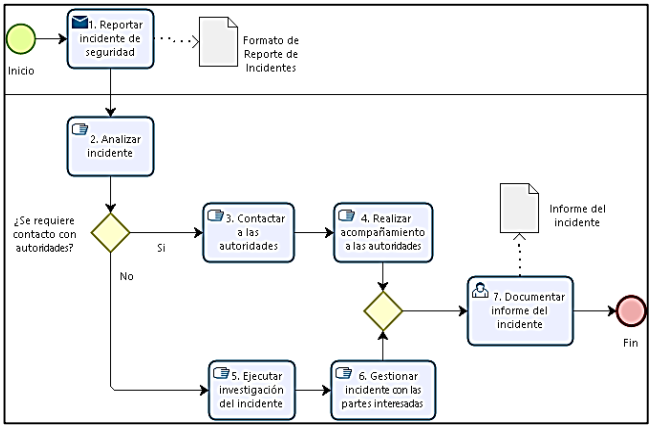
Durante la investigación se desarrollaron actividades de diagnóstico de la situación actual del proceso de gestión de incidentes de TI en la empresa CORRECOL S.A., caracterizando el proceso e identificando los incidentes del SGI, a partir de la información recopilada se establece la metodología para el desarrollo del software y la construcción del sitio WEB.

B. SISTEMA DE GESTION DE LA INFORMACIÓN SGI EN LA EMPRESA CORRECOL SA

El proceso de sistema de gestión de la seguridad de la información en la empresa CORRECOL S.A. está diseñado teniendo en cuenta las especificaciones técnicas que se presentan en la norma ISO /IEC 27001 2013 que debe velar por la preservación de la Confidencialidad, integridad y disponibilidad de los activos de la compañía.

Por lo cual el procedimiento es el siguiente:

Figura 2. Diagrama de flujo de gestión de incidentes en CORRECOL S.A.



Fuente. Correcol S.A. Información corporativa. [CD-ROM]. [Bogotá]: La Empresa, 2018. Gestión de incidentes

Al hacer la revisión detallada del proceso se identificaron falencias como las que se muestran a continuación:

Tabla 3. Hallazgos encontrados

ACTIVIDAD	HALLAZGOS FALENCIAS
A. Inicio	
B. 1. Reportar Incidente de Seguridad	➢No existe priorización del incidente de acuerdo al activo afectado, donde se pueda identificar la urgencia. ➢Falta identificar el lugar del incidente. ➢No existen niveles de escalamiento en la priorización ni SLA's donde se refleje el tiempo de respuesta de acuerdo al tipo de incidente reportado ➢No existen registros de lecciones aprendidas ni base de conocimiento. Documentación fundamental para la gestión. ➢Si el incidente es mayor, no se tiene un flujo diferencial donde el tiempo de respuesta sea más corto ni está asociado a gestión de problemas. ➢Existen usuarios que no han sido capacitados con conceptos de seguridad de la información, esto representa una dificultad a la hora de diferenciar la categoría afectada, tipo de eventos (Vulnerabilidad, Amenaza, Incidente); entre otros.
C. 2. Analizar Incidente	➢No se tiene información histórica de fácil uso, con el fin de identificar si el incidente fue reportado anteriormente con su solución asociada. ➢No existe un identificador de referencia único del incidente. ➢No se tiene una técnica identificada de análisis de la causa raíz. ➢Solo se maneja un nivel de categorías para el incidente, en este caso se recomiendan subcategorías de máximo 4 niveles con el fin de tener información más acertada con fines estadísticos. Ejemplo: Software, Aplicación, Modulo financiero, Sistema de orden de compra. ➢No existe una forma de asociar la urgencia vs el activo afectado de forma paramétrica ➢No existe un estado del incidente (Activo, En espera, Cerrado) ni fecha de cierre ➢No existe un tiempo de resolución del incidente de acuerdo al impacto y prioridad. ➢No se tiene un escalamiento para abordar la incidencia, esto ocasiona que el oficial de seguridad ante los posibles cambios, no pueda agilizar el incidente de la manera adecuada.
E. 5. Ejecutar Investigación del Incidente	➢En algunas ocasiones no se reporta el responsable del incidente ➢No se tiene la duración del incidente desde el momento de su ingreso hasta el cierre
F. 6. Gestionar Incidente con las Partes Interesadas	➢No se tiene un esquema de escalamiento de acuerdo a la complejidad y/o criticidad del incidente
G. 3. Contactar a las Autoridades	➢No existe información histórica sobre intervención de autoridades relacionados a incidentes en CORRECOL S.A.
I. 7. Documentar Informe del Incidente	➢No hay información centralizada ni de fácil acceso para un histórico de incidentes ➢No existen métricas donde se evalúen el total de incidentes en un intervalo de tiempo determinado teniendo en cuenta lo siguiente: Número de incidentes reabiertos, porcentaje de incidentes categorizados incorrectamente, entre otros.

Fuente: Los Autores

C. CARACTERIZACIÓN DE INCIDENTES DEL SGI EN LA EMPRESA CORRECOL SA

En la empresa CORRECOL S.A. se lleva a cabo un proceso de identificación, análisis, investigación y respuesta de los incidentes de TI, esta labor está a cargo del oficial de seguridad de la información el cual se encarga de llevar un registro de los incidentes que se presentan en la compañía por medio de un archivo plano, donde se especifica cual es el activo afectado, una breve descripción del incidente, se clasifica la criticidad del incidente, el diagnóstico realizado y la solución definitiva.

Entre los incidentes reportados se evidencia que los más comunes son los relacionados a caídas del servicio de internet o interrupciones en los canales de comunicación por medio de conexiones por VPN y hurtos de equipos de cómputo de los funcionarios de la empresa.

Actualmente en CORRECOL S.A. se maneja un plan de tratamiento de riesgos en donde se especifican los controles de tratamiento, se evalúa la probabilidad y el impacto de los mismos, entre esta lista se encuentran riesgos asociados a fuga de información, posible afectación a la integridad de la información, entre otros. Llevar un seguimiento continuo de los riesgos y tratamiento adecuado de los mismos, ayudará en gran manera a la prevención de incidentes.

El siguiente análisis corresponde a los incidentes generados desde el año 2014 hasta Julio de 2018.

Tabla 4. Incidentes registrados por año

Etiquetas de fila	Incidentes Registrados
2014	34
2015	26
2016	19
2017	14
2018	4
Total, General	**97**

Fuente. Correcol S.A. (2018)

El porcentaje con mayor incidencia de incidentes correspondió al año 2014 de acuerdo a las siguientes acciones:

- Efectuar mecanismos preventivos, correctivos y concientización a los usuarios de Correcol

- Realizar monitoreo permanente desde TI con el fin de detectar inconvenientes con los sistemas actuales.

Por otro lado, se pudo establecer que en la actualidad la empresa no tiene un mecanismo de priorización de los incidentes, todo se realiza por el juicio de experto que posee el oficial de seguridad de la información, que realiza la priorización de acuerdo con el impacto y urgencia del incidente y dependiendo del activo afectado.

Adicionalmente, el oficial de Seguridad recibe el correo electrónico, realiza la descarga del archivo de registro del incidente y determina los pasos a seguir mediante un análisis inicial del incidente reportado, una vez se conozca la causa y realiza el escalamiento con el área afectada, enviando el plan de acción asociado.

D. METODOLOGÍA PARA EL DESARROLLO DEL SOFTWARE

Con el propósito de gestionar los eventos e incidentes de la manera más adecuada se planteó el desarrollo del sistema de gestión de incidentes según el marco de trabajo ITIL el cual está compuesto por las siguientes etapas:

1. Reporte del incidente. El individuo se percata de que están efectuando un ataque a los activos de la entidad, o es conocedor de que alguna persona de la compañía está violando las políticas de seguridad de la información de TI, está en la obligación de reportar la situación como un evento o incidente de seguridad de la información, debe comunicarse por cualquiera de los canales de comunicación: Correo, teléfono o informando directamente a la mesa de servicios.

2. Registrar incidente. La mesa de servicios toma los datos necesarios para realizar el registro, realiza la categorización inicial del incidente determinando si es un incidente o un evento, si se determina que no es un incidente es posible que sea una solicitud de servicio o un control de

cambios, de lo contrario los datos del incidente los ingresa a la aplicación de gestión de incidentes ingresando la descripción de lo ocurrido con fecha y hora, si lo puede solucionar inmediatamente documenta la solución aplicada.

3. Categorización. La categorización permite asignar el tipo de incidente que está ocurriendo, por lo general las organizaciones utilizan un nivel de categorización de nivel múltiple en el cual el primer nivel consta de pocas categorías que abarcan un nivel amplio de características de alto nivel, por ejemplo categorías de primer nivel: Hardware, Software, Red.

4. Priorización. Al realizar el registro de cada incidente se debe acordar y asignar un código de priorización que sea apropiado, ya que este código determinará como se le dará el manejo al incidente. La priorización la puede efectuar la aplicación web o el personal de la mesa de servicios con el propósito de clasificar la urgencia del incidente.

Tabla 5. Sistema de Priorización

		IMPACTO		
		ALTO	MEDIO	BAJO
URGENCIA	ALTA	1	2	3
	MEDIA	2	3	4
	BAJA	3	4	5
CÓDIGO DE PRIORIDAD		DESCRIPCIÓN	TIEMPO DE RESOLUCIÓN	
1		CRITICO	1 HORA	
2		ALTO	8 HORAS	
3		MEDIO	24 HORAS	
4		BAJO	48 HORAS	
5		PLANIFICACION	PLANEADO	

Fuente. Los Autores

5. Diagnóstico inicial. La mesa de servicio intenta comprender todos los síntomas del incidente para saber cuál es el inconveniente que se presenta y tratar de corregirlo, durante este proceso la mesa de servicio puede recurrir a la base de datos de errores comunes para acelerar la solución del incidente.

6. Investigación y Diagnostico. La investigación y diagnostico tiene las siguientes etapas:

➢**Evaluar el impacto del incidente.** De acuerdo a la norma ISO 27001, posterior a la identificación de los activos, es importante tener en cuenta la identificación de amenazas, vulnerabilidades e impactos asociados que causen la perdida de confidencialidad, integridad y disponibilidad sobre los activos de la organización. De acuerdo a la escala de valoración se planteó lo siguiente:

Tabla 6. Valoración propuesta de los activos en CORRECOL S.A.

Atributo	Nivel	Valor	Descripción
Confidencialidad	>3	Confidencial	Si el active es accedido por personas no autorizadas, el impacto sería muy alto
	1-3	Uso interno	Afectación parcial al uso indebido sin autrización
	<1	Público	No hay afectación, ya que es de uso público
Integridad	>3	Alto	Si la exactitud y el estado completo de la información y métodos de procesamientos son alterados, el impacto sería muy alto
	1-3	Medio	Si la exactitud y el estado completo de la información y métodos de procesamientos, el impacto sería medio y la afectación sería parcial
	<1	Bajo	No se ve afectación importante
Disponibilidad	>3	Altamente disponible	Si no hay acceso a los activos en el momento que se requiere, se tiene un impacto negativa afectando la imagen de la compañía
	1-3	Disponible	El active puede estar disponible por lo menos el 50% del tiempo
	<1	Disponibilidad básica	El active puede estar disponible por lo menos el 15% del tiempo

Fuente. Los Autores

Tabla 7. Niveles de valoración de activos en CORRECOL SA

Atributo	Descripción
Critico	>4
Alto	>3 y <=4
Medio	>2 y <=3
Bajo	>1 y <=2
Muy bajo	<=1

Fuente. Los Autores

En el caso de que la mesa de servicios no pueda darle solución al incidente se escala al segundo nivel donde el oficial de seguridad de la información evaluará el tipo de incidente o evento que se está presentando, cuales activos está afectando, que alcance puede llegar a tener, así como un pronóstico con respecto a la expansión del incidente y daños potenciales a los activos de la compañía.

Para la evaluación es importante tener la relevancia de los activos y el nivel del incidente.

➢**Identificar la relevancia del activo.** Teniendo en cuenta la verificación de los riesgos que tienen relación con los activos, se establecerá el nivel de afectación incluyendo el valor económico y la cantidad de información relevante para la entidad contenida en el activo.

➢**Identificar el nivel del incidente**. El oficial de seguridad de la información tiene la responsabilidad de identificar el nivel de afectación del incidente de acuerdo a los niveles de criticidad establecidos para el incidente. Si el incidente no se encuentra en el nivel de clasificación establecido ya sea porque no tiene una solución propuesta o no corresponde a los niveles de servicio 0 y 1 debe ser derivado a gestión de cambios.

➢**Escalar el incidente**. Para brindar una solución efectiva al incidente, el oficial debe de tener en cuenta los niveles de escalamiento, según su relevancia y complejidad puede realizar un escalamiento funcional o jerárquico.

7. Seguimiento del incidente. El seguimiento está relacionado directamente con el nivel de escalamiento que haya sido asignado para solucionar el incidente, su responsabilidad está en mantener actualizada las bases de datos del sistema de gestión de incidentes para mantener al tanto a los implicados.

8. Resolución del incidente. Cuando el nivel del servicio ha identificado una solución potencial del incidente, debe aplicarse la solución efectuando las acciones específicas a realizar y las personas que participarán en la solución, en la toma de acciones de recuperación varían según la naturaleza de la falla, esto podría implicar lo siguiente:

✓Pedir al usuario que realice actividades dirigiéndolo desde un escritorio remoto.

✓La mesa de servicios implementa una solución de forma centralizada como por ejemplo el reinicio de un servidor

✓Se solicita a un grupo especializado que implementen una solución específica, como por ejemplo la configuración de un enrutador.

✓Se solicita a un proveedor la resolución de la falla

✓Se deben realizar pruebas suficientes para garantizar que el evento de recuperación se haya realizado de manera completa, y que el servicio haya sido restaurado completamente al usuario.

9. Cierre del incidente. El cierre está relacionado directamente con el nivel de escalamiento que haya resuelto el incidente, al cerrarse el incidente se enviará la respuesta al usuario que registró el mismo con la solución establecida, el usuario verifica que la solución del incidente haya sido efectiva, de lo contrario el incidente cambia su estado a, reabierto y se repite el proceso nuevamente. Si el usuario no responde en el tiempo configurable en la aplicación de acuerdo a la prioridad establecida del incidente, el incidente se cerrará automáticamente.

E. CONSTRUCCIÓN DEL SITIO WEB

Para la construcción del aplicativo se identificaron los requerimientos no funcionales; Requerimientos funcionales; Requerimientos recomendados del servidor; la Configuración de puertos y el software, para luego se diseñaron los menús para la gestión de incidentes, se tiene en cuenta el perfilamiento asociado bajo autenticación LDAP.

➢**Administrador**: Configuración general de la aplicación bajo un rol con derechos administrativos, se podrán configurar los parámetros generales de la aplicación, configuración de usuarios, acciones; entre otros.

➢**Bandeja de entrada:** Contiene un listado de notificaciones y mensajes asociados bajo su área.

➢**Incidentes:** Menú que contiene la gestión del incidente (Registro, clasificación, escalamiento, plan de acción, acciones, resolución y cierre.

➢**Estadísticas:** Reportes filtrados por área sobre los incidentes generados en un rango de tiempo dado.

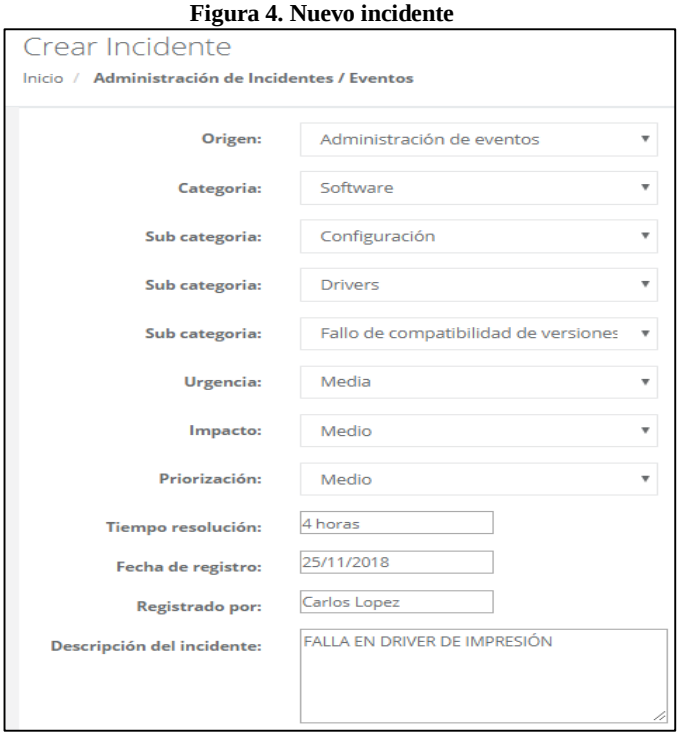
➢**Base de conocimiento:** Registro de solución de incidentes anteriores (CMDB) con el fin de tener funciones de apoyo sobre la solución de los mismos.

➢**Lecciones aprendidas:** Registro de recomendaciones y evidencias asociadas para la aplicación de nuevo conocimiento de manera preventiva para la gestión de los incidentes.

Figura 3. DashBoard Aplicación SGI para CORRECOL SA

Fuente. Los Autores

Figura 4. Nuevo incidente



Fuente. Los Autores

4. CONCLUSIONES

Ante la vanguardia de cambios tecnológicos y modelos de integración continua, los sistemas de información cumplen un papel fundamental en la toma decisiones, buscando facilitar la comunicación entre los diferentes roles de la compañía a través del diseño e implementación de flujos asociados a normas, procedimientos y técnicas bajo un entorno confiable, eficiente y seguro. Con base en lo anterior y el conocimiento adquirido en la especialización, se realizó el análisis y caracterización del sistema actual de la gestión de incidentes en CORRECOL S.A.

Debido a que CORRECOL S.A. está invirtiendo más en tecnología y está comprometida con el mejoramiento del sistema de gestión de la seguridad de la información actual, buscando eliminar brechas asociadas a la ausencia de controles que representan gastos operativos y afectación en los activos de la compañía al no tener información en tiempo real, se identificaron los requerimientos funcionales y no funcionales para la construcción del sistema web bajo un modelo ágil teniendo en cuenta la proyección de la compañía a nivel de escalabilidad.

Para el levantamiento de información se realizaron visitas a la sede de CORRECOL S.A, buscando acercamiento con el oficial de seguridad, el Gerente de TI y la Directora de sistemas de gestión mediante comités periódicos buscando la definición del contexto, oportunidades de mejora, próximos pasos orientados a un cambio cultural y maximización del uso de herramientas de sistemas de información para la gestión de incidentes.

Al implementar un sistema de gestión de incidentes permitirá que la organización tenga un amplio número de beneficios, dentro de las cuales encontramos mayor productividad y eficiencia en los procesos de la empresa, satisfacción de los usuarios, cumplimiento con los requerimientos de disponibilidad de los servicios de TI y oportunidad de mejora alineado a los objetivos misionales de la organización, razón por la cual se logró construir un sistema web capaz de llevar el ciclo de vida de los incidentes de TI.

Resaltamos los conocimientos adquiridos durante la especialización de Seguridad Informática, ya que nos facilitó el análisis, entendimiento y aplicabilidad, buscando orientar a CORRECOL S.A. sobre la importancia de la seguridad de la información y como poder maximizar su beneficio a través de lineamentos de la norma 27001,27035, buenas prácticas en ITIL y apoyo de sistemas de información.

5. REFERENCIAS

[1] Techopedia, «Biblioteca de infraestructura de tecnología de la información (ITIL) Gestión de incidentes,» 2016. [En línea]. Available: https://www.techopedia.com/definition/29291/information-technology-infrastructure-library-itil-incident-management. [Último acceso: 3 Febrero 2019].

[2] P. Sharma, «Sistema de información empresarial: significado, características y componentes,» 2015. [En línea]. Available: http://www.yourarticlelibrary.com/management/information-system/business-information-system-meaning-features-and-components/70319. [Último acceso: 3 Febrero 2019].

[3] R. Steinberg, ITIL v3 Service operation, Norwich: TSO The Stationery Officep, 2015.

[4] S. Ríos Huércano, ITIL v3 Manual integro, Sevilla: Biable Management, Excellence and Innovation, 2014.

[5] C. S.A., Escritor, *Gestión de incidentes*. [Performance]. Información corporativa, 2018.

[6] International Organization For Standardization ISO, Information technology- information security incident management. DUS ISO/IEC 27035, Ginebra: ISO, 2016.

[7] Instituto Colombiano De Normas Técnicas Y Certificación, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. NTC-ISO/IEC27001., Bogotá: ICONTEC, 2006.