GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA

Jesús Armando Pachón Ramírez
japachonr@gmail.com
Universidad Piloto de Colombia

***Resumen*—La Superintendencia Financiera de Colombia ha implementado políticas de seguridad de la información las cuales buscan reducir el riesgo que en forma accidental o intencional permita que se conozca, divulgue, manipule, modifique, destruya o que se use de manera indebida la información o se realicen actos que afecten negativamente la labor y la imagen de la Superintendencia Financiera de Colombia; Como parte de estas se desarrolla un modelo para la gestión de incidentes de seguridad de la información que se desarrollará en la dirección de Tecnología con el aval del área de seguridad.**

***Palabras Clave*—Políticas de seguridad de la información, Implementación, Lineamientos, Modelo de seguridad de la Información, Gestión de Incidentes de Seguridad de la Información.**

***Abstract*—The Financial Superintendence of Colombia performances and have implemented information security policies which aims to reduce the risk of accidentally or intentionally that allow known, disclose, manipulate, alter, destroy or improperly use of information or acts that negatively affect the work and image of the Financial Superintendence of Colombia; As part of such develops a model to manage of information security incidents to be held in the direction of Technology with the support of the information security area.**

***Index Terms*—Information Security Policy, Implementation, Guidelines, Information Security Model, Information Security Incident Management.**

I. INTRODUCCIÓN

EL uso de las tecnologías de la información en el país ha tomado gran auge desde hace ya varios años, lo cual ha hecho que las empresas tanto a nivel privado como gubernamental se interesen en regular y reglamentar los aspectos relacionados con el manejo de la información, por lo que el gobierno nacional expidió una estrategia denominada Gobierno en Línea [1], el cual es liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC [2], que trae un documento modelo que se puede utilizar como guía para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en el estándar NTC:ISO/IEC 27001:2005 [3]; hoy actualizado como NTC:ISO/IEC 27001:2013 [4] y que se ha venido desarrollado dentro de las entidades públicas, al igual puede ser usado como referencia cualquier entidad, empresa u organización que desee iniciar el proceso de implementación del SGSI.

II. JUSTIFICACIÓN

El proceso de implementar un sistema de gestión de incidentes para la superintendencia Financiera de Colombia, es conveniente realizarlo pues en él se desarrollará una metodología aplicada la cual tendrá como beneficio optimizar procesos los cuales pueden incidir de manera significativa en la operación del negocio, aprovechando así las diferentes herramientas con las cuales cuenta la superintendencia Financiera de Colombia y basados en las definiciones de un modelo internacional como base para estructurar los procesos, definir actividades, categorías, responsables, entre otros.

Los beneficios derivados de este modelo para la superintendencia Financiera de Colombia son relevantes, dentro de ellos lo que se busca es, establecer el proceso de gestión de incidentes de seguridad de la información, definir subprocesos de registro y categorización, subprocesos de clasificación de la severidad, subprocesos de validación de la base de conocimiento, subprocesos de investigación y diagnóstico.

Definiendo los procesos del gestor de incidentes, disminuir costos, concientizar a los usuarios de la entidad en la importancia que se debe dar en cuanto a temas de seguridad de la información y en cuanto al proceso metodológico alcanzado en la finalización de éste modelo, establecer acuerdos de nivel de servicio para definir procesos, clasificar incidentes, niveles de atención, definir acuerdos de nivel de servicio con las diferentes áreas, definir roles y responsabilidades de acuerdo al nivel del incidente, y más importante aún tener presentes en futuras ocasiones las lecciones aprendidas.

III. OBJETIVOS

Objetivo General. Implementar de un sistema de gestión de incidentes de seguridad de la información para la superintendencia Financiera de Colombia.

A. Objetivos Específicos

- Determinar la estrategia de creación del sistema de gestión de incidentes.
- Realizar reuniones semanales con el fin de ajustar actividades realizadas durante el proceso de desarrollo.
- Realizar la creación de la metodología que se manejará en el módulo de Incidentes en la Herramienta superIt (Remedy), junto con la plantilla de manejo de incidentes de seguridad de la información.
- Definir los tipos de incidentes a registrar con su respectivo nivel de complejidad y estructurar los niveles de gestión de los mismos.
- Definir la guía de reporte de incidentes para la superintendencia Financiera de Colombia.
- Realizar campañas de divulgación y cultura del manejo de los incidentes y el proceso para mitigar los mismos y registrarlos.
- Realizar la implementación del sistema de gestión de incidentes de seguridad de la información en la superintendencia Financiera de Colombia en dos etapas pre productiva y productiva.
- Presentar el modelo gestión de incidentes a la dirección de tecnología de la superintendencia Financiera de Colombia.

IV. ALCANCE

Aplica para todos los incidentes relacionados con los servicios brindados por la Dirección de Tecnología y Planeación en cuanto a seguridad informática, desde el registro de la ocurrencia hasta su solución y cierre definitivo.

V. RESEÑA NORMATIVA

Por medio de la Directiva Presidencial 02 del 28 de agosto del 2000 [5], el estado colombiano empezó a ver a las tecnologías de la información como una fuente importante de desarrollo económico, la modernización de la sociedad y el acercamiento al conocimiento a través de esta directiva el Gobierno nacional estableció la obligatoriedad para que las entidades públicas cumplan con la "Estrategia de Gobierno en Línea", y así de esta manera integrar a los diferentes actores de la economía nacional en el uso de las tecnologías de la información y con ello, principalmente proporcionar al ciudadano los servicios de las empresas estatales a través de internet. De esta manera las empresas del estado empiezan a implementar la prestación de sus servicios en línea.

VI. MARCO REFERENCIAL

Un sistema de Seguridad de la Información alineado con la misión, visión, procesos claros y definidos, permiten preservar constantemente la confidencialidad, integridad y disponibilidad de la información, considerada como unos de los activos más valiosos para la entidad. Para ello la superintendencia Financiera de Colombia establece que sus funcionarios conozcan y cumplan las políticas, los lineamientos, procedimientos y demás directrices de Seguridad de la Información definidos en este documento.

Para este proceso se tendrán en cuenta conceptos de un modelo internacional llamado CSIRT (Computer Security Incident Response Team - Equipo de Respuesta a Incidentes de Seguridad Informática) [6], en él se detalla una serie de pasos, procedimientos y sugerencias para la implementación de estos procesos en los cuales se pueden involucrar distintas áreas dentro de la organización y las cuales se enfocaran específicamente en las que pudiesen ser fuentes potenciales de incidentes de seguridad de la información y en aquellas que se pueden reorganizar con el fin de obtener procesos claros, precisos y concisos.

El CSIRT, es un centro de coordinación de atención a incidentes de seguridad informática internacional, el cual está en contacto directo con los centros de seguridad de sus empresas afiliadas y está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas por medio de un correo electrónico a la cuenta contacto ATcsirt-ccit.org.co, también mantiene comunicación constante con organizaciones internacionales que trabajan en el sector de la seguridad informática y hace uso de información especializada entregada por estas, para advertir a los integrantes del CERT Colombia, sobre cualquier tipo de contenido malicioso que pueda tener alojado dentro de sus redes, que afecte directamente su operación, o que amenace la seguridad de sus clientes.

El CSIRT es un punto de contacto nacional, mediante el cual la comunidad nacional e internacional puede comunicarse con las más grandes empresas proveedoras de Internet en Colombia, con el objetivo de gestionar una pronta y eficiente atención a los incidentes de seguridad informática que involucren redes y/o servicios Internacionales.

VII. IMPLEMENTACIÓN DEL SGSI EN LAS ENTIDADES DEL ESTADO

Con la obligatoriedad establecida mediante la estrategia de Gobierno en Línea, liderada por el Ministerio de las Tecnologías de la información y las Comunicaciones, las entidades del estado se ven en la necesidad de iniciar el proyecto de implementación de un SGSI.

Para esto, el Ministerio de las tecnologías de la información y las comunicaciones MINTIC, emite el documento denominado "Modelo de seguridad de la Información para la Estrategia de Gobierno en Línea 2.0" el cual se apoya en la creación del Sistema Administrativo de Seguridad de la Información para Gobierno en Línea – SASIGEL [7] y en la conformación de la Comisión de Seguridad de la Información para Gobierno en línea, para tomar acciones estratégicas y definir los lineamientos que permitan la implementación, seguimiento y mantenimiento del Modelo de Seguridad de la Información en cada una de las entidades públicas de orden nacional y territorial y en las entidades privadas que sean proveedoras de los servicios de Gobierno en línea.

Este documento modelo se encuentra alineado con el estándar NTC: ISO/IEC 27001:2005 [3] e incluso se complementa con otros estándares como COBIT [8], ITIL [8] y MECI CALIDAD [9], el SASIGEL [7] se constituye entonces en el conjunto o integración de todos los actores involucrados en la seguridad de la información a nivel nacional, y será el encargado de coordinar las actividades relacionadas con la gestión de la seguridad de la información a nivel nacional, el cual se detalla a continuación:

A. Comisión de Seguridad de la Información para Gobierno en Línea.

Es la máxima autoridad en materia de Seguridad de la Información para la Estrategia de Gobierno en Línea y está compuesta por:

- Presidencia de la República.
- Ministerio de las Tecnologías de la Información y las Comunicaciones.
- Ministerio del Interior y de Justicia.
- Ministerio de Defensa Nacional.
- Ministerio de Comercio, Industria y Turismo.
- Ministerio de Relaciones Exteriores.
- Dirección Nacional de Planeación.
- Contraloría General de la República.
- Comisión de Regulación de las Comunicaciones – CRC.

La Comisión podrá convocar a las siguientes entidades cuando lo considere necesario:

- Fiscalía General de la Nación.
- Procuraduría General de la Nación.
- Superintendencia de Industria y Comercio.
- Comisión Intersectorial de Política y Gestión de Información – COINFO o quien haga sus veces. [10]

B. Grupo Técnico de Apoyo.

Es quien está encargado de la elaboración y preparación de los documentos, políticas, lineamientos, estándares y recomendaciones, las cuales serán aprobadas por la Comisión, estará conformada por personal que tenga formación profesional y experiencia en áreas relacionadas con seguridad de la información.

C. Equipo de Gestión del Proyecto del Nivel Central.

Este equipo es quien debe coordinar lo relacionado con la implementación, administración, seguimiento y control del Modelo de Seguridad a implementar en las Entidades del estado, debe estar conformado por profesionales con experiencia y conocimiento en Administración Pública, gestión y gerencia de proyectos.

D. Equipo de Gestión al interior de cada una de las Entidades.

Es el encargado de realizar las actividades de implementación del SGSI en las entidades del estado, según el Modelo de Seguridad de la Información.

VIII. DEFINICIÓN, CONCEPTOS Y METODOLOGÍA DE CSIRT

Un CSIRT, estudia el estado de seguridad y proporciona servicios de respuesta ante incidentes a víctimas de ataques internos y en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayuda a mejorar la seguridad en los sistemas, a continuación se describen los elementos a tener en cuenta para el desarrollo del proceso en la gestión de incidentes de seguridad de la información,

- Desarrollar políticas de respuesta a incidentes de seguridad de la información.
- Desarrollar procedimientos claros para el manejo de los incidentes que vayan orientados hacia la política.
- Establecer relaciones entre el equipo de respuestas a incidentes y otras áreas de la organización.
- Organizar el equipo de respuesta a incidentes, definir y asignar funciones.
- Determinar qué servicios proveerá el equipo de respuesta a incidentes.
- Entrenar al equipo de respuesta a incidentes.

A. Metodología de gestión de incidentes de seguridad:

Fig. 1. Se muestra el modelo del proceso de gestión de incidentes de seguridad de la información.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

A continuación se describen cada uno de los componentes del proceso de Gestión de Incidentes de Seguridad de la Información.

- **Preparación y Prevención.**

Criterios y categorización de incidentes:

- Por tipo de Incidente.
- Por la envergadura de los daños producidos.

Por tipo de Incidente:

- Denegación de servicios.
- Código malicioso.
- Acceso no autorizado.
- Uso inapropiado.
- Incidente múltiple.

INCIDENTE	EFECTOS NEGATIVOS PRODUCIDOS		
	Grave	Moderado	Leve
Dos			
Código Malicioso			
Acceso no autorizado			
Uso inapropiado			
Incidente múltiple			
Scanning de puertos			
Otro_____			

Tabla. 1. Identificación del incidente de acuerdo a la clasificación preestablecida.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

Los criterios de clasificación de incidentes: se analizan los efectos del incidente y los recursos afectados, consignándolos en la siguiente tabla:

CRITICIDAD DEL INCIDENTE		Criticidad de los recursos afectados		
		Alta	Media	Baja
Efectos negativos producidos por el incidente	Grave	Muy grave	Grave	Moderado
	Moderado	Grave	Moderado	Leve
	Leve	Moderado	Leve	Leve

Tabla. 2. Clasificación del incidente según su impacto.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

RECURSOS	CIRTICIDAD DE LOS RECURSOS AFECTAODS		
	Grave	Moderado	Leve
Servidor web			
Servidor de archivos			
Servidor de aplicación			
Estaciones de trabajo			
Router			
Firewall			
Sistema de gestión			
Otro_____			

Tabla. 3. Recursos afectados por el incidente y la clasificación del efecto sobre estos.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

Mediante el siguiente cálculo se determina el nivel de criticidad del incidente.

Efectos negativos producidos por el incidente	+	Criticidad de los recursos Afectados	=	Criticidad del incidente

Tabla. 4. Fórmula para el cálculo de la criticidad del incidente de seguridad de la información.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

De acuerdo con la criticidad del incidente se determina que este debe ser atendido de acuerdo con la siguiente prioridad.

TIEMPO A TRATAR CADA INCIDENTE	
Muy grave	10 Minutos
Grave	30 Minutos
Moderado	2 Horas
Leve	4 Horas

Tabla. 5. Tiempo determinado para la atención de un incidente de seguridad de la información de acuerdo la criticidad determinada.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

Otras medidas de preparación:

- Definir políticas, normas y procedimientos para la gestión de incidentes.
- Entrenar al personal.
- Documentar un mapa de la topología y arquitectura de la red.
- Comprender el funcionamiento normal.

Prevención de incidentes:

- Análisis periódicos de riesgo.
- Mejores prácticas de seguridad.
- Auditorias periódicas.
- Administración de actualizaciones.
- Fortalecimiento de la seguridad de los equipos.
- Seguridad en la red.
- Prevención de código malicioso.
- Concientización y capacitación de usuarios.

- **Detección y Notificación:**

La detección de un incidente se puede realizar por medio de una advertencia, que es una señal que indica la posible ocurrencia de un incidente; y el indicador, que es una señal de que un incidente ocurrió o está ocurriendo en este momento. Ambos se pueden detectar manual o automáticamente.

Señales de advertencia:

- Anuncios de exploit
- Amenaza de ataque web
- Perdida de un equipo de cómputo.
- Fuga o pérdida de información.
- Virus.

Señales indicadoras de un posible incidente:

- Aviso por un sistema de detección de intrusos.
- Antivirus detectando troyanos o gusanos en los equipos.
- Acceso lento en la red de la organización.
- Cambio de configuración de seguridad en los reportes (log) de un servidor.
- Bloqueo de cuenta por intentos fallidos de ingreso.
- Aviso de un usuario de robo de datos.

Qué permite la detección de incidentes:

- IDS – sistema de detección de intrusiones, ya sean en la red o a nivel de equipos.
- Software de antivirus.
- Software de control de integridad de archivos.
- Análisis de registros de auditoria (logs).
- Información pública.
- Usuarios de la organización.

A continuación se define el diagrama de notificación de incidentes:

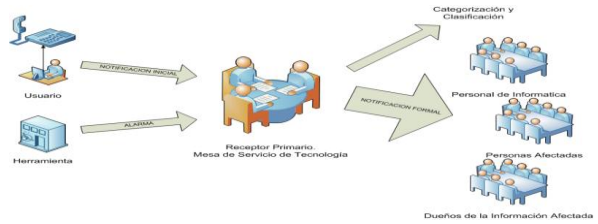

Fig. 2. Diagrama de notificación de Incidentes de Seguridad de la Información.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

Datos que se deben incluir a la hora de notificar incidentes:

Datos del reporte:

- ID.
- Fecha y hora.

Datos del incidente:

- Clasificación
- Breve descripción
- Efectos producidos
- Descripción detallada
- Responsable de atención

Datos de quien reporta:

- Nombre
- Cargo
- Área
- Tel/interno
- Mail

- **Análisis Preliminar:**

En esta parte es donde realmente se debe hacer la pregunta de si realmente se trata de un incidente de seguridad.

Recolección de información para analizar:

- Alcance del incidente, es decir, que sistema y aplicaciones afecta.
- Que origino el incidente.
- Como ocurrió o está ocurriendo el incidente; métodos, herramientas utilizadas, vulnerabilidades explotadas, etc.
- El impacto potencial en las actividades del organismo.

Cómo determinar el alcance:

- Cuantos equipos fueron comprometidos.
- Cuántas redes se vieron envueltas.
- Que tan adentro de la red logró penetrar el atacante.
- Qué nivel de privilegio logró el atacante.
- Qué es lo que está en riesgo, cómo impacta en las actividades de la organización, se encuentran en riesgo aplicaciones críticas.
- Quién sabe acerca del incidente y qué impacto puede tener.
- Cuán conocida es la vulnerabilidad explotada por el atacante, hay otros equipos con la misma vulnerabilidad.

En la siguiente tabla se definen los métodos de recolección de información:

ACCIONES	RESULTADOS
Indagación a los administradores de sistemas	*Obtener datos sobre sucesos anormales en los sistemas*
Personal del organismo	*Obtener datos sobre sucesos anormales en las actividades cotidianas*
Revisión de reportes de herramientas de detección de intrusiones	*Conocer detalles del incidente*
Revisión de logs de comunicaciones plataformas y sistemas	*Detectar actividades anormales*
Revisión de la topología de red y listas de acceso	*Detectar posibles cambios no autorizados*

Tabla. 6. Métodos de recolección de información sobre el incidente de seguridad de la información.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

- **Contención, Erradicación y Recuperación:**

A continuación se describe en que consiste cada uno de los subprocesos de esta etapa.

CONTENCIÓN	Evitar que el incidente siga produciendo daños
ERRADICACIÓN	Eliminar la cauda del incidente y todo rastro de los daños
RECUPERO	Volver el entorno afectado a su estado original

Tabla. 7. Descripción de las etapas del proceso de contención, erradicación y recuperación.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

Se deben considerar los siguientes factores para la selección de una estrategia:

- Daño potencial de recursos a causa del incidente.
- Necesidad de preservación de evidencia.
- Tiempos y recursos necesarios para poner en práctica la estrategia.
- Efectividad de la estrategia (total o parcialmente).
- Duración de las medidas a tomas (periodo sin sistema).
- Criticidad de los sistemas afectados.
- Características de los posibles atacantes.
- Si el incidente es de conocimiento público.
- Pérdida económica.
- Posibles incidencias legales.
- Relación costo-beneficio de la estrategia.
- Experiencias anteriores (lecciones aprendidas).

En la siguiente tabla se definen las estrategias usadas para la contención de incidentes:

INCIDENTE	EJEMPLO	ESTRATEGIA DE CONTENCIÓN
Acceso no autorizado	*Sucesivos intentos fallidos de login*	*Bloqueo de cuenta*
Código malicioso	*Infección con virus*	*Desconexión del equipo afectado de la red*
Acceso no autorizado	*Compromiso del root*	*Apagado del sistema*
Reconocimiento	*Scanning de puertos*	*Incorporación de reglas de filtrado en el firewall*

Tabla. 8. Estrategias de contención del incidente de seguridad de la información de acuerdo al origen de este.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

En la siguiente tabla se definen las estrategias de recuperación de incidentes:

INCIDENTE	EJEMPLO	ESTRATEGIA DE RECUPERACIÓN
DoS	*SYN Flood*	*Restitución del servicio caído*
Virus	*Gusano en la red*	*Corrección de efectos producidos. Restauración de backups*
Vandalismo	*Defacement a un sitio web*	*Reparar el sitio web*
Intrusión	*Instalación de un rootkit*	*Reinstalación de equipo y recuperación de datos*

Tabla. 9. Estrategias de recuperación del incidente de seguridad de la información de acuerdo al tipo de este.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

En la siguiente tabla se definen Estrategias de erradicación de incidentes:

INCIDENTE	EJEMPLO	ESTRATEGIA DE ERRADICACIÓN
DoS	*SYN Flood*	*Reconfigurar el router para minimizar el efecto de flooding*
Uso no autorizado	*Utilizar las PCs laborales para lucro personal*	*Comunicar al personal las políticas de uso de recursos. Implementar monitoreo del uso de las PCs*
Vandalismo	*Defacement a un sitio web*	*Aplicar los parches de seguridad faltantes en plataformas y aplicaciones web*
Robo de información	*Robo de datos sensibles de clientes de la base de datos*	*Reconfigurar la seguridad de la base de datos*
Código malicioso	*Infección de un servidor con virus*	*Detectar el código malicioso y eliminarlo del equipo. Actualizar el software de antivirus*

Tabla. 10. Estrategias de erradicación del incidente de seguridad de la información de acuerdo al tipo de este.
Tomado del modelo de Administración de incidentes y requerimientos, superintendencia Financiera de Colombia.

- **Investigación:**

Durante el proceso de investigación del incidente de seguridad de la información se tienen en cuenta los siguientes aspectos:

- Información basada en Host. Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, backups, archivos copiados recientemente, etc.
- Información basada en red. Logs de IDSs, logs de monitoreo, información recolectada mediante sniffers, logs de routers, logs de firewalls, información de servidores de autenticación.
- Otra información: Testimonio de personal.

Se debe tener en cuenta lo siguiente en la recolección de evidencia:

- Autenticidad: Quien haya recolectado la evidencia debe poder probar que es auténtica.
- Cadena de Custodia: Registro detallado del tratamiento de la evidencia, incluyendo quienes, como y cuando la transportaron, almacenaron y analizaron, con tal fin de evitar alteraciones o modificaciones que comprometan la misma.
- Validación: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

Durante el proceso de recolección de evidencias es necesario que se cumpla de manera estricta con:

- Registrar información que rodea a la evidencia.
- Tomar fotografías del entorno de la evidencia.
- Tomar la evidencia.
- Registrar la evidencia.
- Rotular todos los medios que serán tomados como evidencia.
- Almacenar toda la evidencia de forma segura.
- Generar copias de seguridad de la evidencia original.
- Realizar revisiones periódicas para garantizar que la evidencia se encuentra correctamente conservada.

Actividades posteriores que deben llevarse a acabo:

- Organizar reuniones.
- Mantener la documentación.
- Crear bases de conocimiento.
- Integrar la gestión de incidentes al análisis de riesgo.
- Implementar controles preventivos.
- Elaborar tableros de control.

IX. VENTAJAS DE LA IMPLEMENTACIÓN DE UN CSIRT

Para la superintendencia Financiera de Colombia disponer de un equipo dedicado a la seguridad de TI le será de gran ventaja puesto que aparte de contribuir con la mejora continua del proceso de TI y maduración del mismo, podrán mitigar a su máxima expresión los incidentes que se puedan presentar dando valor a la protección de su patrimonio.

Otras posibles ventajas son:

- Disponer de una coordinación centralizada para las cuestiones relacionadas con la seguridad de las TI dentro de la organización (punto de contacto).
- Reaccionar a los incidentes relacionados con las TI y tratarlos de un modo centralizado y especializado.
- Tener al alcance de la mano los conocimientos técnicos necesarios para apoyar y asistir a los usuarios que necesitan recuperarse rápidamente de algún incidente de seguridad.
- Tratar las cuestiones jurídicas y proteger las pruebas en caso de pleito.
- Realizar un seguimiento de los progresos conseguidos en el ámbito de la seguridad.
- Fomentar la cooperación en la seguridad de las TI entre los clientes del grupo atendido (sensibilización).
- Tratamiento de los incidentes.

X. ¿POR QUÉ SURGE LA IDEA DE IMPLEMENTAR UN SISTEMA DE GESTIÓN DE INCIDENTES PARA LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA?

La necesidad de implementar un sistema de gestión de incidentes de Seguridad de la Información para la superintendencia Financiera de Colombia surge una vez cuando se tuvieron en cuenta las necesidades de establecer las políticas de seguridad de la información. Las cuales se constituirían en un elemento primario de gobierno, que buscan definir los requerimientos mínimos para proteger la información y que su personal tenga claro las políticas definidas por la misma.

Dados los lineamentos actuales, y lo descrito anterior mente, la superintendencia Financiera de Colombia decidió optar por la implantación de las políticas de seguridad las cuales buscarán reducir el riesgo que en forma accidental o intencional permita que se conozca, divulgue, manipule, modifique, destruya o que se use de manera indebida la información o se realicen actos que afecten negativamente la labor y la imagen de la entidad.

Las políticas buscan la ejecución de un programa que comprenda el diseño, implantación, divulgación, preservación y actualización de las estrategias y mecanismos para administrar la seguridad de la información.

XI. IMPLEMENTACIÓN DEL MODELO DE GESTIÓN DE INCIDENTES PARA LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA

Hoy día, el sector empresarial del país tiene cada vez más presentes las tecnologías de la información dentro de su desarrollo corporativo como tal, con el fin de soportar servicios y procesos que se encuentren de cara al negocio y que se han convertido en piezas fundamentales para los diferentes sectores empresariales existentes en nuestro país, por lo tanto una serie de herramientas tecnológicas transforman no solo grandes aspectos del sector empresarial sino también de la sociedad en general permitiendo de esta manera estructurar de manera sólida la consecución de logros mediante las mismas.

Las nuevas tecnologías avanzan en el mundo a pasos agigantados con soluciones cada vez más eficiente trayendo consigo funcionamientos mejorados e innovadores que buscan favorecer de una manera ágil y certera los diferentes campos de operación organizacional a nivel mundial, por lo anterior la tecnología en las organizaciones se convierte en una base fundamental y más para aquellas que actúan como entes regulatorios gubernamentales en los diferentes países.

No obstante, dichos desarrollos tecnológicos traen consigo los riesgos que éstas mismas generan y los cuales deben ser atendidos por las áreas de TI y más específicamente por parte de los equipos de seguridad de la Información y seguridad informática, dado que no es una fantasía, que el entorno digital en el que vivimos, desde tiempo atrás es una realidad, en donde se encuentran diferentes tipos de información que son apetecidos por diferentes sectores o personas los cuales usan estrategias diversas para obtener dicha información sin importar que deban hacer para este fin.

Los riesgos de los que hablamos se traducen a brechas de seguridad y es donde entra a jugar un papel muy importante la seguridad de la información y la Seguridad de la informática y que ellas serán las encargadas de mitigar dichas brechas con diferentes herramientas y sistemas de gestión, en donde cabe resaltar el sistema de gestión de incidentes de seguridad de la información.

Dichos sistemas de gestión de incidentes han generado un impacto positivo en los diversos sectores donde se han implementado nuevas tecnologías que van de la mano con los procesos del negocio y a su vez que han reflejado resultados de carácter significativo para la alta dirección, lo anterior se debe a que un sistema de gestión de incidentes de seguridad de la información ayuda a referir y plasmar un seguimiento claro de los diferentes tipos de problemas y resolución de los mismos en tiempos menores dando como valor agregado las lecciones aprendidas y formas de tratamiento para futuros incidentes, bondades que transforman este tipo de sistemas de gestión en soluciones integrales apetecidas.

XII. ACTUALIZACIÓN DEL SISTEMA NTC: ISO/IEC 27001:2013

Es importante tener en cuenta y se invita a que la entidad opte por ejecutar el proceso de gestión de incidentes de seguridad de la información implementándolo con el modelo actual, el estándar NTC: ISO/IEC 27001:2013.

Es claro que esta nueva versión implicaría realizar una transición de la versión 2005 a la 2013 lo cual trae consigo un esfuerzo adicional.

XIII. RESULTADOS

Se implementó este proceso con el fin de poder ajustar las operaciones normales de los servicios y sistemas en producción, y de esta manera reducir al mínimo el impacto adverso en las operaciones del negocio, así mismo se está asegurando la continuidad, manteniendo los niveles acordados de calidad, disponibilidad del servicio, y sin sobrepasar los límites del marco legal y las acciones involucradas en la toma de decisiones permitidas dentro de la organización.

Con la implementación de este proceso se cubrirán todos los incidentes relacionados con los servicios brindados por la Dirección de Tecnología de la información desde el registro de la ocurrencia hasta la solución y cierre definitivo del mismo.

XIV. CONCLUSIONES

El resultado de implementar un proceso de gestión de incidentes para la superintendencia Financiera de Colombia tiene como objetivo, que sea aplicado para todos los incidentes relacionados con los servicios brindados por la Dirección de Tecnología y Planeación en cuanto a seguridad informática, desde el registro de la ocurrencia hasta su solución y cierre definitivo de este.

REFERENCIAS

[1] *"Estrategia de Gobierno en Línea",* http://programa.gobiernoenlinea.gov.co/donde-nace.shtml

[2] *Ministerio de Tecnologías de la Información y las Comunicaciones,* http://www.mintic.gov.co/portal/604/w3-channel.html

[3] *ISO 27001:2005, Information Security Management, International Organization for Standardization,* http://www.iso.org/iso/es/home/standards/management-standards/iso27001.htm

[4] *ISO 27001:2013, Information Security Management, International Organization for Standardization,* http://www.iso.org/iso/es/home/standards/man agement-standards/iso27001.htm

[5] *Directiva Presidencial 02 del 28 de agosto del 2000,* http://www.mintic.gov.co/portal/604/articles-3646_documento.pdf

[6] *CSIRT (Computer Security Incident Response Team - Equipo de Respuesta a Incidentes de Seguridad Informática),* http://es.slideshare.net/d7n0s4ur70/equipos-de-respuesta-a-incidentes-csirt-cert-clasetresauo?next_slideshow=1

[7] *Sistema de Administración de Seguridad de la Información de Gobierno en Línea "SASIGEL"* http://css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf

[8] COBIT, ITIL, http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

[9] MECI, http://estrategia.gobiernoenlinea.gov.co/623/articles-8240_Orientaciones_DAFP.pdf

[10] COINFO, http://admonpublica.org/preguntas-coinfo/