METODOLOGÍA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS PARA LA PLATAFORMA SIEM DE UNA ENTIDAD FINANCIERA BASADA EN LA NORMA ISO/IEC 27035 E ISO/IEC 27005

YESID ALBERTO TIBAQUIRA CORTES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTA D.C.
2015

METODOLOGÍA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS PARA LA PLATAFORMA SIEM DE UNA ENTIDAD FINANCIERA BASADA EN LA NORMA ISO/IEC 27035 E ISO/IEC 27005

YESID ALBERTO TIBAQUIRA CORTES

Monografía para optar al título de:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

TUTOR(A)
ELEONORA PALTA VELASCO
Ms(c) Ingeniería Telemática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTA D.C.
2015

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del tutor del proyecto

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C., 04 de Mayo de 2015

“Dedicado a Dios, por los regalos maravillosos recibidos de sus manos: 2 familias, una heredada y otra que se ha ido construyendo. Con ambas he labrado un camino que me ha llevado a la consecución de esta meta personal y profesional”
Yesid Alberto Tibaquira Cortes

AGRADECIMIENTOS

Mi más sincero agradecimiento a la Universidad Nacional Abierta y a Distancia, Facultad Tecnológica por ser una guía para la apropiación del conocimiento y las herramientas necesarias para hacer posible la culminación de este proyecto.

Nuestra especial gratitud a:

- ✓ El Ingeniero Luis Fernando Barajas Ardila, tutor del proyecto inicial y a la Ingeniera Eleonora Palta Velasco, por sus orientaciones y recomendaciones que encaminaron a la realización del mismo.

- ✓ Compañeros de carrera y profesores, quienes con su apoyo tanto espiritual como académico se convirtieron en colaboradores activos del mismo.

- ✓ Todas aquellas personas que confiaron en nuestras capacidades y que en algún momento de sus vidas soñaron vernos cumpliendo esta meta.

- ✓ Y sin ser menos importante que los anteriores, a ese ser que día tras día pone su fe y su amor en nosotros: Dios.

ABSTRACT

The work accomplished is supported in the definition of a model for the security incident management and risks management on those incidents; they are detected or derived of the deployment and operation on a tool called SIEM (Security Information Event Management). The definition of the models was carried out under the standards ISO 27035 for security incidents and 27005 for risk management.

Initially were identified the information critical assets, those were configured into the SIEM to define the design's scope in the deployment of the models. Later, the security policies were defined, where are described the guidelines that should be followed for the incidents and risks management.

Finally, the models were defined, along with the deployment and the tools that will help their operation, based in the recommendations that show each standard to each model.

RESUMEN

El trabajo desarrollado se basa en la definición de un modelo de gestión de incidentes de seguridad de la información y de gestión de riesgos sobre estos incidentes, que son detectados o derivados de la implementación y operación de una herramienta SIEM (Correlacionador de Eventos de Seguridad). La definición de los modelos de gestión se realizó bajo las normas ISO 27035 para incidentes de seguridad y 27005 para la gestión de riesgos.

Inicialmente fueron identificaron los activos de información críticos que se encuentran configurados en el SIEM para definir el alcance del diseño en implementación de los modelos. Posterior, se definieron las políticas de seguridad de la información, en donde son descritos los lineamientos que se deben seguir para la gestión de incidentes y riesgos.

Por último, fueron definidos los modelos, junto con la implementación y las herramientas que apoyarán su operación, basados en las recomendaciones que expresa cada una de las normas para cada modelo.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

INTRODUCCIÓN

El crecimiento en la implementación de herramientas de seguridad informática en los últimos años se ha acelerado, a raíz de la evolución de los diferentes métodos (vectores) de ataque informático. Este crecimiento también ha sido promovido por aquellas organizaciones que se encargan de definir requerimientos, estándares generales en algún tipo de industria, con el fin de buscar la protección de la información contra cualquier intento de sustraer, alterar o eliminar la información; un ejemplo de estos estándares son: PCI-DSS (Requerimientos de Seguridad para Información de Tarjetas de Crédito), Cloud Security Alliance (Requerimientos de Seguridad para la Información almacenada o procesada en Cloud Computing), entre otros.

Sin embargo, el tener instalada y configurada las mejores herramientas de seguridad informática, aquellas que se encuentran en el cuadrante mágico de Gartner; no asegura que se esté un 100% protegido. Toda herramienta, necesita ser respaldada por un conjunto de lineamientos los cuales den peso al porqué de su implementación. Lineamientos que estén homologados con los objetivos estratégicos de cada organización y que expresen en un lenguaje de alto nivel cómo las tecnologías, en este caso en el contexto de seguridad, se convierten en un gran aliado para el desarrollo continuo, con un costo eficiente y minimicen los riesgos de Ciberseguridad a los que se encuentra expuesta cualquier organización.

1 FASE DE DEFINICIÓN, PLANEACIÓN Y ORGANIZACIÓN

1.1 TITULO

METODOLOGÍA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS PARA LA PLATAFORMA SIEM DE UNA ENTIDAD FINANCIERA BASADA EN LA NORMA ISO/IEC 27035 E ISO/IEC 27005

1.2 DEFINICIÓN DEL PROBLEMA

1.2.1 Planteamiento del Problema. En la actualidad uno de los inconvenientes que enfrenta el responsable de la seguridad de la información en cualquier organización es la gestión de los incidentes de seguridad y sus riesgos asociados, que son resultados de una plataforma SIEM, lo que indica que no existe el conocimiento de lo que está sucediendo en los sistemas tecnológicos que soportan los procesos críticos para el negocio, en temas de seguridad de la información y una adecuada gestión sobre los riesgos resultantes de la identificación de los incidentes de seguridad que se están presentando sobre estos procesos críticos.

Los profesionales de seguridad de la información de una Entidad Financiera no se encuentran ajenos a estos inconvenientes, y en este caso la Entidad Financiera carece de una metodología de gestión de incidentes de seguridad y de sus riesgos, resultantes de un SIEM, el cual se encuentra actualmente en operación monitoreando la infraestructura tecnológica que respalda los procesos críticos del negocio.

1.2.2 Formulación del problema. ¿La definición e implementación de una metodología de gestión de incidentes de seguridad detectados por una

herramienta SIEM y la posterior valoración de los riesgos asociados puede contribuir a mejorar la gestión de seguridad de la información dentro de la Entidad Financiera?

1.3 JUSTIFICACIÓN

En nuestros tiempos la información se ha convertido en uno de los recursos más importantes tanto a nivel empresarial como a nivel personal, por ello se han implementado normas las cuales definan los requisitos básicos que debe comprometerse a cumplir cualquier organización para salva guardar la información crítica para su negocio.

La información que fluye a través de la infraestructura tecnológica de las entidades financieras no es ajena a estas normas, es más, las normas inicialmente fueron diseñadas para este tipo de organizaciones. Por esta principal razón, es necesario desarrollar y ejecutar buenas prácticas para la gestión de eventos de seguridad que impacten de forma negativa (incidentes) el flujo de la información, principalmente en 3 ámbitos: confidencialidad, integridad y disponibilidad.

Una de las plataformas que en los últimos años ha emergido y ha tenido un desarrollo rápido son las plataformas SIEM, y hoy en día constituyen un punto céntrico de gobernabilidad y administración en la gestión de eventos de seguridad sobre los componentes tecnológicos de una organización. Sin embargo esa administración debe estar enmarcada y respaldada por las buenas prácticas que han sido definidas en temas de seguridad de la información por la industria.

Dentro de estas buenas prácticas se han definido varias normas, entre ellas se encuentran la ISO 27035, que especifica los lineamientos para una efectiva gestión de incidentes de seguridad y la ISO 27005, descendiente de la ISO 35000

(Administración del Riesgo), que es una guía para la gestión de riesgos de seguridad de la información.

1.4 OBJETIVOS

1.4.1 Objetivo General. Definir e implementar la metodología de gestión de incidentes de seguridad y gestión de riesgos asociados a los incidentes identificados por la plataforma SIEM de la Entidad Financiera, teniendo como referencia las normas ISO/IEC 27035 e ISO/IEC 27005.

1.4.2 Objetivos Específicos

- ✓ Identificar y analizar los componentes tecnológicos que actualmente se encuentran configurados en la plataforma SIEM de la entidad financiera

- ✓ Identificar los eventos de seguridad que son posible detectar con la plataforma SIEM.

- ✓ Clasificar los diferentes tipos de incidentes de seguridad asociados a los eventos detectados con la plataforma SIEM.

- ✓ Definir la metodología, política y procesos de gestión de incidentes de seguridad teniendo como base la ISO/IEC 27035 para la plataforma SIEM.

- ✓ Definir la metodología, política y procesos de gestión riesgos teniendo como base la ISO/IEC 27035 para los incidentes de seguridad identificados en la plataforma SIEM.

- ✓ Realizar y presentar un análisis de la implementación de la metodología propuesta basado en la detección de incidentes de seguridad por la plataforma SIEM y la gestión de riesgos de los mismos.

1.5 ALCANCES Y DELIMITACIONES

1.5.1 Alcances

- ✓ La metodología se basa en las normas ISO 27035 y 27005 (Gestión de Incidentes de Seguridad y Gestión de Riesgos de Seguridad de la Información)

- ✓ Las metodologías se implementaran para aquellos incidentes que sean detectados en el SIEM de la Entidad Financiera.

- ✓ Se definirán herramientas para el apoyo de las metodologías basadas en aplicaciones de ofimática (Word y Excel)

1.5.2 Delimitaciones

- ✓ Temática: Es necesario tener un conocimiento en procesos de Gestión de Incidentes de Seguridad de la Información y Gestión de Riesgos Tecnológicos.

- ✓ Temporal: El desarrollo del modelo se realizará entre Enero del 2015 y Marzo de 2015.

- ✓ Tecnológica: SIEM de la Entidad Financiera.

1.6 MARCO DE REFERENCIA

1.6.1 Marco Teórico

SIEM: Inicialmente las plataformas SIEM fueron desarrolladas para la gestión de amenazas externas por decirlo así ruidosas, específicamente para contrarrestar al malware denominado: gusano. Se orientaron este tipo de plataformas a las redes de datos, para analizar en tiempo real los eventos que sucedían sobre estas y apoyar el trabajo del grupo de respuesta a incidentes de seguridad. Posterior algunos vendedores adicionaban características a estas herramientas cómo el análisis histórico y la tendencia del comportamiento de estos eventos, con el fin de servir de insumo a las actividades forense. Es donde nace el término de Gestión de Eventos de Seguridad (SEM – Security Event Management), de esta forma se tenía un sistema que monitoreaba y analizaba los eventos de seguridad.

Sin embargo, era necesario auditar todos estos eventos, no solo identificarlos, esto significa que los eventos identificados necesitaban ser validados y confrontarlos con las diferentes leyes, normas y estándares que iban surgiendo en el mercado. Es así como surge la Gestión de la Seguridad de la Información (SIM - Security Information Management), el cual permitía monitorizar, gestionar, auditar y procesar los eventos de seguridad identificados.

A pesar de que en el mercado por un tiempo se presentaron sistemas SIM y SEM, en el 2005, se define un término el cual combinaría las dos funcionalidades en solo una plataforma, impulsada por la convergencia de los productos desde el 2004, globalizando el término de SIEM, propuesto inicialmente por Mark Nicolett. (Williams, 2007).

ISIRT (Information Security Incident Response Team): Equipo conformado por miembros confiables de la Entidad, que cuentan con las habilidades y

competencias para tratar los incidentes de seguridad de la información, durante el ciclo de vida de estos.

ISO/IEC 27035: El 12 de Octubre de 2004 la Organización Internacional de Estandarización (ISO – International Organization for Standardization) publicó el reporte técnico ISO/IEC TR 18044:2004, con el objetivo de presentar una guía del manejo de incidentes de seguridad de la información para los administradores de sistemas y de seguridad, para los administradores de sistemas de información y los administradores de seguridad de cualquier organización (Bryant, 2008). La administración de incidentes consiste de 4 procesos:

- ✓ Planear y preparar: Para la gestión de incidentes de seguridad se requiere realizar una adecuada planeación y preparación para la respuesta a la materialización de estos incidentes.
- ✓ Uso: Esta es la implementación del plan de gestión de incidentes de seguridad. Se detecta, reporta, analiza, clasifica y se comunican los resultados de la investigación del incidente.
- ✓ Revisar: Se valida de nuevo el incidente, en caso de ser necesario, se definen las lecciones aprendidas, y se implementan mecanismos de mejora según las vulnerabilidades detectadas.
- ✓ Mejorar: El proceso de gestión de incidentes es un proceso iterativo, esto significa que está en constante mejora, tanto en sus normas como en su implementación.

En el 2011 la ISO cambia la naturaleza del documento, de reporte técnico a noma internacional, y que hace parte de la familia de normas de la ISO 27000. Esta norma queda definida como la ISO/EIC 27035: 2011 Gestión de incidentes de seguridad de la información, que define un enfoque estructurado y planificado para:

- ✓ Detectar, informar y evaluar los incidentes de seguridad de información.
- ✓ Responder a incidentes y gestionar incidentes de seguridad de la información

- ✓ Detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información.
- ✓ Mejorar continuamente la seguridad de la información y la gestión de incidentes, como resultado de la gestión de incidentes de seguridad de la información y las vulnerabilidades.

ISO/IEC 27005: La primera versión de la norma fue publicada el 4 de Junio de 2008. En ella se definen los lineamientos para la gestión del riesgo en la seguridad de la información, sin separarse de los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Previo a esta primera versión, posterior a la publicación de la ISO/IEC 27001:2005, BSI (British Standards Institution – Institución de Estándares Británica) publicó la norma BS7799-3:2006, enfocada en la gestión de riesgos de seguridad de los sistemas de información. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. (ISO 27000.ES, 2008).

1.6.2 Marco Conceptual

Evento: Un evento corresponde a una ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad (Garcia, 2013).

Incidente: Uno o más eventos de seguridad de la información no deseados o no esperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazan la seguridad de la información (Garcia, 2013).

ISO 27005: Norma que provee una guía para la gestión de riesgos para la seguridad de la información, alineada a la ISO 35000, de gestión de riesgos. (ISO/IEC 27005:2011 Information Technology -- Security Techniques -- Information Security Risk Management).

ISO 27035: Norma que provee una guía para la gestión de incidentes de seguridad en medianas y grandes organizaciones. (ISO/IEC 27035:2011 Information Technology -- Security Techniques -- Information Security Incident Management)

Proceso: Forma especificada de llevar a cabo una actividad o un proceso.

Política: Mecanismo orientado en forma ideológica a la toma de decisiones de un grupo u organización para alcanzar ciertos objetivos.

Riesgo: Es el potencial que dada una amenaza, esta explote una vulnerabilidad de un activo o de un grupo de activos y de esta forma cause daño en la organización.

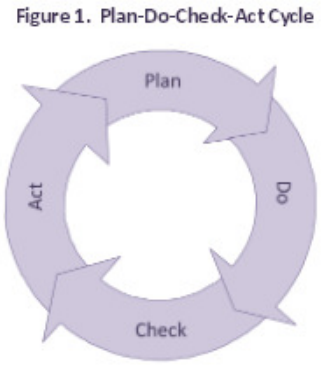
SIEM: (Security Information and Event Management – Gestión de Eventos y Seguridad de la Información) Es un enfoque de la gestión de la seguridad que pretende dar una visión holística de la seguridad de Tecnología de la Información de una organización. Un SIEM combina la gestión de la seguridad de la información (SIM – Security Information Management) y la gestión de eventos de

seguridad (SEM – Security Event Management) en un sistema de gestión integral de seguridad. (Rouse, 2012).

1.7 DISEÑO METODOLÓGICO

1.7.1 Metodología PHVA

Figura 1. Ciclo PHVA



Fuente [1]

El ciclo PHVA fue desarrollado en 1920 por Walter Shewhart y popularizado por Edwars Deming, por eso es también llamado el ciclo de Deming. El enfoque de este ciclo es establecer y gestionar un sistema de gestión en cualquier nivel de la organización, de tal forma que el proceso donde se implemente sea sostenible y se encuentre en mejora continua. La implementación del ciclo PHVA en cualquier sistema de gestión se basa en 4 fases (Universidad de Washington, 2011):

- ✓ Planificación (Plan): Identificar primero cuál es el problema. El uso de herramientas como los diagramas de Causa y Efecto o los 5 (cinco) porqués ayuda a la identificación del problema raíz. Los resultados de estas

[1] UNIVERSIDAD DE WASHINGTON. Plan – Do – Check - Act (PDCA). [En línea]. WASHINGTON: UNIVERSIDAD DE WASHINGTON. 2011. Disponible en: https://depts.washington.edu/oei/resources/toolsTemplates/plan_do_check_act.pdf

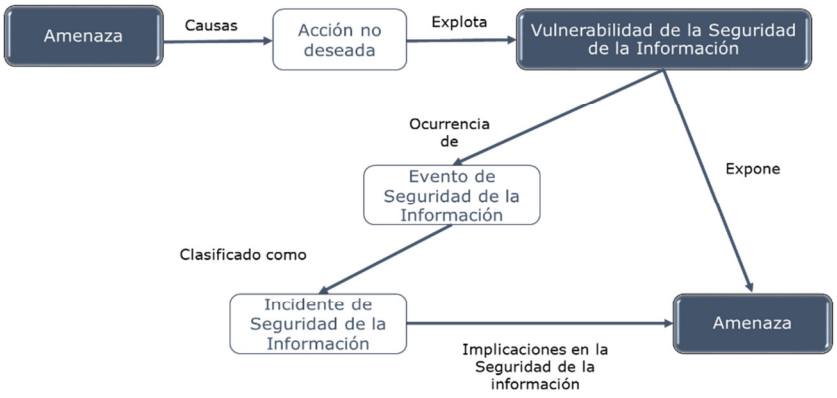
herramientas sirven de insumo para diseñar un mapa del proceso, con el fin de atacar el problema.

- ✓ Hacer (Do): Esta fase involucra, inicialmente la reunión de posibles soluciones al problema y posterior, realizar un análisis de estas soluciones para seleccionar aquella que más se adapte a las necesidades y recursos de la organización, y por último desarrollar programas piloto para implementar la solución seleccionada. Esta fase no es explícitamente llevar a producción la solución, en esta fase se "intenta" y se prueba o se realiza test de lo propuesto.
- ✓ Verificar (Check): Se realiza la medición de la ejecución del piloto implementado en la fase de Hacer. Se recogen y analizan los resultados de ese piloto, con el fin de establecer, de ser necesario, mejoras en el proceso y de esta forma definir el alcance y las áreas de implementación. Es posible repetir la fase Hacer, posterior al análisis de los resultados.
- ✓ Actuar (Act): Por último, posterior a la implementación completa del proceso, el ciclo de Deming, es un ciclo de mejora continua, lo que significa que se hace necesario, volver a la primera fase Planificación, y estar en constante planificación, ejecución y validación de mejoras el proceso.

1.7.2 ISO/IEC 27035. Norma que especifica los lineamientos para una efectiva gestión de incidentes de seguridad, establecida como tal en el año de 2011 por la ISO. En un SGSI (Sistema de Gestión de Seguridad de la Información) la implementación de políticas y controles no garantizan una total protección de la información y de los sistemas que la procesan. Posterior a su despliegue se encuentra un riesgo residual, el cual se puede materializar por la existencia de alguna vulnerabilidad por pequeña que sea y donde los controles implementados son inefectivos. Para estos tipos de casos, es necesario implementar un sistema de administración de aquellos incidentes de seguridad que puedan hacer realidad este riesgo residual. La gestión se encuentra organizada en 5 fases (ICONTEC, 2011):

- ✓ Planear y Preparar: En esta fase de planea y se define la política de gestión de incidentes de seguridad, alineada a la política de seguridad de la información y de análisis de riesgos, además de concientizar a la gerencia. Se debe definir un equipo de respuesta a incidentes de seguridad de la información
- ✓ Detección y Reporte: Es la detección y el registro o reporte del incidente, donde se realiza la recolección asociada al incidente. Es la primera fase del proceso operacional de la gestión.
- ✓ Evaluación y Decisión: Es la evaluación de la información recolectada y un análisis para validar si el evento reportado es un incidente de seguridad.
- ✓ Respuesta: Respuesta al incidente de seguridad, con el análisis forense si fue necesario realizarlo, dependiendo de la decisión tomada en la fase de Evaluación y Decisión, y la respectiva entrega del reporte a las personas involucradas.
- ✓ Lecciones Aprendidas: Se identifican las lecciones aprendidas del incidente de seguridad y la mejora del proceso o del SGSI. De ser necesario validar el proceso de gestión de incidentes para implementar mejoras, debido a la lección aprendida del resultado del incidente de seguridad.

Figura 2. Estructura ISO 27035



Fuente [2]

[2] El Autor.

1.7.3 ISO/IEC 27005. La ISO 27005, se definió para la administración de riesgos informáticos, y se encuentra alineada a la ISO 31000, la cual se desarrolló para la administración de riesgos en cualquier área de una organización y como otras normas ISO, tiene como metodología de implementación y mejora continua PHVA (Planear-Hacer-Verificar-Actuar). Las etapas de la ISO 27005 son (Ramirez & Ortiz, 2011):

- ✓ Establecimiento de plan de comunicación interno y externo.
- ✓ Definición del contexto organizacional interno y externo.
- ✓ Valoración de riesgos tecnológicos.
- ✓ Tratamiento de riesgos tecnológicos.
- ✓ Monitoreo y mejora continua del proceso de gestión.

A continuación se presenta una imagen de la alineación entre el ciclo de Deming PHVA, ISO 27035 y la ISO 27005:

Figura 3. PHVA – ISO 27035 – ISO 27005

<table>
<tr><th>PHVA</th><th>ISO 27035</th><th colspan="3">ISO 27005</th></tr>
<tr><td rowspan="8">PLANEAR</td><td>Política de Gestion de Incidentes</td><td colspan="2">Definición plan de gestión de riesgos</td><td rowspan="13">Proceso de Gestión del Riesgo</td></tr>
<tr><td>Políticas de seguridad de la información y gestión de riesgos actualizadas a nivel corporativo, sistemas, servicio y red.</td><td colspan="2">Establecimiento del contexto</td></tr>
<tr><td>Establecimiento del ISIRT (Equipo de respuesta a incidentes del Seguridad de la Información).</td><td>Identificación del riesgo</td><td rowspan="3">Valoración del Riesgo</td></tr>
<tr><td>Concientización sobre gestión de incidentes de seguridad de la información.</td><td>Estimación del riesgo</td></tr>
<tr><td rowspan="3">Esquema de pruebas de la gestión de incidentes de seguridad de la información.</td><td>Evaluación del riesgo</td></tr>
<tr><td colspan="2">Plan de tratamiento del riesgo</td></tr>
<tr><td>Aceptación del riesgo</td><td></td></tr>
<tr><td rowspan="2">HACER</td><td>Detección y Reporte del Evento de seguridad de la información</td><td colspan="2">Implementar el plan de tratamiento</td></tr>
<tr><td>Evaluación de eventos de seguridad de la información y decisión sobre si es un incidente de seguridad de la información.</td><td colspan="2">Implementar el plan de divulgación del riesgo</td></tr>
<tr><td>VERIFICAR</td><td>Respuesta del incidente de seguridad según decisión de la evaluación de los eventos</td><td colspan="2">Monitoreo y revisión del Riesgo</td></tr>
<tr><td rowspan="4">ACTUAR</td><td>Identificación de lecciones aprendidas.</td><td colspan="2" rowspan="4">Mantener y mejorar el proceso de gestión del riesgo</td></tr>
<tr><td>Identificación y mejora de seguridad de la información.</td></tr>
<tr><td>Identificación y mejora de la evaluación de riesgos de seguridad de la información y resultados de la revisión de la dirección.</td></tr>
<tr><td>Identificación y mejora del esquema de gestión de incidentes de seguridad de la información.</td></tr>
</table>

Fuente[3]

[3] El Autor.

1.7.4 Técnicas de Recolección. A continuación se presentan las técnicas de recolección de información que se implementaran en el desarrollo del proyecto:

Lluvia de ideas. Es técnica se utilizará para la definición de las herramientas, las políticas de incidentes, de riesgos, y la metodología de cada uno de estos procesos, teniendo en cuenta estándares y normas definidas en la industria de la seguridad. Esta técnica es efectiva cuando se tienen diferentes puntos de vista sobre varios temas, y/o se tienen varias fuentes para abarcar un mismo tema.

Mapas Conceptuales. Estos mapas se utilizarán para definir de forma global los procedimientos y comprender los flujos del seguimiento a los incidentes de seguridad tratados bajo la implementación del presente modelo. Con los mapas conceptuales se podrá comprender de mejor forma la organización que se le va a dar al modelo, y a la interacción con cada uno de los procesos que se vayan a definir.

Reuniones. Bajo el seguimiento de reuniones periódicas no superiores a 15 días se hará validación de la evolución del proyecto, se validarán si es necesario hacer redefiniciones del proyecto a pequeña escala de tal forma que no afecten la consecución del mismo, y se harán realimentaciones tanto sobre los avances de los proyectos como de la información que provea la entidad financiera.

Adicional a las anteriores técnicas, se tiene contemplado de ser necesarios, envío de correos electrónicos como medio alternativo para compartir la información y/o sesiones de mensajería y conversación por medio de Skype, cuando lo amerite.

1.8 RECURSOS

1.8.1 Recursos Tecnológicos. Para el desarrollo del proyecto se utilizará un equipo cómputo de propiedad del autor del proyecto:

- ✓ Portátil Toshiba de 15’.
- ✓ Disco Duro de 1 TB
- ✓ Memoria RAM de 8GB
- ✓ Puertos USB 2.0 y 3.0

- ✓ Unidad de DVD R/RW.
- ✓ Sistema Operativo y aplicaciones utilitarias.
- ✓ Paquete de ofimática para realizar las respectivas tareas de consolidación de información y diseño de los procedimientos y políticas necesarias.

Cabe adicionar que la plataforma SIEM que la Entidad Financiera tiene implementada en sus sistemas tecnológicos también se cuenta como un recurso tecnológico. El SIEM es Nitrosecurity de la empresa McAfee.

1.8.2 Recursos Humanos. El proyecto será desarrollado por el estudiante Yesid Alberto Tibaquira Cortes de la Universidad Nacional Abierta y a Distancia, del post-grado Especialización en Seguridad Informática y el Coordinador de Seguridad Informática y de la Información de la Entidad Financiera, quién bajo acuerdo de confidencialidad suministrará la información necesaria para la implementación del proyecto.

1.8.3 Recursos Financieros. El presupuesto inicial que tiene la compañía para el desarrollo del proyecto es de $ 30.000.000 (Treinta millones de pesos), teniendo en cuenta que el proyecto se desarrollará en un tiempo que oscila entre los 3 a 4 meses. El stakeholder del proyecto por parte de la Entidad, inicialmente validó el perfil de la persona que contratada por estos 4 meses, que mínimo requería que tuviera una certificación en temas de seguridad como CISSP (Certified Information Systems Security Professional) de (ISC)[4], CISM (Certified Information Security Manager) o CRISC (Certified in Risk and Information Systems Control) de ISACA [5]. El profesional con este perfil indicaba que cobraba de 7 a 8 millones de pesos mensuales para la implementación del proyecto en mención, lo que máximo en 4

[4] (ISC)[2]. CISSP® - Certified Information Systems Security Professional [en línea]. Clearwater: 2015. Disponible en: https://www.isc2.org/CISSP/Default.aspx

[5] ISACA [en línea]. ISACA Certification: IT Audit, Security, Governance and Risk. Rolling Meadows: 2015. Disponible en: https://www.isaca.org/Pages/default.aspx.

meses, tendría un costo total entre $28.000.000 a $32.000.000 (veintiocho a treinta y dos millones de pesos), valores cercanos al presupuesto inicial destinado por la Entidad para el desarrollo del proyecto.

Como se puede visualizar en la siguiente tabla, la suma total de los costos necesarios para este proyecto en total, es casi el 30% del presupuesto inicial definido, lo que brindaría una relación costo – beneficio, relativamente eficiente y efectiva.

Tabla 1. Presupuesto

Ítem	Descripción	Cantidad	Unitario	Proyectado Mes 1	Proyectado Mes 2	Proyectado Mes 3	Proyectado Mes 4	Total
Ingresos		**0**	**$ 30.000.000**	**$ -**	**$ -**	**$ -**	**$ -**	**$ 30.000.000**
Valor del proyecto	Valor del proyecto		$ 30.000.000					
Gastos de Personal				**$ 1.500.000**	**$1.500.000**	**$1.500.000**	**$1.500.000**	**$ 6.000.000**
Sueldo	Ingeniero con estudios en especialización - Medio tiempo	1	$ 1.500.000	$ 1.500.000	$ 1.500.000	$ 1.500.000	$ 1.500.000	$ 6.000.000
Gastos Generales				**$ 860.000**	**$ 860.000**	**$ 860.000**	**$ 860.000**	**$ 3.440.000**
Transporte	Transporte			$ 100.000	$ 100.000	$ 100.000	$ 100.000	$ 400.000
Servicios Técnicos				$ 500.000	$ 500.000	$ 500.000	$ 500.000	$ 2.000.000
Materiales y suministros	Papelería, fotocopias, etc.			$ 200.000	$ 200.000	$ 200.000	$ 200.000	$ 800.000
Servicios públicos	Luz, teléfono e internet			$ 60.000	$ 60.000	$ 60.000	$ 60.000	$ 240.000
Inversión				**$ 1.800.000**	**$ -**	**$ -**	**$ -**	**$ 1.800.000**
Equipo Portátil	Estación de trabajo	1	$ 1.800.000	$ 1.800.000	$ -	$ -	$ -	$ 1.800.000
GRAN TOTAL								**$ 11.240.000**

Fuente [6]

[6] El Autor.

1.9 CRONOGRAMA

CRONOGRAMA								
Actividades	**1ra Quincena Enero 2015**	**2da Quincena Enero 2015**	**1ra Quincena Febrero 2015**	**2da Quincena Febrero 2015**	**1ra Quincena Marzo 2015**	**2da Quincena Marzo 2015**	**1ra Quincena Abril 2015**	**2da Quincena Abril 2015**
1. Planear								
1.1 Levantamiento de información proceso actual de gestión de incidentes	X							
1.2 Análisis de la información recolectada	X	X						
1.3 Validar el proceso actual de Análisis de Riesgos VS Incidentes de Seguridad	X	X						
2. Hacer								
2.1 Diseñar la política se gestión de incidentes según necesidades de la entidad			X					
2.2 Diseñar el o los procedimientos que respalden la operación de la política				X				
2.3 Empalmar la política y los procedimientos con la gestión de riesgos tecnológicos				X				

2.4 Ajuste de los procedimientos según implementación de la gestión de riesgos tecnológicos.					X			
3. Verificar								
3.1 Divulgación de la política y los procedimientos al área de seguridad de la información						X		
3.2 Análisis de la implementación de los procedimientos en un área de la entidad.							X	
4. Actuar								
4.1 Divulgación oficial de la política y los procedimientos que respalden la gestión de incidentes de seguridad.								X
4.2 Mejora continua del proceso con auditorías periódicas del mismo								X

Fuente[7]

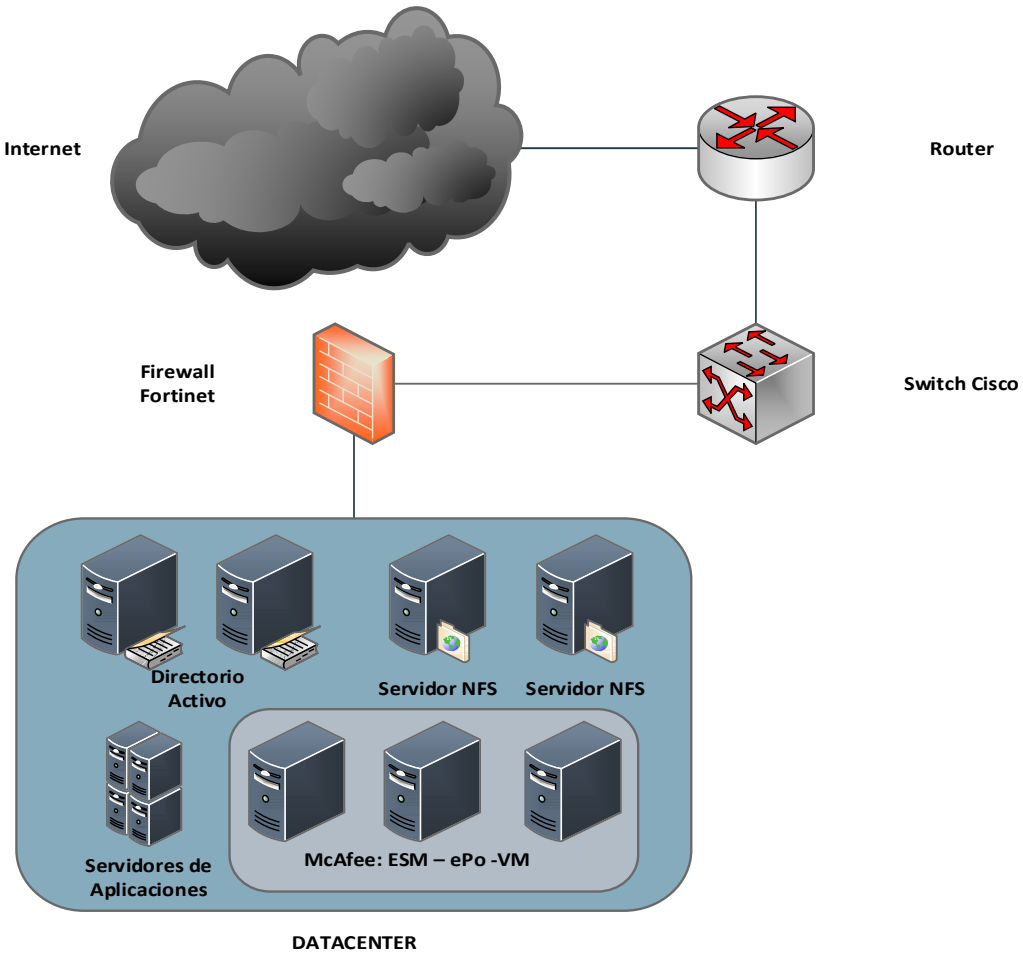
[7] El Autor.

2 SITUACIÓN ACTUAL

2.1 PLATAFORMA TECNOLÓGICA

La Entidad Financiera ha definido la plataforma tecnológica que está cubierta por la implementación del SIEM. La siguiente figura permite visualizar de una forma general la red física y lógica de la plataforma.

Figura 4. Diagrama de Red Actual



Fuente [8]

[8] El Autor.

2.2 ANÁLISIS DE LOS COMPONENTES TECNOLÓGICOS

La identificación de la plataforma tecnológica que hace parte del alcance de la implementación del SIEM, se realizó con base en definición previa de los sistemas críticos de la entidad (incluyendo procesos) y posteriormente seleccionando los recursos tecnológicos que soportaban estos sistemas. En segunda medida, se tuvo en cuenta los aspectos legales que serían apalancados por la herramienta.

2.2.1 Dispositivos. Los dispositivos configurados en el SIEM soportan sistemas como, el Directorio Activo, el Firewall configurado para el Centro de Datos, los servidores y las consolas para la administración del Antivirus, Integrador de Productor McAfee (ePO) y el correlacionador de eventos, el servidor de archivos en red (NFS), el switch core del Centro de Datos, el controlador de redes inalámbricas, y, el aplicativo Guardium. En la siguiente tabla es posible identificar los dispositivos asociados a cada uno de estos sistemas:

Tabla 2. Dispositivos

Nombre del Dispositivo	Descripción	Fabricante
SRVBOGAD01	Directorio Activo de la Compañía	Windows
SRVBOGAD02	Directorio Activo de la Compañía	Windows
SRVBOGALO	Aplicación Aurolog	Windows
SRVBOGEPO	Aplicación para la integración de los productos de McAfee	McAfee
SRVBOGNFS	File Server de la compañía	Windows
COMBOGFW	Firewall DMZ de la compañía	Fortinet
SRVBOGGUA	Aplicativo Guardium	IBM
SRVBOGREG	Aplicaciones para las Regionales	Windows
SRVBOGTRA	Aplicación de Transferencia de Archivos (NFS)	Windows
COMBOGWLC	Controlador de la Red Inalámbrica	Cisco

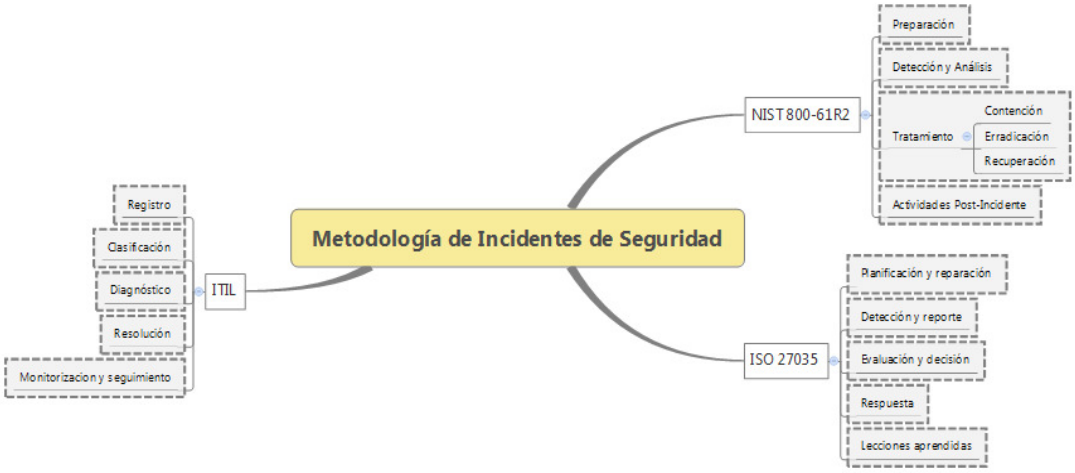
Fuente [9]

[9] El Autor.

2.3 INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de Seguridad de la Información es el área encargada de la recolección y posterior análisis de los eventos, según previa configuración realizada por el proveedor de la herramienta, ajustada a las necesidades de la entidad. Actualmente la recolección de los eventos se realiza inmediatamente en el momento que sucede en los dispositivos configurados, y el análisis de los mismos, se ejecuta teniendo como insumo el reporte mensual configurado para su envío automático al área y/o cuando se dispara una de las alarmas previamente definidas en la configuración de la herramienta. Para la definición de la metodología se tuvieron en cuenta 3 modelos, los cuales establecían las etapas que se deben implementar para la gestión de in incidente de seguridad. En la figura 5, se pueden evidenciar los modelos más implementados.

Figura 5. Metodologías Incidentes de Seguridad



Fuente [10]

[10] El Autor.

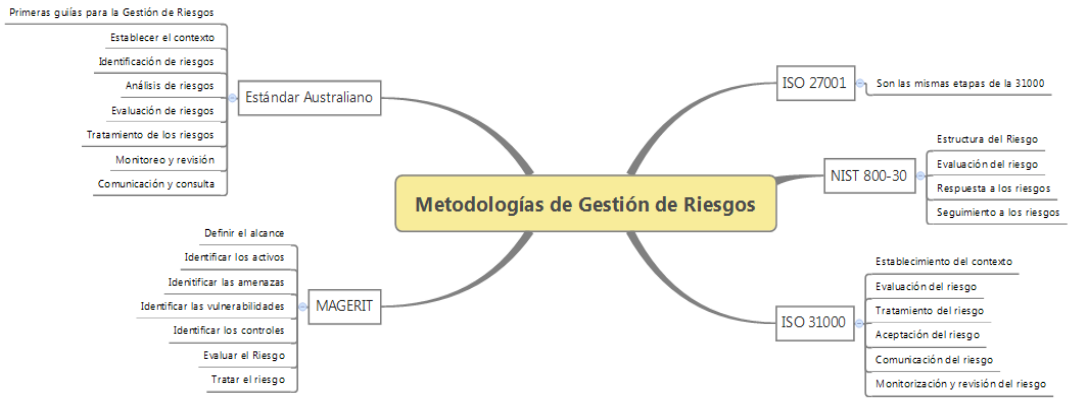
Se menciona ITIL (Information Technology Infrastructure Library - Biblioteca de Infraestructura de Tecnologías de Información) debido a que es un modelo de facto ampliamente implementado en la gestión de Incidentes, y es posible adaptarlo al contexto de seguridad.

2.4 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En el caso de la gestión de riesgos derivados de los incidentes de seguridad, la Dirección de Seguridad de la Información aún no ha definido un flujo o un proceso específico para su alineación. Sin embargo los riesgos tecnológicos son registrados dentro de la herramienta SIEM de McAfee **Enterprise Security Manager and Event Receiver**, la cual se encarga de la recopilación y valoración de los riesgos según los criterios definidos en la misma bajo la ISO 27001:2005. Se contemplaron varias metodologías de gestión de riesgos, como se puede evidenciar en la Figura 6, sin embargo debido a que la Entidad ha venido definiendo su modelo de seguridad de la información bajo la norma ISO 27001:2005, se necesitaba una norma la cual tuviera fácil adaptación a esta norma y que además fuera un soporte estable para todo el modo, por lo tanto se definió servirse de guía la norma ISO 27005:2008.

Actualmente los dos procesos, Gestión de Incidentes de Seguridad y Gestión de Riesgos, derivados de la herramienta implementada para la correlación de Eventos (SIEM por sus siglas) se encuentra, según el modelo de capacidad de procesos de COBIT 5 (ISACA, 2012), como un proceso ejecutado, el cual está implementado y está cumpliendo su propósito.

Figura 6. Metodologías de Gestión de Riesgos



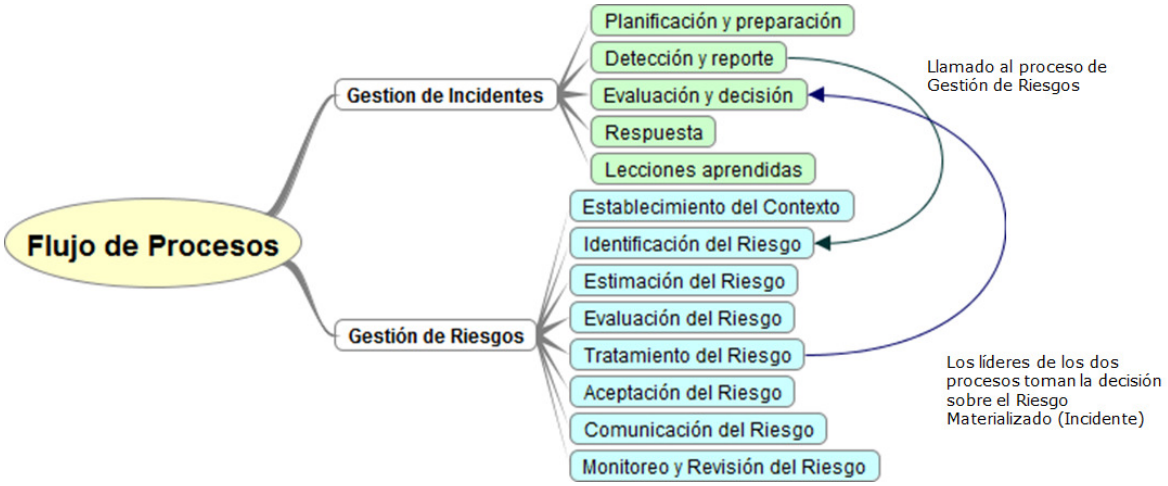
Fuente [11]

2.5 METODOLOGÍAS GESTIÓN RIESGOS E INCIDENTES DE SEGURIDAD

En la figura 7, se indica la relación que tienen de forma global las metodologías de gestión de riesgos e incidentes de seguridad de la información. Es válido aclarar que cuando se presenta un incidente (Fase 2: Detección y reporte), éste automáticamente se convierte en un riesgo materializado, por lo tanto se convierte en una entrada de la Fase 2, de la metodología de gestión de riesgos (Identificación del Riesgo). Durante la valoración del riesgo, se evalúa el riesgo según la metodología, además de realizar la evaluación del incidente, según los criterios que se definan para cada actividad. Así se trabaje en paralelo estas actividades, la definición de un plan de tratamiento del riesgo es un insumo para la decisión de la acción que se debe ejecutar según los resultados de la evaluación. Por último, en el proceso de gestión de incidentes, se da una respuesta al mismo, y se validan las lecciones aprendidas; por otro lado, se toma una decisión frente al riesgo ocasionado por el incidente, se comunica y se realiza un monitoreo sobre el mismo, según los criterios definidos para la gestión de riesgos.

[11] El Autor.

Figura 7. Interacción de los procesos. Riesgos e Incidentes



Fuente[12]

[12] El Autor.

3 METODOLOGÍA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

3.1 MODELO – ISO 27035:2011

Dentro de los objetivos que debe tener toda área de Seguridad de la Información es el definir controles y procedimientos para el manejo de los incidentes de seguridad de la información en la organización. Estas acciones desde el enfoque corporativo, promueven el cumplimiento de un objetivo principal: ayudar a contener y/o administrar el impacto de los incidentes para reducir costos directos o indirectos causados por los mismos.

La norma ISO 27035:2011 ha definido dentro del proceso de gestión de incidentes de seguridad de la información 5 fases para cumplir con ese objetivo principal (ICONTEC, 2011):

Figura 8. Fases de la Gestión de Incidentes

Fuente [13]

[13] El Autor.

En general, la primera se especifica todo los que se necesita para que el proceso se ejecute de manera éxitos, las otras cuatro fases son la ejecución del proceso.

3.2 DEFINICIÓN E IMPLEMENTACIÓN DE LA METODOLOGÍA

3.2.1 Fase 1: Planificación y preparación. Generalmente esta es la fase en que se especifica la mayor parte de la documentación del modelo. Para la entidad, específicamente para los incidentes seguridad derivados del SIEM, el modelo propuesto dentro de esta fase define:

- ✓ Política de Gestión de Incidentes de Seguridad de la Información (Ver Anexo A).
- ✓ Procedimiento y esquema del proceso de Gestión de Incidentes de Seguridad de la Información.
- ✓ Establecimiento del ISIRT (Information Security Incident Response Team – Equipo de respuesta a Incidentes de Seguridad de la Información)

3.2.2 Fase 2: Detección y reporte. El personal definido por la Dirección de Seguridad de la Información para la administración de la herramienta SIEM, es el responsable de detectar y reportar de manera inmediata a través de los canales o medios definidos al Gestor de Incidentes de Seguridad de la Información y al administrador o dueño del sistema o sistemas afectados, cualquier incidente de seguridad derivado de los eventos identificados en la herramienta que puedan impactar de forma negativa la integridad, confidencialidad y disponibilidad de los activos que se encuentran configurados en la misma. Además entre otras funciones tales como:

- ✓ Monitorear todos los eventos que puedan ser causales de incidentes de seguridad de la información.

- ✓ Recolectar la información necesaria sobre los eventos que produzcan incidentes de Seguridad de la Información.
- ✓ Gestionar (Detectar, reportar y tratar) las vulnerabilidades que se identifiquen sobre la infraestructura tecnológica del SIEM.
- ✓ Diligenciar el Formato de Detección del Incidente (Ver Anexo C)

3.2.3 Fase 3: Evaluación y decisión. Según la información contenida en el formato de reporte de Incidentes de Seguridad, el Gestor de incidentes, junto con el ISIRT, deben validar si el incidente reportado es un incidente de seguridad.

Identificación y Clasificación de Eventos de Seguridad

La entidad para este proceso ha definido una categorización de incidentes de seguridad que pueden ser identificados teniendo como fuente principal la herramienta SIEM y las alarmas que fueron configuradas en la misma. Esta categorización no es definitiva, pero sí son un primer paso para la definición de una base de conocimiento:

Tabla 3. Categorización de Incidentes

Categoría	Descripción	Ejemplo
Incidente de daño físico	La pérdida de seguridad de la información es causada por acciones físicas accidentales o deliberadas	Incendio, agua, electrostática, destrucción de equipos, destrucción de medios, tobo de equipos, pérdida de equipos, alteración de equipos, etc.
Incidente de fallas de infraestructura	La pérdida de seguridad de la información es causada por fallas en los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información	Fallas en la alimentación eléctrica, en las redes, en el aire acondicionado, en el suministro de agua, etc.
Incidente de falla técnica	La pérdida de seguridad de la información es causada por fallas en los sistemas de información o en instalaciones no técnicas relacionadas, al igual que problemas humanos no	Falla del hardware, mal funcionamiento del software, sobrecarga (saturación de la capacidad de los sistemas de información), etc.

	intencionales que dan como resultado la no disponibilidad o destrucción de los sistemas de Información	
Incidente de Malware	La pérdida de seguridad de la información es causada por programas maliciosos creados y divulgados en forma deliberada. Un programa malicioso se inserta en los sistemas de información para afectar la confidencialidad, la integridad o disponibilidad de los datos, las aplicaciones o sistemas operativos, y/o afectar la operación normal de los sistemas.	Virus informáticos, gusanos de red, troyanos, botnet, ataques combinados, páginas web con códigos maliciosos, APT (Advanced Persistence Threat – Amenazas Persistentes Avanzadas)
Incidente de Ataque Técnico	La pérdida de seguridad de la información es causada por el ataque a sistemas de información, a través de redes u otros medios técnicos, ya sea mediante el aprovechamiento de las vulnerabilidades de los sistemas de información en cuanto a configuraciones, protocolos o programas, o por la fuerza, lo que da como resultado un estado anormal de los sistemas de información, o daño potencial a las operaciones presentes en el sistema.	Escaneo de redes, aprovechamiento de vulnerabilidades, aprovechamiento de puertas traseras (backdoors), intento de ingreso, interferencia, denegación de servicio, etc.
Incidente de puesta en riesgo de la información	La pérdida de seguridad de la información es causada al poner en riesgo en forma accidental o deliberada la seguridad de la información, por ejemplo, en cuanto a confidencialidad, integridad y disponibilidad.	Interceptación, espionaje, divulgación, enmascaramiento, ingeniería social, phishing de redes, robo y/o pérdida de datos, alteración de datos, etc.
Otros Incidentes	No clasificados en algunas de las anteriores categorías.	N/A

Fuente [14]

[14] El Autor.

Evaluación de los Incidentes

El Gestor del Incidente de Seguridad de la Información evalúa la información asociada a los eventos reportados como incidentes, la analiza y define el alcance del incidente (Sistema de información, infraestructura tecnológica, infraestructura física) o la información misma procesada en estos sistemas. Durante la evaluación es necesario solicitar información como:

- ✓ En qué consiste el incidente de seguridad de la información, según los eventos identificados
- ✓ Identificación de los activos afectados (Sistemas de Información, Información, Procesos)
- ✓ Cómo fue causado, y qué o quién lo causó
- ✓ Fecha y hora de ocurrencia. Frecuencia de la ocurrencia.
- ✓ Impacto real del incidente sobre el negocio.
- ✓ Tratamiento temporal del incidente.

Es recomendable que esta información el Administrador de la Herramienta SIEM, la suministra a modo de relato o según los criterios que se hayan definido en el formato del reporte de Incidentes de Seguridad de la Información.
Posterior al análisis de la información, el Gestor del Incidente determina si es un incidente dentro del contexto de Seguridad de la Información, escalándolo posteriormente al ISIRT.

Priorización del Incidente

Esta etapa busca clasificar el incidente tomando en cuenta el impacto sobre los servicios y sistemas afectados y acordando la asignación de prioridad para todos los recursos necesarios para su contención y recuperación, incluyendo el personal adecuado para el tratamiento del incidente dentro del ISIRT.

Previo al tratamiento del incidente, es indispensable priorizar el incidente teniendo en cuenta los siguientes factores:

- ✓ Impacto al negocio: Incidentes contra los sistemas de TI que soportan las principales funcionalidades del core del negocio. El impacto no sólo debe ser tenido en cuenta en el instante actual, sino también en la probabilidad futura de la concurrencia del incidente.

- ✓ Impacto en la Información: El grado de afectación de la confidencialidad, integridad y disponibilidad de la información de la Entidad. La información que se procesa en los sistemas del alcance de este procedimiento, es sensible y confidencial para la Entidad, por lo cual cualquier incidente que afecte los criterios anteriormente nombrados es valorado como **Crítico**.

- ✓ Recuperación del incidente: El tamaño del incidente y los sistemas afectados (su infraestructura, redes y sistemas), determinará la cantidad de tiempo y recursos que deben ser destinados para la recuperación de ese incidente. Para aquellos casos donde no es posible la recuperación de un incidente, se pone a consideración del ISIRT, destinar recursos para la gestión prolongada del incidente, teniendo en cuenta que generalmente en estos tipos de incidentes, se asignan recursos para trabajar en asegurar y evitar la materialización de los incidentes en un futuro.

  El Equipo de Respuesta a Incidentes debe considerar el esfuerzo necesario para recuperar realmente del incidente y valorarlo contra el valor del esfuerzo de recuperación que se generará y los requerimientos asociados al manejo del incidente.

La combinación resultante del impacto funcional y del impacto de la información, determina el impacto del incidente.

La recuperación del incidente define las posibles respuestas que el ISIRT puede tomar en la gestión. Sin embargo la estimación de recursos y esfuerzos necesarios, no deja de ser un criterio a tener en cuenta para la priorización del incidente, junto con el impacto del incidente.

Para asignar una calificación de severidad para un incidente es necesario determinar por cada incidente, el impacto funcional actual y futuro del incidente si no es contenido inmediatamente (NIST - National Institute of Standards and Technology , 2012).

Tabla 4. Definiciones Clasificaciones de Impacto

Valor	Escala	Definición
0.25	Bajo	Efecto insignificante en sistemas o infraestructura critica de la Compañía. La organización puede proporcionar servicios críticos a los usuarios.
0.50	Medio	Mínimos efectos sobre Sistemas o infraestructura crítica y/o usuarios. La Compañía puede Proporcionar servicios críticos a los usuarios, pero ha perdido eficiencia.
0.75	Alto	Efecto significativo e inmediato sobre los sistemas o infraestructura crítica y usuarios. La Compañía ha perdido la capacidad de proporcionar un servicio crítico o un grupo de usuarios del sistema.
1.00	Crítico	Graves efectos sobre un gran número de sistemas, usuarios o infraestructura crítica para la Compañía. La Compañía no puede prestar u ofrecer algunos servicios considerados críticos, a los usuarios.

Fuente [15]

Posterior a la identificación del impacto, se debe asignar una criticidad de los sistemas o recursos involucrados en el incidente, de acuerdo a la siguiente tabla:

[15] El Autor.

Tabla 5. Definiciones de Criticidad

Valor	Escala	Definición
0.25	Bajo	Pequeño número de recursos tecnológicos
0.50	Medio	Sistema o sistemas, servicios o infraestructura considerados no críticos.
0.75	Alto	Sistemas, servicios o infraestructura critica para la Compañía.
1.00	Crítico	Sistema o Sistemas que son de misión crítica para los procesos de Negocio.

Fuente [16]

Para determinar el resultado total de la severidad para un incidente, la persona definida por el ISIRT para la priorización del incidente debe utilizar la siguiente fórmula:

Severidad general / **Score del Efecto =** Entero ((Valuación Actual del efecto * 2.5) + (
Valuación proyectada efecto * 2.5) + (Valuación criticidad del sistema * 5)).

Con el resultado se indica la valoración del incidente de la siguiente manera:

Tabla 6. Escala Impacto del Incidente

Rango	Escala	Tiempo de Respuesta
0.00 – 2.49	Mínimo	48 Horas
2.50 – 3.74	Bajo	24 Horas
3.75 – 4.99	Medio	8 Horas
5.00 – 7.49	Alto	3 Horas
7.50 – 10.00	Crítico	Inmediato

Fuente [17]

En este caso la Entidad ha definido que:

[16] El Autor.

[17] El Autor.

- ✓ Cualquier incidente de seguridad de la información que se detecte en los sistemas configurados en la herramienta SIEM, tiene como valoración de su impacto: Alto
- ✓ Cualquier incidente de seguridad de la información que se detecte en los sistemas configurados en la herramienta SIEM, tiene como valoración de su Criticidad: Alto
- ✓ Como resultado de las anteriores definiciones, se indica que cualquier incidente de seguridad de la información sobre los sistemas configurados en la herramienta SIEM, tienen finalmente un impacto **Crítico**, lo que indica que las acciones de recuperación frente a estos incidentes no deben tardar más de 3 horas.

3.2.4 Fase 4: Respuesta

Respuestas Inmediatas

Posterior a la evaluación y las decisiones tomadas por el ISIRT como resultado de la fase anterior, en esta fase y dependiendo de la valoración del incidente, el ISIRT debe definir un conjunto de actividades de forma casi inmediata a la detección del incidente, como:

- ✓ Identificar las acciones de respuesta inmediata para el tratamiento del incidente.
- ✓ Definir y documentar controles de emergencia según los resultados de la evaluación del incidente.
- ✓ Notificar los interesados (stakeholders) sobre los resultados de la evaluación del incidente y las acciones sugeridas para una pronta recuperación (controles de emergencia).
- ✓ Dependiendo del grado de afectación del incidente sobre los activos de información de la compañía, se tomaría la decisión de la conformación de

una sala de crisis, para darle prioridad al tratamiento del incidente, sin dejar de implementar las acciones d respuesta inmediata.

Durante la ejecución de las respuestas inmediatas, se debe tener en cuenta que en paralelo, es posible actualizar los resultados de la evaluación del incidente, producto de una continua realimentación según la investigación que se esté llevando a cabo, incluyendo la divulgación de estas actualizaciones al líder del ISIRT y a cada uno de los stakeholders. Esta actualización también debe incluir un estado del incidente, donde se indique si el incidente es recurrente, si se está tratando, si se encuentra bajo control o si definitivamente se ha solucionado.

En cada informe de la actualización del estado del incidente, el ISIRT y los stakeholders deben definir las estrategias necesarias para la contención del incidente según los resultados de cada evaluación. Este es un proceso cíclico hasta que el incidente se encuentre solucionado y/o bajo control, y posteriormente se definan las respuestas adicionales, si se considera necesario, y se identifiquen las lecciones aprendidas del incidente.

Erradicación y recuperación

Tan pronto las respuestas inmediatas han sido implementadas, se debe determinar la causa o las causas del incidente y su posterior erradicación.

La erradicación puede ser producto de la ausencia de instalación de un parche de seguridad sobre los sistemas afectados, algún desarrollo mal implementado sobre los sistemas, la detección de un ataque de denegación de servicio por la identificación de múltiples eventos ejecutados desde direcciones IP que se encuentran en la Watchlist de la herramienta SIEM.

Algunas actividades en esta fase incluyen:

- ✓ Determinar los signos y causa de incidentes
- ✓ Localizar la versión más reciente de copias de seguridad de los sistemas afectados.
- ✓ Removiendo la causa raíz. En el evento de infección de gusanos o virus, puede ser eliminado en el despliegue de parches de seguridad y software antivirus actualizado.
- ✓ Mejora de las defensas mediante la implementación de técnicas de protección.
- ✓ Realización de análisis de vulnerabilidad para encontrar nuevas vulnerabilidades introducidas por la causa raíz.

Se recomienda realizar las actividades de erradicación y recuperación por fases y por priorización, con el fin de ir evaluando y minimizando la causa raíz del incidente.

Es necesario hacer énfasis que todos los involucrados en la gestión (ISIRT y los administradores o dueños de cada sistema impactado) deben registrar cuidadosa y detalladamente todas las actividades realizadas para un análisis post-mortem del incidente. Toda esta información recopilada debe tener una cadena de custodia, ya que se considera confidencial para la Entidad, además de que la misma pueda ser comprobable y tenga su copia de respaldo.

Las medidas implementadas para el control del incidente deben ser monitoreadas, con el fin de validar su efectividad y servir de base de conocimiento para futuros incidentes.

3.2.5 Fase 5: Lecciones aprendidas. La última fase del proceso operativo de gestión de incidentes de seguridad se lleva a cabo cuando se tiene la certeza que el incidente ha sido solucionado o cerrado. Se tiene conocimiento del estado del incidente con la elaboración por parte del ISIRT de un reporte, donde se

identifique la causa o causas del incidente, las actividades realizadas, las medidas que fueron adoptadas y los resultados de la implementación de esas medidas.

El ISIRT completará cualquier documentación que no se hizo durante el incidente, además de aquella información que sea beneficiosa para el tratamiento de futuros incidentes.

Dentro de las actividades que se deben realizar son:

- ✓ Ejecución de un análisis forense (si así lo considera el ISIRT) sobre los sistemas impactados por el incidente.
- ✓ Identificación de las lecciones aprendidas y de las nuevas vulnerabilidades identificadas durante la evaluación y plan de respuestas del incidente.
- ✓ Validación de mejoras en la implementación de controles de seguridad de la información en los sistemas afectados.
- ✓ Identificar y valoración de los riesgos identificados según los resultados de la evaluación de los incidentes.
- ✓ Identificar mejoras en el proceso de gestión de incidentes de seguridad de la información
- ✓ Actualización de los incidentes de seguridad de la información gestionados para posteriores informes o insumos para otros procesos de la Dirección de Seguridad de la Información o el área que bajo justificación y demanda lo requiera.
- ✓ Comunicación de los resultados a los stakeholders de los sistemas afectados por el incidente, teniendo en cuenta que la clasificación de la información compartida es confidencial. Dentro de esta comunicación, el informe de los resultados debe responder preguntas como:
    - Exactamente, ¿Qué pasó, y cuantas veces?

- ¿Qué tan bien realizaron su trabajo el Personal y la Dirección de Seguridad de Seguridad de la Información en relación con el incidente?
- ¿Están documentadas las actividades ejecutadas para la erradicación y recuperación de los sistemas ante el incidente? ¿Fueron las actividades adecuadas?
- ¿Eran las medidas o acciones tomadas que podrían haber inhibido la recuperación?
- ¿Qué haría diferente el Personal y la Dirección la próxima vez que ocurra un incidente similar?
- ¿Qué acciones correctivas pueden prevenir incidentes similares en el futuro?
- ¿Qué precursores o indicadores deben ser observados para en el futuro para detectar incidentes similares?
- ¿Qué herramientas adicionales o recursos son necesarios para detectar, analizar y mitigar futuros incidentes?

4 METODOLOGÍA DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

4.1 MODELO – ISO 27005:2008

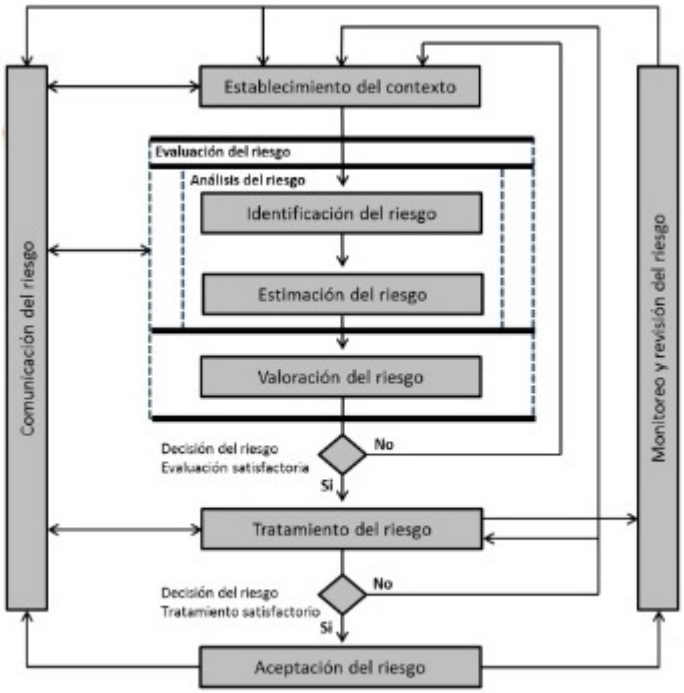
La identificación de un incidente en el contexto tecnológico, es en otras palabras la materialización de un riesgo. Y la materialización de un riesgo, sin importar si éste es reincidente o es identificado por primera vez, implica la definición e implementación de un procedimiento de gestión de riesgos en el contexto tecnológico, para este caso. El objetivo principal de una gestión de riesgos es la identificación de las necesidades de una organización en el cumplimiento de los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI por sus siglas).

El proceso de gestión de riesgos en todo departamento de Seguridad de la Información y en toda organización contribuye con:

- ✓ La identificación de los riesgos
- ✓ Valoración de los riesgos de acuerdo a su probabilidad e impacto en la organización.
- ✓ Definición de la priorización de los planes de acción o tratamiento del riesgo.
- ✓ Participación de los interesados (stakeholders) en la toma de decisiones sobre la gestión del riesgo.
- ✓ Eficacia en el monitoreo y cumplimiento de los planes de acción definidos.

Para realizar esta contribución, es necesario implementar una metodología la cual cubra de principio a fin la gestión del riesgo, en este caso, sobre los incidentes de seguridad derivados de la herramienta SIEM de la entidad. La metodología seleccionada se basa en Norma ISO 27005:2008 (ICONTEC, 2009). La metodología o el modelo sugerido por la norma se visualizan en la siguiente imagen:

Figura 9. Proceso de Gestión del Riesgo en la Seguridad de la Información



Fuente [18]

Como se puede visualizar el proceso es iterativo para las actividades de valoración y tratamiento del riesgo. De forma general, inicialmente se define el contexto, posterior se realiza la identificación del riesgo (esto incluye la identificación de los activos), luego se realiza una estimación del riesgo, si se tiene información suficiente, se pasa al tratamiento del riesgo, de lo contrario se realiza una valoración o evaluación del riesgo. Si la evaluación del riesgo no es suficiente se realiza otra iteración, hasta que se contenga la información necesaria para los planes de tratamiento; finalizados los planes de tratamiento, los cuales son monitoreados durante su implementación, se busca conseguir que la valoración del riesgo se encuentre dentro de los niveles de aceptación del mismo. Cada una

[18] Urbina, R. (2012). Metodología para relacionar la efectividad del sistema de gestión de la seguridad de la información con los elementos del negocio. Universidad Diego Portales. Recuperado de http://image.slidesharecdn.com/tesisrurbinaabril2012v3presentacionpb-130131075945-phpapp02/95/tesis-r-urbinaabril2012v3presentacionpb-26-638.jpg?cb=1359640973

de las actividades debe ser reportada a los directores y stakeholders del contexto definido en el primer paso del proceso.

4.2 DEFINICIÓN E IMPLEMENTACIÓN DE LA METODOLOGÍA

4.2.1 Establecimiento del Contexto. El diseño y la implementación del modelo se encuentran asociados a la Política de Gestión de Riesgos de TI – Incidentes de Seguridad (ver Anexo B).

Alcance

Gestión de Riesgos sobre los incidentes derivados de la herramienta SIEM, implementada por la Entidad. Esto incluye, la información que procesan los sistemas configurados en el SIEM, la infraestructura tecnológica donde se encuentra implementada la herramienta y la infraestructura de cada sistema configurado.

Criterios de Evaluación del Riesgo

La Dirección de Seguridad de la Información ha definido los criterios de la evaluación de los Riesgos, estos se encuentran alineados con las definiciones establecidas en la gestión del riesgo operativo de la Entidad:

Tabla 7. Escala de Valoración del Riesgo

Valoración	Definición
Riesgo Extremo	Se estima que este nivel de riesgo supera el Nivel de Aceptación de la Entidad. Su nivel es considerable teniendo en cuenta la frecuencia de materialización del riesgo y el impacto generado. Para los riesgos ubicados en este nivel, se debe generar una respuesta o planes de acción inmediatos.

Riesgo Crítico	Es un riesgo elevado y requiere mitigación dentro de límites de tiempo determinados (mediano plazo), aunque se encuentre de los niveles de aceptación de la Entidad.
Riesgo Tolerable	Se considera un nivel de riesgo normal con el que la Entidad puede coexistir. Para los riesgos ubicados en este nivel, no se descartan acciones de mejora en un tiempo discrecional y definido por la Entidad; con el fin de ubicarlos en un nivel de severidad menor.
Riesgo Aceptable	Indica un nivel de riesgo, en donde la relación de impacto y probabilidad es muy baja y pueden ser gestionados con procedimientos rutinarios.

Fuente [19]

Criterios de probabilidad

La probabilidad se estima de la frecuencia de ocurrencia de un riesgo en un periodo específico. La escala de probabilidad definido por la Entidad se relaciona en la siguiente tabla:

Tabla 8. Escala de Probabilidad del Riesgo

Nivel	Criterio cualitativo	Descripción	Frecuencia
1	Remota	Muy baja probabilidad de ocurrencia – El evento puede ocurrir sólo bajo circunstancias excepcionales.	1 vez por año
2	Baja	Limitada probabilidad de ocurrencia – El evento puede ocurrir muy esporádicamente.	1 vez por semestre
3	Moderada	Mediana probabilidad de ocurrencia – El evento ocurrirá en algún momento.	Entre 2 y 5 por trimestre
4	Alta	Significativa probabilidad	Entre 6 y 12

[19] El Autor.

		de ocurrencia – El evento ocurrirá casi en cualquier circunstancia.	por mes
5	Muy Alta	Muy alta probabilidad de ocurrencia – Se espera la ocurrencia del evento en la mayoría de los casos.	Más de 12 veces por mes

Fuente [20]

Criterios de Impacto

Los criterios de impacto se definen en función de la afectación de la confidencialidad, integridad y disponibilidad de la información, en caso de la materialización del riesgo:

Tabla 9. Escala de Impacto del Riesgo

Nivel	Criterio cualitativo	Descripción
1	Bajo	No hay afectación en la confidencialidad, integridad y disponibilidad de la información, por ser información pública de la Entidad
2	Menor	Afectación en la confidencialidad, integridad y disponibilidad de la información pública de la Entidad
3	Medio	Afectación en la confidencialidad, integridad y/o disponibilidad de la información de uso interno de la Entidad o de terceros
4	Mayor	Afectación en la confidencialidad, integridad y/o disponibilidad de la información privada de la entidad o de terceros, sin implicaciones legales o de carácter reputacional
5	Crítico	Afectación en la confidencialidad, integridad y/o disponibilidad de la información privada de la Entidad o de terceros, con implicaciones legales o de carácter reputacional

Fuente [21]

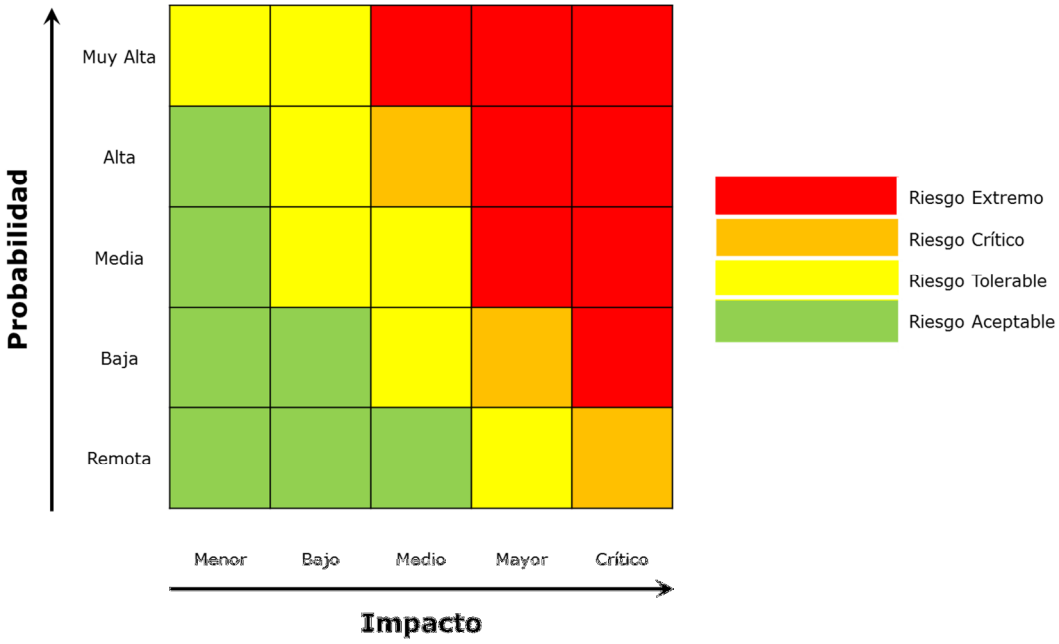
[20] El Autor.

[21] El Autor.

Mapa de Calor

Con base en las anteriores definiciones de la escala de probabilidad y de impacto, se define el mapa de calor para la Entidad, el cual permite identificar de forma visual la evaluación o valoración del riesgo según su impacto y su probabilidad, y de esta manera identificar el perfil del riesgo de los incidentes de seguridad procedentes de la herramienta SIEM.

Figura 10. Mapa de Calor



Fuente [22]

Criterios de aceptación del riesgo

El nivel de aceptación de riesgos de la Entidad, corresponde a los riesgos que posterior a su evaluación se encuentran ubicados en las zonas de Riesgo Tolerable y Aceptable.

[22] El Autor.

Los riesgos que no se encuentren en el nivel de aceptación de riesgos de la Entidad, deben definir un plan de tratamiento a corto plazo (6 meses) y mediano plazo (un año), para Riesgo Extremo y Riesgo Crítico, respectivamente.

4.2.2 Identificación del Riesgo. El resultado de esta fase es el listado de riesgos de seguridad de la Información provenientes de los incidentes que son identificados en la herramienta SIEM de la Entidad. Previo a la identificación de los riesgos se deben definir los activos sobre los cuales se va a realizar la gestión de riesgos y valorarlos de acuerdo a los criterios de confidencialidad, integridad y disponibilidad de la información que procesan.

Identificación de los activos

Los activos a valorar son todos aquellos servicios y/o componentes tecnológicos configurados en la herramienta SIEM. Para la valoración de cada activo se deben tener en cuenta los siguientes criterios de confidencialidad, integridad y disponibilidad de la información:

Tabla 10. Criterios de Valoración de Activos

Criterio	Confidencialidad	Integridad	Disponibilidad
Alto	Administra o procesa información confidencial y su uso inadecuado puede generar graves consecuencias para la entidad (demandas, pérdidas económicas, de reputación o imagen, etc.)	La información que administra o procesa apoya la toma de decisiones estratégicas de la entidad. No se admiten errores, los errores deben ser solucionados de inmediato.	Apoya los procesos críticos de la entidad y se requiere de una recuperación inmediata en caso de falla.
Medio	Administra o procesa información interna y su uso inadecuado puede generar medianas consecuencias para la entidad (Reclamaciones de las áreas que soporta).	La información que administra o procesa apoya la toma de decisiones de las áreas de la entidad. Permite una brecha en los errores de la información. Los errores pueden ser solucionados	Apoya los procesos no críticos de la entidad y permite su recuperación en un tiempo no mayor a 2 días.

		a corto plazo.	
Bajo	El activo administra o procesa información pública y su divulgación no le genera consecuencias negativas a la entidad.	La información que administra o procesa apoya la toma de decisiones de las áreas de la compañía. Permite una brecha en los errores de la información. Los errores pueden ser solucionados a mediano plazo.	Apoya los procesos no críticos de la entidad y permite su recuperación en un tiempo superior a 2 días.

Fuente [23]

La valoración de los activos se realiza en el formato definido para la identificación y valoración de activos y riesgos, en la hoja *ACTIVOS* del formato: *FSI-021 Formato Matriz de Riesgos de TI*

Identificación de los riesgos

Posterior a la valoración de los activos, la identificación de los riesgos se basa en los incidentes que son resultado de la herramienta SIEM. Todo incidente resultante, en primera instancia, se considera un incidente de seguridad de la información, y debido a su presencia tiene como consecuencia la materialización de un riesgo que es identificado de forma post-mortem.

Para la identificación de los riesgos, se deben tener en cuenta las vulnerabilidades asociadas a los activos identificados y con base en la experiencia de Analista de Riesgos, se deben definir e implementar los controles necesarios para el tratamiento del riesgo, según los resultados de la evaluación.

[23] El Autor.

Para esta actividad se ha definido un catálogo de riesgos, junto con sus vulnerabilidades el cual se puede encontrar en *CSI-010 Catalogo de Riesgos y Vulnerabilidades de SI*.

4.2.3 Estimación del Riesgo. Para la estimación del riesgo se debe definir una metodología, la cual presente como resultado la lista de riesgos con su valoración y/o severidad, teniendo en cuenta la criticidad del activo de información y los criterios para la valoración del riesgo.

Generalmente se tienen 2 metodologías para la estimación del riesgo: Cualitativa y cuantitativa. La metodología que en su uso es más frecuente es la primera, la cual se basa en la definición de una escala descriptiva de atributos que califican el impacto y la probabilidad del riesgo.

La metodología cuantitativa radica en el uso de una escala numérica para la calificación del impacto y de la probabilidad. Para este caso, se definió utilizar la estimación cualitativa, como se puede identificar en la *Tabla 8. Escala de Probabilidad del Riesgo* y la *Tabla 9. Escala de Impacto del Ries*go, en el numeral 4.2.1.

4.2.4 Evaluación del Riesgo. En esta fase se evalúa el riesgo según la valoración de los activos, la valoración en cuento a impacto y probabilidad de los riesgos identificados en el numeral 4.2.2, durante la implementación del proceso de riesgos, basándose en el modelo definido para la estimación del riesgo (Cualitativo). Para esta evaluación también se deben tener en cuenta los controles que se tienen implementados con miras a la reducción de la valoración del riesgo.

El formato donde se realizará esta evaluación es el mismo donde se realizó previamente la identificación y valoración de los activos en la hoja *RIESGO* del formato: *FSI-010 Formato Matriz de Riesgos de TI*. En este formato para la evaluación de los riesgos se realizan los siguientes pasos:

1. Identificación del riesgo y de la vulnerabilidad asociada ver el Catálogo: *CSI-010 Catalogo de Riesgos y Vulnerabilidades de SI*.
2. Identificación de los controles implementados para el tratamiento del riesgo.
3. Valoración de la probabilidad y el impacto del riesgo según la metodología de estimación definida. El resultado de este paso es la valoración del riesgo según la *Tabla 7. Escala de Valoración del Riesgo*, definida en el numeral 4.2.1.

4.2.5 Tratamiento del Riesgo. Para los riesgos que como resultado de su evaluación se encuentren valorados como *Riesgo Extremo* o *Riesgo Crítico*, debe definirse obligatoriamente un plan de tratamiento. Para aquellos *Riesgos Extremos*, este plan de tratamiento debe ser definido e implementado a corto plazo (6 meses, máximo); y, para los *Riesgos Críticos*, el plazo se encuentra entre 6 meses y máximo 1 año.

Estos planes tienen como objetivo realizar un tratamiento de los riesgos según las siguientes opciones:

- ✓ Reducción del Riesgo (Mitigación): Implementación de controles los cuales minimizan la frecuencia de la probabilidad y/o reducen el impacto del riesgo. El plan se define con acompañamiento del Analista de Riesgos de la Dirección de Seguridad de la Información y es implementado por el área responsable y/o dueño del sistema donde se identificó el riesgo.
- ✓ Retención del Riesgo (Aceptación): Los riesgos son aceptados, de forma objetiva y con conocimiento de las áreas responsables del sistema o activo, donde se identificó el riesgo. Esta aceptación debe satisfacer las políticas de la Entidad y debe basarse en los criterios de aceptación de la misma. Para el caso de los riesgos en el nivel *Riesgo Extremo*, no deberían ser aceptados, sin embargo, si la Vicepresidencia de Tecnología de la Información, que es dueña de los activos que se encuentran configurados en el SIEM, decide aceptar el riesgo, debe quedar en el informe de la

Gestión de Riesgos (*Ver Anexo D Informe de Gestión de Riesgos*) esta decisión, y la evidencia de que el Vicepresidente conoce y acepta la misma.

- ✓ Evitación del Riesgo: Es la decisión de no implementar la actividad o la acción la cual es causa del riesgo. Para los riesgos que provienen de los incidentes de seguridad, esta opción de tratamiento se estimaría que es poco útil, debido a la materialización del riesgo. Sin embargo, para evitar la recurrencia del incidente, es posible que la Vicepresidencia de TI, en cabeza, junto con el área dueña del sistema impactado y la Dirección de Seguridad, decida dejar de ejecutar aquellas actividades las cuales estén provocando el riesgo.
- ✓ Transferencia del Riesgo: Para el caso que el riesgo provenga de alguno de los proveedores o fabricantes de los sistemas configurados en el SIEM. En este caso el riesgo debe ser transferido al proveedor o fabricante. Esto indica que es posible que el proveedor requiera realizar un análisis de riesgos según sus políticas, lo que podría generar la aparición de nuevos riesgos o la alteración en la valoración de los mismos. Sin embargo se debe definir en conjunto con el proveedor las acciones necesarias para el tratamiento del riesgo.

Independientemente de la opción seleccionada para el tratamiento del riesgo, se deben indicar las acciones necesarias para implementar el plan. Estas acciones deben quedar registradas en el *FSI-010 Formato Matriz de Riesgos de TI*, en la hoja de *TRATAMIENTO*, asociado al *Riesgo Extremo* o *Riesgo Crítico* identificado.

4.2.6 Aceptación del Riesgo. Para los riesgos que se encuentren valorados como *Riesgo Tolerable* o *Riesgo Aceptable,* se recomienda definir planes de tratamiento a largo plazo (a partir de un año en adelante). El criterio de aceptación de estos riesgos debe quedar en el informe de Gestión de Riesgos según formato en el *Anexo D Informe de Gestión de Riesgos*.

4.2.7 Comunicación del Riesgo. El proceso de comunicación es transversal a todas las anteriores fases descritas del modelo de Gestión de Riesgos. Durante todo el ciclo de vida de la Gestión de Riesgos, deben estar involucrados las áreas de la Vicepresidencia de Tecnología de la Información dueñas de los sistemas configurados en el SIEM y las cuales sean impactadas por los riesgos identificados a partir de los incidentes de seguridad materializados, provenientes del SIEM.

Dentro de esta comunicación se debe concienciar no sólo a la Vicepresidencia de Tecnología de la Información, sino a la Alta Gerencia, que el proceso de Gestión de Riesgos de TI, en este caso para los incidentes de seguridad, son un componente que permitirá la consecución de los objetivos estratégicos de la Entidad.

La comunicación efectiva, se realizará en cada una de las sesiones de trabajo en cada fase del modelo, y como comunicado final será el Informe de Gestión de Riesgos según el formato del *Anexo D Informe de Gestión de Riesgos*.

4.2.8 Monitoreo y Revisión del Riesgo. Esta fase involucra, en primera medida, la evaluación de la eficacia de la implementación del modelo de Gestión de Riesgos, además de la identificación de las mejoras que se necesite realizar al mismo. Y por otro lado es el monitoreo de los riesgos identificados, la actualización de los controles definidos, modificación, en caso de requerirse, de los criterios de valoración del riesgo, su impacto, su probabilidad, la identificación de nuevas amenazas y vulnerabilidades.

Monitoreo y Revisión del Proceso

De forma semestral la Dirección de Seguridad debe definir el alcance de la Gestión de Riesgos, teniendo en cuenta:

- ✓ Criticidad de los activos y riesgos identificados

- ✓ Validación de los tiempos de respuesta en cada una de las fases, cuando se requiere dar una comunicación desde la Dirección de Seguridad de la Información a las áreas involucradas en el proceso.
- ✓ Validar las herramientas que respaldan el proceso, incluyendo las actualizaciones que se requieran sobre estas para la mejora del desempeño del proceso.
- ✓ Validar el alcance en temas legales del proceso de Gestión de Riesgos (Cumplimiento de Regulaciones Internas o Externas)
- ✓ Validación de los criterios de valoración de activos, de activos, niveles de aceptación de riesgos.
- ✓ Validación de la documentación y de las políticas que respaldan la ejecución del proceso.

Además de forma anual, por certificación ISO 9001, se debe revisar todo el proceso de Gestión de Riesgos, con el fin de identificar mejoras, que el cumplimiento de la norma requiera. El alcance de esta certificación es toda la documentación del proceso, junto con la evidencia de las actividades que se realizan durante su ejecución.

Monitoreo y Revisión de Los Factores de Riesgo

Este monitoreo consiste en el constante seguimiento sobre los siguientes puntos:

- ✓ Planes de Tratamiento
- ✓ Nuevas amenazas sobre los activos configurados en la herramienta SIEM.
- ✓ Vulnerabilidades sobre los activos, por la no actualización deficiente administración de los mismos.
- ✓ Impacto y probabilidad de la materialización del riesgo, según los resultados de las alarmas y monitoreo del SIEM.
- ✓ Identificación de nuevas causas de materialización del riesgo o deficientes implementaciones de los controles.
- ✓ Actualización de las valoraciones de los riesgos.

4.3 ANALISIS DE IMPLEMENTACIÓN DE LAS METODOLOGÍAS PROPUESTAS

La definición de las metodologías y de las herramientas que las apoyan en la ejecución de cada uno de sus procesos; según lo planteado basado en las normas ISO 27035 (Gestión de Incidentes de Seguridad de la Información) e ISO 27005 (Gestión de riesgos en la Seguridad de la Información), es la parte fundamental para llevar a cabo la ejecución de un proyecto, en el cual se implementen las 2 metodologías presentadas y se haga uso de las herramientas definidas con el fin de realizar una validación y evaluación de la propuesta metodológica, para la gestión de incidentes de seguridad de la información y de los riesgos consecuentes de la materialización de estos incidentes.

Actualmente la Entidad Financiera, se encuentra solventando un inconveniente por temas SOx[24], el cual radica en el cierre de un Material Weakness (hallazgo), que fue reportado a la SEC (Securities Exchange Commision), entidad que es un veedor para aquellas empresas que cotizan en la Bolsa de Valores de New York. Este hallazgo se encentra relacionado con el Monitoreo de Eventos y Logs, en la plataforma tecnológica que soporta las aplicaciones de alcance SOx, la cual se encuentra identificada en este documento en el apartado 2.1 (Plataforma Tecnológica).

La Entidad Financiera se encuentra realizando reingeniería sobre el SIEM, herramienta que apoya el cumplimiento del control que provocó el hallazgo, y debido a la situación crítica por el incumplimiento, no permitieron la implementación de las metodologías, sólo hasta que cierren el hallazgo y que la Auditoria Externa (quién reporta a la SEC) lo apruebe, valide y de la satisfacción de lo mismo.

---

[24] La Ley Sarbanes Oxley, cuyo título oficial en inglés es Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (30 de julio de 2002), es una ley de Estados Unidos también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. También es llamada SOx, SarbOx o SOA.

5 CONCLUSIONES

- ✓ Teniendo como base las normas ISO 27035:2011 e ISO 27005:2008 se logra construir un modelo íntegro que abarca la gestión de incidentes y la gestión de riesgos asociada a estos incidentes, el cual permitió inicialmente la identificación y análisis de los componentes que hacen parte del establecimiento del contexto bajo el cual se implementaron las normas.

- ✓ Adicional a las guías tomadas por las normas anteriormente nombradas, se puede evidenciar cómo estas normas permiten la integración de otros marcos de referencia en el momento de diseñar e implementar procesos que respalden un programa de seguridad de la información para una organización, como son: NIST SP 800-61 Rev 2 (Gestión de Incidentes de Seguridad) y la ISO 31000 (Gestión del Riesgo).

- ✓ Dentro de los beneficios de implementar un modelo basado en un estándar se encuentran: la estructuración de un proceso, lograr controlar cada una de las actividades definidas dentro del proceso, la eficiencia de los resultados, responsabilidades claramente definidas y la validación misma del proceso para identificar mejoras en el mismo.

- ✓ La definición de los modelos requirió tener una visión global del negocio, aunque no fue necesario; y no indica que no es importante; no hubo necesidad de un conocimiento técnico y profundo sobre la herramienta SIEM, para esta definición. De hecho, siguiendo como base las normas, se estableció una base de incidentes de seguridad a evaluar, relacionándolo con las configuraciones realizadas sobre la herramienta, de tal forma que los criterios para la evaluación de los incidentes, como aquellos necesarios para la valoración de los riesgos heredados de los incidentes, estaban alineados con el SIEM.

- ✓ Para el contexto del presente proyecto, los modelos se definieron para una Entidad Financiera, sin embargo, durante el desarrollo, se recalca que los modelos se pueden adaptar fácilmente para cualquier tipo de organización.

6 RECOMENDACIONES

- ✓ Definir un modelo de madurez para cada uno de los modelos trabajados, el cual permita establecer indicadores y medir a mejora continua del proceso.

- ✓ Diseñar los mecanismos necesarios para alinear los modelos de Incidentes de Seguridad y de Gestión de Riesgos de TI, con los modelos de Gestión de Incidentes y Gestión de Riesgos Corporativos de la Entidad.

- ✓ Automatizar los procesos con la implementación de una herramienta tecnológica íntegra que sea conector entre los modelos trabajados, y que permita la alineación con otros procesos. En definitiva es la implementación de un sistema GRC (Governance Risk and Compliance – Gobierno, Riesgos y Cumplimiento de TI).

- ✓ Teniendo en cuenta los riesgos identificados de la herramienta SIEM, definir un modelo de estimación cuantitativo para la valoración de los riesgos.

BIBILIOGRAFÍA

Bryant, I. (25 de Septiembre de 2008). *Terena.* Obtenido de Terena: http://www.terena.org/activities/tf-csirt/meeting25/bryant-iso27035.pdf

CINTEL. (27 de Diciembre de 2011). Obtenido de http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/Modelo_Seguridad_Informacion_2_0.pdf

Garcia, M. (20 de Octubre de 2013). *Disaster Recovery en Español.* Obtenido de Disaster Recovery en Español: http://www.drjenespanol.com/home/Portals/0/Archivos/Conferencias/2013/PRESENTACIONES/Maricarmen%20Garc%C3%ADa%20de%20Ure%C3%B1a.pdf

ICONTEC. (2009). *Gestión del Riesgo enla Seguridad de la Información ISO/IEC 27005.* Bogota: ICONTEC.

ICONTEC. (2011). *Gestión de Incidentes de Seguridad de la Información ISO/IEC 27035.* Bogota: ICONTEC.

ISACA. (2012). Cobit 5 framework. Rolling Meadows: ISACA.

ISO 27035. (24 de Febrero de 2013). *Google Sites.* Obtenido de Google Sites: https://sites.google.com/a/ist033.org.uk/public/home/4/cg-ip/27035

ISO 27000.ES. (30 de Agosto de 2008). *ISO 27000.ES.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO 27001 Security. (2013). *ISO 27001 Security*. Obtenido de ISO 27001 Security: http://www.iso27001security.com/html/27005.html

ISO 27001 Security. (2013). *ISO 27001 Security*. Obtenido de ISO 27001 Security: http://www.iso27001security.com/html/27035.html

NIST - National Institute of Standards and Technology . (2012). *Computer Security Incident Handling Guide.* Gaithersburg: NIST.

Paz, S. (27 de Diciembre de 2010). Obtenido de http://www.agesic.gub.uy/innovaportal/file/1217/1/Guia_de_procesos_en_gestion_de_incidentes.pdf

Ramirez, A., & Ortiz, Z. (15 de Agosto de 2011). *Revistas Universidad Distrital.* Obtenido de Revistas Universidad Distrital: http://revistas.udistrital.edu.co/ojs/index.php/reving/article/viewFile/3833/5399

Rouse, M. (Octubre de 2012). *Search Security.* Obtenido de http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

Talledo, M. (2009). *Guía del PMBOK 4ta Edición.* Pennsylvania: Project Management Institute, Inc.

UNAD. (6 de Septiembre de 2012). *Universidad Nacional Abierta y a Distancia.* Obtenido de Universidad Nacional Abierta y a Distancia: http://estudios.unad.edu.co/images/ecacen/Investigacion/Linea_de_Investigacion_-_Gestion_de_las_Organizaciones.pdf

Universidad de Washington. (21 de Novimebre de 2011). *Universidad de Washington.* Obtenido de Universidad de Washington: https://depts.washington.edu/oei/resources/toolsTemplates/plan_do_check_act.pdf

Williams, A. (01 de Enero de 2007). *Amrit Williams Blog*. Obtenido de http://techbuddha.wordpress.com/2007/01/01/the-future-of-siem-%E2%80%93-the-market-will-begin-to-diverge/

ANEXOS

ANEXO A. Política de Gestión de Incidentes de Seguridad

Entidad Financiera de Colombia

Políticas de Seguridad de la Información					
Política de Gestión de Incidentes de Seguridad de la Información					
Política	PSI-010	Fecha	01/03/2015	Correo	seguinfo@enficol.com
Versión	1.0	Contacto	Gilberto Silva		

Tabla de Contenido

PROPÓSITO

Esta política define los requerimientos para la gestión de los incidentes de seguridad de la información de la Entidad Financiera de Colombia.

ALCANCE

Esta política aplica a todos los incidentes de seguridad de la información de la Entidad Financiera de Colombia derivados de la herramienta SIEM.

POLÍTICA

Organización del Programa

Equipo de respuesta a Incidentes de Seguridad de la Información – La Vicepresidencia de TI debe organizar y mantener un Equipo de respuesta a Incidentes de Seguridad de la Información (ISIRT) que proveerá una gestión inmediata sobre el incidente identificado por el SIEM (Notificación, evaluación, respuesta y lecciones aprendidas).

Plan de Respuesta de Incidentes - El plan de Respuesta a Incidentes debe incluir los roles, las responsabilidades y las estrategias de comunicación en caso de la identificación de un incidente, incluyendo la notificación a socios externos de la entidad.

Incidentes de Seguridad de la Información – Todos los incidentes de seguridad de la Información derivados del SIEM se deben registrar, evaluar, asignar, responder e identificar la lección aprendida consecuente de la materialización del incidente.

Roles y Responsabilidades

ISIRT – Investigar, analizar y dar una respuesta a todo incidente de seguridad de la información que sea identificado; además de definir mecanismos preventivos y reactivos ante la identificación de un incidente de seguridad de la información.

Director de Seguridad de la Información – Análisis de las situaciones de riesgo que pueden derivar del proceso de gestión de incidentes de seguridad. Coordinar los servicios que presta la dirección, relacionados con la gestión de incidentes de seguridad y, la implementación y sostenibilidad de la herramienta SIEM. Organizar, dirigir y controlar el personal que hace parte de la implementación del proceso de

gestión de incidentes de seguridad y que se encuentran dentro de la dirección de seguridad de la información.

Gestor de Incidente de Seguridad – Es el primer punto de contacto para el proceso de gestión de incidente de seguridad. Registrar, analizar y validar que el incidente esté asociado a eventos de seguridad de la información. Escalar el incidente al ISIRT.

Administrador SIEM – Supervisar, monitorear y analizar todos los eventos detectados por el SIEM. Reportar eventos que puedan propender en un incidente de seguridad de la información al Gestor de Incidentes de Seguridad. Realizar un reporte periódico de los eventos más concurrentes.

Procedimientos

Procedimiento Gestión de Incidentes de Seguridad de la Información – La entidad Financiera de Colombia define el procedimiento de Gestión de Incidentes de Seguridad donde se indican las acciones a realizar en las fases de Detección y Reporte, Evaluación y Decisión, Respuesta y Lecciones aprendidas.

Monitoreo de Incidentes

Alertas de Incidentes – Los eventos configurados en el SIEM, implementado por la Entidad Financiera de Colombia, son la fuente principal de identificación y notificación de incidentes de seguridad de la información.

Reporte de Eventos de Seguridad de la Información

Los incidentes de seguridad de la información proceden de las alarmas configuradas en la herramienta SIEM, definidas por la misma Entidad:

Fallos físicos – Alarmas relacionados con problemas físicos en los dispositivos configurados en el SIEM, como, espacio en disco duro, problemas con los procesadores, daos físicos en los appliances y uso de memoria RAM.

Watchlist – Cualquier evento que se origine desde una dirección IP que se encuentre en este listado, sobre los dispositivos configurados en el SIEM.

Escaneo de Puertos Externo – Cualquier escaneo de puertos que se ejecute desde una dirección IP externa a la red de la Entidad.

El Administrador del SIEM debe registrar y reportar todo evento derivado de la materialización de las alarmas anteriormente nombradas, al Gestor de Incidente de Seguridad, con el fin de iniciar el correspondiente proceso de Gestión de Incidentes de Seguridad de la Información.

SANCIONES

En caso de identificar que algún empleado, tercero o accionista, se encuentre involucrado en la ejecución de un incidente de seguridad de información, según los resultados de la investigación realizada sobre el incidente, y que, se evidencie que se tenía la intención de inferir en la ejecución del mismo; o, se identifique alguna violación a la presente política; la Entidad puede hacer efectiva las sanciones disciplinarias que considere, incluso hasta la terminación del contrato.

La Entidad se reserva el derecho de notificar a las autoridades competentes cualquier actividad ilegal y cooperar con la investigación de dicha actividad.

DEFINICIONES

Dirección IP – Número único e irrepetible que identifica a un dispositivo (computadora, equipo de comunicación) conectado a una red.

ISIRT – Equipo conformado por miembros confiables de la Entidad, que cuentan con las habilidades y competencias para tratar los incidentes de seguridad de la información, durante el ciclo de vida de estos.

Incidente – Una ocurrencia que actualmente o potencialmente pone en peligro la confidencialidad, integridad o disponibilidad de un Sistema de información o de los sistemas que procesan, almacenan o transmiten información, o, que constituyen una violación o inminente amenaza a las políticas y/o procedimientos de seguridad.

Malware – Un programa que se instala en otro sistema, usualmente encubierto, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistemas de la víctima.

Tercero – Cualquier otra empresa contratada por la Entidad para proveerle, con recursos propios o ajenos, un servicio a la Entidad.

Watchlist – Listado de direcciones IP externas detectadas por la Entidad como maliciosas por su actividad relacionada con la generación o uso de malware.

REFERENCIAS

ISO/IEC 27002 – 13 Gestión de Incidentes de Seguridad de la Información

ISO/IEC 27035 – Gestión de Incidentes de la Seguridad de la Información.

DOCUMENTOS RELACIONADOS

Charles Cresson. Information Security Policies - Made Easy

REGISTRO DE REVISIONES

Versión	Descripción	Fecha de Revisión	Fecha de Aprobación	Nombre Aprobador
1.0	Versión Inicial	01/03/2015	31/03/2015	Gilberto Silva

ANEXO B. Política de Gestión de Riesgos de TI – Incidentes de Seguridad

Entidad Financiera de Colombia

Políticas de Seguridad de la Información					
Política de Gestión de Riesgos de TI – Incidentes de Seguridad					
Política	PSI-013	Fecha	15/03/2015	Correo	seguinfo@enficol.com
Versión	1.0	Contacto	Gilberto Silva		

Tabla de contenido

PROPÓSITO

Esta política define los lineamientos de la Gestión de Riesgos de TI, para la identificación y valoración de los riesgos, y la definición de los controles necesarios para la reducción del impacto de los riesgos asociados a los activos que se encuentran configurados sobre la herramienta SIEM implementada por la Entidad.

ALCANCE

Esta política aplica a todos los activos tecnológicos que se encuentran configurados en la herramienta SIEM de la compañía.

POLÍTICA

Proceso de Gestión de Riesgos

Evaluación de Riesgos de Seguridad – Cada año el área de Gestión de Riesgos de TI de la Entidad debe llevar a cabo una valoración de los riesgos generalizada de los riesgos materializados identificados por la herramienta SIEM. Dentro de este reporte se debe incluir una descripción detallada de los actuales riesgos de seguridad identificados y las recomendaciones desde la Dirección de Seguridad de la Información para la prevención o mitigación de los mismos.

Evaluaciones de Riesgos Unidades de Negocio – Cada unidad de negocio de la Entidad que administre alguno de los sistemas configurados en el SIEM debe realizar, al menos anualmente, un análisis de riesgos basado en lineamientos de seguridad de la información, de los mismos sistemas, coordinado con la Dirección de Seguridad de la Información, donde se certifique que en los sistemas se han implementado las medidas para la prevención o mitigación de riesgos.

Reporte Anual de Riesgos Tecnología de la Información – Para el Comité Estratégico de la Vicepresidencia de Tecnología de la Información, la Dirección de Seguridad de la Información debe enviar un reporte de los riesgos identificados en el último año. Dentro de estos riesgos se deben adicionar los riesgos derivados de la herramienta SIEM. Este reporte debe incluir el detalle de cada riesgo gestionado, incluyendo el resultado de la valoración y los planes de tratamiento implementados para la reducción de su impacto y/o los planes que se encuentran en ejecución.

Metodología de Evaluación de Riesgos – La Entidad requiere, cuando sea apropiado, el uso de una metodología de evaluación de riesgos que apoye las políticas de Seguridad de la Información y/o el cumplimiento de leyes o regulaciones. Esta metodología está basada en la ISO 27005:2008 – Gestión del Riesgo en la Seguridad de la Información.

Materialización Riesgos de Seguridad de la Información – Por cada riesgo materializado como producto de la gestión de Incidentes de Seguridad del SIEM,

debe tomarse una decisión específica a nivel de cada Unidad de Negocio impactada, sobre el tratamiento del riesgo, ya sea la reducción, retención, evitación, transferencia o aceptación del riesgo, siempre buscando la reducción del impacto y de las pérdidas razonables que pueda ocasionar a la Entidad.

Gestión de Riesgos en sistemas de Información

Evaluaciones de Riesgo Sistemas en Producción - Al menos cada año, debe realizarse una gestión de riesgos sobre los sistemas configurados en la herramienta SIEM. Adicional, todas las mejoras, actualizaciones y cambios asociados a estos sistemas deben ser precedidos por una evaluación de riesgos. Las específicas instancias que requieren de esta evaluación incluyen:

1. Cuando los sistemas vayan a ser implementados y se encuentren en una fase preliminar a la salida en producción.
2. Cuando en los sistemas se vayan a realizar modificaciones o mejoras significativas.
3. Cuando se contemple que la administración y/l el despliegue de estos sistemas sea ejecutado por terceros.

Análisis de Amenazas y Vulnerabilidades

Validaciones de Cambios en los Sistemas Operativos – Se deben realizar análisis de vulnerabilidades periódicos sobre los sistemas operativos que se encuentran implementados en la herramienta SIEM.

Escaneo de los Sistemas Expuestos a Internet – Cada componente configurado en la herramienta SIEM accesible desde una red externa, debe ser escaneado por la herramienta de vulnerabilidades definida por la Entidad para evitar que hayan vulnerabilidades que puedan ser explotadas desde redes externas.

Reportes de Vulnerabilidad – Una vez por semana, los Administradores de los sistemas configurados en la herramienta SIEM, deben consultar los boletines de seguridad de la información que el fabricante de estos publica, con el fin de identificar vulnerabilidades y/o amenazas sobre los sistemas y realizar las acciones necesarias para controlarlas.

Identificación de Vulnerabilidades – Para asegurar que los administradores de los sistemas han tomado las medidas de seguridad adecuadas, los sistemas de la herramienta SIEM que se conectan a Internet deben ser sujetos de evaluaciones de riesgos derivados de la identificación de vulnerabilidades al menos una vez al mes.

Actualizaciones de Seguridad – Toda actualización asociada a un problema de seguridad emitida por el Fabricante de los sistemas configurados en la herramienta SIEM (Hardware y Software) debe ser validada, evaluada e implementada.

Escaneo Equipos de Cómputo - Todos los equipos desde los cuales se realizan tareas de administración y uso de los sistemas configurados en la herramienta SIEM, deben ser regularmente escaneados, con el fin de identificar y tratar vulnerabilidades que puedan impactar a los sistemas.

SANCIONES

En caso de alguna violación de esta política por parte de algún empleado, tercero o accionista, la Entidad puede hacer efectiva las sanciones disciplinarias que considere, incluso hasta la terminación del contrato.
La Entidad se reserva el derecho de notificar a las autoridades competentes cualquier actividad ilegal y cooperar con la investigación de dicha actividad.

ROLES Y RESPONSABILIDADES

Administrador SIEM – Proveer la información de los eventos detectados por el SIEM que fueron la causa de la materialización de un riesgo.

Director de Seguridad de la Información – Análisis y reporte al Comité Estratégico de las situaciones de riesgo que pueden derivar del proceso de gestión de incidentes de seguridad, ya sea bajo demanda o por los períodos que sean definidos en el comité.

Gestor del Riesgo – Cada uno de los dueños y administradores de los sistemas configurados en la herramienta SIEM que son responsables de la implementación de los controles adecuados para asegurar la integridad, confidencialidad y disponibilidad de los sistemas. Generalmente los dueños de los sistemas son los responsables de los cambios en los mismos. Su rol dentro de la Gestión de riesgos es la valoración de cada uno de los componentes de los sistemas como activos y la

valoración de los riesgos según el impacto y probabilidad, en conjunto con el Líder Asesor del Riesgo.

Líder Asesor del Riesgo – Identificar junto con el Administrador del SIEM, los riesgos derivados de los eventos. Identificar los activos impactados por los riesgos. Valorar junto con el Gestor del Riesgo los activos, según su confidencialidad, integridad y disponibilidad; y, la valoración de los riesgos, según su impacto y probabilidad de forma cualitativa. Además de realizar asesorías para la definición e implementación de planes de tratamiento para cumplir con los controles que reduzcan el impacto del riesgo.

DEFINICIONES

Disponibilidad – Estado de la información cuando la misma se encuentra accesible y se puede utilizar bajo demanda por un usuario autorizado.

Confidencialidad – Estado de la información cuando es almacenada y es protegida de su entrega no autorizada a individuos, entidades o procesos.

Control – Mecanismo de seguridad implementado para prevenir, detectar, reducir o eliminar la materialización de un riesgo. Los controles deben mantener las propiedades de integridad, confidencialidad y disponibilidad de la información.

Integridad – Estado de la información que indica que durante el procesamiento de la misma (creación, almacenamiento, comunicación) no ha sido alterada o destruida de forma no autorizada.

Activo de Información – Todo aquello que contiene o procesa información con valor para la Entidad y por tanto necesita protegerse.

Riesgo – Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la Entidad.

Evaluación de Riesgos – Es la valoración cuantitativa o cualitativa en cuanto a la probabilidad y el impacto de un riesgo. El resultado de una evaluación de riesgos es generalmente la identificación y valoración de los activos, las vulnerabilidades, la

probabilidad, el impacto de la materialización del riesgo y los controles que se deben implementar para el tratamiento del mismo.

Riesgo Residual – El riesgo que permanece después de la implementación de un control. Este riesgo no es eliminado con la implementación del control.

Tratamiento del Riesgo – Proceso de priorizar, implementar y mantener las adecuadas medidas de control para la reducción del riesgo, según recomendaciones realizadas por el Líder Asesor del Riesgo.

Amenaza – Potencial causa de un incidente no deseado, el cual puede causar daño a un sistema o a una organización.

Vulnerabilidad – Debilidad en una Sistema de información que puede ser explotada por una amenaza.

REFERENCIAS

ISO/IEC 27005:2008 – Gestión del Riesgo en la Seguridad de la Información
NIST SP 800-30 – Guía de Evaluación de Riesgos

DOCUMENTOS RELACIONADOS

Charles Cresson. Information Security Policies - Made Easy

REGISTRO DE VERSIONES

Versión	Descripción	Fecha de Revisión	Fecha de Aprobación	Nombre Aprobador
1.0	Versión Inicial	18/03/2015	31/03/2015	Gilberto silva

ANEXO C. Formato de Reporte de Incidentes de Seguridad de la Información

Entidad Financiera de Colombia

Dirección de Seguridad de la Información					
Formato de Reporte de Incidentes de Seguridad de la Información					
Formato	FSI-020	Fecha	01/04/2015	Correo	seguinfo@enficol.com
Versión	1.0	Contacto	Gilberto Silva		

Tabla de contenido

INFORMACIÓN DE QUIÉN REPORTA

Nombre	
Cargo	
Área	
Teléfono	

INFORMACIÓN DEL INCIDENTE

Fecha de Detección	DD/MM/YYYY
Tipo de Incidente	✓ Incidente de daño físico ___ ✓ Incidente de fallas de infraestructura ___ ✓ Incidente de falla técnica ___ ✓ Incidente de Malware ___

	✓ Incidente de Ataque Técnico ___ ✓ Incidente de puesta en riesgo de la información ___ ✓ Otro ___
Impacto	✓ Confidencialidad ___ ✓ Integridad ___ ✓ Disponibilidad ___
Descripción en caso que sea Otro Tipo de Incidente	
Activo(s)/Sistema(s) Afectado(s)	
Lugar de Ocurrencia	
Descripción del Incidente	
Información Adicional	

ANEXO D. Formato Informe Gestión de Riesgos de TI

Entidad Financiera de Colombia

Políticas de Seguridad de la Información					
Formato Informe de Gestión de Riesgos de TI					
Formato	FSI-022	Fecha	01/03/2015	Correo	seguinfo@enficol.com
Versión	1.0	Contacto	Gilberto Silva		

Tabla de contenido

PARTICIPANTES

Indicar a continuación los participantes que hicieron parte en todo el proceso de Gestión de Riesgos de TI:

Nombre	Cargo

LISTADO DE ACTIVOS

Mencionar los activos que se identificaron en el proceso, incluyendo su valoración en Confidencialidad, Integridad y Disponibilidad, y su valoración final:

Activo	Tipo de Activo	Valoración			
		C	I	D	Valor

- ✓ **C:** Confidencialidad
- ✓ **I:** Integridad
- ✓ **D:** Disponibilidad

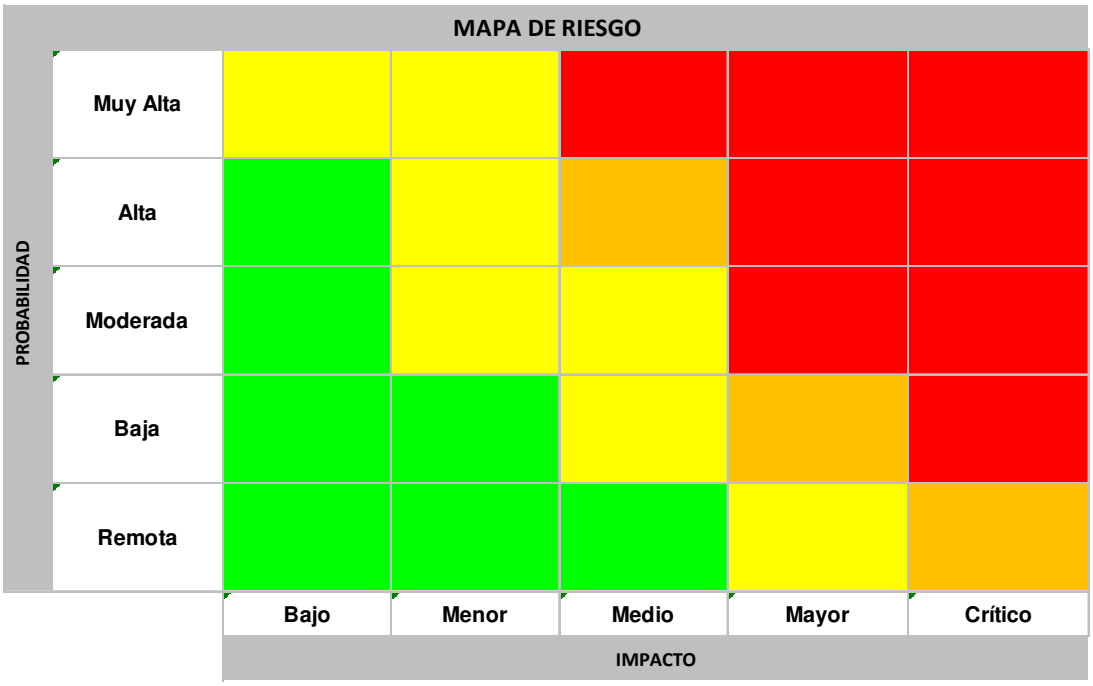
LISTADO DE RIESGOS

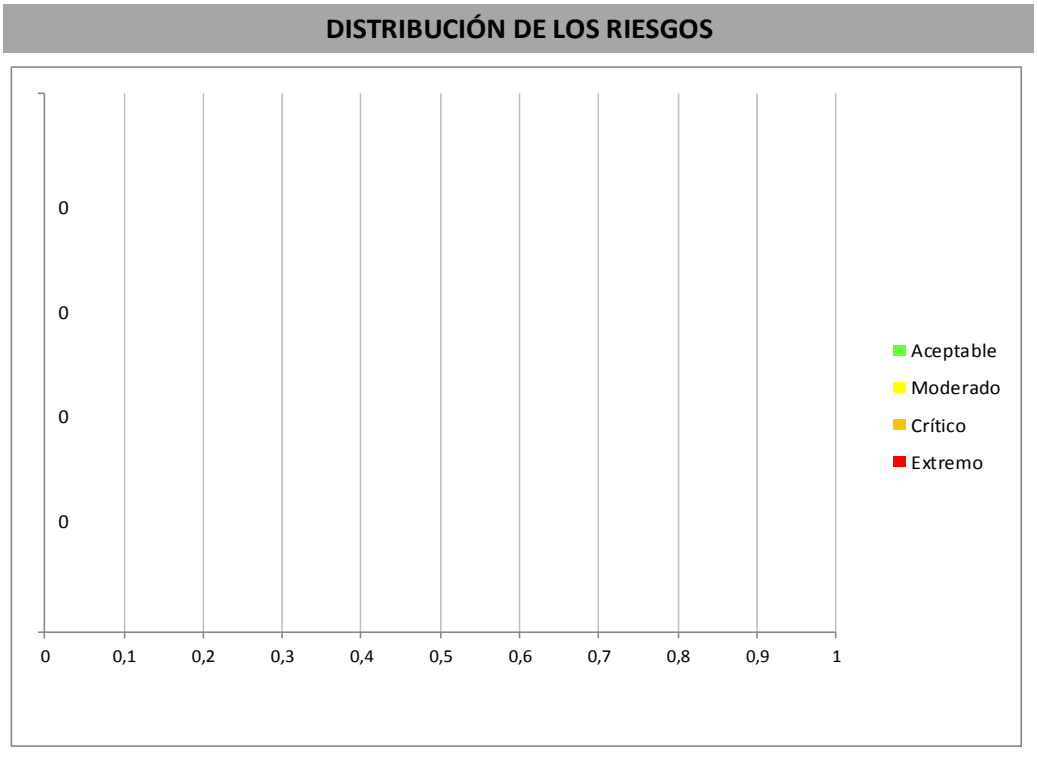
Mencionar los riesgos que se identificaron en el proceso, relacionando su Vulnerabilidad, y su valoración final:

Referencia del Riesgo	Riesgo	Vulnerabilidad	Valoración

MAPA DE CALOR Y DISTRIBUCIÓN DE LOS RIESGOS

Relacionar el mapa de calor y la distribución todos los riesgos identificados durante el proceso:





TRATAMIENTO DE LOS RIESGOS

De acuerdo a la valoración de cada riesgo y a los planes de tratamiento definidos se relacionan a continuación las opciones de tratamiento de los riesgos identificados:

Referencia del Riesgo	Opción de Tratamiento	Descripción del Plan	Responsable	Fecha de Cierre

CONSIDERACIONES

<<Relacionar observaciones adicionales que se consideren relevantes para el informe>>

REGISTRO DE REVISIONES

Versión	Descripción	Fecha de Revisión	Fecha de Aprobación	Nombre Aprobador
1.0	Versión Inicial	01/03/2015	31/03/2015	Gilberto Silva