SOLUCIÓN DE LA SITUACIÓN PROBLEMA DE CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA UNA ENTIDAD FINANCIERA

TRABAJO DE GRADO

JOSE LUIS MARTINEZ PINEDA

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2016

SOLUCIÓN DE LA SITUACIÓN PROBLEMA DE CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN PARA UNA ENTIDAD FINANCIERA

TRABAJO DE GRADO

JOSE LUIS MARTINEZ PINEDA

9821040274

GIOVANNY ANDRÉS PIEDRAHITA SOLÓRZANO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2016

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Ciudad, Fecha

Contenido

INTRODUCCIÓN

En toda compañía se presentan problemas que pueden afectar el correcto funcionamiento de sus procesos, en muchos casos no se cuenta con un método que aporte a la implementación de soluciones para dichos problemas quedando brechas por atender y dejando el problema real sin solución.

Durante la Especialización de Seguridad de la Información se adquiere el conocimiento necesario para poder identificar e implementar los componentes que establecen un nivel de seguridad óptimo, garantizando el adecuado funcionamiento de una compañía, manteniendo controlado los efectos negativos que se pueden percibir en su operación y aprovechando las oportunidades que nacen de la gestión oportuna de los frentes de trabajo.

A partir de un análisis previo a una situación problema identificado, se establecen los lineamientos que se consideran necesarios para controlar de la mejor manera los efectos que pueden presentarse para una Compañía con las mismas características.

OBJETIVO

Definir la estrategia que mejor se ajuste para tratar una situación particular de Seguridad de la Información que afecte el logro de los objetivos estratégicos de una Compañía Financiera.

ALCANCE

La propuesta que se presenta, da inicio a partir de la situación problema identificada, que mediante la implementación del Sistema de Gestión de Seguridad de la Información y sus componentes basados en las mejores prácticas de seguridad plasmadas en los documentos reconocidos por la industria, para lo cual se limita el alcance en el desarrollo de la solución y el diseño del plan de trabajo.

1. RESUMEN EJECUTIVO

El proyecto consiste en establecer e implementar el mejor tratamiento posible para atender una situación problema de una compañía financiera, en la cual se presentan temas de falta de conciencia hacia la protección de la información por parte de los empleados, los cuales no tienen dentro de sus objetivos atributos como confidencialidad, integridad y disponibilidad.

Esta situación podría acarrear impactos para la Compañía, de tipo económico, reputacional, legal u operativo; la entidad por ser parte de un sector regulado por el estado, debe cumplir con requisitos mínimos que garanticen el tratamiento seguro de la información de sus clientes durante e incluso después de la prestación de los servicios contratados.

El objetivo principal es identificar los componentes que se deben implementar en la entidad con el fin de mantener un nivel de seguridad aceptable que cumpla con las regulaciones y se base en las mejores prácticas de Seguridad de la Información, de esta forma, se apoya el cumplimiento de los objetivos estratégicos y se proporciona una generación de valor para los productos y servicios que se ofrecen a los clientes.

Como resultado de la implementación de los componentes, le empresa puede lograr los siguientes beneficios:

- Mayor tranquilidad para los clientes y accionistas.
- Ofrecer procesos seguros que superen las expectativas de sus clientes.
- Ser referente en el mercado por mantener la seguridad de la información de sus clientes como prioritaria.
- Mayor captación de mercado.
- Cumplir con los lineamientos regulatorios emitidos por la Superintendencia Financiera de Colombia.

La estrategia que se define con el fin de lograr los objetivos propuestos y dar un tratamiento eficaz a la situación problema, es identificar las causas que generan la situación presentada, definir los mecanismos necesarios que puedan ser mitigantes y presentar ante la Junta Directiva el plan de trabajo junto con sus beneficios para lograr el apoyo e implementación de la solución presentada.

Los componentes o elementos que se proponen como solución y hacen parte del plan de trabajo están dados de la siguiente manera:

- Establecer un área de Seguridad de la Información que lidere la implementación de las mejores prácticas de Seguridad de la Información basadas en el core de negocio.

- Implementar un Sistema de Gestión de Seguridad de la Información.

- Establecer objetivos de seguridad de la información alineados con los objetivos de negocio de la Compañía.

- Definir, implementar y seguir una metodología de riesgos de seguridad de la información identificando los criterios necesarios para establecer el nivel de aceptación de impacto para la Compañía.

- Diseñar planes de trabajo donde se relacionen las actividades de concienciación que lleguen a toda la Compañía, incluyendo terceros y proveedores.

La propuesta incluye los lineamientos y el plan de trabajo, el detalle de cada uno de los componentes deberá ser desarrollado durante la implementación del proyecto una vez la Junta Directiva de la empresa apruebe los recursos necesarios para su puesta en producción.

A su vez, se encuentra en el presente documento, indicadores de gestión que se pueden llevar a cabo en la implementación de la propuesta, se plantean los escenarios pesimista y optimista, en donde este último se considera bastante alentador y puede ser una opción prometedora al tener en cuenta los beneficios ofrecidos y los recursos necesarios para el proyecto, al momento de tomar una decisión por parte de los directivos de la entidad.

2. ETAPAS DEL PROYECTO

Fase 1. Diagnóstico

Durante la primera fase, se identifica la situación problema, los actores relevantes o partes involucradas, a su vez, se realiza un análisis de causas detonantes de la situación problema y los riesgos más relevantes ocasionados por la situación de seguridad de la información presentada.

Fase 2. Tratamiento

Una vez se establece el diagnóstico de la Compañía relacionada con la situación problema de seguridad de la información, se definen los diferentes escenarios de donde se extraen los controles necesarios para mitigar los riesgos evidenciados en el diagnóstico.

Fase 3. Implementación

La tercera y última etapa, consta de la implementación de la solución, dentro de la cual se realiza la ejecución del Plan de Trabajo planteado y la formalización de los entregables.

3. JUSTIFICACIÓN

La justificación del proyecto se basa en el estudio realizado durante el trayecto de la especialización, el cual permite desarrollar una propuesta que apoye el tratamiento de una situación problema presentada en una empresa de un sector previamente identificado.

Para efecto del ejercicio se tiene en cuenta una situación problema presentada en una empresa del sector financiero, la cual podría llegar a ser generadora de impactos económicos y de otras índoles, significativos para la Compañía.

3.1. SITUACIÓN – PROBLEMA

Una compañía financiera cuenta con un problema de conciencia hacia la protección de la información, sus empleados no están interesados en mantener la confidencialidad, integridad y/o disponibilidad de la información de la Compañía.

3.2. ACTORES RELEVANTES

A continuación se enuncian los actores relevantes que intervienen en la situación problema presentada como marco inicial del anteproyecto.

- **Grupo Corporativo:** Grupo que define, implementa y realiza seguimiento a los lineamientos en las empresas que lo conforman.

- **Socios**: Grupo de personas que tienen participación económica de las acciones de la Compañía.

- **Compañía**: Ente que presta servicios a los clientes generando valor para sus socios.

- **Alta dirección**: Grupo que representa la Compañía frente al grupo corporativo, define, implementa, adopta y adapta los lineamientos del ente principal como lo es el grupo corporativo.

- **Gerentes**: Encargados de direccionar a la Compañía según los requerimientos de la Alta Dirección. Los gerentes presentan proyectos a la Alta Dirección para apoyar el logro de los objetivos organizacionales.

- **Departamento de Riesgos:** Área encargada de identificar, tratar y mantener riesgos, asegurando un impacto aceptable para la Organización.

- **Clientes**: Personas que se benefician de los servicios que presta la Compañía, a su vez, comparten su información personal con la empresa.

- **Entes de control externos (Superintendencia financiera):** Entidad encargada de definir y seguir los lineamientos que garanticen seguridad en los procesos que ofrecen las diferentes entidades financieras.

3.3. CAUSAS

Las causas se refieren a los detonantes de la situación, es decir a los posibles situaciones que generan el problema, estas se presentan en dos tipos, la primera son las que están bajo el gobierno de la entidad y son de gestión interna, las demás, se refieren a las que están sin gobierno de la entidad, para las cuales es necesario interacción con el entorno exterior de la compañía.

A continuación se enuncian las principales causas identificadas que pueden generar la situación problema de la Compañía.

Gobierno de la entidad

- Se definen políticas enfocadas únicamente a tecnología.
- Los objetivos de riesgos están alejados de los estratégicos
- La Alta Dirección no conoce lo riesgos que afectan a la compañía
- La vicepresidencia de riesgos piensa que implementar buenas prácticas y certificarse es un llamado para los atacantes
- Se muestran indicadores alejados de la realidad
- Se realiza seguimiento a las actividades sin tomar evidencias significativas
- Los monitoreos son realizados sin análisis especializado
- Falta de comunicación efectiva entre la vicepresidencia de riesgos y la alta dirección
- No existe un ejemplo positivo por la alta dirección
- No existe un área que lidere la implementación de buenas prácticas
- No se evalúan riesgos de seguridad
- No hay planes de concienciación para sus empleados
- Funcionarios renuentes al cambio

Sin gobierno de la entidad

- Difícil acceso a las normas externas emitidas por los entes reguladores
- Los funcionarios no son conscientes de los riesgos de información en su entorno social
- Falta de auditorías externas

3.4. INDICADORES

Con el fin de realizar una medición que genere valor y evidencie el estado relacionado con el problema relacionado a la Seguridad de la Información, se establecen los siguientes indicadores.

Tratamiento de incidentes

Indicador= (Cantidad de Incidentes/ Cantidad de eventos identificados)*100

Análisis: El 100% indica que por cada evento presentado se genera un incidente, esto significa que no hay controles o que son deficientes.

Insumo: Reportes de incumplimiento a las políticas de la Compañía.

Análisis de Impacto

Cantidad de incidentes * valor de activos comprometidos

Análisis: El valor de los incidentes supera el nivel estimado de aceptación del impacto por la Organización.

Insumo: Valor de los activos

Gestión trabajo de concienciación

Indicador: (Actividades realizadas / actividades programadas en el periodo) * 100

Análisis: La meta es del 100% siempre que exista un programa de concienciación, al no tener un programa el indicador es de 0. Ratificando el desinterés de cambiar la cultura respecto a la protección de la Información.

Insumo: Mapa de trabajo de concienciación - Seguimiento a las actividades

3.5. FLUJO GRAMA EXPLICATIVO

Para poder contar con una visión más entendible de la situación evaluada en la empresa, en la siguiente figura, se desarrolla el flujograma explicativo.

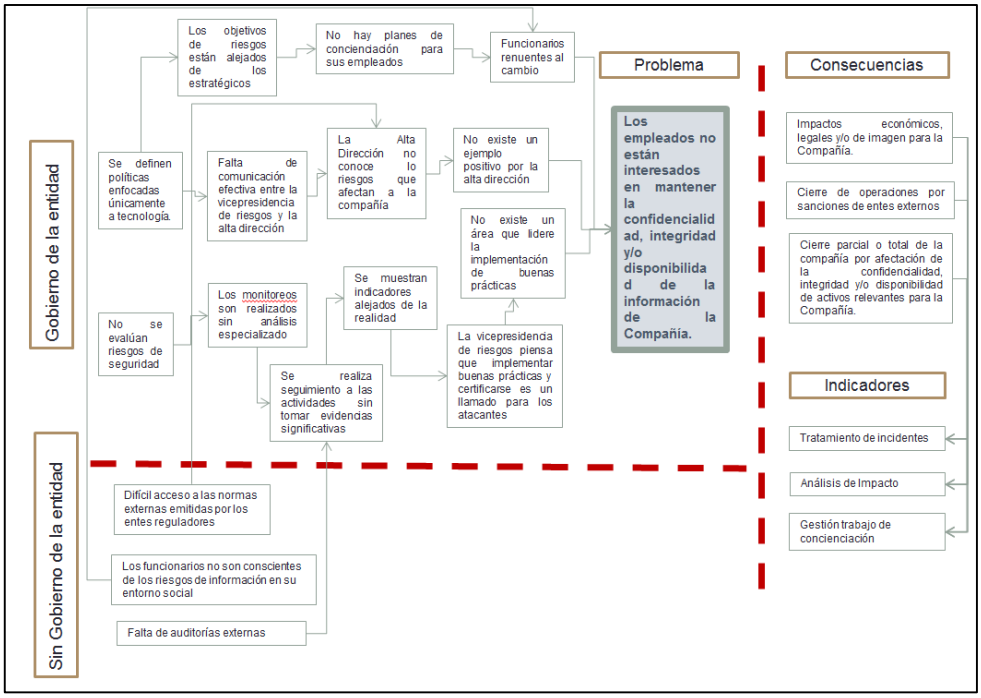


Figura 1 Flujograma Explicativo.

3.6. ANÁLISIS DE RIESGOS

Con el fin de realizar un análisis de riesgos oportunos, se identifican los siguientes activos como los más relevantes de la Compañía:

- Bases de Datos Lógicas y Físicas
- Data Center
- Aplicaciones
- Equipos Tecnológicos
- Comunicaciones

Dentro de los riesgos más relevantes que se pueden presentar asociados con la situación relacionada con la concienciación de los colaboradores acerca de la protección de la información de la Compañía, generada por múltiples causas, se pueden evidenciar algunos que impactan tanto de forma económica, legal y reputacionalmente a la Entidad.

A continuación se enuncian los riesgos identificados:

- Fuga de Información sensible de clientes por errores en los diferentes procesos.
- Perdida de integridad de la información core de la Compañía por falta de controles de protección.

- Perdida de confidencialidad de la información de la Compañía por falta de controles físicos y lógicos.
- Impactos económicos por incumplimiento a la regulación vigente relacionada con la protección de la información.

Una vez identificados los riesgos más relevantes, cabe anotar que a raíz de la falta de conciencia de protección de la información se pueden desencadenar diversos riesgos que en el presente trabajo no se establecen pero con las soluciones planteadas se pretende dar cubrimiento.

3.7. TRATAMIENTO

Luego de identificar los riesgos que pueden impactar a la Compañía, se desarrolla la fase de tratamiento, para lo cual se establece la situación esperada, el análisis de prospectiva, el análisis de viabilidad, el Plan de trabajo y por último la definición de los entregables que soportan la solución planteada.

3.7.1. SITUACIÓN ESPERADA

Como inicio de una etapa en donde la Compañía le dé la relevancia que la información necesita para poder seguir el negocio adelante, antes de recibir un impacto que lleve al cierre de las operaciones, se espera que desde la Alta Dirección hasta el nivel operativo de la entidad se comprometan a desarrollar sus actividades manteniendo lo más seguro posible la información en las actividades que ejerce cada actor.

Se espera una comunicación más coordinada entre la vicepresidencia de riesgos con la Alta Dirección, entregando la información que puede ser necesaria para tomar decisiones que mantengan la seguridad del negocio.
Crear planes de trabajo de concienciación coordinando actividades con las diferentes áreas de la Compañía, como recursos humanos quienes pueden programar temas para asegurar activos de información desde la vinculación, ejecución del cargo y retiro de la compañía.

La Compañía debe basar su seguridad en marcos de gestión que los puedan guiar para reducir los posibles impactos que puedan repercutir con el negocio mediante la implementación de las mejores prácticas de seguridad de la información.

3.7.2. ANÁLISIS PROSPECTIVA

Escenario Pesimista

En la entidad se requiere crear cultura de seguridad de la información en todos los procesos, para poder implementar planes de concienciación es necesario que la Alta Dirección apruebe la definición de los programas y la participación de los colaboradores en las actividades.

El peor de los casos es que la Alta Dirección no permita asistir a las actividades programadas y por otra parte desarrolle sanciones para quienes asistan.

La implementación de un Sistema de Gestión de Seguridad de la Información basado en marcos de acción de buenas prácticas, permitirá que la Compañía proteja los activos de información, para que esta solución funcione se debe crear un área que lidere el tema, se deben aprobar recursos tanto humanos como físicos y tecnológicos; todo está unido con la decisión que se tome desde la Alta Dirección.

La aprobación de los recursos e implementación del Sistema de Gestión de Seguridad de la Información es puede ser negada por la Alta Dirección y la Compañía no avanzaría en el cambio de cultura y protección de la Información.

La Organización ya que es una entidad financiera, está obligada a cumplir con ciertos requerimientos de la Superintendencia Financiera de Colombia, esté sería un método para llegar a la Alta Dirección e implementar acciones que fortalezcan la cultura de la Organización con respecto a la Seguridad de la Información.

La situación que no se debe permitir es la toma de los requerimientos solamente como obligatorios sin entender que pueden ser favorables para la Compañía, es decir, que no se realicen actividades solamente por cumplir, ya que esto permite tomar información poco real solamente por cubrir requerimientos.

Escenario Optimista

El escenario esperado es donde con el visto bueno de la Alta Dirección se pueden implementar las siguientes acciones:

- Establecer un área de Seguridad de la Información que lidere la implementación de las mejores prácticas de seguridad basadas en el core de negocio.

- Establecer objetivos de seguridad de la información alineados con los objetivos de negocio de la compañía.

- Diseñar planes de trabajo donde se relaciones actividades de concienciación que lleguen a toda la Compañía, incluyendo terceros y proveedores.

- Implementar un Sistema de Gestión de Seguridad de la Información.

- Definir, implementar y seguir una metodología de riesgos de seguridad de la información identificando los criterios necesarios para establecer el nivel de aceptación de impacto para la Compañía.

Se considera que la implementación de las actividades propuestas en el escenario optimista, son el mejor plan de acción para las causas definidas en el presente trabajo; por otra parte estaría dándole un adecuado tratamiento a la situación problema y todas las situaciones presentadas como consecuencias, a su vez, mediante la implementación de indicadores de gestión la Alta Dirección puede ver el avance en las actividades realizadas por el equipo que lidera el programa propuesto.

3.7.3. VIABILIDAD, GOBERNABILIDAD Y PERTINENCIA

Acción	Valoración de Gobernabilidad		Valoración de Impacto		Valoración de Pertinencia		
Establecer un área de Seguridad de la Información que lidere la implementación de las mejores prácticas de seguridad basadas en el core de negocio.	3	La Compañía tiene como líder visible un área responsable de diseñar, implementar y socializar las propuestas y resultados que mantengan la seguridad de la información de la Compañía. Se cuenta con una línea directa con la Alta Dirección que evidencia el estado de la seguridad de los activos de la Compañía.	2	Se deben aprobar recursos necesarios para implementar un área que lidere los temas de seguridad de la información, se considera un beneficio ya que el costo de implementación no superaría el costo de los impactos que se pueden evitar.	2	Es viable la creación de un área de Seguridad de la Información que lidere la implementación de las mejores prácticas de seguridad.	7
Establecer objetivos de seguridad de la información alineados con los objetivos de negocio de la compañía.	3	La definición de los objetivos de seguridad de la información da mayor claridad del enfoque del área y delas actividades que se deben realizar para fortalecer la cultura de seguridad en la compañía, a su vez, la Alta Dirección tiene la visibilidad completa de las actividades de Seguridad de la Información.	3	Las actividades de negocio están respaldadas por las de Seguridad de la Información, generando un valor agregado en la prestación de servicios y productos a los clientes.	3	Se cuenta con una viabilidad respaldada en las áreas de negocio, quienes pueden encontrar en Seguridad de la Información apoyo para generar valor a los productos ofrecidos.	9
Diseñar planes de trabajo donde se relaciones actividades de concienciación que lleguen a toda la Compañía, incluyendo terceros y proveedores.	3	Se debe tener en cuenta que las actividades programadas no entorpezcan la ejecución de los procedimientos de la Compañía	2	El tiempo empleado por los funcionarios no debe generar impactos en la operación.	3	Es viable bajo la premisa de no entorpecer las actividades del negocio.	8

Implementar un Sistema de Gestión de Seguridad de la Información.	3	Se organizan las actividades que se deben realizar por las diferentes partes involucradas, manteniendo un liderazgo centralizado en Seguridad de la Información con apoyo de la Alta Dirección.	2	Se deben aprobar recursos necesarios para organizar los procedimientos de Seguridad de la Información, diseñar políticas e implementa herramientas de Seguridad.	3	Es viable siempre que no supere el presupuesto otorgado anualmente para las actividades de seguridad de la información.	8
Definir, implementar y seguir una metodología de riesgos de seguridad de la información identificando los criterios necesarios para establecer el nivel de aceptación de impacto para la Compañía.	3	Esta actividad es liderada por el área de Seguridad de la información y garantiza la centralización de la identificación de riesgos y el tratamiento de los mismos.	3	Se deben programar actividades de implementación de la metodología que no impacten al negocio; los planes de acción deben contar con un estudio de costo beneficio para tomar decisiones por la Alta Dirección.	3	Es viable la implementación de la metodología de riesgos la cual se recomienda ser evaluada por personal especializado.	9

Figura 2 Análisis de Viabilidad – Gobernabilidad - Pertinencia

3.7.4. PLAN DE TRABAJO

Prioridad	Acción	Actividades	Responsable	Recursos	Tiempo
1	Establecer un área de Seguridad de la Información que lidere la implementación de las mejores prácticas de seguridad basadas en el core de negocio.	Identificar los procesos que se lideran desde el área de Seguridad de la Información. Identificar los recursos necesarios para liderar los procesos. Identificar los recursos físicos y tecnológicos. Identificar la infraestructura física que se necesita.	Vicepresidencia de Riesgos	Dos personas especializadas en Seguridad de la Información, cada una con un equipo portátil y acceso a las políticas y lineamientos de negocio.	3 meses
2	Implementar un Sistema de Gestión de Seguridad de la Información.	Identificar la documentación requerida. Identificar el marco de acción a seguir. Revisar los requerimientos de negocio. Revisar los requerimientos de entes externos. Identificar los procesos de la Compañía. Establecer las políticas de seguridad necesarias. Definir los estándares necesarios de seguridad de la Información.	Área de Seguridad de la Información	Los definidos para el área de Seguridad de la Información. Se estiman un Oficial de Seguridad de la Información, tres analistas especializados en gobierno, arquitectura y gestión de incidentes, tres auxiliares operativos.	12 meses
3	Establecer objetivos de seguridad de la información alineados con los objetivos de negocio de la compañía.	Identificar los requerimientos del negocio. Identificar los objetivos estratégicos.	Área de Seguridad de la Información	Coordinador de Seguridad de la Información, Analista de Gobierno de	2 meses

		Alinear los procedimientos de Seguridad de la Información con los objetivos estratégicos.		seguridad de la Información	
4	Definir, implementar y seguir una metodología de riesgos de seguridad de la información identificando los criterios necesarios para establecer el nivel de aceptación de impacto para la Compañía.	Identificar los criterios de impacto. Identificar los criterios de análisis de riesgos. Identificar la escala de análisis de riesgos. Establecer el nivel de aceptación de impacto para la Compañía.	Área de Seguridad de la Información	Área de Seguridad de la Información	8 meses
5	Diseñar planes de trabajo donde se relaciones actividades de concienciación que lleguen a toda la Compañía, incluyendo terceros y proveedores.	Establecer las actividades de concienciación Presentar ante la Alta Dirección el programa con las actividades relacionadas. Ejecutar el plan de trabajo.	Área de Seguridad de la Información	Área de Seguridad de la Información	12 meses

Figura 3 – Plan de Trabajo

3.7.5. DEFINICIÓN DE ENTREGABLES

La definición de los entregables, son el resultado final que soporta la solución desarrollada que mediante el tratamiento de la situación problema identificada y pretende mitigar los riesgos asociados.

En esta fase de entrega, se formaliza con la Juta Directiva y posteriormente se socializa con la totalidad de la compañía la documentación de respaldo y cada uno de los componentes que soporta el desarrollo de las diferentes fases estipuladas en el plan de trabajo.

Los entregables son:

- Política de Seguridad de la Información.
- Objetivos de Seguridad de la Información.
- Metodología de Riesgos de Seguridad de la Información.
- Plan de Concienciación de Seguridad de la Información para toda la Compañía.

Estos entregables son tomados como la línea base para establecer una estrategia de Seguridad de la Información manteniendo alineados los objetivos de negocio con los planteados por el Sistema de Gestión.

4. MARCO TEÓRICO Y REFERENTES

Una vez identificado el problema y definido los componentes necesarios para subsanar la situación problema; así como presentar los beneficios y diversos

escenarios que se evalúan; se desarrolla el plan de trabajo con los elementos primordiales para llevar a buen término la solución.

Como parte de los elementos de Seguridad de la Información, se toman guías de referencia reconocidas en la industria que apoyan la estrategia de la solución planteada.

A continuación se define para cada una de las acciones del plan de trabajo los aportes de la industria referenciados según su participación.

Para la primera acción, en donde se plantea el establecer un área de Seguridad de la Información al interior de la Compañía, se recomienda tomar como referencia para el desarrollo de las actividades los lineamientos que describe el estándar ISO 27001:2013 [1].

En el estándar se resaltan los siguientes puntos, los cuales se desarrollarán según las definiciones de la norma con el fin de garantizar la implementación de las mejores prácticas de seguridad de la información.

- Contexto de la Organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del Desempeño
- Mejora

A su vez, se sugiere realizar una declaración de aplicabilidad del anexo A de la norma ISO 27001:2013, la cual está explícitamente descrita en la norma ISO27002:2013 [2], con el fin de identificar el alcance de los dominios de la norma que se aplican para la compañía y se pueden implementar.

Como especialistas en la implementación de Seguridad de la Información, se considera que la totalidad de los dominios descritos en el anexo de la norma aplican para una compañía de tipo financiera, como lo es el caso de estudio.

Dentro de los lineamientos establecidos en la guía de referencia para la implementación del sistema de gestión de Seguridad de la Información, se sugiere implementar un sistema de gestión de riesgos, para lo cual se pueden tomar diferentes estándares, como lo son Magerit 3.0 [3], EBIOS [4], ISO 27005 [5], o si se desea utilizar una metodología de gestión integral de riesgos en donde se puedan complementar los diferentes sistemas de gestión de la compañía, se sugiere utilizar como marco de referencia la guía de Gestión de Riesgos ISO 31000 [6].

Para efectos del ejercicio, se recomienda diseñar una metodología de riesgos que utilice como referencia la norma ISO 27005:2008, en donde se

Como complemento a la gestión de riesgos se extraen los siguientes conceptos de las diferentes normas referenciadas.

Se tiene en cuenta la definición de activos de información de Magerit 3.0 en donde se especifica lo siguiente: *"La tipificación de los activos es tanto un información documental de interés como un criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo. La siguiente tabla no puede ser exhaustiva, ni tan siquiera válida para siempre. La relación que sigue clasifica los activos dentro de una jerarquía, determinando para cada uno un código que refleja su posición jerárquica, un nombre y una breve descripción de las características que recoge el epígrafe. Nótese que las pertenencia de un activo a un tipo no es excluyente de su pertenencia a otro tipo; es decir, un activo puede ser simultáneamente de varios tipos*." [3]

A su vez se realiza una unificación de las amenazas planteadas por la metodología Magerit 3.0 y las emitidas por la norma ISO 27005:2008 diseñando un catálogo lo suficientemente amplio para identificar los riesgos que se puedan identificar en los procesos de la entidad.

Uno de los puntos más importantes para establecer el sistema de gestión de Seguridad de la Información y el sistema de gestión de riesgos, es la definición del contexto, donde se ubican los escenarios de actuación de la entidad y se establece el alcance del mismo.

En la norma ISO27001: 2013 se define el contexto de la Organización de la siguiente manera: *"La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.*

NOTA: La determinación de estas cuestiones hace referencia a establecer el contexto externo e interno de la organización, considerado en el apartado 5.3 de la ISO 31000:2009." [1]

Si nos acercamos a la ISO 31000:2009 y extraemos la definición de contexto encontramos lo siguiente:

Contexto externo. Ambiente externo en el cual la organización busca alcanzar sus objetivos.

NOTA: El contexto externo puede incluir:
El ambiente cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local; impulsores clave y tendencias que tienen impacto en los objetivos de la

organización; y relaciones con las partes involucradas y sus percepciones y valores.
Contexto interno. Ambiente interno en el cual la organización busca alcanzar sus objetivos.

NOTA: El contexto interno puede incluir:
Gobierno, estructura organizacional, funciones y responsabilidades; políticas, objetivos y estrategias implementadas para lograrlos; las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo capital, tiempo, personas, procesos, sistemas y tecnologías); sistemas de información, flujos de información y procesos para la toma de decisiones (tanto formales como informales); relaciones con las partes involucradas internas y sus percepciones y valores; la cultura de la organización; normas, directrices y modelos adoptados por la organización; y forma y extensión de las relaciones contractuales. [6]

Con el fin de realizar una implementación de los sistemas de gestión relacionados con la seguridad de la información, se define el contexto de la Organización teniendo como base la definición de la norma ISO31000:2011, la cual permite complementar tanto para la información tanto para la administración del sistema como la gestión de riesgos.

Una vez identificado e implementados los lineamientos de seguridad de la información en la Compañía, se define la estrategia de concienciación, para lo cual se tiene en cuenta las tendencias en torno a la industria financiera y los ataques que se pueden presentar en el sector.

5. METODOLOGÍA

La metodología a utilizar para el desarrollo de la solución al problema planteado, se basa en la implementación de la mejores prácticas de Seguridad de la Información desarrolladas en el estándar ISO 27001:2013, IO 27002:2013, para riesgos se tiene en cuenta la definición del estándar ISO 31000:2011 y 27005:2008.

Dentro de los estándares definidos, se recogen los lineamientos necesarios para implementar un sistema de gestión de seguridad de la información y una metodología de riesgos ajustada a la necesidad de la compañía.

Con el fin de mantener un sistema funcionando oportunamente, dentro de la estrategia se define un ciclo de mejora continua basado en el ciclo PHVA – (Planear, Hacer, Verificar y Actuar) en donde cada uno de los elementos debe cumplir con el ciclo de mejora establecido.

Las fases del proyecto se desarrollan utilizando el ciclo definido PHVA, con el fin de mantener la mejora continua.

6. RESULTADOS Y DISCUSIÓN

Como parte de los resultados esperados luego de la implementación de la propuesta de solución presentada, se definen los siguientes entregables que sustentan el logro del objetivo planteado.

En relación con las actividades y los lineamientos definidos en las guías utilizadas, se establecen como entregables los documentos de:

- Política de Seguridad de la Información.
- Objetivos de Seguridad de la Información.
- Metodología de Riesgos de Seguridad de la Información.
- Plan de Concienciación de Seguridad de la Información para toda la Compañía.

La construcción de los entregables se realizó tomando como soporte las guías que se establecen en el marco teórico y pretenden alinear los objetivos y la estrategia de Seguridad de la Información con los objetivos estratégicos.

7. CONCLUSIONES

Una vez realizada la implementación de la solución de tratamiento a la situación problema de concienciación, se enuncian las siguientes conclusiones.

Luego de la implementación del plan de concienciación se evidencia una participación más activa por los colaboradores de la Compañía en las actividades de Seguridad de la Información.

Se han disminuido significativamente los eventos que pueden permitir la fuga de información en los procesos de la Compañía.

Durante las etapas de validación a los proyectos ejecutados en la Compañía, se evidencia la conciencia sobre la identificación oportuna de riesgos y controles para la salida a producción de los mismos, manteniendo ambientes seguros y dando cumplimiento a la regulación existente.

Se evidencia la participación del equipo de Seguridad de la Información en los proceso de la Entidad, emitiendo oportunamente las recomendaciones necesarias para mitigar impactos.

La Junta Directiva se percibe más interesada en la gestión de seguridad de la Información y apoya los lineamientos emitidos al respecto.

Como un tema adicional a la solución, se contrató una auditoría externa para que evaluara el nivel de madurez del sistema de gestión de seguridad de la información, tomando como guía la norma ISO 27001: 2013, para la cual se evidencian resultados satisfactorios ratificando que el plan de trabajo implementado.

8. BIBLIOGRAFÍA

[1] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[2] ISO/IEC 27002:2013, *Information technology — Security Techniques — Code of practice for information security controls*

[3] *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*

[4] EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité - Sección 5 Herramientas Para El Tratamiento De Los Riesgos Ssi

[5] ISO/IEC 27005:2008- Information technology – Security techniques – Information security risk management

[6] *ISO/IEC 31000: 2011, RISK MANAGEMENT. PRINCIPLES AND GUIDELINES*

9. ANEXOS

Anexo 1

9.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información se dividen en dos partes, la primera es la política general de seguridad de la información y la segunda parte está compuesta por políticas específicas a cada uno de los dominios.

Política General de Seguridad de la Información

Para la compañía, la información es catalogada como uno de los activos fundamentales del negocio y del correcto funcionamiento de los procesos definidos que lo soportan; por tal motivo y mediante la implementación de buenas prácticas de seguridad de la información, lideradas por recurso humano y apoyado por la utilización de tecnologías aprobadas por la Alta Dirección, se gestiona la implementación de metodologías, técnicas y regulación normativa aplicable, encaminando sus esfuerzos en pro del mantenimiento de la Confidencialidad, Integridad y Disponibilidad de sus activos de información, a su vez, la organización se compromete en la protección de los datos sensibles de los clientes, ejecutando los procesos de manera segura y manteniendo la privacidad de la información.

A continuación se enuncia el conjunto de políticas que se deben establecer para cada uno de los dominios de Seguridad de la Información, según el marco de referencia:

- Política para dispositivos móviles
- Política teletrabajo
- Política de control de accesos
- Política de escritorio limpio y pantalla limpia
- Política de respaldo de la información
- Política y estándares de transferencia de información
- Política de desarrollo seguro
- Política de seguridad de la información para la relación con proveedores
- Política de Uso de Correo Corporativo e Internet
- Política de Controles Criptográficos

Anexo 2

9.2. Objetivos de Seguridad de la Información

Cada uno de los procesos de seguridad de la información cuenta con objetivos definidos, que apoyan el cumplimiento de los objetivos de la organización.

Para asegurar el logro de los objetivos de seguridad de la información, se gestionan los procedimientos implementados que administra el equipo de seguridad de la información siempre contando con el apoyo de la Alta Dirección, los dueños de los procesos y los colaboradores en general.

Los procesos y objetivos definidos, se describen a continuación:

9.2.1. Gobierno de Seguridad de la Información

El gobierno de Seguridad de la Información es un proceso mediante en el cual se diseña y define el marco de referencia y la estructura de seguridad de la información, que la compañía decide implementar con el fin de mantener el aseguramiento de los atributos de la información, teniendo en cuenta la optimización de riesgos y de recursos.

En este proceso se define la estrategia de Seguridad de la Información, encargada de orientar, definir, implementar y comunicar los lineamientos que los colaboradores, terceros y demás partes involucradas deben cumplir con el fin de evitar la materialización de impactos significativos para la compañía.

Objetivos

- Apoyar el crecimiento de la Organización de manera segura, manteniendo la confidencialidad, integridad y/o disponibilidad de sus activos.

9.2.2. Gestión de Riesgos de Seguridad de la Información

El proceso de gestión de riesgos de seguridad de la información, consta de procedimientos enfocados en diseñar e implementar actividades que generan valor para la Compañía apoyando el logro de los objetivos de la Organización, mitigando la materialización de riesgos que puedan generar impactos negativos para la Compañía, siempre teniendo como punto de partida la seguridad de la información que se maneja en los distintos procesos definidos.

Objetivos

- Mantener ambientes de seguridad óptimos para la gestión adecuada de los procesos de la compañía evaluando la utilización de nuevas tecnologías y tendencias en el mercado respecto a temas de Seguridad de la Información.

- Generar un ambiente de confianza para los socios y clientes, gestionando de manera adecuada el uso de la información.

- Ofrecer servicios adecuados a nuestros clientes gestionando oportunamente la revisión de los procesos críticos de la compañía.

- Identificar y tratar oportunamente los riesgos que pueden impactar la organización.

9.2.3. Gestión de Cumplimiento Interno y Regulatorio

La Gestión de cumplimiento interno y regulatorio, hace referencia por una parte, al adecuado comportamiento de los colaboradores, a la correcta utilización de los elementos suministrados para llevar a cabo las actividades y al cumplimiento de los lineamientos corporativos; por otra parte, busca recopilar las evidencias necesarias con que la entidad cumple con los requerimientos de los entes externos desde el actuar de Seguridad de la Información.

Objetivos

- Apoyar a la Organización en el logro de los objetivos gestionando oportunamente los lineamientos establecidos por el sistema de gestión de seguridad de la información.

- Apoyar el cumplimiento de los lineamientos definidos por los entes de regulación que se encuentren al alcance de Seguridad de la Información.

9.2.4. Gestión de Accesos

El proceso de gestión de accesos, ejecuta acciones que apoyan la implementación de buenas prácticas relacionadas con ingresos, segregación de funciones y ciclo de vida de los usuarios en los sistemas, es decir, desde el momento de la creación de un usuario nuevo hasta su eliminación, pasando por el mantenimiento y asignación de roles necesarios para ejercer las diferentes actividades.

Objetivos

- Garantizar la implementación de buenas prácticas en el manejo de la información basados en la segregación de funciones.

9.2.5. Gestión de Incidentes

Una vez identificados incidentes de seguridad en la compañía, éste será tratado en el menor tiempo posible creando planes de acción que mitiguen el impacto que

se pueda generar, tomando control de la situación presentada, evitando impactos significativos para la Organización.

Objetivos

- Identificar y responder eventos inesperados con el fin de controlar el impacto dentro de los niveles de aceptación

9.2.6. Gestión de Proyectos

El equipo de Seguridad de la Información, se encuentra disponible para apoyar los diferentes proyectos que se implementen en la Organización, gestionando y aportando las recomendaciones necesarias, emitiendo los conceptos necesarios para mantener la confidencialidad, integridad y disponibilidad de la información de la compañía.

Objetivos

- Apoyar la consolidación del negocio generando ambientes de seguridad en cada uno de sus proyectos de innovación y mantenimiento.

9.2.7. ALINEACIÓN DE OBJETIVOS

Los objetivos de seguridad de la información se encuentran alineados con los objetivos de la organización, es decir, el cumplimiento de los objetivos propuestos por el área apoyan el cumplimiento de los objetivos estratégicos de la compañía.

De esta forma el área de Seguridad de la Información gestiona todos sus procedimientos apoyando la estrategia de la Compañía, cada uno de las actividades definidas para el área pretende generar valor al negocio con lineamientos de seguridad, siempre buscando mantener la confidencialidad, integridad y disponibilidad de la información utilizada en los diferentes procesos.

ALINEACIÓN ESTRATÉGICA						
SGSI - Sistema de Gestión de Seguridad de la Información	**Estratégicos**					
	FINANCIERO	**CLIENTES**	**EFICIENCIA**	**INNOVACIÓN**	**CAPACIDAD**	**SOSTENIBILIDAD**
Apoyar el crecimiento de la Organización de manera segura, manteniendo la confidencialidad, integridad y/o disponibilidad de sus activos.	**X**				**X**	

Generar un ambiente de confianza para los socios y clientes, gestionando de manera adecuada el uso de la información.	X	X	X			
Mantener ambientes de seguridad óptimos para la gestión adecuada de los procesos de la Compañía evaluando la utilización de nuevas tecnologías y tendencias en el mercado respecto a temas de Seguridad de la Información.			X		X	
Ofrecer servicios adecuados a nuestros clientes gestionando oportunamente la revisión de los procesos críticos de la Compañía.		X	X	X		
Identificar y tratar oportunamente los riesgos que pueden impactar la Organización.			X			X
Apoyar a la Organización en el logro de los objetivos gestionando oportunamente los lineamientos establecidos por el Sistema de Gestión de Seguridad de la Información.	X	X	X	X	X	X
Apoyar el cumplimiento de los lineamientos definidos por los entes de regulación que se encuentren al alcance de Seguridad de la Información.	X					X
Garantizar la implementación de buenas prácticas en el manejo de la información basados en la segregación de funciones.			X	X		
Identificar y responder eventos inesperados con el fin de controlar el impacto dentro de los niveles de aceptación.	X		X	X		
Apoyar la consolidación del negocio generando ambientes de seguridad en cada uno de sus proyectos de innovación y/o mantenimiento.	X		X	X		

Anexo 3

9.3. Metodología de Riesgos de Seguridad de la Información

9.3.1. Metodología

La guía metodológica que se toma como marco de referencia para el análisis de riesgos de seguridad de la información es la que se propone en la norma ISO 27005 y se encuentra alineada con la norma de gestión de riesgos ISO 31000, a su vez, la metodología es complementada con conceptos de diferentes metodologías como Magerit 3.0 y Ebios.

9.3.2. Criterios de Evaluación del Riesgo

Para la Compañía, la información es catalogada como uno de los activos más importantes, por lo tanto es vital administrarlos de manera segura, generando ambientes propicios que mantengan la confidencialidad, integridad, disponibilidad de los mismos.

En todos los procesos de la compañía se utiliza información, sin ésta, no sería posible el correcto funcionamiento de los mismos ocasionando el incumplimiento de los objetivos propuestos, por lo tanto, es necesario contar con un inventario de activos de información, el cual es la base para realizar análisis de riesgos y definir los controles que mitiguen el impacto que se pueda generar para la compañía al comprometer la confidencialidad, integridad, disponibilidad.

Contando con el inventario de activos de información, se deben evaluar las posibles amenazas y vulnerabilidades que pueden afectar uno o varios de los criterios de seguridad de la información, desencadenando la materialización de un riesgo que podría impactar significativamente a la Organización; por último, se relacionan los controles existentes que la compañía ha implementado en los diferentes procesos; de esta forma se obtiene la identificación del riesgo que puede impactar a la compañía, para lo cual se deben tomar las mejores decisiones de tratamiento que mitiguen dichos riesgos.

9.3.3. Criterios de Impacto

Al clasificar los activos de información de la compañía, ubicados en los diferentes procesos, el área de Seguridad de la Información identificará riesgos asociados a éstos, para tal fin, se cuenta con un universo de amenazas y vulnerabilidades, extraídas de diversas metodologías de riesgos de Seguridad de la Información.

La pérdida de confidencialidad, integridad y/o disponibilidad de la información, como el compromiso de la privacidad de los datos personales, genera un impacto

para la organización en mayor o menor medida, por lo tanto es vital priorizar el nivel de impacto que tienen los activos de información sobre la organización.

Priorizando el impacto que los activos que generan a la organización, por afectaciones de la confidencialidad, integridad y/o disponibilidad, es posible enfocar los esfuerzos de la gestión de riesgos identificando y mitigando la materialización de los riesgos de mayor relevancia, evitando pérdidas sustanciales o impactos significativos para el negocio.

Los riesgos de seguridad de la información identificados, deben ser gestionados adecuadamente utilizando un tratamiento correcto que impida su materialización; durante el análisis de riesgos y tomando como base el inventario de activos de información, es posible identificar el tipo de impacto en que se puede ver afectada la Organización.

Los tipos de impacto que la compañía evalúa desde el punto de vista de la protección de la información y controla mediante la implementación de la metodología de Riesgos de Seguridad de la Información son:

- Impacto Financiero
- Impacto Legal, Contractual o Regulatorio
- Impacto de Reputación o Imagen

Durante la clasificación de activos de información se realiza la valoración del impacto en que éstos pueden llegar a afectar a la organización al comprometer uno de los atributos de seguridad de la información utilizando escalas definidas según el core de negocio.

Impacto Financiero

Perdida de dinero para la Compañía; efecto generado con la materialización de riesgos por afectación de los criterios de Seguridad de la Información; éste puede reflejarse en diferentes cuantías, desde una cuantía menor que no genera impacto significativo para el negocio y la Compañía puede continuar con su operación normal sin verse afectada, hasta una escala de mayor cuantía, donde la empresa se ve implicada en pérdidas económicas significativas poniendo en riesgo la continuidad del negocio.

La identificación del impacto financiero y de los demás impactos (Reputacional y Legal), se evalúan por cada uno de los activos de información identificados en la Compañía, es decir, en que escala de impacto recibe la entidad al recibir una afectación de confidencialidad, integridad y/o disponibilidad en uno de sus activos de información.

Impacto Financiero		
Cuantitativo	Cualitativo	Descripción
5	Muy Alto	El evento genera pérdidas mayores a 50.000 millones.

4	Alto	El evento que genera pérdidas entre 5.000 y 50.000 millones.
3	Medio	El evento que genera pérdidas entre 400 y 5.000 millones.
2	Bajo	El evento que genera pérdidas entre 50 y 400 millones.
1	Muy Bajo	El evento que genera pérdidas hasta 50 millones.

Impacto Legal, Regulatorio o Contractual

Sanciones económicas o destituciones de personal de niveles jerárquicos altos, es decir, personal que tienen a cargo las diferentes dependencias de la institución; como consecuencia de incumplimientos legales, regulatorios o contractuales, o manejos inadecuados en la función prestada. Se mide desde una escala Muy Bajo en donde el impacto no es significativo, hasta una escala Muy Alto que repercute en cambio de personal estratégico de la entidad y cambio de estrategias en la función.

Impacto Legal, Regulatorio y Contractual		
Cuantitativo	Cualitativo	Descripción
5	Muy Alto	El evento genera despidos masivos de personal de alguna entidad del grupo empresarial por incumplimientos regulatorios que equivalgan a un impacto económico muy alto.
4	Alto	El evento genera el cese de actividades de alguna entidad del grupo empresarial por incumplimientos regulatorios o sanciones que equivalgan a un impacto económico alto.
3	Medio	El evento genera sanciones que equivalgan a un impacto económico medio para la compañía.
2	Bajo	El evento genera incumplimientos en regulaciones ocasionando multas que equivalgan a un impacto bajo para la compañía.
1	Muy Bajo	El evento da lugar a una no conformidad frente a procedimientos internos puede ocasionar multas equivalentes a un impacto bajo o no genera sanciones económicas.

Impacto de Reputación o Imagen

Impacto que puede afectar a la compañía perdiendo el buen nombre o generando un ambiente de desconfianza frente a la población del país o fuera de éste, todo como consecuencia de la materialización de riesgos, se mide con una escala inicial de muy bajo donde el incidente se conoce al interior de la institución, hasta una escala denominada como muy alto, donde el incidente es conocido por medios masivos de comunicación a nivel internacional.

Impacto de Reputación o Imagen		
Cuantitativo	Cualitativo	Descripción
5	Muy Alto	El evento es conocido en medios masivos de comunicación a nivel internacional.
4	Alto	El evento es conocido al interior del país sin repercutir en la imagen internacional.
3	Medio	El evento es conocido al interior del gobierno institucional presente.
2	Bajo	El evento es conocido al interior de la Entidad.
1	Muy Bajo	El evento es conocido al interior de un área de la Entidad

Los activos de información serán valorados por el responsable de los mismos, identificando la escala del impacto que se puede generar para la compañía al verse afectada la confidencialidad, integridad y/o disponibilidad.

Atributos de Seguridad de la Información

La definición de los atributos de Seguridad de la Información en los cuales se basa la gestión de riesgos es la siguiente:

Confidencialidad
Propiedad de la información que garantiza que esta sea accesible únicamente por personal autorizado.

Integridad
Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es decir, libre de cualquier modificación indebida que afecte el orden lógico de los datos cambiando su estructura o significado. La información debe ser manipulada únicamente por los autorizados.

Disponibilidad
Característica que permite que la información sea accesible en el momento que sea necesario y por las personas, sistemas o procesos indicados.

Etiquetado de la Información

Una vez inventariados los activos y estando valorados, se contará con una clasificación, la cual genera una etiqueta para cada uno de éstos.

Información Secreta
De uso exclusivo del responsable de la información, la pérdida de confidencialidad, integridad y/o disponibilidad puede afectar significativamente la entidad, los colaboradores o un tercero. Este tipo de información no se puede compartir sin la autorización específica y debe contar con los más altos niveles de protección.

Información Confidencial
Hace referencia a la información que por su naturaleza no sea posible compartir con personas diferentes a las autorizadas por el responsable del activo, está información se considera sensible o critica para la Organización; está ligada a un proceso exclusivo que puede ser conocida únicamente por los funcionarios relacionados con las tareas asignadas o terceros relacionados estrictamente según la operación del negocio.

La información Confidencial al ser revelada a personas no autorizadas puede comprometer la continuidad de la operación del negocio y/o tener un fuerte

impacto en la información financiera, asuntos legales y/o en la imagen de la entidad.

Información Interna
Información que contiene datos necesarios para la gestión de los procesos internos de la organización y cuya circulación fuera de la compañía está restringida y el conocimiento externo no es conveniente, en el evento de ser conocida al exterior de la entidad representa un riesgo bajo, no produciría un impacto significativo para la compañía.

Información pública
Información que no necesita ninguna protección especial y puede ser compartida sin ningún protocolo de seguridad al interior o exterior de la organización sin causar un impacto negativo o afectar la integridad de la empresa o de un tercero.

Probabilidad de Ocurrencia

Luego de identificar los riesgos asociados a los activos de información, se evalúa la probabilidad de ocurrencia de materialización de los mismos, para tal fin, es necesario tener en cuenta criterios como motivación y capacidad de un atacante, a su vez se evaluarán eventos ocurridos históricamente en caso de contar con el registro, se analizaran causas reportadas por diferentes fuentes de información de la industria y se evaluarán los controles existentes en los casos que sea necesario.

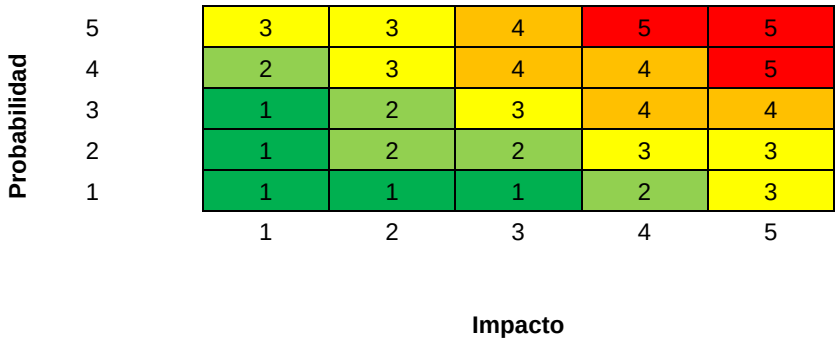
Probabilidad de Ocurrencia		
Cuantitativo	Cualitativo	Descripción
5	Muy Alta	La fuente de amenaza está altamente motivada y es suficientemente capaz ó ha se han alertado en promedio 10 o más eventos en el periodo de un año.
4	Alta	La fuente de amenaza está motivada y es capaz o se han alertado 5 a 9 eventos en el periodo de un año.
3	Media	La fuente de amenaza está motivada y podría contar con la capacidad o se han alertado 2 a 4 eventos en el periodo de un año.
2	Baja	La fuente de amenaza tiene una escasa motivación y capacidad o se ha alertado una vez en el periodo de un año.
1	Muy Baja	La fuente de amenaza tiene no es motivante y la capacidad debe ser demasiado alta para explotar una vulnerabilidad o no existen eventos alertados.

La motivación es uno de los criterios más importantes para definir en la probabilidad y se refiere al apetito que puede generar la explotación de una vulnerabilidad o la generación de un ataque a la Organización causando un impacto para la misma; la capacidad se refiere a las competencias que se deben adquirir para llegar a materializar un riesgo explotando una vulnerabilidad o los recursos financieros necesarios para tal fin.

Con el fin de realizar una gestión adecuada de riesgos se consideran las amenazas y vulnerabilidades de diferentes fuentes de la industria así como las alertas reportadas por las herramientas implementadas para la compañía.

Mapa de Riesgos

Se valora el Riesgo utilizando el siguiente mapa de riesgos, teniendo como insumo el Impacto y la Probabilidad de Ocurrencia identificada.



Escala		Definición
Ponderación	Nivel	
5	**Muy Alto**	Pone en peligro la continuidad del negocio, requiere acción "inmediata“ para el tratamiento del riesgo
4	**Alto**	Requiere planes urgentes para el tratamiento del riesgo
3	**Medio**	Se requiere tratar el riesgo a mediano plazo
2	**Bajo**	Se requiere evaluar si se implementan acciones o se decide asumir el riesgo
1	**Muy Bajo**	Se asume el riesgo

9.3.4. Criterios de la Aceptación de Riesgos

Los riesgos identificados durante el proceso de análisis, que puedan generar un nivel de impacto bajo o muy bajo en el mapa de riesgos; es decir que su valoración entre impacto y probabilidad esté en el rango de 1 y 2 en la escala cuantitativa; se asumirán siempre y cuando no sean asociados a temas de estricto cumplimiento o repercuta en impactos legales, regulatorios o contractuales, de lo contrario son tomados como riesgos prioritarios cuyo tratamiento deba ser de manera inmediata.

Los niveles medio, alto y muy alto, deben ser analizados y tratados oportunamente implementando controles que permitan reducir, evitar y/o transferir el riesgo.

9.3.5. Alcance y límites

La metodología de Gestión de Riesgos Seguridad de la Información contempla el mantenimiento de los atributos de confidencialidad, integridad y disponibilidad de

la información en todos los procesos de la Organización, creando de esta manera ambientes que aseguren el logro de los objetivos del negocio.

Con el fin de lograr el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información propuestos, los cuales están encaminados al logro de los objetivos de la Organización, se implementa la metodología de Gestión de Riesgos de Seguridad de la Información en todos los procesos definidos por la Compañía que se encuentran documentados en el sistema de calidad, tomando como base el inventario de activos de información el cual es documentado con el apoyo de las áreas responsables de los procesos.

Cada vez que los procesos de la compañía sean actualizados o se generen nuevos procesos, el inventario de activos de información deberá ser actualizado y se identificaran los posibles riesgos que se puedan presentar.

La implementación de las medidas de control o fortalecimiento de los controles existentes definidos, deberán ser aprobados por la Alta Dirección con el fin de gestionar los recursos necesarios; a su vez, se socializan con las partes involucradas y responsables de los activos relacionados.

9.3.6. Valoración del Riesgo

La valoración de riesgos es la fase en donde se identifica el impacto que cada activo puede llegar a generar para la Organización al comprometer los atributos de confidencialidad, integridad, y/o disponibilidad; estos datos son identificados en la clasificación de activos durante el levantamiento de la información de cada proceso, se reflejan de manera cuantitativa o cualitativa dependiendo del caso, siempre tomando como referencia los criterios definidos en el contexto de la metodología de gestión de riesgos y con el apoyo del responsable de la información.

La valoración del riesgo se logra con la implementación de dos componentes, el primero es el análisis del riesgo que a su vez se divide en identificación y estimación del riesgo, y por otra parte está la evaluación del riesgo.

9.3.7. Análisis del Riesgo

La fase de análisis del riesgo corresponde a la identificación del riesgo en los procesos, tomando como base la clasificación de los activos de información, identificando las amenazas que pueden causar daños a dichos activos y posterior a esto identificando las vulnerabilidades que puedan ser explotadas causando la materialización de un riesgo determinado que afecte los atributos de la información e impacte a la Organización significativamente.

Identificación de Riesgos

La identificación de riesgos se compone de varios elementos, los cuales se definen a continuación; es necesario identificar los activos de información y los impactos que pueden generar a la compañía la afectación de los mismos, una vez definido lo que se elabora, consume, transporta, destruye y demás, con respecto a la información, se analizan las amenazas y vulnerabilidades que pueden estar presentes en los procesos.

Por otra parte, con el fin de evitar incurrir en sobrecostos o gastos innecesarios en la adquisición de controles, se identifican los controles existentes, ya que con ésta información posteriormente se evalúa la necesidad de implementar nuevos controles, robustecer los actuales o definir controles complementarios que mitiguen los riesgos.

Identificación de Activos de Información

La identificación de activos de información se realiza mediante visitas realizadas a los dueños o líderes de los procesos definidos siempre apoyadas por los colaboradores de los procesos de la Organización, la entrevista es el método utilizado para la recopilación de información necesaria durante la gestión de Riesgos, este método se debe utilizar moderadamente con el fin de no entorpecer el funcionamiento normal de la operación.

Documentación: Actividad que se utiliza para plasmar el resultado de la entrevista realizada; se deben relacionar las variables necesarias para la identificación del riesgo; para el caso de Seguridad de la Información se relacionan los activos de información utilizados en el proceso, adicionalmente se registran las siguientes variables:

- Área/ Proceso
- Entrevistado
- Activo de información
- Descripción
- Tipo de Contenedor
- Contenedor
- Propietario
- Custodio
- Valoración del Impacto

Validación: Esta actividad se realiza con los responsables de los procesos, y consta de la aprobación de lo relacionado en la documentación de la entrevista, luego de esto, es posible ajustar el documento resultado.

Visto Bueno Responsable: Luego de ajustar la documentación y contar con las variables necesarias para la identificación del riesgo, se debe recibir el Visto Bueno del responsable del proceso, dejando como evidencia que lo relacionado y clasificado es veraz.

Valoración del Activo: La valoración del activo de información se realiza con el responsable del proceso, hace referencia al Impacto Financiero, Impacto Legal, Regulatorio y/o Contractual ó al Impacto de Imagen, en que puede verse afectada la Organización al comprometer la Confidencialidad, Integridad o Disponibilidad del Activo de información clasificado.

Etiquetado de la Información: La información se clasifica en cuatro niveles, los cuales se definen según su naturaleza teniendo en cuenta los datos personales y el tipo de información que contienen, además, el proceso se apoya en lineamientos descritos en la ley 1581 de 2012 y el decreto 1377 de 2013; tomando como base estas premisas los activos de información se clasifican según los conceptos definidos en los criterios de impacto.

- Información Secreta
- Información Confidencial
- Información Interna
- Información pública

Identificación de Amenazas y Vulnerabilidades de Seguridad de la Información

Luego de contar con un inventario de Activos de Información, el siguiente paso es identificar amenazas y vulnerabilidades que pueden afectar la confidencialidad, integridad y/o disponibilidad de la información en cada uno de los procesos de la compañía.

La identificación de Amenazas y Vulnerabilidades para la gestión de riesgos de Seguridad de la Información, se lleva a cabo en los procesos definidos para la compañía teniendo en cuenta los activos, priorizando de esta forma el impacto más significativo para la organización y asegurando los activos que por su naturaleza necesitan niveles de protección adecuados y efectivos.

El universo de amenazas y vulnerabilidades es el insumo utilizado para identificar los posibles riesgos que pueden desencadenar un impacto para la organización, éste se construye tomando como base estándares como ISO 27005, Magerit, Ebios, amenazas reportadas por OWASP y demás entidades de la industria.

Una vez se construye el universo de amenazas y vulnerabilidades, se identifican las posibles amenazas que pueden explotar las vulnerabilidades en los activos; de esta forma se define el riesgo y el atributo de la información que se ve comprometido.

Identificación de Controles Existentes

Con el fin de evitar incurrir en costos innecesarios o sobrecostos, al momento de implementar controles que ayuden a mitigar los riesgos identificados, es necesario

realizar un levantamiento de los controles que se encuentran implementados en la Compañía, de esta manera, se realiza un análisis del riesgo inherente con controles existentes si los hay, resultado del análisis realizado se toman decisiones sobre cómo es la forma más eficiente de mitigar los riesgos que pueden presentarse para la Compañía, siempre partiendo del costo beneficio al momento de tomar la decisión correcta.

Las decisiones que pueden surgir con respecto a los controles, son, fortalecimiento de controles existentes, definición de nuevos controles o definición de controles complementarios.

9.3.8. Evaluación del Riesgo

La etapa de evaluación de los riesgos, es realizada con el fin de tomar decisiones acerca de las actividades que se deben ejecutar una vez identificados los riesgos que pueden afectar a la compañía.

La evaluación permite priorizar los riesgos identificados, analizando el tratamiento correspondiente que se tiene que realizar para mitigar la materialización de los riesgos; es una decisión de la Compañía, el establecer el nivel de aceptación de impacto que se está dispuesto a asumir, pero se deja claro que todos los riesgos inherentes identificados deben contar con una evaluación y análisis para decidir si se les da tratamiento o no.

La priorización de los riesgos durante la evaluación, está dado según su grado de impacto; es decir, los impactos Muy Altos, Altos y Medios, son los primeros que se deben evaluar e identificar la mejor forma de tratamiento, luego, vienen los de menor escala como lo son los de grado Bajo y Muy Bajo, los cuales se deben evaluar posteriormente sin dejarlos de lado; es de aclarar que todos los riesgos deben ser evaluados y es decisión de la Compañía si el universo de riesgos debe ser controlado.
La identificación del riesgo se realiza tomando el criterio según el impacto que se encuentre por encima del nivel de aceptación, es decir, si el impacto que genera el activo está dado por Confidencialidad, el riesgo debe estar asociado a la pérdida del mismo atributo.

9.3.9. Tratamiento de riesgos

Una vez analizados y cuantificados los riesgos, así como identificado el impacto que pueden generar a la entidad por la afectación de la confidencialidad, integridad y/o disponibilidad es necesario analizar las opciones de tratamiento que lleven el riesgo inherente a un nivel de aceptación definido por la organización.

Opciones propuestas de tratamiento:

Transferencia del Riesgo (TR): Estrategia cuyo objetivo es compartir el riesgo, puede realizarse mediante pólizas u otras formas de contrato.

Retención del Riesgo (RT): Es la opción de aceptar el riesgo y asumir las consecuencias que esto implica.

Reducción del Riesgo (RD): Se refiere a definir e implementar controles que reduzcan la probabilidad de ocurrencia o impacto de un riesgo.

Evitar el Riesgo (EV): Es la opción de tomar la decisión de no realizar con la realización de una actividad propuesta o la eliminación de un proceso ya establecido.

Teniendo en cuenta las cuatro maneras de tratar un riesgo, se sugiere implementar cada una de la siguiente manera, cabe anotar que es decisión del equipo evaluador el guiarse por la propuesta o escoger la mejor estrategia siempre teniendo en cuenta el costo beneficio del tratamiento de cada uno de los riesgos.

RD	RD	RD - TR	EV – RD - TR	EV – RD - TR
RT	RD	RD - TR	RD - TR	EV – RD - TR
RT	RT	RD	RD - TR	RD - TR
RT	RT	RT	RD	RD
RT	RT	RT	RT	RD

Se debe plantear el plan de tratamiento según corresponda, posteriormente se realiza una valoración del tratamiento de riesgo propuesto analizando el costo beneficio de la solución, se identifican los riesgos residuales y ubicar en el mapa de calor identificando si se encuentra en un nivel de aceptación de riesgo, es decir, se encuentra en la opción de retención de riesgo (RT).

Luego de establecer los controles e identificar los riesgos residuales, se debe definir el mantenimiento del sistema de gestión de riesgos el cual es repetir el ciclo desde el principio, actualizar el inventario de activos de información, identificar las amenazas y vulnerabilidades, el riesgo inherente, evaluar la eficacia de los controles propuestos y sacar las conclusiones de mejora al sistema.

Definición de Controles

Cuando se toma la decisión de implementar un control para tratar un riesgo inherente en la Compañía, se deben definir las características del mismo, es decir, si es detectivo o preventivo.

Control Detectivo: Control que permite identificar la ocurrencia de un evento adverso a la seguridad e iniciar la estrategia de reacción o activar el plan de gestión de incidentes.

Control Preventivo: Técnicas que permiten establecer mecanismos para disuadir, evitar y/o proteger de cualquier afectación a los activos de información.

Anexo 4

9.4. Plan de Concienciación de Seguridad de la Información

Objetivo

- Generar una cultura de seguridad de la información en la compañía donde los colaboradores puedan aplicar los conocimientos adquiridos en el ámbito laboral como cotidiano.

Actividades

- Establecer el programa de concienciación para la compañía.
- Implementar el programa de concienciación para la compañía.
- Diseñar los temas de interés para los comunicados periódicos.
- Realizar las inducciones periódicas según requerimientos de Talento Humano.
- Realizar seguimiento al curso e-learning.
- Diseñar y socializar comunicados de concienciación para proveedores.
- Realizar charlas de concienciación para proveedores.

Cronograma

Programa	Q1			Q2			Q3			Q4			Meta
	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.	
Comunicados		1	1	1	1	1	1	1	1	1	1	1	11
Charlas											2		2
E-learning							2000						2000
Inducciones	1	2	2	2	2	2	2	2	2	2	2	1	22

Seguimiento

El seguimiento muestra el porcentaje de actividades relacionadas con las comunicaciones necesarias que permiten encaminar a la Organización a crear y adoptar una cultura de seguridad de la información, teniendo en cuenta las políticas, estándares y demás temas relacionados.

Para realizar el seguimiento necesario a los temas de concienciación y verificar el avance del indicador, se ingresan los datos descritos en el registro “Plan de concienciación”.

Dentro del registro “Plan de concienciación” se tienen en cuenta diferentes actividades como lo son los comunicados periódicos con temas de seguridad que se envían a través de los canales destinados para la difusión de información, curso e-learning, inducciones a la compañía y charlas realizadas en la semana de la seguridad; estas actividades no mantienen una periodicidad constate durante el año y pueden variar.

Los parámetros mínimos que se deben tener en cuenta para verificar el avance y el logro propuesto, son los siguientes:

- Es necesario tener como mínimo un comunicado mensual, para toda la compañía.
- Cada vez que ingrese personal a la compañía, este debe recibir una presentación de inducción de seguridad de la información.
- El curso de e-learning deberá ser realizado por lo menos una vez en el año por todos los colaboradores.
- Anualmente se debe realizar para la compañía por lo menos una charla de un experto en temas de seguridad.

Cada una de las actividades cuenta con una valoración diferente, ya sea por su dificultad en la implementación y su alcance definido; con el fin de contar con un indicador más acertado se realizan las siguientes formulas:

$$K_{31} = \left[\frac{\#\text{de comunicados enviados a la compañía}}{\#\text{ de comunicados programados durante el año}} \right] * 35\%$$

$$K_{32} = \left[\frac{\#\text{ de charlas realizadas en el año}}{\#\text{ de charlas programadas al año}} \right] * 15\%$$

$$K_{33} = \left[\frac{\#\text{ de personas que presentaron el curso e –learning}}{\#\text{ Total de personas}} \right] * 15\%$$

$$K_{34} = \left[\frac{\#\text{ de personas que reciben la inducción}}{\#\text{de personas que ingresan a la compañía}} * 15\% \right] + \left[\frac{\#\text{ de personas que pasaron el examen con 80}}{\#\text{ de personas que ingresan a la compañía}} * 20\% \right]$$

$$\mathbf{K3 = K_{31} + K_{32} + K_{33} + K_{34}}$$