DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA AGENCIA DE VIAJES Y TURISMO.

TRABAJO DE GRADO

MONICA BUESAQUILLO OSORIO
DARWIN NICOLAS LOPEZ HERRERA
ANDRES FELIPE GARCIA HENAO

INSTITUICIÓN UNIVERSITARIA POLITECNICO GRAN COLOMBIANO
FACULTAD DE INGENIERIA Y CIENCIAS BASICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ
2017

DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA AGENCIA DE VIAJES Y TURISMO.

TRABAJO DE GRADO

Docente:
ALEJANDRO CASTIBLANCO

MONICA BUESAQUILLO OSORIO
DARWIN NICOLAS LOPEZ HERRERA
ANDRES FELIPE GARCIA HENAO

INSTITUICIÓN UNIVERSITARIA POLITECNICO GRAN COLOMBIANO
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
OPCION DE GRADO
BOGOTÁ
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firma de los Jurados

Bogotá, 29 de mayo de 2017

TABLA DE CONTENIDO

INTRODUCCIÓN

En la actualidad vemos que día a día la operación de negocios en el mundo, está sufriendo una transformación gracias a los cambios tecnológicos que constantemente sufrimos a raíz de las empresas tecnológicas en su proceso de investigación y acapararían del mercado, dispositivos más potentes, acceso a la información en tiempo real, pero con ello también aparecen los riesgos inherentes al mercado, y con ello los ciberdelicuentes innovan estrategias para tener acceso a la información, y logrando con ello la alteración o robo de la misma, lo cual ocasiona a las empresas pérdida de imagen corporativa, procesos legales, pérdida de clientes, pérdida de oportunidades de negocio.

Es de carácter imperativo para las empresas brindar seguridad y protección a los datos que se recolectan dentro de su ejercicio económico, los cuales son de mayor relevancia información de clientes, proveedores, trabajadores, estrategias comerciales y demás, con la innovación tecnológica, se han visto las empresas más expuestas en el momento de garantizar los pilares fundamentales de la Seguridad de la Información – (Confidencialidad, Integridad, Disponibilidad y no Repudio), es así que el mismo estado colombiano a legislado en pro de garantizar la información de los Colombianos, y esto basado en las evoluciones que tiene el mundo digital.

Actualmente no importa el tamaño de la empresa, si es persona natural o jurídica, solo se tiene claro que lo que represente información – (Datos), están expuestos a amenazas las cuales se encuentran en riego latente de sufrir un incidente de seguridad, de allí nace la necesidad de contrarrestar este tipo de delincuencia cibernética, lo cual dentro de estos procesos de una empresa debe ser integral y transversal a las organizaciones, motivo que todas las partes que intervienen en el proceso de T.I.

Teniendo en cuenta esto se hace necesario que los comercios opten por salvaguardar la información que es entregada por sus clientes, proveedores, trabajadores y demás, generando con ello un margen de seguridad para la continuidad de negocio, seguridad de sus clientes, resguardo del patrimonio de la empresa, para nuestro caso la agencia de viajes se ve en la necesidad de alinearse a las mejores prácticas en cuanto a seguridad de la información, esto se lleva a cabo mediante la implementación de controles que sean transversales a una empresa u organización.

Dado la tendencia se opta como medida de aseguramiento el realizar el análisis e implementación de un Sistema de Gestión de Seguridad de la Información – (SGSI), basados en la normativa Iso 27001, y con la alineación a otras normatividades como Itil, Cobit, Coso, para complementar todo el SGSI.

➢ RESUMEN EJECUTIVO

1.1 DESCRIPCION GENERAL

Es una agencia de viajes la cual está dedicada dentro de su actividad económica a la prestación de servicios en el sector turismo, como lo son tiquetes aéreos, hoteles, cruceros, eventos – (Nacionales e Internacionales) parques, etc.

Dentro del Proceso de innovación tecnológica que ha establecido la Agencia de Viajes, evaluado el estado de la seguridad de la estructura de Tecnologías de la Información y con ello evaluar el nivel de riesgo que existe ante las nuevas tendencias de cibercrimenes que tiene el mundo virtual, se evidencio que existen vulnerabilidades tanto externas como internas que pueden afectar a la empresa.

Identificar los mecanismos de aseguramiento de en aras de mitigar las amenazas a nivel de Tecnologías de la Información y con ello la definición de un plan pruebas de seguridad con el ánimo de mitigar semestralmente los riegos que se generen a raíz de los múltiples cambios que se realizan en las plataformas tecnológicas e ir estableciendo protocolos y procedimientos, para garantizar la información de la empresa.

Dado el alto incremento en la actualidad de la información que se recopila, almacenada, procesa, transferida la cual se administra en las organizaciones se ve abocada a muchos riesgos, se hace necesario fortalecer el proceso y fortalecimiento del Sistema de Gestión de Seguridad de la Información, dado que no existen Políticas claras sobre la identificación de activos, plan de continuidad de negocio, gestión del riesgo, manejo apropiado de la seguridad física, falta de procesos de concientización a nivel de riesgo latentes en el mundo digital, todo esto se puede determinar que se ha mantenido de esta manera dado a la misma cultura corporativa que ronda nuestro país, y la falta de apoyo por parte del estado, lo cual establece menos probabilidades de aseguramiento del negocio por parte de todos los actores de la empresa.

Es de vital importancia que se cuente con un Sistema Gestión de la Información dado que permite conocer la falencias con que cuenta una empresa, esto conlleva a identificar e instaurar políticas, procedimientos, controles y procesos adecuados que cumplan con la seguridad y permitiendo el buen desarrollo de la Organización, adicionalmente brinda una visión global de la fase de cumplimiento en aras de la seguridad y mantener la operación de la actividad comercial de la empresa en óptimas condiciones, adicionalmente este tipo de actividades ayuda a los directivos y a la alta gerencia a tomas decisiones más acertadas a la realidad y con mayor impacto económico.

La implementación de un Sistema de Gestión de Seguridad de la Información – **SGSI**, en una empresa u Organización requiere que la misma pueda establecer una concientización dentro de todos sus colaboradores a nivel de los riegos y amenazas a los que está expuesta la Empresa u Organización, y que los mismo se encuentran tanto

a nivel Interno como externo, para que con ello se genere un sentido de pertenencia dentro de los mismo contribuyendo desde cada uno de los puestos de trabajo a ir identificando los riesgo a nivel de seguridad de la información, lo cual permite tener mayores actores en aras de salvaguardar la Información de la misma.

El proceso de implementación de un Sistema de Gestión de Seguridad de la Información - **SGSI**, que la Organización destine recursos adecuados, tanto tecnológicos como humanos, dado que dentro de este proceso se deben realizar tareas como: clasificación de activos, levantamiento de documentación, políticas y procedimientos, verificación de los procesos y controles establecidos, verificación de los parámetros que atañen a la legislación colombiana, adecuación de los modelos de capacitación y concientización de Sistema de Gestión de Seguridad de la Información.

Dada la situación encontrada y la necesidad evolutiva de la empresa, es de carácter imperativo que la Organización establezca un Sistema de Gestión de Seguridad de la Información – SGSI, mediante el cual logre establecer las métricas necesarias para salvaguardar la misma, dando con ello cumplimiento a los pilares fundamentales de la Seguridad de la Información, como lo son Confidencialidad – Disponibilidad – Integridad, y No Repudio, en aras de proteger todos los actores del proceso.

La agencia de Viajes y Turismo, se ve en la necesidad de establecer un – **SGSI**, que tenga como derrotero salvaguardar la información, que solicita, captura, procesa, almacena y elimina, dado con ello que también se debe mantener el objeto y objetivo del negocio, ya que con ello se logra a un incremento económico, social y cultural de la Organización, en aras de mejorar continuamente.

Para llevar a cabo este proceso, la Agencia de Viajes, se ve en la necesidad de Analizar, Diseñar, Establecer, Implementar y Mantener el Sistema de Gestión de Seguridad de la Información, lo cual le permitirá conocer el estado de sus activos, basado en esto se pueden mitigar, pérdidas de información, accesos no autorizados, acciones legales de los dueños de la información, desconocimiento por parte de los trabajadores de riesgos de la información, llevando con esto a que se minimicen las amenazas que están asociadas a la seguridad de la información.

Dado lo anterior se realizó una evalución del proceso de cumplimiento de la normatividad ISO 27001, para lograr establecer el nivel de cumplimiento de la Agencia de Viajes, frente a esta norma, en la cual se puedo evidenciar que el nivel de cumplimiento se encuentra por encima del 50%, adicionalmente se evidenciaron los controles que requieren ser manejados con mayor rapidez y cuales se pueden ir manejando después, también se realizó la ejecución de un análisis GAP, para determinar los riesgos inherentes al proceso de desarrollo, ya que este es uno de los eslabones más débiles a nivel de T.I., por los diferentes modelos de desarrollos y los modelos de actividades que puedan desarrollar cada uno de los mismos actores que intervienen en el proceso, encontrando con ellos que para los procesos de identificación se debe generar procesos alineados a buenas prácticas de desarrollo seguro.

Como alcance fundamental del proyecto se determina evaluar el cumplimiento de la normatividad ISO 27001, dentro de la agencia de viajes y turismo, logrando con ello establecer las falencias o carencias frente a la norma en mención, adicionalmente

identificar, cuáles son los ítems de mayor carencia de cumplimiento, para que a futuro se puedan tomar las medidas a que allá lugar y lograr su cumplimiento.

El presente proyecto no da alcance a los procesos de Planificación, Implementación, y seguimiento de mejoras a los controles establecidos en la norma ISO 27001.

Este proyecto se realizará a los procesos que hacen parte de la agencia de viajes, en el cual se evaluara el proceso de Diseño de un sistema de Gestión de Seguridad de la Información – SGSI.,

El impacto del presente proyecto, es establecer un óptimo diseño de un Sistema de Gestión de Seguridad de la Información, el cual se encontrara fundamentado en la norma ISO-IEC 27001:2013, para que dicho objetivo este constituido dentro de todo el entorno comercial de la Agencia de Viajes.

1.2 ESTADO DE LA SEGURIDAD DE LA INFORMACION EN LA AGENCIA DE VIAJES.

Dentro del Proceso de innovación tecnológica que ha establecido la presidencia de la Agencia de Viajes, con el apoyo del Departamento Interno de Auditoria, han evaluado el estado de la seguridad de la estructura de Tecnologías de la Información y con ello evaluar el nivel de riesgo que existe ante las nuevas tendencias de cibercrimenes que tiene el mundo virtual, se evidencio que existen vulnerabilidades tanto externas como internas que pueden afectar a la empresa, estas se evidenciaron mediante pruebas de pen test a través de una empresa dedicada a tal fin, en el cual se pudieron evidenciar falencias dentro de las plataformas tecnológicas, dado esto y el alto grado de vulnerabilidad al que se encontraba la empresa realiza el informe manifestado el alto riesgo de vulnerabilidades que se encontraron y sugirió el subsana miento de algunos riegos encontrados, sin embargo la recomendación inicial era que se debía implementar un SGSI – (Sistema de Gestion de Seguridad de la Información), en aras de dar cumplimiento a la Normatividad ISO 270001, con la cual se lograría realizar la mitigación de los riesgos en un 95%.

En aras de lograr mitigar las vulnerabilidades encontradas, en el tercer trimestres del año 2015 la presidencia toma la determinación de establecer una Dirección de Seguridad de la Información y adicionalmente a esto, que se establezca un seguimiento y cumplimiento a todas las normatividades y buenas practicas a que haya lugar, con el fin de evaluar:

- Estructura de redes.
- Manejo de desarrollo seguro.
- Definición del proyecto de implementación del SGSI.
- Seguridad Física.

Dado lo anterior, se debieron definir mecanismos de aseguramiento de en aras de mitigar las amenazas a nivel de Tecnologías de la Información y con ello la definición de un plan anual de pruebas de seguridad semestrales con el ánimo de mitigar semestralmente los riegos que se generen a raíz de los múltiples cambios que se realizan en las plataformas tecnológicas e ir estableciendo protocolos y procedimientos, para garantizar la información de la empresa.

Con la continua evolución de los procesos tecnológicos, en el año 2016 la Agencia de Viajes, inicia un proceso de implementación y certificación basados en la normatividad PCI-DSS, el cual es transversal a la compañía y toma bases fundamentales de la norma ISO 270001, dado con esto también se encuentra el estricto cumplimiento a la norma 1581 y el decreto 1377.

Para estos procesos de cumplimiento legislativo, la Dirección de Seguridad de la Información establece una revisión por parte de un QSA, para determinar las falencias que se presentan a nivel de cumplimiento de PCI – DSS e ISO 27001, en la cual se evidencio que existe incumplimiento a las normas anteriormente descritas, en procesos como Gobernabilidad, falta de controles a nivel de redes, falta de una estructura de análisis de riesgos, falta de una metodología clara de Gestión de Seguridad de la Información, de acuerdo a la revisión efectuada a la agencia de viajes estableció que se debe iniciar con un proceso de cumplimiento como primera medida un Sistema de Gestión de Seguridad de la Información, con el cual se podrían dar cumplimiento a las demás normatividades que eran necesarias para el manejo del negocio y aseguramiento de la misma.

1.3 IDENTIFICACION DEL PROBLEMA.

Dada el alto incremento en la actualidad la información que se recopila, almacena, procesa, transfiere y se administra en las organizaciones se ve abocada a muchos riesgos, se hace necesario fortalecer el proceso y fortalecimiento del Sistema de Gestión de Seguridad de la Información, dado que no existen Políticas claras sobre la identificación de activos, plan de continuidad de negocio, gestión del riesgo, manejo apropiado de la seguridad física, falta de procesos de concientización a nivel de riesgo latentes en el mundo digital, todo esto se puede determinar que se ha mantenido de esta manera dado a la misma cultura corporativa que ronda nuestro país, y la falta de apoyo por parte del estado, lo cual establece menos probabilidades de aseguramiento del negocio por parte de todos los actores de la empresa.

La agencia de viajes no cuenta con un Sistema de Gestión de seguridad de la Información conveniente, para mitigar los cambios tecnológicos en cuanto a la seguridad de la información los cual expone con mayor riesgo toda la operación del negocio, con lo cual se ve expuesta principalmente a fuga de información por parte de empleados inconformes, perdida de información por causa de ataques informáticos, los

ciberdelicuentes aprovechan las brechas existentes desde el eslabón más débil en la cadena de seguridad que es el ser humano, fallas de configuración en servidores, errores de desarrollo, que estas organizaciones tienen frente a la seguridad de la información.
Adicionalmente las Organizaciones que prefieren realizar sus desarrollos de acuerdo a sus necesidades comerciales no contemplan establecer mecanismos mínimos de seguridad en el proceso de desarrollo y tienen mayor riesgo de ser vulnerables a las últimas tendencias de ciberdelincuencia, falta de procedimientos, documentación de procesos, falencias en el control de acceso a la información, falta de clasificación de la información, configuraciones de servidores y aplicaciones de desarrollo por defecto.

Todo lo anterior deja expuesta a las Organizaciones a riegos altos de fuga de información, colocando el patrimonio de la empresa y la imagen corporativa a pérdidas significativas de dinero, clientes o proveedores.

1.4 PLANTEAMIENTO DEL PROBLEMA

Es de vital importancia que se cuente con un Sistema Gestión de la Información dado que permite conocer la falencias con que cuenta una empresa, esto conlleva a identificar e instaurar políticas, procedimientos, controles y procesos adecuados que cumplan con la seguridad y permitiendo el buen desarrollo de la Organización, adicionalmente brinda una visión global de la fase de cumplimiento en aras de la seguridad y mantener la operación de la actividad comercial de la empresa en óptimas condiciones, adicionalmente este tipo de actividades ayuda a los directivos y a la alta gerencia a tomas decisiones más acertadas a la realidad y con mayor impacto económico.

La implementación de un Sistema de Gestión de Seguridad de la Información – **SGSI**, en una empresa u Organización requiere que la misma pueda establecer una concientización dentro de todos sus colaboradores a nivel de los riegos y amenazas a los que está expuesta la Empresa u Organización, y que los mismo se encuentran tanto a nivel Interno como externo, para que con ello se genere un sentido de pertenencia dentro de los mismo contribuyendo desde cada uno de los puestos de trabajo a ir identificando los riesgo a nivel de seguridad de la información, lo cual permite tener mayores actores en aras de salvaguardar la Información de la misma.

El proceso de implementación de un Sistema de Gestión de Seguridad de la Información - **SGSI**, que la Organización destine recursos adecuados, tanto tecnológicos como humanos, dado que dentro de este proceso se deben realizar tareas como: clasificación de activos, levantamiento de documentación, políticas y procedimientos, verificación de los procesos y controles establecidos, verificación de los parámetros que atañen a la legislación colombiana, adecuación de los modelos de capacitación y concientización de Sistema de Gestión de Seguridad de la Información.

Dada la situación encontrada y la necesidad evolutiva de la empresa, es de carácter imperativo que la Organización establezca un Sistema de Gestión de Seguridad de la Información – **SGSI**, mediante el cual logre establecer las métricas necesarias para

salvaguardar la misma, dando con ello cumplimiento a los pilares fundamentales de la Seguridad de la Información, como lo son Confidencialidad – Disponibilidad – Integridad, y No Repudio, en aras de proteger todos los actores del proceso.

La agencia de Viajes y Turismo, se ve en la necesidad de establecer un – **SGSI**, que tenga como derrotero salvaguardar la información, que solicita, captura, procesa, almacena y elimina, dado con ello que también se debe mantener el objeto y objetivo del negocio, ya que con ello se logra a un incremento económico, social y cultural de la Organización, en aras de mejorar continuamente.

Para llevar a cabo este proceso, la Agencia de Viajes, se ve en la necesidad de Analizar, Diseñar, Establecer, Implementar y Mantener el Sistema de Gestión de Seguridad de la Información, lo cual le permitirá conocer el estado de sus activos, basado en esto se pueden mitigar, perdidas de información, accesos no autorizados, acciones legales de los dueños de la información, desconocimiento por parte de los trabajadores de riesgos de la información, llevando con esto a que se minimicen las amenazas que están asociadas a la seguridad de la información.

Adicional el control de acceso un proceso transversal a la agencia, ya que fundamentado en el control que tengan los usuario (trabajadores, proveedores, clientes), se puede tener un mayor control de la integridad, disponibilidad, confiabilidad y no repudio de la información que custodia la Organización, fundamentados en visualización de información de personal no autorizado, puntos de acceso remoto con falencias de seguridad, bajo nivel de seguridad en las contraseñas, credenciales de acceso de desarrollo en producción, usuarios con excesivos privilegios de acceso, falencia o falta de registros de log de trazabilidad.

1.5 ALCANCE

Este proyecto se realizará a los procesos que hacen parte de la agencia de viajes, en el cual se evaluara el proceso de Diseño de un sistema de Gestión de Seguridad de la Información – SGSI.

Dentro del proyecto, se utiliza como derrotero la norma NTC-ISO-IEC 27001 en su versión 2013, el cual está representado con una normatividad que rige a nivel mundial.

1.6 IMPACTO DEL PROYECTO

El impacto del presente proyecto, es establecer un óptimo diseño de un Sistema de Gestión de Seguridad de la Información, el cual se encontrara fundamentado en la norma ISO-IEC 27001:2013, para que dicho objetivo este constituido dentro de todo el entorno comercial de la Agencia de Viajes.

Como resultado del presente proyecto, se espera establecer un diseño del modelo de Seguridad de la Información para la agencia de viajes, el cual tiene el enfoque de generar los siguientes beneficios:

Misión y Visión: Establecer un Diseño de un Sistema de Gestión de Seguridad de la Información – SGSI, el cual tiene como pilar fundamental la Norma ISO-IEC 27001:2013, permitirá establecer los adecuados controles, que constituirán la confidencialidad, disponibilidad e integridad de la información, que enmarca toda la agencia de viajes.

Imagen Corporativa: Dada la alta masificación del concepto de seguridad de la información, tanto en medios de comunicación – (Prensa, Internet, Televisión, Radio), como por entes públicos y privados, se hace necesario contar con un Sistema de Gestión de Seguridad de la Información - SGSI, el cual permite que todos los intervinientes con la agencia de viajes, tenga la confianza de que su información se encuentra protegida, lo que le permitirá a la Agencia de Viajes y Turismo, crecer comercialmente.

Costos: Diseñar un Sistema de Gestión de Seguridad de la Información – SGSI, al poder los procesos y procedimientos, permite optimizar los mismos, lo que generaría una disminución de costos bien sean de factor humano o tecnológico sin afectar la productividad y seguridad de la misma.

Normatividad: Un Sistema de Gestión de Seguridad de la Información – SGSI, permite identificar cuáles son la leyes, decretos, circulares, y los normas de buenas prácticas en cuanto a seguridad de la información lo que permite establecer los riesgo que pueden afectar legalmente a la empresa, con ello mitigarlas y no incurrir en pérdidas económicas, de imagen corporativas y clientes.

1.7. OBJETIVOS

1.7.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información, para la agencia de viajes frente a la seguridad de la información, tomando como referencia la norma NTC-ISO-IEC 27001:2013.

1.7.2 OBJETIVOS ESPECÍFICOS:

OE1**.** Realizar un análisis GAP de la situación actual con base en la Norma ISO 27001:20113 con el fin de determinar el grado de madurez en cuanto a esta norma.

OE2. Determinar el nivel de cumplimiento, frente a los controles establecidos en el anexo A de la norma.

OE3. Estipular las necesidades y requerimientos necesarios en el proceso de diseño del sistema de gestión de seguridad de la información.

OE4. Determinar el modelo metodológico, que permita identificar, clasificar, valorar y tratar las amenazas de la seguridad de la información.

OE5.Definir la Política de Seguridad de la Información de la agencia de viajes, tomando como lineamiento la norma ISO 27001:2013.

1.8. PLAN DE TRABAJO:

Tabla 1: Plan de trabajo

FASE	ACTIVIDAD	FECHA INICIO	FECHA FIN	ESTADO
Diagnostico	Realizar un análisis GAP para verificar el estado actual de la Agencia frente al cumplimiento de los requisitos y el anexo A de la norma 27001:2013	1/08/2017		En revisión
	Revisar la política de SGSI que actualmente tiene implementada la Agencia	1/08/2017	22/03/2017	Revisada y ajustada
	Establecer la metodología para el tratamiento de riesgos	6/05/2017	15/05/2017	Seleccionada la metodología de riesgo
	Identificación de los riesgos a los cuales se encuentra expuesta la Agencia de viajes	1/05/2017	15/08/2017	
Diseño	Ajustar la politica de SGSI	22/02/2017	22/03/2017	
	Diseñar el mapa de riesgos de acuerdo a los riesgos identificados en la etapa de diagnostico.	20/08/2017	1/09/2017	En actualización

1.9. ENTREGABLES DEL TRABAJO.

A continuación se relacionan los entregables del presente trabajo:

1. Análisis GAP del cumplimiento a la norma 27001:2013, Anexo 1,

El análisis GAP se realizó con el fin de verificar el cumplimiento de la Agencia de viajes frente a los controles definidos en el Anexo A de la norma 27001:2013, en el cual se obtuvo lo siguiente:

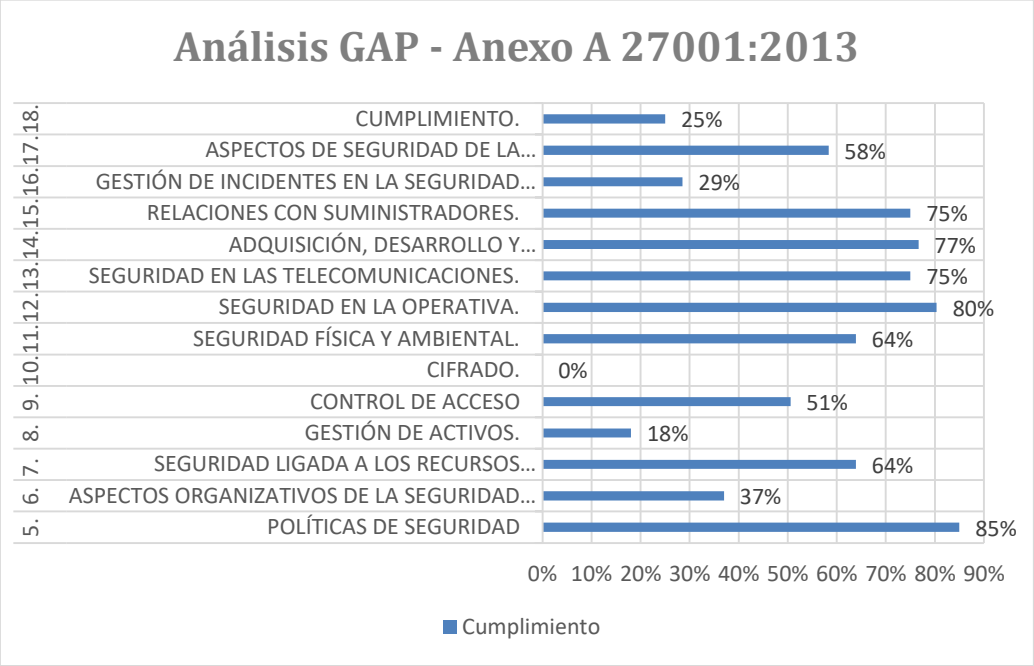

Figura 1: Análisis GAP – Anexo A norma 27001_2013

La agencia de viajes cumple con el 52.7% de la aplicación de los controles establecidos en el anexo A de la norma 27001:2013, donde los dominios de control que presentan menor cumplimiento son: Cifrado con el 0%, Gestión de activos 18%, Cumplimiento 25%, Gestión de incidentes de seguridad 29%, aspectos organizativos de la seguridad 37%.

La Agencia de Viajes cuenta con el 17.9% de cumplimiento a los requisitos establecidos en la norma 27001:2013.

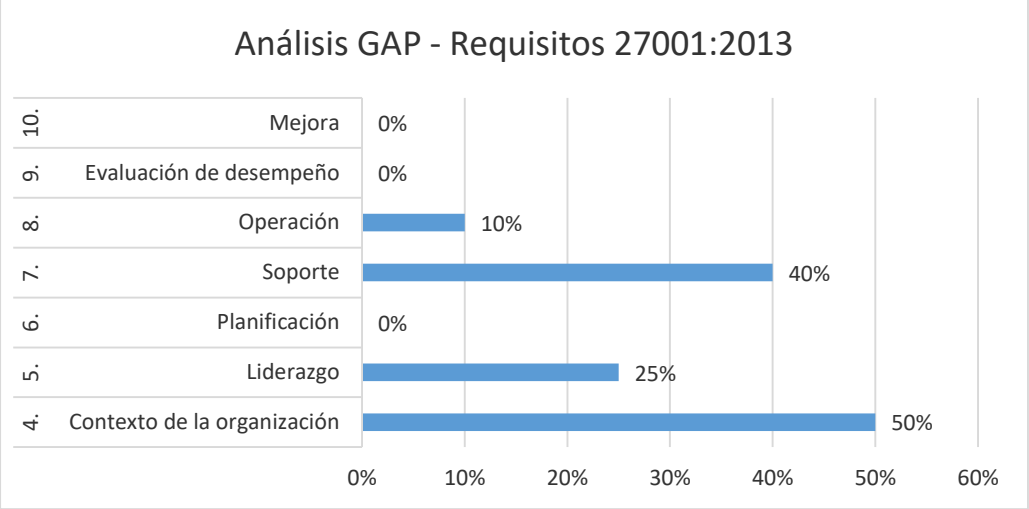

Figura 2: Análisis GAP – Requisitos norma 27001_2013

2. Política de seguridad de la información ajustada: al verificar el respectivo manual de políticas de seguridad de la Información, se realiza la modificación y se crean dos ítem más a dicho manual dado que no existían políticas para ítems como computación en la nube y bring your own device, dado que son las nuevas tendencias de Tecnologías de la Información esto se encuentra en el anexo 3

3. Mapa de riesgos, asociando los riesgos a los cuales se encuentra expuesta la organización de manera General: Los riesgos identificados en Agencia de Viajes se encuentran relacionados en el anexo 2.

4. La metodología a utilizar para el tratamiento y análisis de los riesgos en la agencia de viajes es Magerit junto con lo establecido en la norma 31000, Se realizó la segmentación de la metodología utilizada y el proceso realizado, la evidencia encontrada y el proceso realizado, adicionalmente se incluye la normatividad 31000 dado que es una norma internacional que permite entender cuál es la mejor forma de realizar el gestiona miento de los riesgos y se utiliza como un complemento a la metodología seleccionada para la identificación de riegos en entornos de T.I. anexo 4

2. JUSTIFICACION

De acuerdo a los multiplex escenarios que actualmente nacen en el Cibercrimen, se hace necesario realizar la evaluación de los diferentes actores que intervienen en los procesos tecnológicos de la Organización, para poder determinar los riesgos que se encuentran asociados a cada uno de ellos, y poder establecer procesos y procedimientos que mitiguen las brechas de riesgo en cuanto a fugas de información.

Para nuestro caso, se tomó como ejercicio de desarrollo, el evaluar todo el estado de cumplimiento de la Agencia de Viajes, en cuanto a lo relacionado con un Sistema de Gestión de Seguridad de la Información – (**SGSI**), esto dado los altos índices de incidentes de seguridad que vienen sufriendo las empresas alrededor del mundo, dado su objeto económico, se hace de suma importancia que siempre se encuentre alineada a las mejores prácticas, normatividades y legislación vigente, con el ánimo de salvaguardar la información tanto de sus clientes, como de sus procesos internos.

El diagnosticar el estado de cumplimiento de la Seguridad de la Información, tomando como base la norma ISO-IEC 27001:2013, con el fin de determinar el grado de madurez, determinar los puntos de incumplimiento, le permitirá a la agencia de viaje, establecer un modelo de trabajo para el cumplimiento a cabalidad de la misma, con ello se logra robustecer los procesos ya existentes y la adecuación de los faltantes, en cuanto a seguridad de la Información.

El proceso inicial de la identificación de las falencias o falta de controles de acuerdo a la norma ISO-IEC 27001:2013, se realizara mediante la ejecución de un análisis GAP, el cual permitirá determinar el estado de cumplimiento de los 12 Requerimientos y a su vez los controles de cada uno de los mismo, dado lo anterior se tendrá con mayor claridad el estado actual, proceso que se debe llevar a cabo con cada una de las áreas para iniciar con el proceso de implementación de los requerimientos faltantes o ajuste de los mismos.

Se evaluaran de forma inicial, un segmento de riesgos, los cuales se considera generan un mayor impacto en la agencia de viajes en el caso de que exista una materialización de los mismos, esto permitirá determinar cuál sería el modelo de remediación más óptimo, y cuál sería la forma de abordarlo adecuadamente sin generar el menor impacto en la actividad económica, y menor fricción tanto para clientes internos, externos y proveedores.

El poder establecer un modelo funcional de un Sistema de Gestión de Seguridad de la Información – **SGSI,** establece conceptos muy claros dentro de la cultura Organizacional frente a la seguridad de la información, tanto en su ámbito interno, como externo, dando mayor conocimiento de los conceptos de prevención de la información a sus trabajadores, llevando con ello a establecer una cultura de prevención y protección, tato de la información de la empresa, como la que generan cada uno de sus trabajadores.

Identificar estrategias de prevención desde cada uno de los puestos de trabajo, lo que permite que el proceso de PHVA, sea más dinámico dado que a mayor grado de aceptación por parte de los trabajadores, mayor será su contribución a mejorar el SGSI, en el manejo de riesgos, normatividad, cumplimiento de procesos, procedimientos.

3. MARCO TEORICO Y DE REFERENCIA

3.1 MARCO TEORICO

Dado la evolución tecnológica, que se ha visto en los últimos años en el mundo, asociado a la globalización de los mercados, los avances en las comunicaciones, innovación de las nuevas aplicaciones, estructuras más robustas a nivel de almacenamiento, procesamientos de datos a gran escala, el gran apetito por establecer y dominar nuevos nichos de mercado, permite que las oportunidades de negocio sean más grandes, pero también ligado a esto están más presentes los riesgos a nivel de seguridad, cada día la tendencia a la cibercriminalidad, a conseguir dinero de forma ilegal, ha permitido que los ataques informáticos sean más sofisticados, complejos y con un gran impacto de perdidas hacia las empresas, con ello se ven comprometidos datos de toda índole, es tanto así que los gobiernos mundiales día a día presentan alertas por estas situaciones, donde todas las empresas sin importar su actividad económica se ven en alto riesgo de sufrir un incidente de seguridad, es por ello que los estados se han visto abocados a establecer regulaciones que mitiguen estas amenazas, estos tipos de controles desde la legislación son mandatorios lo cual obliga a las empresas a cumplirlo sin excepción, garantizando así mitigar los riesgos de acuerdo a los estándares establecidos.

Por ello para lograr un adecuado Sistema de Gestión de Seguridad de la Información – (SGSI), se deben establecer factores claros de cumplimiento del mismo, dentro de estos se debe establecer la metodología clara, optima y evolutiva de los riesgo, lo cual permite identificar y establecer (I) el estado de cumplimiento actual de la seguridad de la información, (II) identificar y cuantificar las amenazas que comprometen la seguridad de la información, (III) determinar los mecanismos, medidas y controles que permitirán mitigar el impacto de posibles ataques informáticos donde se vean comprometidos la Disponibilidad, Integridad, Confidencialidad y No Repudio de la información.

En aras de dar claridad a los diferentes términos que atañen a un Sistema de Seguridad de la Información, se hace necesario enmarcar los diferentes conceptos de la terminología que se utilizar en el presente documento, los cuales se encuentran en el capítulo “3.2 Marco Conceptual (Glosario de Términos)”, para brindar al lector una mayor comprensión.

3.1.1 SEGURIDAD DE LA INFORMACION

De acuerdo a Wikipedia, establece que la Seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la

confidencialidad, la disponibilidad e integridad de datos y de la misma (**https://es.wikipedia.org/wiki/Seguridad_de_la_información**).

La real academia española para la calidad la define como La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

(**http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion**)

La norma internacional iso 27001

En la actualidad los datos representa el activo más importante de una empresa u organización, dado que es la materia prima de toda la operación comercial de la misma, lo que la hace un recurso muy apetecido en cualquier ámbito, llevando con ello a generar unos altos grados de amenazas por obtener las misma, y de allí surge la necesidad de la delincuencia de obtenerlo a cualquier costo, colocando en riesgo, la integridad, disponibilidad, confidencialidad y no repudio, no importa el medio en el que se encuentre la información, es de suma importancia que las empresas u organizaciones estén conscientes de los riesgos actuales y generen las medidas y controles adecuados para salvaguardar la misma.

El objetivo fundamental por el cual nace la seguridad de la información radica, en tres pilares primordiales Integridad, Disponibilidad y Confidencialidad, por lo cual establece un grupo de métodos, conceptos, normas, controles y herramientas para la debida administración de la información, establece la forma mediante la cual se deben implementar medidas y mecanismos de seguridad en todos el ámbito en el cual se solicite, capture, procese, almacene y destruya información, no importa si es fisca o digital, dando con ello las pautas necesarias para mitigar el riesgo al que se encuentra expuesta la misma.

Un Sistema de Gestión de Seguridad de la Información, es un proceso cíclico a partir de su implementación de identificación, control y mejoras, con lo cual hace partícipe a todos los actores que intervienen con una organización, todo esto se hace posible debido a que la seguridad de la información está Organizada de acuerdo a unos principios fundamentales:

Confidencialidad: Que solo el personal autorizado pueda tener acceso a la información.

Disponibilidad: Que sin importar el motivo la información debe estar disponible en cualquier momento, para aquellos que la requieran y estén autorizados.

Integridad: Que la información no sea alterada, por entes diferentes a los autorizados para tal fin, y bajo un argumento válido.

Autenticidad: que la información es real, que la información realmente representa a su dueño, y que no sea la representación de una suplantación de identidad.

No Repudio: se establece como mecanismo de control para establecer que un actor fue el emisor o receptor de la información, evitando así que se niega el origen o destino de la misma.

Trazabilidad: La propiedad del resultado de una medida o del valor de un estándar donde éste pueda estar relacionado con referencias especificadas, usualmente estándares nacionales o internacionales, a través de una cadena continúa de comparaciones todas con incertidumbres especificadas.

3.1.2 ISO 31000

La ISO 31000 tiene como objetivo “ayudar a generar un enfoque para mejorar la gestión del riesgo, de manera sistemática” y brindar diversidad de posibilidades para que de manera integral haya una gestión que permita lograr a cabalidad los objetivos de las compañías. El documento normativo establece procesos y principios para la gestión de riesgo, en la que recomienda a las organizaciones el desarrollo, la implementación y el mejoramiento continuo, como un importante componente de los Sistemas de Gestión.
La ISO 31000 permite a las organizaciones:

- Fomentar una gestión proactiva libre de riesgo.
- Mejorar la identificación de oportunidades y amenazas.
- Cumplir con las exigencias legales y reglamentarias, además de las normas internacionales.
- Aumentar la seguridad y confianza y mejorar la prevención de pérdidas y manejo de incidentes.
- Mejorar el aprendizaje organizacional.
- Mejorar la eficiencia y eficacia operacional.[1]

[1] Boletin informativo INCONTEC. Marzo 2011. http://www.tiqal.com/index.php/sistemas-de-gestion/65-iso-31000-principios-y-directrices-para-la-gestion-de-riesgos

Proceso para la gestión del riesgo:

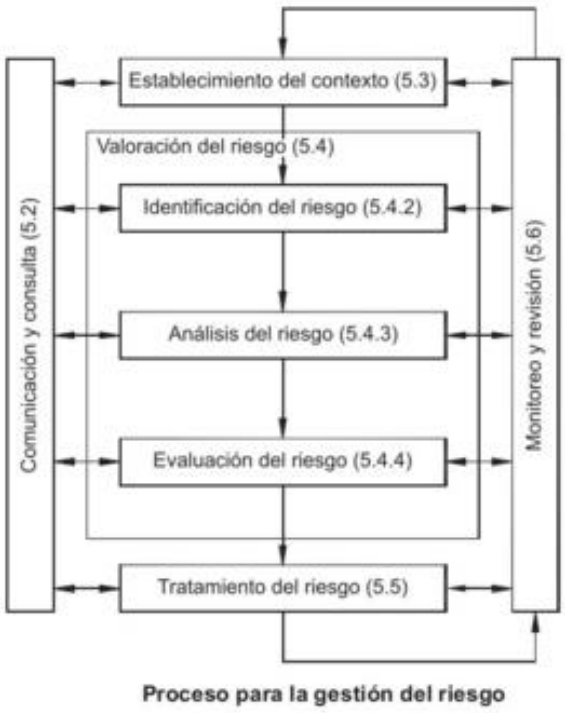

Figura 3: Proceso para la gestión del riesgo

Establecimiento del contexto: Al establecer el contexto la organización articula sus objetivos, define los parámetros externos e internos que se van a considerar al gestionar el riesgo y establece el alcance y los criterios del riesgo para el resto del proceso.

Identificación del riesgo: La organización deberá identificar las fuentes del riesgo, las áreas de impacto, los eventos y sus causas y consecuencias potenciales. El objetivo de esta fase es generar una lista exhaustiva de riesgos con base en aquellos eventos que podrían crear, aumentar, prevenir, degradar acelerar y retrasar el logro de los objetivos.

Análisis del riesgo: El análisis del riesgo implica el desarrollo y compresión del riesgo, este análisis brinda una entrada para la evaluación del riesgo y las decisiones sobre si es necesario o no tratar el riesgo y sobre las estrategias y métodos más adecuados para su tratamiento.

El análisis del riesgo involucra la consideración de las causas y fuentes de riesgo, sus consecuencias positivas y negativas y la probabilidad que tales consecuencias puedan ocurrir. Se deberán identificar los factores que afectan a las consecuencias y a la probabilidad.

Evaluación del riesgo: El propósito de la evaluación del riesgo es facilitar la toma de decisiones, basados en los resultados de dicho análisis, acerca de cuáles riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento.

La evaluación del riesgo implica la comparación del nivel del riesgo observando durante el proceso de análisis y de los criterios del riesgo establecidos a considerar en el contexto.
La evaluación del riesgo también puede tener como resultado la decisión de no tratar el riesgo de ninguna manera diferente al mantenimiento de los controles existentes.

Tratamiento del riesgo: El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones una vez implementado, el tratamiento suministra controles o los modifica.

El tratamiento del riesgo implica un proceso cíclico de:

- Valoración del tratamiento del riesgo,
- Decisión sobre si los niveles de riesgo residual son tolerables,
- Si no son tolerables, generación de un nuevo tratamiento para el riesgo, y
- Valoración de la eficacia de dicho tratamiento.

Las opciones para el tratamiento del riesgo no necesariamente son mutuamente excluyentes ni adecuadas en todas las circunstancias. Las opciones pueden incluir las siguientes:

- Evitar el riesgo a decidir no iniciar o continuar la actividad que lo origino;
- Tomar o incrementar el riesgo para perseguir una oportunidad;
- Retirar la fuente del riesgo;
- Cambiar la probabilidad;
- Cambiar las consecuencias;
- Compartir el riesgo con una o varias de las partes (incluyendo los contratos y la financiación del riesgo); y
- Retener el riesgo mediante una decisión informada.

Monitoreo y revisión: Los procesos de monitoreo y la revisión de la organización deberán comprender todos los aspectos del proceso para la gestión del riesgo con el fin de:

- Garantizar que los controles son eficaces y eficientes tanto en el diseño como en la operación;
- Obtener información adicional para mejorar la valoración del riesgo;
- Analizar y aprender lecciones a partir de los eventos (incluyendo las causas accidentales), los cambios, las tendencias, los éxitos y los fracasos;
- Detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios del riesgo y en el riesgo mismo que pueden exigir revisión de los tratamientos del riesgo y las prioridades; y

- Identificar los riesgos emergentes. [2]

Debido a que la agencia de viajes no cuenta con un sistema de gestión, que permita realizar un adecuado manejo de la información, y debido a que esta es un recurso que, como el resto de los activos, tiene valor para una organización y por consiguiente debe ser debidamente protegida, y de acuerdo a la metodología utilizada para el análisis del riesgo la norma 31000 y junto con la 27001, se realizará la identificación de los riesgos para las área de ventas y la TI.

3.1.3 METODOLOGÍA DE RIESGOS - MAGERIT:

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.[3]

MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Magerit persigue los siguientes objetivos:

1. concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
4. preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.[4]

3.1.4 CICLO DE MEJORA PARA EL SGSI:

Con el fin de mantener e implementar un Sistema de Gestión de Seguridad de la Información, es necesario tener en cuenta el ciclo de mejora del SGSI, para el cual se debe tener una planeación, antes de llevar a cabo las tareas, luego de llevarlas a cabo se debe verificar si esta cumplimiento con el requerimiento para así mismo en caso necesario realizar las correcciones a que haya lugar.

---

[2] Compendio de normas de gestión de riesgo. 30-05-2014. http://es.slideshare.net/delosaga72/norma-iso-31000

[3] MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WQ991DDhDIU.

[4] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. octubre 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[5]

Figura 4: PHVA

Planear:

- **Contexto de la organización** se resalta la necesidad de hacer un análisis para identificar los problemas externos e internos que rodean a la organización. De esta forma se puede establecer el contexto del SGSI incluyendo las partes interesadas y que deben estar en el alcance del SGSI.
- **Liderazgo**, se definen las responsabilidades de la Alta Dirección respecto al SGSI, principalmente en aquellas que demuestren su compromiso, como la definición de la política de seguridad de la información alineada a los objetivos del negocio y la asignación de los recursos necesarios para la implementación del sistema.
- **Planeación**, se prioriza la definición de objetivos de seguridad claros que permita relacionar planes específicos asociados a su cumplimiento. Dentro de la evaluación de riesgos el enfoque se orienta hacia la identificación de aquellos riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, donde el nivel de riesgo aceptable se debe definir en función de la probabilidad de ocurrencia del riesgo y las consecuencias generadas en caso de que este llegara a materializarse (impacto).
- **Soporte** se relacionan los requerimientos para implementar el SGSI incluyendo recursos, personas y el elemento de comunicación para las partes interesadas en el sistema.

Hacer:

- **Operación**, se establecen los mecanismos para planear y controlar las operaciones y requerimientos de seguridad, siendo el las evaluaciones de riesgos periódicas el enfoque central para la gestión del sistema. En cuanto a los

[5] Publicación ISO 2017:2013, cambios en la norma para gestionar la seguridad de la información. 09-10-2013 https://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

activos de información, las vulnerabilidades y las amenazas se utilizan para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad.

Verificar:

- **Evaluación del desempeño** se definen las bases para medir la efectividad y desempeño del sistema de gestión a través de las auditorías internas y otras revisiones del SGSI, que plantean planes de acción que permitan atender y solucionar las no-conformidades.

Actuar:

- **Mejora** propone a partir de las no-conformidades identificadas establecer las acciones correctivas más efectivas para solucionarlas y teniendo el control de que no se repitan.[6]

3.2 MARCO CONCEPTUAL (Términos y definiciones):

Aceptación del riesgo: decisión de asumir un riesgo

Activo: cualquier cosa que tiene valor para la organización

Análisis de riesgo: uso sistemático de la información para identificar las fuentes y estimar el riesgo

Amenaza: Es la causa potencial de un daño a un activo de información.

Causa: Razón por la cual el riesgo sucede.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información

Declaración de aplicabilidad: documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada

Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo

---

[6] Publicación ISO 2017:2013, cambios en la norma para gestionar la seguridad de la información. 09-10-2013 https://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión del Riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Riesgo residual: nivel restante de riesgo después del tratamiento del riesgo.

Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

Sistema de gestión de la seguridad de la información: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

Valoración del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.[7]

4. METODOLOGÍA:

La metodología que utilizaremos para la problemática presentada en la Agencia de Viajes, es basada en lo establecido en la norma 27001:2013, magerit con el complemento de la norma 31000, las cuales permitirán la implementación de un sistema de gestión de seguridad de la información para la agencia.

4.1 TIPO DE INVESTIGACIÓN:

El tipo de investigación que utilizaremos es la investigación de campo, ya que se trata de la investigación aplicada para comprender y resolver alguna situación, necesidad o

[7] NTC-ISO-IEC 27001:2013, Pág. 11-12, http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

problema en un contexto determinado[8]. Con este tipo de investigación se pretende dar solución a la necesidad que actualmente presenta la Agencia de Viajes, en cuanto al manejo y protección de la información tanto de los clientes como de la misma organización.

4.2 LINEA DE INVESTIGACIÓN:

La línea de investigación que tendremos en cuenta para la problemática de la agencia de viajes, es basarnos en los requerimientos y el anexo A de la norma 27001:2013, y la gestión de riesgos establecida en la metodología Magerit y la norma 31000.

4.3 INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN:

Los instrumentos que utilizaremos para la recolección de la información son:

- Análisis GAP con el fin de verificar el cumplimiento de los controles establecidos en el anexo A de la norma 27001:2013 y los requisitos de la misma.
- Entrevistas al personal del área de seguridad de la información de la Agencia de Viajes.
- Revisión de la documentación existente en la agencia frente a la seguridad de la información.

4.4 FASES DE METODOLOGÍA:

Con el fin de dar cumplimiento a las metodologías planteadas anteriormente que es la norma 27001:2013, magerit y norma 31000 se llevaran a cabo las siguientes fases que hacen parte del ciclo de mejora del SGSI:

Fase I

Diagnóstico: en esta fase se realizará el análisis GAP con el fin de identificar el estado en que se encuentra la agencia de viajes frente a los controles establecidos en el Anexo A y los requisitos de la norma 27001:2013, verificación de la política de seguridad de la información, identificación de los riesgos a los cuales se encuentra expuesta la Agencia e identificación de la metodología para el tratamiento de los mismos.

Fase II

Diseño: se realizará el mapa de riesgo de acuerdo a los riesgos identificados en la fase anterior, ajuste de la política de SGSI para la Agencia de Viajes.

---

[8] http://www.ecotec.edu.ec/documentacion%5Cinvestigaciones%5Cdocentes_y_directivos%5Carticulos/4955_Fcevallos_00009.pdf

5. RESULTADO Y DISCUSIÓN:

5.1 FASE I DIAGNOSTICO:

Esta fase se planteó con la certeza de alcanzar a desarrollar los objetivos específicos establecidos en el presente trabajo, donde los resultados de los diagnósticos permitieron.

- El estado actual de la seguridad que se encuentra justificado en el capítulo **3.1.1 SEGURIDAD DE LA INFORMACION** del presente escrito, por medio de este podremos alcanzar el OE1, junto con la creación del análisis GAP se determinó la madurez como está la entidad con respeto a la norma ISO 27001-2013 esto se encuentra justificado en el anexo **ANALISIS GAP**
- Con la creación del anexo A se determina el nivel de cumplimiento a los controles establecidos en la norma. Por medio de este podremos alcanzar el OE2.
- Identificación de las necesidades y planificación que se encuentra definida en el capítulo **3.1.4 CICLO DE MEJORA PARA EL SGSI** con esto se logra alcanzar el OE3.

PLANEAR	Establecer los métodos que se necesitan para verificar el estado en que se encuentra la Agencia de viajes frente al cumplimiento de los requisitos de la norma 27001:2013.
	Generar un plan de trabajo para llevar a cabo el diseño de la implementación de SGSI para la agencia de viajes.
HACER	Ajustar la política de seguridad de la información
	Realizar un GAP analisis para verificar el estado actial de la agencia frente los requisitos establecidos en la norma 27001:2013
	Identificación de los riesgos a los cuales se encuentra expuesta la organización.
	Establecer la metodología para la gestión de riesgos.
VERIFICAR	Verificar el cumplimiento a lo establecido en el hacer: el mapa de riesgo creado cumpla con la metodología MAGERIT y la ISO 31000, que la política de SGSI para la Agencia de viajes haya quedado ajustada. Y por ultimo tener un análisis de la información obtenida del GAP.
ACTUAR	Realizar acciones de mejora o no conformidades frente a lo establecido en el hacer.

- Determinar el modelo metodológico, que permita identificar, clasificar, valorar y tratar las amenazas de la seguridad en el capítulo **3.1.3 METODOLOGÍA DE RIESGOS - MAGERIT** con esto se logra alcanzar el OE4.
- Verificar que la Política de Seguridad de la Información de la agencia de viajes, se encuentre alineada a la norma ISO 27001:2013 para lograr alcanzar el OE5.

OE1. Análisis de la situación actual de la entidad y análisis GAP.

La situación actual de la entidad con base a la implementación de un SGSI, se determinó mediante estudio realizado en el capítulo **1.2 ESTADO DE LA SEGURIDAD DE LA INFORMACION EN AGENCIA DE VIAJES** del presente escrito en donde se pudieron identificar las dificultades con que cuenta la entidad en materia de

vulnerabilidades con respeto de no contar con un Sistema de Gestión de Seguridad de Información.

Para el levantamiento de esta información se realizó a través de recolección de datos donde se vieron involucradas todas las áreas de la entidad.

Con base a que uno de los autores de este escrito labora en la entidad y conoce información de primera mano se dio a la tarea de identificar las situaciones más críticas y vulnerables dentro de la entidad.

- Se involucró a la alta gerencia y al área de control interno en las prioridades de implementar controles por medio de un SGSI
- Se recolecto información de documentación impresa y digital en donde se encontraron falencias en materia de protección de datos
- Haciendo un consenso general en toda la entidad se identificó lo siguiente:

    - La falta de concientización y apropiación por parte de los empleados en temas de seguridad.
    - No existe una integración coactiva de todas las áreas en la definición de los controles de seguridad con respecto a los riesgos.
    - Los funcionarios no asocian la diferencia entre seguridad informática y seguridad de la información
    - Se encontraron falencias en controles a nivel de redes.
    - Falta de una metodología clara de Gestión de Seguridad de la Información.

De acuerdo a la revisión efectuada a la agencia de viajes estableció que se debe iniciar con un proceso de cumplimiento como primera medida un Sistema de Gestión de Seguridad de la Información.

Por medio de este análisis se consolido el estado actual de la entidad con respecto al cuestionario que allí se formula, se desarrolló en compañía del personal involucrado en seguridad. Donde se identificaron cuales se cumplen y cuáles no, generando un estado del arte para poder logar la implementación del SGSI. La cual permitirá alcanzar el OE1

OE2. Anexo A

Con este se logra determinar el nivel de cumplimiento a los controles establecidos por la norma. Con la ayuda de este análisis se logra alcanzar el OE2.

OE3. Necesidades y planificación.

Con el fin de implementar un Sistema de Gestión de Seguridad de la Información, es necesario tener en cuenta el ciclo de mejora del SGSI, para el cual se debe tener una planeación, antes de llevar a cabo las tareas.

Con el fin de lograr establecer un SGSI, optimo y que sea gestionable sin generar traumatismo a la operación comercial se deben identificar las falencias en la actualidad del SGSI, para lo cual se realizó un análisis gap, el cual permitió identificar el grado de cumplimiento por cada uno de los ítem que atañen a la norma ISO 27001, para poder determinar el grado de cumplimiento, adicional a esto se logró establecer los ítems que se encuentran más avanzados, y cuales se encuentran más avanzados y cuáles no para dar mayor prioridad a aquellos que tienen un cumplimiento inferior al 50%, dado lo anterior se logra evidenciar que los ítems de menor cumplimiento . Las necesidades más relevantes son las siguientes:

- Políticas claras sobre la Gestión de Activos
- Plan de continuidad de negocio
- Gestión de Incidentes.
- Cifrado.
- desarrollo en aplicativos
- Clasificación de la información

Debido a que la entidad no cuenta con un Sistema de Gestión de Seguridad de la Información conveniente y con la identificación de las necesidades antes expuestas; se puede llegar a alcanzar o cumplir el OE3.

OE4. Metodología de la medición del riesgo.

La metodología que se quiso implementar y la cual nos pareció la más acertada fue la metodología del análisis y gestión de riesgos la cual se conoce con el nombre de MAGERIT en donde reza "*la respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.*

Implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Sus objetivos son:

- concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Con esta metodología se pretende preparar a la entidad en el manejo de los riesgos que se presentan a diario y la forma más adecuada de hacerles frente y mitigar los

daños que se llegaran a presentar y de una u otra manera preparar y enfocar a la entidad en los objetivos que se presentan en esta metodología. Con esto se logra alcanzar a cumplir con el OE4.

OE5. Políticas.

Al verificar la política que actualmente tiene establecida la Agencia de viajes debe ser ajustada para dar cumplimiento a los requisitos establecidos en la norma 27001:2013. Con esto se logra darle alcance al OE5.

5.2 FASE I DISEÑO:

En esta fase se llevó a cabo la creación del mapa de riesgo de acuerdo a las vulnerabilidades y amenazas evidencias en la Agencia frente a al SGSI, el cual se encuentra en el Anexo 2: Mapa de riesgos.

La política del SGSI ajustada para la Agencia de Viajes es:

La información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección y cuidado de sus propiedades más significativas, como parte de una estrategia orientada a la continuidad de la actividad comercial y la consolidación de una cultura de seguridad de la información.

Los objetivos son:

- Proteger los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información de la Agencia de Viajes.
- Asegurar la implementación de las medidas de seguridad comprendidas en esta Política.
- Establecer, mantener y controlar las políticas en seguridad de la información de la Agencia de Viajes, con el fin de regular la gestión de la seguridad de la información al interior de la compañía.

6. CONCLUSIONES:

Como se ha mencionado en este trabajo, que debido a que en la actualidad los ciberdelicuentes cada vez implementan nuevas técnicas con el fin de modificar o robar la información, se ve la necesidad de que las organizaciones implemente un SGSI, con el fin de salvaguardar la información que manejan.

Por lo anterior este trabajo se basa en el diseño para la implementación de un Sistema de Gestión de Seguridad de la Información basado en un modelo de la norma ISO/IEC

27001:2013 acompañada de la norma 31000, en la Agencia de viajes con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, adicional a esto ayudará identificar los posibles riesgos a los cuales se encuentra expuesta la organización.

7. BIBLIOGRAFÍA

- Boletin informativo INCONTEC. Marzo 2011. http://www.tiqal.com/index.php/sistemas-de-gestion/65-iso-31000-principios-y-directrices-para-la-gestion-de-riesgos
- https://es.wikipedia.org/wiki/Seguridad_de_la_información
- http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion
- Compendio de normas de gestión de riesgo. 30-05-2014. http://es.slideshare.net/delosaga72/norma-iso-31000
- Publicación ISO 2017:2013, cambios en la norma para gestionar la seguridad de la información. 09-10-2013 https://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/
- NTC-ISO-IEC 27001:2013, Pág. 11-12, http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf
- http://www.ecotec.edu.ec/documentacion%5Cinvestigaciones%5Cdocentes_y_directivos%5Carticulos/4955_Fcevallos_00009.pdf
- Las
- situaciones problemáticas implementadas como una estrategia importante .http://ayura.udea.edu.co/logicamatematica/sit_problematicas.htm
- Seguridad de la información. 2016. https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
- Las pruebas de vulnerabilidad. http://www.stealth-iss.com/securityes/vulassess.html.
- MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WQ991DDhDIU.
- MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. octubre 2012. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

8. ANEXOS

A. Anexo 1: Análisis GAP.

Dentro del proceso de alineación y buenas practicas que tiene establecido la Agencia de viajes y turismo, se hizo necesario el realizar un análisis GAP, mediante el cual se pudiera establecer el grado de cumplimiento de la empresa frente a la norma ISO 27001, con el fin de establecer los puntos que se cumplían a cabalidad y cuales no y su grado de cumplimiento a nivel porcentual, para establecer el nivel de cumplimiento.

Dentro del análisis realizado se pudo establecer que se cumple la norma ISO 27001, en un 52,7% lo cual permite establecer que existe un avance significativo, pero que falta trabajo por realizar el cual demanda recursos e inversión económica, a continuación veremos una breve descripción a grandes rasgos de cada uno de los Ítems de cumplimiento:

- **(5.) Políticas de Seguridad:** El cumplimiento de este requerimiento se encuentra en el 85%, teniendo faltante realizar el proceso de adecuación que demanda la ley anualmente.
- **(6.) Aspectos Organizativos de la Seguridad de la Información:** para este ítem el cumplimiento se encuentra 37%, no se encuentra completa la asignación de responsabilidades a cada uno de los actores que intervienen en el proceso, y no existe claridad en el proceso de móviles y teletrabajo.
- **(7.) Seguridad Ligada a los Recursos Humanos:** En la actualidad tiene como implementación un 63,9%, estando en estado pendiente procedimientos de antecedentes, capacitación, manejo de puestos de trabajo.
- **(8.) Gestión de Activos:** para este ítem el grado de implementación es de un 18.1%, dados que no existe procedimientos claros para la responsabilidad de los activos, no hay proceso de clasificación, ni proceso de almacenamiento demarcado.
- **(9.) Control de Accesos:** El avance se encuentra en el 50,6%, actualización de política de control de accesos, implementación y adecuación los derechos y responsabilidades de los usuarios, como adecuación de controles de acceso.
- **(10.) Cifrado:** no se han establecido procesos, ni procedimientos criptográficos, por lo cual este ítem se encuentra en un 0.0%.
- **(11.) Seguridad Física y Ambiental:** Para este punto se encuentra el proceso totalmente ejecutándose pero no existe una documentación de los ítems anexos, por lo cual su cumplimiento se encuentra en un 77,8%.
- **(12.) Seguridad Operativa:** para este ítem existe un grado de cumplimiento del 80,4%, dado que se encuentra pendiente la mayoría de la documentación y los procesos de registro y supervisión.

- **(13.) Seguridad en las Telecomunicaciones:** para este ítem se establece un cumplimiento del 75,0%, dado que no existe la mayoría de la documentación del ítem en mención.
- **(14.) Adquisición, Desarrollo y Mantenimiento de los Sistemas:** se encuentra en cumplimiento en el 76,7%, dado que se encuentra pendiente los procedimientos y parte de los procesos de protección de software.
- **(15.) Relación con los Suministradores:** Se encuentra en un 75%, dado que se deben acondicionar y crear los procedimientos faltantes.
- **(16.) Gestión de Incidentes de Seguridad de la Información:** para este ítem hacen falta procedimientos y ajustar procesos de acuerdo a los avances tecnológicos, por lo cual su avance se encuentra en el 28,6%.
- **(17.) Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio:** No está claro el proceso de continuidad de negocio, se debe ajustar el actual, los recientes y continuos cambio de tecnología, y establecer los modelos de prueba pertinente, por lo cual su cumplimiento es del 58,3%.
- **(18.) Cumplimiento:** A nivel de cumplimiento se evidencia un avance del 25,0% dado que hace falta, todo el proceso de documentación, y formatos de revisiones.

B. Anexo 2: Mapa de riesgos.

Dentro del proceso de ejecución del mapa de riesgos, se contempló inicialmente los procesos que atañen a T.I., y con el cual la seguridad de la información se ve más afectada por los procesos de descuido de los desarrolladores en el momento de realizar la codificación de los programas bien sea para necesidades pequeñas como para el manejo grandes proyectos de implementación, sin embargo dentro del análisis realizado se evidenciaron que pueden existir grandes brechas de seguridad a nivel de los proveedores o de los mismos trabajadores internos, los cuales por desacuerdo en su terminación laboral o en desacuerdo con las políticas de la empresa pueden colocar en riesgo el negocio.

Dado lo anterior se evaluaron condiciones como políticas de acceso, perfiles y roles de cada uno de los cargos que pudiesen existir, como también el acceso con el que cuentan los proveedores dependiendo del proceso que deban realizar, llevando con ello a identificar que los riesgos están latentes en cada uno de los actores que intervienen en cada proceso, y que dependiendo de su actividad laboral, pueden colocar en riesgo más o menos la información de la empresa, exponiéndola a pérdidas económicas, de imagen corporativa, sanciones legales, perdidas de clientes y demás.

La presente recopilación tiene como objetivo fundamental establecer las brechas de seguridad más evidentes y así poderlas mitigar, sin importar el ámbito en el cual se presenten, llevando con ello a estar preparados ante ataques de hackers que puedan ser contratados por la competencia, empleados desleales o la simple mitigación del entorno de cyberterrorismo y cyberdelincuencia que está proliferando en estos últimos tiempos.