FORMULACIÓN DE ACCIONES DE MEJORA DEL PROCESO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA LITIGAR PUNTO COM BASADOS EN LA NORMA ISO/IEC 20000-1 Y LAS BUENAS PRÁCTICAS DE ITIL V3 EN LA CIUDAD DE BOGOTÁ

PRESENTADO POR:

DIANA MARCELA CAVIEDES

NUBIA ESPERANZA ROA VANEGAS

UNIVERSIDAD COOPERATIVA DE COLOMBIA FACULTAD INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
BOGOTÁ
2019

FORMULACIÓN DE ACCIONES DE MEJORA DEL PROCESO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA LITIGAR PUNTO COM BASADOS EN LA NORMA ISO/IEC 20000-1 Y LAS BUENAS PRÁCTICAS DE ITIL V3 EN LA CIUDAD DE BOGOTÁ

PRESENTADO POR:
DIANA MARCELA CAVIEDES MONROY
NUBIA ESPERANZA ROA VANEGAS

Modalidad de grado Seminario de perfeccionamiento
Requisito Parcial para obtener el título de Ingeniero de Sistemas

Director
JOSÉ FERNANDO SOTELO CUBILLOS

UNIVERSIDAD COOPERATIVA DE COLOMBIA FACULTAD INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
BOGOTÁ
2019

NOTA DE ACEPTACIÓN

PRIMER JURADO

SEGUNDO JURADO

Bogotá, marzo, 2019

CONTENIDO

LISTA DE TABLAS

LISTA DE GRÁFICAS

LISTA DE ANEXOS

GLOSARIO

Activos: Son los bienes, derechos y otros recursos controlados económicamente por la empresa.

Alertas: Hace referencia a una situación de vigilancia o atención. Un estado o señal de alerta es un aviso para que se extremen las precauciones o se incremente la vigilancia.

Confidencialidad: Es la cualidad de confidencia que se dice o hace en confianza y seguridad entre dos o más individuos.

Defensa: Esta acción, por su parte, refiere a cuidar, resguardar o conservar algo. La defensa, por lo tanto, es aquello que brinda protección de alguna forma o el resultado de defenderse.

Diligencias: Acta que se extiende para acreditar la comparecencia de una person a.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

ITIL: Biblioteca de infraestructura TI

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Litigar: Enfrentarse o disputar sobre una cosa en un juicio.

Políticas: Es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos. También puede definirse como una manera de ejercer el poder con la intención de resolver o minimizar el choque entre los intereses encontrados que se producen dentro de una sociedad.

Resguardada: Es proteger o defender a una persona o cosa.

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.

INTRODUCCIÓN

En los últimos años la seguridad de las tecnologías de la información se ha convertido en una de las preocupaciones más importantes de las empresas. La información es quizá uno de los activos más críticos, sin información o con una información alterada, las compañías no pueden desarrollar su actividad. Pero aun conservando la información, si ésta es accedida y cae en manos de la competencia, o es divulgada en el mercado, el daño puede ser aún mayor.

La facilidad de acceso a cualquier parte del mundo mediante la gran red Internet, pone al alcance de la mano cualquier ordenador que esté conectado a ella. Los ataques, los virus, los gusanos y los troyanos son cada vez más frecuentes. La adecuada gestión de la seguridad de la información se ha convertido por obligación en uno de los objetivos estratégicos de toda compañía.

Por esta razón es importante implementar un sistema de gestión de la seguridad de la información basado en la norma ISO IEC 20000 y buenas prácticas de ITIL V3 en la empresa litigar punto com, para que sea gestionada la confidencialidad, la disponibilidad y la integridad de los datos y propiedad intelectual de la organización.

Con la implementación del proceso de gestión de seguridad de la información basados en la norma ISO IEC 20000 e ITIL V3 podremos obtener beneficios significativos para la compañía litigar punto com, esto permitiendo que la empresa sea confiable ante sus clientes puesto que la seguridad de la información va a estar basada en esta norma y buenas prácticas por lo cual la norma obliga a tener una serie de políticas y planes de seguridad del negocio, planes y requerimientos futuros del negocio e ITIL permite unas buenas práctica.

FORMULACIÓN DE ACCIONES DE MEJORA DEL PROCESO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA LITIGAR PUNTO COM BASADOS EN LA NORMA ISO/IEC 20000-1 Y LAS BUENAS PRÁCTICAS DE ITIL V3 EN LA CIUDAD DE BOGOTÁ

1. DESCRIPCIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Formulación del Problema:

La empresa litigar punto com dedicada a ofrecer servicios de revisión y vigilancia de procesos judiciales, carece de un debido proceso de Gestión de seguridad de la información que les garantice a los clientes y miembros de la empresa que su información está resguardada de forma segura y confiable.

Proceso que debe garantizar el nivel de seguridad requerido sobre los activos utilizados por la organización para la prestación de los servicios de TI. ¿Qué acciones de mejora pueden aportar beneficios al proceso de Gestión de seguridad de la información en la compañía Litigar Punto com apoyados en la norma ISO/ IEC 20000 e ITIL V3 que mitigue toda clase de ataques y vulnerabilidades de la información, como principal activo de la organización?

1.1.2 Justificación del problema:

Actualmente en la empresa litigar punto com maneja aproximadamente 250 clientes y más de 500 personas laborando en la compañía. Su principal problemática es que el proceso de gestión de seguridad de la información no cuenta con los estándares adecuados y nadie hace un control para analizar si se está cumpliendo lo allí mencionado, esto aumentando el riesgo de pérdida de la información, secuestro de información, alteraciones en la información, problemas de acceso a las aplicaciones y autenticación de usuarios, en la actualidad se tiene aproximadamente un 80% de vulnerabilidad en la seguridad de la información, es por esta razón que con la implementación del proceso de gestión de seguridad de la información basados en la norma ISO/IEC 20000 y en la buenas prácticas de ITIL, en la sede principal ubicada en la ciudad de Bogotá, podremos aporta a la reducción de riesgos de virus, troyanos, gusanos, mejor custodia de los activos de información de la empresa, aumenta la fiabilidad de los servicios, reduciendo la probabilidad de incidentes de seguridad, desarrollo de métodos más eficientes de seguridad, una gestión integral que proporcione una visión conjunta del impacto de la seguridad del negocio y mejora continua del nivel de riesgo de los servicios prestados a clientes.

El modelo de Gestión de Seguridad de la información basado en la norma ISO/IEC 20000 e ITIL debe garantizar el nivel de seguridad requerido sobre los activos utilizados por la organización para la prestación de los servicios de TI

.

1.2. OBJETIVOS DEL PROBLEMA

1.2.1 Objetivo General:

Formulación de acciones de mejora en el proceso de gestión de seguridad de la información de la empresa Litigar punto com basados en la norma ISO/IEC 20000 1:2011 y las buenas prácticas de ITIL V3 en la ciudad de Bogotá, que asegure que los activos de información utilizados en la prestación de los servicios se encuentren en unos niveles de exposición al riesgo aceptables para el negocio

1.2.2 Objetivos específicos:

1. Diagnosticar las condiciones actuales de gestión de seguridad de la información en la empresa litigar punto com evaluando los activos, amenazas de seguridad, vulnerabilidades, probabilidades, impacto y nivel de riesgo

2. Identificar el riesgo de seguridad en la empresa litigar punto com, declararlos y crear el plan de tratamiento de los riesgos de seguridad.

3. Formular un sistema de políticas en la empresa litigar punto com, para identificar, controlar y proteger la información y cualquier equipamiento empleado junto con el almacenamiento, transmisión y procesamiento de dicha información.

4. Definir las acciones de mejoramiento para el desarrollo eficiente del proceso de gestión de seguridad de la información de la empresa litigar punto com, basada en la norma ISO 20000 1:20011 e ITIL

2. MARCOS DE REFERENCIA

2.1 Marco Teórico

El proyecto se basará con la teoría que hace relación a la gestión de seguridad de la información basado en la norma ISO/IEC 20000 y en las buenas prácticas de ITIL, con esto se busca mejorar la gestión de la información en la empresa litigar punto com.

“Las Tecnologías de Información y Comunicaciones (TIC) son recursos esenciales para la productividad y competitividad de las organizaciones; sin embargo, como cualquier recurso, está sujeto a múltiples amenazas que se pueden materializar en riesgos, con múltiples consecuencias.

Hoy en día las amenazas tecnológicas son parte de nuestra cotidianeidad y más aún de la vida organizacional, las cuales van desde diversas formas de virus, pasando por los recientes ataques de *ransomware* hasta amenazas sofisticadas como los ataques día cero (en inglés, *zero-day attack*) lo cual requiere la implementación de controles que puedan ser gestionados a través de un adecuado enfoque de seguridad de la información.

La seguridad de la información es un proceso en el que se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión organizacionales, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, etc. abarcando no solo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales, humanos, etc.

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia

organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de estos.

2.1.1 Marco ITIL

ITIL, la versión original de ITIL fue un manual publicado en la década de 1980 para ayudar a los departamentos gubernamentales de TI en el Reino Unido a establecer un marco para las mejores prácticas . Si bien ITIL v2 se mantuvo enfocado en las operaciones de TI básicas, ITIL v3 enfatiza el concepto de que TI es un servicio que respalda los objetivos comerciales.

El marco ITIL v3 se divide en cinco secciones:

Estrategia de servicio de ITIL

Especifica que cada etapa del ciclo de vida del servicio debe permanecer enfocada en el caso de negocio , con los objetivos de negocio definidos, los requisitos y los principios de administración del servicio.

Diseño de servicios ITIL

Proporciona orientación para la producción y el mantenimiento de políticas, arquitecturas y documentos de TI.

Transición del servicio ITIL

Se enfoca en el rol de la administración del cambio y las prácticas de liberación, brindando orientación y actividades de proceso para la transición de servicios al entorno empresarial.

Operación del servicio ITIL

Se centra en las actividades de proceso de entrega y control basadas en una selección de puntos de control de prestación de servicio y soporte de servicio.

Mejora continua del servicio de ITIL

Se centra en los elementos del proceso involucrados en la identificación e introducción de mejoras en la gestión del servicio, así como en los problemas relacionados con la jubilación del servicio."[1]

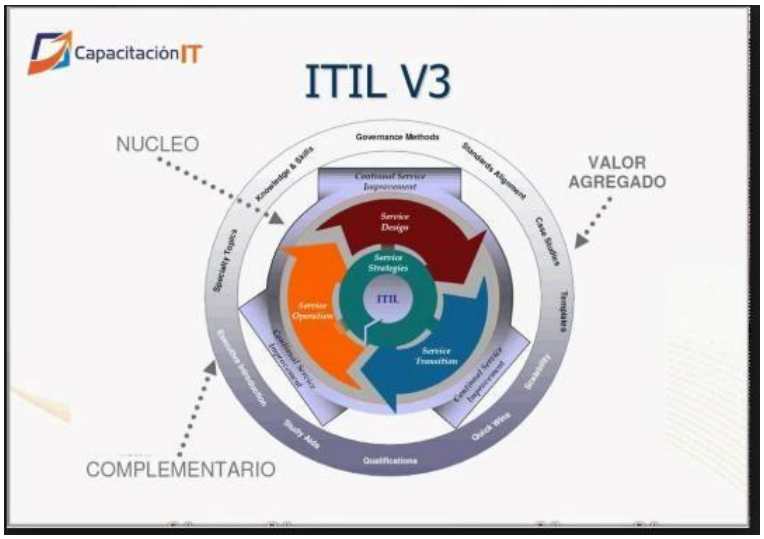


Ilustración 1/ITIL V 3.

2.1.2 Marco ISO/IEC 20000-1 2011

"La norma ISO/IEC 20000 promueve la adopción de un enfoque de procesos integrados, para una provisión eficaz de servicios gestionados que satisfaga los requisitos del negocio y de los clientes.

[1]ROUSE, Margaret. ITSM-gestión-de-servicios-de-TI. [En línea]. 1a ed.2016. [Citado 10-marzo-2019]. Disponible en internet: https://searchdatacenter.techtarget.com/es/definicion/ITSM-gestion-de-servicios-de-TI

(Sistema de Información Científica Red de Revistas Científicas de América Latina y el Caribe, España y Portugal)

ISO/IEC 20000-1:2005 Information technology - Service management - Part 1: Specification, ISO/IEC, 2005.

"La diferencia básica entre ISO 20000 e ITIL es que ISO 20000 le proporciona la metodología y el marco (suministrando las partes con las cuales construir el rompecabezas de ITSM), mientras que ITIL le brinda los detalles (mejores prácticas) sobre cómo gestionar todos y cada uno de los procesos de TI en su organización (es decir, armar el rompecabezas).

Una buena forma de pensarlo es que ISO 20000 le dice qué necesita hacer, mientras que ITIL le dice cómo hacerlo.

ISO 20000 no funciona completamente aislado. Se puede implementar en forma separada de ITIL, pero es una realidad que sí van muy bien juntos.

Distinto a una norma, ITIL es un marco práctico de mejores prácticas que se enfoca en alinear sus servicios de TI con las necesidades mayores de su negocio. Como empresa, usted no puede ser certificado por ITIL, solo puede cumplir las directrices de mejores prácticas.

ISO 20000 está basada en los principios fundamentales de ITIL y es una norma ante la cual puede certificar a su empresa.

Los individuos que buscan excelencia en ITSM, y una certificación internacionalmente reconocida, pueden ser certificados ante ITIL e ISO 20000 (por ejemplo, el curso de fundamentos mencionado más abajo).

La certificación ISO 20000 para organizaciones es esencialmente la evidencia de que se han implementado las mejores prácticas. No se necesita ITIL para obtener la certificación ISO 20000, pero es más fácil conseguirla si usted sigue el enfoque de ITIL para la gestión de servicios de TI."[2]

[2] SEGOBIA, Antonio José. Guía simplificada sobre requerimientos de ISO 20000. [En línea]. 1ª ed. [Citado 10-marzo-2019]. Disponible en internet: https://advisera.com/20000academy/es/que-es-iso-20000/

2.2 Marco Institucional

2.2.1 Plataforma estratégica de la empresa litigar punto com

2.2.1.1 Visión

Ser reconocida en el año 2020 como la compañía de mayor cubrimiento, calidad y desarrollo tecnológico, en la prestación de servicios judiciales.

2.2.1.2 Misión

Trabajar con un grupo humano altamente capacitado y comprometido, aplicando tecnologías adecuadas para la entrega de información oportuna y confiable requerida por nuestros clientes; enmarcado dentro de la ética empresarial.

2.2.1.3 Objetivos estratégicos:

- Generar valor a nuestros accionistas y aliados.
- Satisfacer plenamente la promesa de valor pactada con nuestros clientes mediante un grupo humano idóneo y feliz apoyados en tecnologías adecuadas.
- Establecer un modelo empresarial sostenible

2.2.2 Política y principios de litigar punto com

LITIGAR PUNTO COM S.A. realiza para la prestación del servicio de vigilancia judicial, la siguiente metodología y/o procedimientos:

LITIGAR PUNTO COM S.A. visita de forma diaria los despachos judiciales, a nivel nacional, donde estén ubicados procesos de sus USUARIOS. La visita, es realizada en forma simultánea a las 8 am por nuestro equipo de DEPENDIENTES JUDICIALES, que con un aplicativo móvil reportan al sistema y software de Litigando.com los estados que han sido publicados en carteleras.

Ilustración 2./Vigilancia judicial diaria

El sistema realiza de forma automática, una verificación de la información enviada por el DEPENDIENTE e identifica cuáles de los procesos publicados en carteleras son de interés para LITIGAR PUNTO COM S.A. y en todo caso para sus USUARIOS. Una vez identificados los procesos de interés, el sistema y/o software notifica al DEPENDIENTE de cuál proceso debe solicitar auto, el DEPENDIENTE solicita el expediente en ventanilla, toma foto del auto con su aplicación móvil y de forma inmediata la información viaja al sistema, cargándose en la Hoja de Vida del proceso al que hace referencia.

Una vez consolidada la información diaria, LITIGAR PUNTO COM S.A. le notificará al USUARIO, a través de un correo electrónico, a más tardar 11 pm del mismo día para procesos ubicados en Bogotá, y a más tardar 2 pm del día siguiente para procesos ubicados en municipios, cuando alguno de sus procesos presente un movimiento. El correo, contendrá un archivo PDF en el que aparecerán enlistados los procesos que se movieron durante el día, y en cada uno de ellos, encontrará un ícono de Hoja de Vida que le permitirá enlazar el proceso con la Plataforma web de LITIGAR PUNTO COM S.A.

En la Hoja de Vida del proceso, el USUARIO podrá conocer el historial de movimientos de su proceso, realizar un requerimiento puntual sobre el mismo y descarga autos. Para cumplir con nuestros niveles de servicio, LITIGAR PUNTO COM S.A. cuenta con un departamento de AUDITORÍA encargado de realizar la verificación de la información transmitida y/o publicada en la Plataforma Web.

2.2.3 Líneas de Servicios o productos

- **SEGUIMIENTO DIARIO DE PROCESOS JUDICIALES**

800.00 mensuales

Nuestra gestión diaria permite conocer de primera mano la información de los procesos de nuestros clientes en los despachos judiciales a través de los Estados, Traslados, Emplazamientos, Fijaciones en lista, Avisos de remate y Edictos.

Realizamos vigilancia en:

- Juzgados
- Civiles Municipales
- Civiles del Circuito De Familia
- Laborales Administrativos
- Tribunales Administrativos
- Tribunales del Distrito Judicial (Salas Laboral, Civil, Familia y Penal)
- Penales (Solo en Bogotá)
- Fiscalías (Solo en Bogotá)
- Consejo de Estado
- Altas Cortes
- Superintendencias de Industria y Comercio
- Financiera de Sociedades

- **DEFENSA JUDICIAL**

Ejercemos la Representación Judicial de sus procesos a nivel nacional. Presentamos en su nombre demandas o contestación de estas, asistimos en las audiencias de conciliación, pactos de cumplimiento o diligencias de pruebas que sean programadas por los despachos judiciales. Efectuamos la presentación de alegatos y de los diferentes recursos a que haya lugar.

- **UBICACIÓN PLENA DE PROCESOS**

12.00 mensuales

Nos especializamos en la ubicación de cada uno de los procesos en los despachos judiciales y precisamos cuáles se encuentran activos, inactivos o archivados, con el objeto de evitar un riesgo jurídico en caso de una notificación.

- **ASISTENCIA A AUDIENCIAS**

180 mensuales

Lo representamos en audiencias sin importar la naturaleza de la diligencia.

- **AUDITORÍA JUDICIAL DE PROCESOS**

700 mensuales

Creamos con herramientas diseñadas a las necesidades de cada cliente, el historial de actuaciones procesales desde el momento de su radicación hasta la etapa más reciente.

- **ACTUALIZACIÓN E-kogui**

Creamos y actualizamos procesos en el sistema único de información litigiosa del estado colombiano.

- **ENTREGA DE DOCUMENTOS ANTE DESPACHOS JUDICIALES**

15.0000 mensuales

Radicamos oportunamente contestaciones y documentos que impliquen vencimiento de términos en cualquier lugar del país.

- **PROYECTOS A SU MEDIDA**

Nos adaptamos a las necesidades de cada cliente ofreciendo soporte y acompañamiento.

Digitalización de piezas: Obtención digital de copias adicionales del expediente.

Notificación de Providencias: Representación a los clientes mediante abogados adscritos de notificación ante despachos judiciales

- **El servicio de Vigilancia Judicial incluye:**
- **Acceso a página web**

Tendrá acceso a un software a través de la página web: www.litigando.com, contará con su línea con una clave de entrada y contraseña que le permitirá visualizar los movimientos de los procesos presentados por usted desde la firma del contrato a través de una Hoja de vida del mismo. También podrá realizar búsquedas avanzadas de su información judicial o:

Crear tickets o solicitudes, que podrán ser clasificados según la prioridad del requerimiento y de acuerdo con ello se estimulará el tiempo de respuesta.

Ver el historial virtual de cada proceso Cambiar su contraseña Descargar y fotos cada auto notificado en formato PDF

Consultar en la plataforma fotos de publicaciones por fecha y/o despacho judicial.

Solicitar la exclusión o inclusión de procesos cuando lo considere necesario.

Capacidad de alimentar la base de datos de cada Entidad, toda vez que contamos con un Software ajustable a cualquier necesidad.

- **Notificaciones diarias**

Recibirá a su correo electrónico un archivo PDF que le informará los datos demográficos, fecha, tipo de publicación, etapa, actuación procesal, enlace a foto del auto y resumen del auto de los procesos notificados. En Bogotá, a más tardar a las 11:00 p.m. del mismo día de la publicación.

Resto del país, a más tardar a los 2:00 p.m. del día hábil siguiente a la publicación

- **Alerta de diligencias**

Recibirá alertas sobre diligencias, se le informarán los posibles cambios de despacho, realización de próximas diligencias y vencimiento de términos; siempre y cuando nuestros dependientes cuenten con las debidas autorizaciones y acceso a los expedientes.

- **Alertas de nuevos hallazgos**

Recibirá diariamente un correo electrónico con el listado de procesos que no se encuentran en la base inicial.

- **Consultas dinámicas**

Podrá recibir información diaria en formato Excel de sus procesos según su necesidad. Podrá consultarlos por etapa procesal, cédula, obligación, abogado, ciudad, despacho, etc.

- **Asignación de Gestor**

Le asignamos un ejecutivo de cuenta, que se encargará de acompañarle, asesorarle y resolver todas las inquietudes que surjan en la prestación del servicio. Podrá contactarte por correo, celular o telefónicamente.

Solo se agregarán con autorización previa de lunes a jueves hasta el mediodía. Se iniciarán la revisión el lunes siguiente.

3. METODOLOGÍA

Este proyecto utilizará la metodología de ITIL V3 y la norma ISO 20000 para el proceso de gestión de seguridad de la información debido a que gracias al uso de estas buenas prácticas lograremos mejorar la entrega y manejo de la información para que esta sea más oportuna, confiable y así darles una mejor atención a los clientes.

Se decide formular acciones de mejora a este proceso anteriormente mencionados en la empresa litigar punto com debido a que por medio de una auditoría interna se evidenciaron varias falencias y amenazas para el sistema de gestión de la seguridad de la información.

El proceso de gestión de seguridad de la información será aplicado en la compañía para mejorar las políticas de seguridad y así poder aplicar de manera eficiente las restricciones impuestas por litigar punto com.

Para lograr los objetivos propuestos es necesario realizar un diagnóstico dentro de la empresa para conocer cuáles son sus mayores vulnerabilidad y riesgos:

Las actividades que se realizaron son:

- Identificación del recurso de información
- Auditoría para identificar inconsistencias en el proceso
- Análisis inicial de vulnerabilidades y riesgos
- Formulación de políticas de seguridad de la información
- Definición de acciones de mejoramiento para el desarrollo eficiente del proceso de gestión de la información.

3.1 Población

De acuerdo con los datos adquiridos a través de las encuestas y auditorias podemos establecer que el promedio de la población en la empresa Litigar punto com sede Bogotá es de 120 empleados los cuales todos manejan información valiosa para el negocio.

3.2 Técnicas para la recolección y análisis de la información

Técnicas utilizadas:

La observación: Durante la auditoría se observó que la empresa no cuenta con unas políticas adecuadas de la seguridad de la información, se observaron equipos de cómputo sin control de inactividad cuando sus usuarios no están en el puesto de trabajo, esto genera un alto riesgo en la seguridad de la información, dando lugar a que una persona mal intencionada pueda alterar la información allí guardada.

Recopilación de documentos: Al solicitar todos los documentos donde se establecen las políticas de seguridad de la información y formatos que se requieren para una adecuada gestión de la seguridad de la información no cuentan con los parámetros establecidos por la norma ISO 20000 y carece de las buenas prácticas de ITIL

La entrevista: En la entrevista con el director de departamento TI se evidencia falta de conocimiento en la norma ISO 20000 y en las buenas prácticas de ITIL, esto permitiendo identificar que no se hace un seguimiento del proceso de gestión de seguridad de la información lo cual no permite tener una mejora continua del proceso y en su defecto mejora continua del servicio, esto también permite identificar que no se hacen los respectivos análisis de riesgo y prevención ante vulnerabilidades.

La encuesta: esta técnica nos permitió saber si los empleados de la compañía tenían conocimiento de las políticas de seguridad de la información, implementadas por litigar punto com. Al analizar los resultados evidenciamos que los empleados no tienen el conocimiento sobre las políticas de seguridad de la información que tiene la empresa litigar punto com y por consiguiente no se cumplen.

3.3 Técnicas, herramientas y métodos para el diseño e implementación de los sistemas de gestión tecnológica

Las herramientas que se deben usar para un control de políticas de seguridad de la información son:

Firewall: A través del cual se ejecutan las políticas de acceso a internet, escaneos de programados, alertas de seguridad, actualizaciones, desde esta herramienta permite crear políticas por perfiles de usuarios esto garantizando que los funcionarios estén utilizando adecuadamente los activos de litigar punto com.

Antivirus: Herramienta encargada de realizar análisis de escaneo de intrusos en los equipos de la red, esto evitando riesgos de seguridad de la información

Capacitaciones a los funcionarios: Con esta herramienta mitigamos riesgos como pérdida de información, secuestro o alteración de esta, ya que la mayoría de los ataques que son satisfactorios es por desconocimiento del personal.

Tablero de control: con esta herramienta puedo hacer un análisis de los riesgos sobre los activos de la información en función de la amenazas, vulnerabilidades y controles (salvaguardas) que existen en la organización, con el tablero de control puede definir la fase del riesgo e identificar en cuál de las fases estoy como, por ejemplo: Fase 1. Definir el alcance del análisis del riesgo, Fase 2. identificación de activos, Fase 3. Identificación de amenazas, Fase 4. Identificación de vulnerabilidades, Fase 5 Evaluación del riesgo y Fase 6 Tratar el riesgo

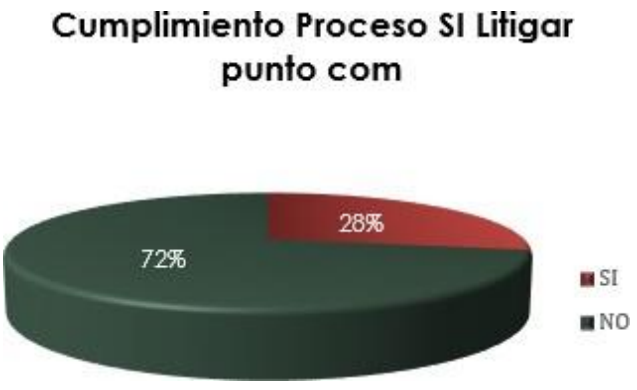
4. DIAGNÓSTICO

Se tuvieron en cuenta a todos los usuarios de la empresa para saber qué tanto conocimiento tienen respecto a la seguridad de la información y por medio de encuestas se evidenció que la mayoría del personal desconoce la importancia de tener un sistema seguro y del inconveniente que puede acarrear que mucha información confidencial pueda caer en manos indebidas, los resultados de dichas encuestas arrojaron que los usuarios no tenían claves seguras adicional compartían mucha información importante por plataformas inseguras, algunos deshabilitaron los antivirus para tener un mejor desempeño de sus equipos.

De acuerdo con los resultados obtenidos del proceso anterior, se realiza un análisis para determinar el estado actual de los servicios de TI, de lo anterior se concluye que se requiere de manera inmediata charlas preventivas para así concientizar a los involucrados en manejar toda la información y de esta manera poder implementar los procesos de gestión de seguridad de la información bajo la norma ISO 20000 y gestión de acceso aplicando la metodología ITIL V3. (Ver Anexo 8)

4.1 Estado de las condiciones actuales

Se realiza a través de una lista de chequeo la evaluación del estado actual relacionado con el proceso de gestión de seguridad de la información encontrando que es deficiente y cumple con un 28%.



4.2 Determinación de factores críticos

Utilizando las herramientas de lista de chequeo, espina de pescado y matriz de riesgos se identifican los siguientes factores críticos:

-Involucrar y lograr el apoyo de las directivas de la compañía en el proceso de gestión de seguridad de la información.

-Asignar los roles necesarios para ajustar e implementar el proceso de gestión de seguridad de la información.

4.3 Identificación de hallazgos significativos

De acuerdo con el análisis de la información se observa que existe documentación referente al proceso de gestión de la seguridad de la información, sin embargo, este proceso no tiene responsables y no está siendo implantado.

No existen implementadas políticas de seguridad de la información que garanticen la disponibilidad, confidencialidad e integridad de la información.

4.3.1 Análisis matriz de riesgos

Inexistencia del rol responsable de la gestión de la seguridad de la información: De acuerdo con las buenas prácticas ITIL se sugiere contar con la implementación de una matriz RACI para la asignación de responsabilidades. Ya que actualmente la compañía no cuenta con un encargado, responsable y tampoco con un informado con quienes se puedan realizar un alineamiento de los procesos del área de seguridad de la información.

4.3.2 Diagrama causa y efecto:

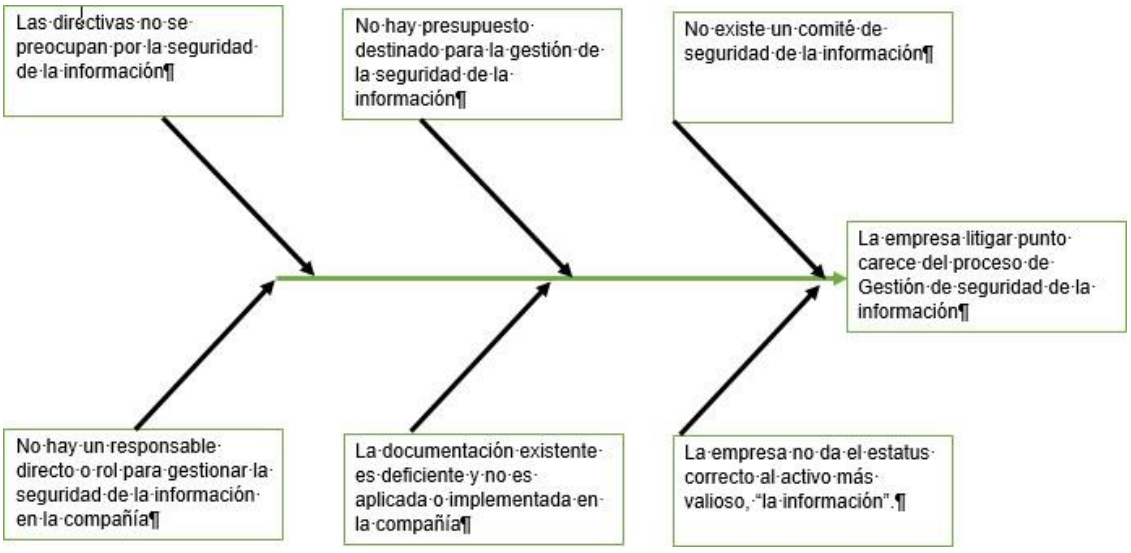


Ilustración 3. /Diagrama causa y efecto

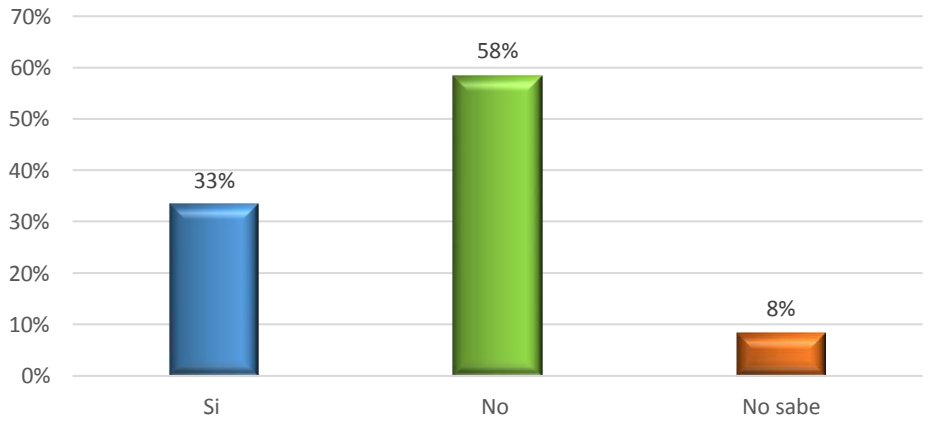
4.3.3 Encuesta de conocimiento de seguridad de la información de empleados litigar punto com

Se realiza encuesta con el fin de medir el conocimiento que tienen los empleados de la compañía litigar punto com respecto a la seguridad de la información y al manejo que les dan a todos los datos que manejan respecto a los procesos de sus clientes. (Ver ANEXO 1 con la encuesta realizada a los empleados de la compañía.)

4.3.3.1 Resultados de la encuesta

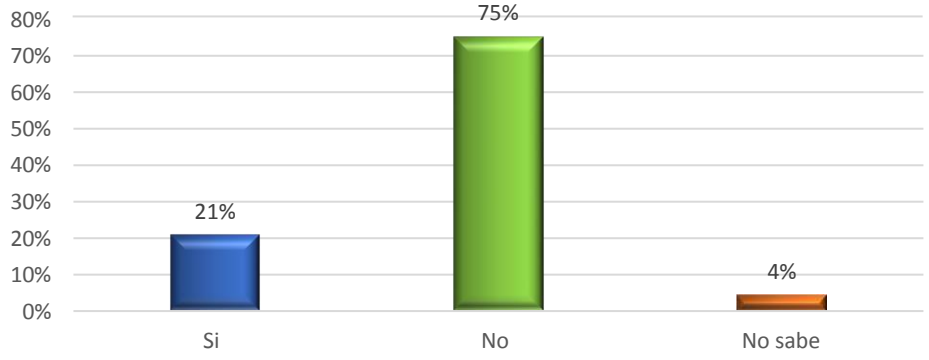
Mediante la encuesta realizada a los 120 empleados de la empresa litigar punto com, se obtuvieron los siguientes resultados.

1. ¿Sabe usted que es un incidente de seguridad y cuál es el procedimiento para reportarlo?



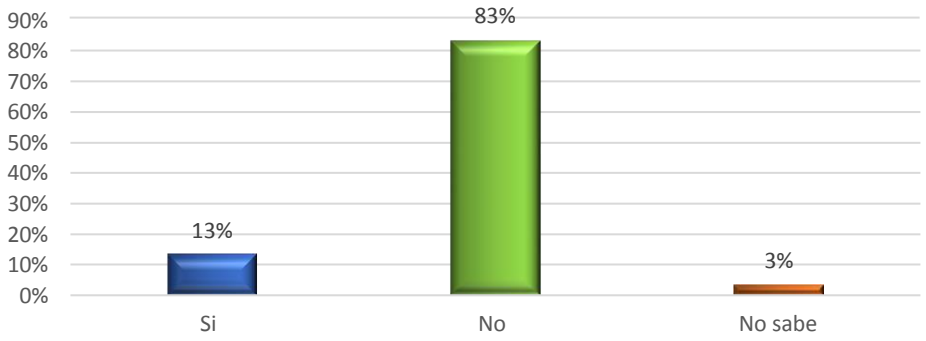
1. A la pregunta Conoce usted el grado de confidencialidad de la información que maneja. Se obtienen los siguientes resultados: de los 120 encuestados 90 respondieron que No, 25 respondieron que Si y 5 no respondieron nada.

2. **¿Conoce usted el grado de confidencialidad de la información que maneja?**



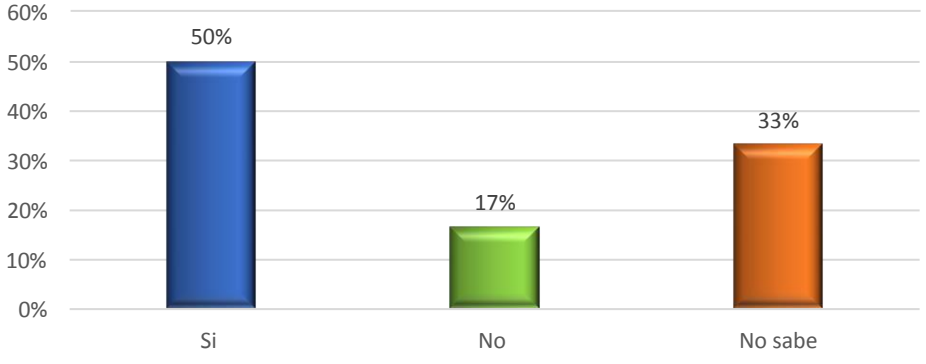
2. A la pregunta Conoce usted si la información manejada tiene protección de copia, se obtienen los siguientes resultados: de los 120 encuestados 100 respondieron que No, 16 respondieron que Si y 4 no respondieron nada.

3. ¿Conoce usted si la información manejada tiene protección de copia ?

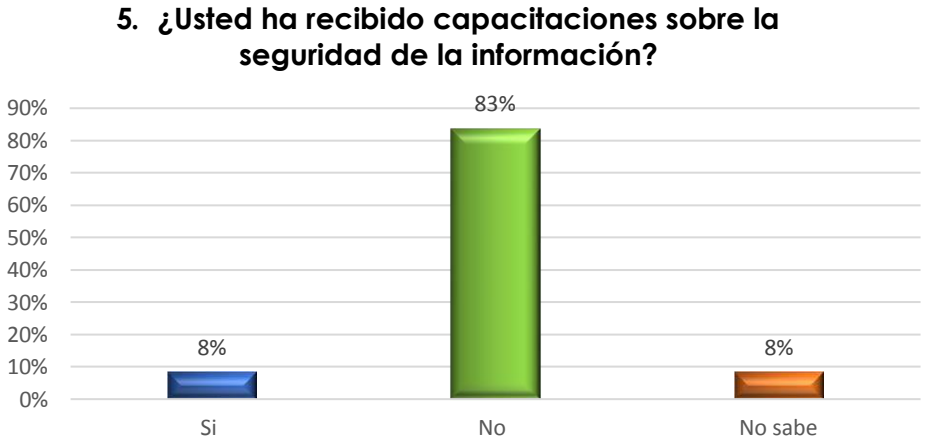


3. A la pregunta ¿Su equipo de cómputo cuenta con un antivirus actualizado?, se obtienen los siguientes resultados: de los 120 encuestados 20 respondieron que No, 60 respondieron que Si y 40 no respondieron nada.

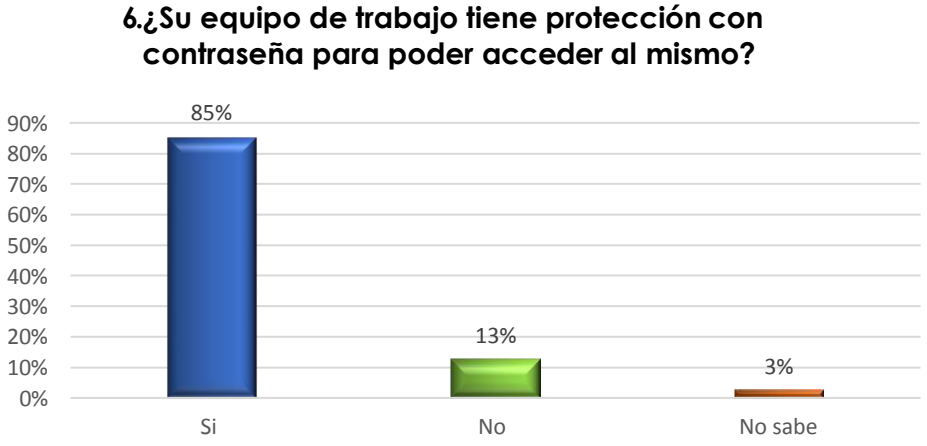
4. ¿Su equipo de cómputo cuenta con un antivirus actualizado?



4. A la pregunta ¿Usted ha recibido capacitaciones sobre la seguridad de la información?, se obtienen los siguientes resultados: de los 120 encuestados 100 respondieron que No, 10 respondieron que Si y 10 no respondieron nada.

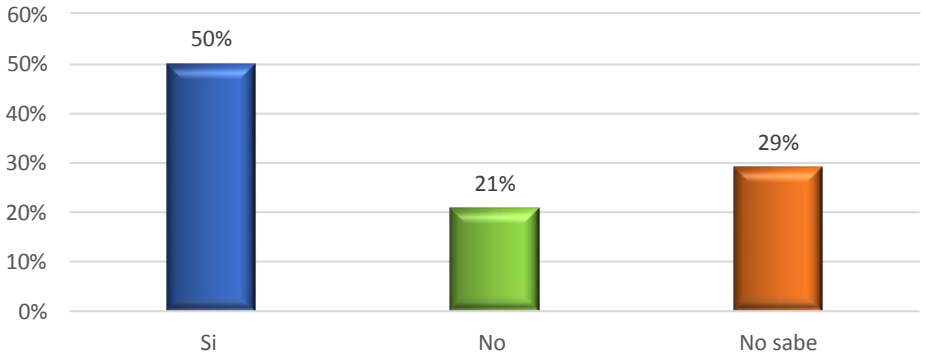


5. A la pregunta ¿Su equipo de trabajo tiene protección con contraseña para poder acceder al mismo?, se obtienen los siguientes resultados: de los 120 encuestados 15 respondieron que No, 102 respondieron que Si y 3 no respondieron nada.



6. A la pregunta ¿Realiza copia de seguridad en su equipo de forma diaria y/o semanal?, se obtienen los siguientes resultados: de los 120 encuestados 25 respondieron que No, 60 respondieron que Si y 35 no respondieron nada.

7. **¿Realiza copia de seguridad en su equipo de forma diaria y/o semanal?**



4.3.3.2 Análisis encuesta de conocimiento

Los resultados muestran que un 64% de los empleados de la empresa litigar punto com carecen de conocimiento con respecto a la seguridad de la información, lo cual genera preocupación entre las partes interesadas del negocio, ya que la información de la empresa se considera un activo clave para el funcionamiento de la compañía, los resultados anteriormente obtenidos se pondrán a disposición del área encargada para la implementación del respectivo plan de mejora.

Ilustración 4. / Resultados encuestas

4.3.4 Auditoría ISO 20000-1 2011

Se realiza auditoria para Evaluar la eficiencia, eficacia y efectividad del proceso de GESTION DE SEGURIDAD DE LA INFORMACION en la empresa LITIGAR PUNTO COM basados en la norma ISO/IEC 20000-1 2011.

4.3.4.1 Planeación de la auditoria

Se realiza la planeación de la auditoria entre el auditor líder, el equipo y el jefe del área de TI de la empresa Litigar Punto com. (Ver anexo 3)

4.3.4.2 Plan de la auditoría

Se realiza la socialización de la planeación de auditoría y se define el plan de auditoria a realizar en la empresa Litigar Punto com. (Ver anexo 4)

4.3.4.3 Auditoría

Se realizó la auditoría en los tiempos establecidos, se realiza inicialmente con el Gerente de la compañía y luego con el director del Área TI y algunos empleados de la compañía a los cuales se les solicita las diferentes evidencias dentro del proceso de gestión de seguridad de la información. (Ver anexo 5)

4.3.4.4 Informe de Auditoría

Una vez terminada la auditoría se reúne el equipo auditor de acuerdo con el cronograma a realizar el informe de auditoría para socializarlo con la alta dirección, se presenta un resumen ejecutivo y la conclusión de la auditoria en la empresa litigar punto com. (Ver anexo 7)

En la empresa Litigar Punto com dentro de su proceso de Gestión de seguridad de la información se encontró a modo de resumen los siguiente:

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: La empresa presenta 4 conformidades en cuanto a la eficacia, eficiencia de gestión de seguridad de la información y 9 no conformidades porque no mostraron evidencia de que se cumpliera con estos ítems. 13 ítem auditados.

5. DISEÑO DE INGENIERÍA

Formulación acciones de mejora del proceso de gestión de seguridad de la información en la empresa litigar punto com basados en la norma ISO/IEC 20000 y las buenas prácticas de ITIL v3 en la ciudad de Bogotá

5.1 Especificaciones del problema

En la empresa Litigar punto com encargada de hacer vigilancia y seguimiento de procesos judiciales se encuentra implementado el proceso de gestión de seguridad de la información, el cual permite que la información este siempre disponible para sus empleados y clientes mediante la página web.

Sin embargo, el proceso de gestión de seguridad de la información no ha generado los resultados esperados, provocando de esta forma que la confidencialidad, integridad y disponibilidad de la información se vea afectada.

Para formular acciones de mejora se debe dar solución a los siguientes interrogantes:

5.1.1 ¿Cuáles son las necesidades de los usuarios?

- **Como empleado de Litigar punto com**

  - Tener la información procesada resguardada
  - Quiero asegurar que la información consultada sea confiable e integra.
  - Capacitaciones constantes sobre cómo proteger la información

- **Como cliente de la compañía:**

  - Tener la información de sus procesos siempre disponible
  - Quiero asegurar que la información este siempre actualizada y sea confiable
  - Quiero confirmar que pueda ver los procesos de su interés
  - Poder tener de forma oportuna información sobre las audiencias de sus procesos

- **Como miembro TI**

    - Tener control de la información
    - Garantizar a los clientes y usuarios internos que la información esta resguardada de una forma segura e integra.
    - Tener control los respectivos controles de acceso a la aplicación y las personas que se logen cuenten con un perfil estándar y que solo puedan acceder a la información propia del cliente.

5.1.2 ¿Cuál debería ser la solución?

Realizar un análisis de la situación actual con ayuda de una auditoria al proceso de gestión de seguridad de la información donde se puedan identificar claramente que parte del proceso no se está cumpliendo para así realizar las respectivas mejoras en el proceso

Se tiene como alternativa para la formulación de acción de mejora del proceso de gestión de seguridad basada en la norma ISO/IEC 20000 y las buenas prácticas de ITIL V3 una concientización a los empleados ya que de acuerdo con el diagnóstico realizado el principal inconveniente es el desconocimiento de la importancia del manejo de la información y su seguridad.

Adicional se trabajará con un método publicitario por medio del correo empresarial divulgando tips para mejorar en los puntos más débiles.

Se crea y se sugieren unas políticas de seguridad de la información para que sean divulgadas a todo el personal por medio de capacitaciones.

5.1.3 ¿Cuáles son los límites del problema, también imposiciones y restricciones?

Contar con el apoyo de la alta gerencia para que las mejoras formuladas al proceso de seguridad de la información sean aplicadas y que se realicen las respectivas capacitaciones al personal.

5.1.4 ¿Cuáles son las características de la población que se verá beneficiada con las acciones de mejora propuestas para el proceso de gestión de aplicaciones?

Empleados: Profesionales de todas las áreas que con altas capacidades.

Clientes: Persona natural o jurídica que contrata servicios con la empresa.

Miembro TI: Personas responsables enfocadas en alcanzar la meta de negocio con metas TI.

5.2 FORMULACIÓN DE ACCIONES MEJORA

5.2.1 Formulación de mejora de acuerdo con el estado de la lista de chequeo de evaluación del estado actual relacionado con el proceso de gestión de seguridad de la información

1. Definir acciones proactivas en cuanto a la gestión de seguridad de la información, buscando de esta forma mitigar riesgos de seguridad en la empresa litigar punto com, declararlos y crear el plan de tratamiento de los riesgos de seguridad.

2. Formular un sistema de políticas en la empresa litigar punto com, para identificar, controlar y proteger la información y cualquier equipamiento empleado junto con el almacenamiento, transmisión y procesamiento de dicha información.

3. Establecer capacitaciones periódicas al personal de la compañía, para el desarrollo eficiente del proceso de gestión de seguridad de la información de la empresa litigar punto com, basada en la norma ISO 20000 1:20011 e ITIL

5.2.2 Formulación de mejoras de acuerdo con el análisis de la espina de pescado

1. Lograr que las directivas se interesen por la seguridad de la información de la compañía.

2. Crear un comité de seguridad de la información, creando sus respectivos roles para gestionar la seguridad de la información en la compañía.

3. Se formula que la documentación existente sobre el proceso de gestión de seguridad de la información se debe aplicar en la compañía para minimizar los riesgos de la información.

4. Por medio de capacitaciones al personal de la compañía se quiere concientizar a los integrantes de que la información es el principal activo y por esta razón todos deben adoptar prácticas adecuadas para que no evitar perdida, secuestro o alteración de esta.

5.2.3 Formulación de mejoras de acuerdo con el análisis de la matriz de riesgo

1. Se formula una adecuada administración de la información, esto manteniendo herramientas que permitan tener de una forma segura la información. Como crear políticas de restricción dentro del antivirus y firewall de la compañía, esto permitiendo que los intrusos que quieren tener acceso a la información no logren saltarse este filtro.

2. Se fórmula crear dentro del directorio activo de la compañía usuarios estándar para no tengan acceso a toda la información dentro de la empresa, se debe tener un usuario administrador encargado de la red y que garantice que siempre esté disponible y segura la información.

3. Se sugiere crear un plan de continuidad y contingencia del negocio para garantizar a los clientes y empleados de la compañía, que la información siempre estará en un lugar seguro y no ocurrirá perdida, secuestro o manipulación de esta.

4. Por medio de capacitaciones al personal de la compañía se quiere concientizar a los integrantes que la información es el principal activo y por esta razón todos deben aplicar unas buenas prácticas para que no existe perdida, secuestro o alteración de esta.

5. Se formulan un listado de políticas de seguridad de la información para que estas sean aplicadas dentro de la compañía, para preservar el principio de la información que es garantizar la confidencialidad, integridad y disponibilidad de esta.

5.2.4 Formulación de mejoras de acuerdo con el análisis de la encuesta de conocimiento de seguridad de la información a los empleados de la empresa Litigar punto com.

1. Se formula que la compañía debe implementar cursos de seguridad de la información para capacitar a los empleados e incluir dentro de las obligaciones y deberes el cumplimiento de esta política. La compañía junto con el comité de seguridad de la información debe tener un control para que se realice de forma periódicas estas capacitaciones. Para crear conciencia en todos los integrantes de la empresa sobre la importancia de hacer uso de las buenas prácticas en cuanto al manejo del principal activo de la compañía.

   Con la implementación de esta buena práctica se logra que los empleados cumplan con los objetivos planteados por la alta gerencia de la compañía.

2. Se sugiere que la compañía junto con el comité de seguridad de la información socialice de forma periódica las políticas creadas para la seguridad de la información.

5.2.5 Formulación de mejoras de acuerdo con el análisis de la auditoria del proceso de gestión de seguridad de la información basados en la norma ISO 20000

1. Se formula que la compañía debe hacer constantemente auditorías internas en pro de la mejora continua del proceso de gestión seguridad de la información, porque evidenciamos que se realizan las auditorias, pero no se corrige en lo que está fallando.

2. Se formula capacitaciones a los trabajadores para darles a conocer los objetivos de la compañía y el objetivo de gestión de seguridad de la información y comunicar las políticas de seguridad de la información.

3. Se sugiere que la compañía junto con el comité de seguridad de la información realice controles periódicos para la seguridad de la información.

5.3 Plan de mejoramiento

Con respecto al estudio realizado en las auditorias y en las cuentas, se generó un plan de mejoramientos donde resaltan el área a mejorar, las causas principales, objetivos, acciones de mejora, prioridad e impacto en la organización. (Ver anexo 9)

5.3.1 Estudio técnico de la alternativa

De acuerdo con el estudio realizado es viable debido a que se evidenciaron varios puntos en los que no se está dando cumplimiento, si se mejoran estos puntos críticos se va a tener una mejoría notable.

5.3.2 Estudio operativo de la alternativa

Se requiere coordinación con la empresa litigar punto com para conocer la disponibilidad de sus empleados y el tiempo con el que disponen para las charlas y capacitaciones, adicional se debe contar con un lugar adecuado para llevar a cabo dicho programa.

5.4 Propuesta económica

Objeto: Implementación de acciones de mejora del proceso de gestión de seguridad de la información: Establecer el respectivo proceso, basándose en la norma ISO 20000, modelo de capacitación, Implementar un plan de recuperación ante desastres, implementación de base de datos que cumpla con las políticas de seguridad, registro y control de las licencias del software, cronograma para el mantenimiento correctivo del software, plan de seguimiento de las no conformidades.

5.4.1 Estudio técnico

En conjunto con las tareas declaradas por el personal del área de TI, las auditorías realizadas y el resultado de las encuestas, se obtiene la información necesaria para realizar un informe detallado del estado actual de la compañía y de esta forma generar una propuesta de aspectos a mejorar y optimizar.

5.4.2 Estudio operativo

Para la implementación de todas las acciones de mejora se requiere un personal calificado que ejecute el plan propuesto. Para lo anterior se requiere el siguiente personal con un determinado horas de trabajo:

PERSONAL REQUERIDO	CANTIDAD	HORAS
Instructores especializados en herramientas de la seguridad de la información	5	240
Auditor Norma ISO 20000	1	100
Especialistas ITIL	2	150

Tabla 1, personal requerido

De los puntos anteriores se genera una propuesta económica donde se incluyen herramientas informáticas, material informativo, personal requerido y mano de obra.

ACCION	HERRAMIENTAS	COSTO
Establecer proceso basado en la norma ISO 20000	Documento detallado de acuerdo con la normativa	$ 800.000
Dictar capacitaciones	Material informativo de acuerdo con los diferentes roles de la empresa	$ 3.000.000
Implementar plan de recuperación de desastres	Documento y manuales detallados de acuerdo con la normativa	$ 1.200.000
Implementar Base de datos	Optimización de las bases de datos actual, con nuevos actuales sistemas de codificación	$ 6.500.000
Usar herramientas de validación de licencias	Compra, instalación y validación de herramientas que detecten licencias vencidas	$ 2.500.000
Realizar mantenimiento	Cronograma de mantenimiento para verificar el software validado	$ 1.000.000
Crear plan de seguimiento de las no conformidades	Proceso de auditoría interna	$4.000.000
	TOTAL	**$19.000.000**

Tabla 2, Costo total

6. CONCLUSIONES

- Conociendo que ITIL, hace referencia a un modelo basado en las mejores prácticas, es indispensable incorporar en el proceso de gestión de seguridad de la información estas buenas prácticas para que haya un buen funcionamiento dentro del proceso.

  Es importante adoptar todo el plan de mejora que se propuso para la empresa Litigar Punto com, en el proceso de gestión de seguridad de la información, ya que, con estas buenas prácticas que se formularon, la información estará resguardada y protegida, reduciendo el riesgo de pérdida, secuestro o alteración de esta.

- Se concluye que el análisis y diagnóstico de la situación actual nos permitió conocer a fondo el manejo en la empresa litigar punto com del proceso de gestión de seguridad de la información donde se evidencian que no se aplica las buenas prácticas de ITIL, esto provocando que el proceso no funcione adecuadamente.

  También el análisis y diagnóstico nos permitió detectar riesgos para minimizarlos en las funciones más importantes de la entidad y poder cumplir con los principios de seguridad de la información, permitió establecer políticas, procedimientos e instrumentos en materia de seguridad.

- Se formularon acciones de mejora para el proceso de gestión de seguridad de la información basados en la norma ISO/IEC 20000-1 2011 y en las buenas prácticas de ITIL que permite a la compañía mejorar el proceso, esto permitiendo que la información siempre contenga confidencialidad, integridad y disponibilidad como principal activo de la compañía.

7. RECOMENDACIONES

Se recomienda usar antivirus con detección de software malicioso, actualizador de software, control de aplicaciones y análisis de vulnerabilidades. Esto se debe instalar en todos los dispositivos electrónicos con acceso a la red de la compañía, un solo dispositivo desprotegido puede generar daño en las bases de datos y perdida de información.

El software utilizado en todas las áreas de la compañía debe estar optimizado para implementar funciones complicadas desde los servidores de la compañía y no en los dispositivos electrónicos de los usuarios finales, esto con el fin de garantizar la entrega y recepción de información de manera completa.

En todas las áreas de la compañía en especial las áreas de tecnología, no se debe dejar visible información de acceso a las bases de datos o conexión a la red de empresa. además, dejar todos dispositivos electrónicos protegidos con contraseña.

Las contraseñas de acceso a los dispositivos electrónicos, bases de datos y software se deben cambiar periódicamente, y usar niveles de seguridad altos.

Todo software que tenga acceso a la red debe tener un sistema de cifrado, si el software no cuenta con uno deberán instalarle uno externo.

La instalación y mantenimiento de cualquier software se debe realizar por el personal seleccionado en el plan de implementación.

8. BIBLIOGRAFÍA

I&T SOLUTIONS. (2019). ISO 20000 Material del Alumno. Bogotá D.C.

I&T SOLUTIONS. (2019). ITIL Material del Alumno. Bogotá D.C.

Norma **ISO 20000-1 2011 material entregado por la Docente** I&T SOLUTIONS

9. INFOGRAFÍA

https://searchdatacenter.techtarget.com/es/definicion/ITSM-gestion-de-servicios-de-TI

https://advisera.com/20000academy/es/que-es-iso-20000/

Anexo 1

Encuesta de conocimiento realizada a los empleados de litigar punto com.

Responda la encuesta de acuerdo con el conocimiento.

1. Sabe usted que es un incidente de seguridad y cuál es el procedimiento para reportarlo.

    a. Si
    b. No

2. Conoce usted el grado de confidencialidad de la información que maneja.

    a. Si
    b. No

3. Conoce usted si la información manejada tiene protección de copia.

    a. Si
    b. No

4. ¿Su equipo de cómputo cuenta con un antivirus actualizado?

    a. Si
    b. No

5. ¿Usted ha recibido capacitaciones sobre la seguridad de la información?

    a. Si
    b. No

6. ¿Su equipo de trabajo tiene protección con contraseña para poder acceder al mismo?

    a. Si
    b. No

10. ¿Realiza copia de seguridad en su equipo de forma diaria y/o semanal?

    a. Si
    b. No

Anexo 2

Checklist

Estado Actual	CUMPLIMIENTO
Se realizan backups de la información	NO
Se hacen de forma periódica backups	NO
Hay un estándar para crear las contraseñas	NO
Las contraseñas caducan de manera automática	NO
Se realiza mantenimiento preventivo del software	NO
Es periódico el mantenimiento preventivo del software	NO
Se realiza mantenimiento correctivo del software	SI
Es periódico el mantenimiento correctivo del software	NO
Existe documentación relacionada con el proceso de gestión de seguridad de la información	SI
Existe software antivirus actualizado	NO
Existen licencias del software instalado	SI
Hay un registro y control del licenciamiento de software	NO
Se realiza revisión de software instalado sobre los equipos	SI
Los usuarios finales tienen restringido instalar software en sus equipos	SI
Hay un proceso para la gestión de las contraseñas de administrador de los sistemas de información de misión crítica	NO
Las contraseñas de los sistemas de información de misión crítica están almacenadas de forma segura	NO
Existe plan de recuperación ante desastres (DRP)	NO
Hay un registro de aplicaciones e infraestructura que soporta el core del negocio	NO

Anexo 3

	PLANEACIÓN DE AUDITORÍA
OBJETIVO DE LA AUDITORIA	Evaluar la eficiencia, eficacia y efectividad del proceso de GESTION DE SEGURIDAD DE LA INFORMACION en la empresa LITIGAR PUNTO COM basados en la norma ISO/IEC 20000-1 2011
AUDITOR LIDER	DIANA MARCELA CAVIEDES
EQUIPO AUDITOR	NUBIA ESPERANZA ROA VANEGAS

			FECHAS DE AUDITORIA								
			Marzo								
N°	**PROCEDIMIENTO**	**RESPONSABLE**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**
1	Definir el plan de la auditoria	Nubia Roa									
2	Verificar que la alta direccion y el personal estan alineados con los objetivos de la empresa	Diana Caviedes									
3	Verificar que se tiene el proceso documentado para la gestión de seguridad de la información	Nubia Roa									
4	Verificar que el personal de TI tienen las competencias necesarias para la funcion que ejercen en la empresa	Diana Caviedes									
5	Verificar que se implementan las políticas de seguridad de la informacíon	Diana Caviedes									
6	Verificar las valoraciones de riesgo para la seguridad de informacíon y los criterios de aceptacion del riesgo	Nubia Roa									
7	Verificar si las auditorías interneas se realicen	Nubia Roa									
8	Verificar si los resultados de la auditoría se revisan para identificar las oportunidades de mejora	Diana Caviedes									
9	ELABORACION DE INFORME DE AUDITORIA	Nubia Roa									
10	ENTREGA DE INFORME Y RECOMENDACIONES	Nubia Roa									

Anexo 4

	PLAN DE AUDITORIA	VERSION WLI-001
Litigando.com Información judicial al día, esté donde esté		

N° AUDITORIA	**001-2019**
OBJETIVO	**Evaluar la eficiencia, eficacia y efectividad del proceso gestión de la seguridad de la informacion (ITIL) basados en la norma ISO 20000-1 2011**
DESCRIPCION	**La empresa litigar punto com dedicada a ofrecer servicios de revisión y vigilancia de procesos judiciales, tiene implementado el proceso de Gestión de seguridad de la información que les garantice a los clientes y miembros de la empresa que su información está resguardada de forma segura y confiable. Apoyados en la norma ISO/ IEC 20000 e ITIL V3**
ALCANCE	**Formulación de acciones de mejora para la el procesos de gestión de seguridad de la información en la empresa litigar punto com, con una duración de un mes**
REFERENCIA	**ISO/IEC 20000**
LUGAR	**Empresa Litigar Punto com en la ciudad de Bogotá**
CONTACTO	**Jefe del Area TI**
EQUIPO AUDITOR	**DIANA MARCELA CAVIEDES - NUBIA ESPERANZA ROA VANEGAS**

FECHAS	AUDITOR	PROCESO	NORMA ISO	OBSERVACIONES
Inicia el 15 de Marzo y finaliza el 23 de Marzo	DIANA MARCELA CAVIEDES	REUNIÓN PRESENTACIÓN PLAN DE AUDITORIA	N/A	Se realiza con el Gerente de la empresa, se le comunica a los demas trabajadores de la compañía y al area de TI
	NUBIA ROA VANEGAS	Revisión de política de seguridad de la información, objetivos para la gestión de la información, gestion del riesgo para la seguridad de la información	6.6.1	Se realiza con el Gerente de la empresa y el Director de TI
	NUBIA ROA VANEGAS	Revisión de las auditorias internas para la seguridad de la información	6.6.1	Se realiza con el Jefe de seguridad informática y se solicita algunos trabajadores para ser auditados
	DIANA MARCELA CAVIEDES	Revisión de controles para la seguridad de la información	6.6.2	Se realiza con el Jefe de seguridad informática y se solicita algunos trabajadores para ser auditados
	DIANA MARCELA CAVIEDES	Revisión de cambios e incidentes en la seguridad de la información	6.6.3	Se realiza con el Jefe de seguridad informática y se solicita algunos trabajadores para ser auditados
	DIANA CAVIEDES - NUBIA ROA	EVALUACIÓN Y SOCIALIZACIÓN DE INFORME FINAL DE AUDITORÍA	N/A	Se realiza con el equipo auditor y se socializa con el gerente de la empresa

Anexo 5

		RESULTADOS			
ITEM	**PREGUNTAS DE ACUERDO CON LA NORMA**	**C**	**NC**	**HALLAZGOS**	**EVIDENCIAS**
1	¿Comunica la política de seguridad de la información y la importancia de su cumplimiento a al personal apropiado del prestador del servicio, del cliente y de los proveedores externos?		**X**	NINGUNO	No presenta sop orte
2	¿Se establecen los objetivos para la gestión de seguridad de la información?		**X**	En las políticas establecidas no se evidencia cual es el objetivo de la implementación del proceso	No presenta soporte.
3	¿Tienen definidos los criterios de aceptación del riesgo?	**X**		Ninguno	Se presenta acta de reunión en la que se acordaron los criterios de aceptación del riesgo
4	¿Realizan las valoraciones de riesgo para la seguridad de la información en		**X**	No cuentan con documentos que las valoracione	No presenta soporte.

	intervalos?			s	
5	¿Realiza auditorías internas para la seguridad de la información?	X		NINGUNA	Presentan las actas de las auditorías internas realizadas
6	¿Se asegura que los resultados de la auditoría se revisan para identificar la mejora continua?		X	NINGUNO	No presenta soporte.
7	¿Preserva la confidencialidad, integridad y accesibilidad de los activos de la información?	X		NINGUNO	Muestra evidencia de en las herramientas de Firewall y Antivirus donde crean políticas de seguridad de la información
8	¿Cumplen con los requisitos de la política de seguridad de la información?		X	No se evidencia que cumplan con los requisitos	No presenta soporte.
9	¿Se han logrado los objetivos de seguridad de la información?		X	No presentan soportes donde se evidencie que se han cumplido los objetivos .	No presenta soporte.
10	¿Gestiona los riesgos relacionados con la seguridad de la		X	No presentan soporte donde de evidencia	No presenta soporte.

	información?				
11	¿Los controles de seguridad se en encuentran documentados		X	No presentan soporte donde de evidencia	No presenta soporte
12	¿Se evalúan los cambios de incidentes de seguridad de la información?	X		Presentan documentación	Presentan formatos de donde esas evidencias los cambios en incidentes de seguridad de la información
13	¿Se evalúa el impacto potencial sobre los controles y la política de seguridad de la información?		X	No presentan documentación	No presenta soporte.
En constancia firman quienes intervinieron en la auditoria a los 23 días del mes de marzo de 2019					
AUDITOR LIDER: Diana Caviedes				**GERENTE DE LA EMPRESA: Gabriel Parodi**	
EQUIPO AUDITOR: Nubia Roa				**AUDITADO: Guillermo Hernández**	

Anexo 5: Auditoría

Anexo 6

HALLAZGOS DE AUDITORÍA
6.6 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
CONFORMIDADES
1.1 COMPROMISO DE LA ALTA DIRECCIÓN: Se evidencia que existe compromiso de la alta dirección, ya que están dispuestos a mejorar en las no conformidades halladas.
1.2 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN : Se evidencia que definen el enfoque que se ha de tomar para la gestión de los riesgos de la seguridad de la información y los criterios de la aceptación de los riesgos, la alta dirección se asegura que las auditorías internas se realicen **(Numeral 6.6.1 literal c, e).**
1.3 CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN: Se evidencia que utilizan herramientas como antivirus y firewall para preservar la confidencialidad, integridad y accesibilidad de la información **(Numeral 6.6.2 Literal a)**.
1.4 CAMBIOS E INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN: Se presentaron actas y formatos donde se evidencia los cambios en incidentes de seguridad de la información y solicitudes del impacto potencial sobre controles de la política de seguridad de la información, . **(Numeral 6.6.3).**
NO CONFORMIDADES
1.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN: No se encuentra evidencia donde se les comunique al personal la política de seguridad de la información, no se evidencia un objetivo establecido para la gestión de seguridad de la información, no se evidencia valoraciones del riesgo en intervalos planificados, no se evidencia que las auditorías internas sean usadas como oportunidad para la mejora ya que no mostraron documentos que soporten que se cumple con estos literales. **(Numeral 6,6,1 Literal a,b,d,f)**.
1.6 CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN: No cumplen con los requisitos de la política de seguridad de la información, no se evidencia que el objetivo de la gestión de seguridad de la informacíon se cumpla, tampoco aportan documentos donde se gestione los riesgos relacionados con la seguridad de la información. **(Numeral 6.6.2 Literal b,c,d).**
En constancia firman quienes intervinieron en la auditoria a los 23 días del mes de marzo de 2019
AUDITOR LIDER Diana Caviedes — **GERENTE DE LA EMPRESA: Gabriel Parodi**
EQUIPO AUDITOR AUDITADO: Nubia Roa

Anexo 7

Litigando.com Información judicial al día, esté donde esté	INFORME DE AUDITORIA	VERSION WLI-001
N° AUDITORIA	001-2019	
OBJETIVO	Evaluar la eficiencia, eficacia y efectividad del proceso gestión de la seguridad de la informacion (ITIL) basados en la norma ISO 20000-1 2011	
DESCRIPCION	La empresa litigar punto com dedicada a ofrecer servicios de revisión y vigilancia de procesos judiciales, tiene implementado el proceso de Gestión de seguridad de la	
ALCANCE	Formulación de acciones de mejora para la el procesos de gestión de seguridad de la información en la empresa litigar punto com, con una duración de un mes	
REFERENCIA	ISO/IEC 20000	
LUGAR	Empresa Litigar Punto com en la ciudad de Bogotá	
CONTACTO	Jefe del Area TI	
EQUIPO AUDITOR	DIANA MARCELA CAVIEDES – NUBIA ESPERANZA ROA VANEGAS	

RESUMEN EJECUTIVO

En el desarrollo de la auditoría en la empresa Litigar Punto Com se evaluó la eficiencia, eficacia y efectividad del proceso gestión de la seguridad de la información encontrando como resultado en la auditoría los siguientes aspectos.

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En cuanto al proceso de gestión de seguridad de la información se encuentra un alto compromiso por parte de la alta dirección puesto que muestran interés en mejorar las no conformidades, tiene bien definido el enfoque ante la gestión del riesgo, se aseguran que las auditorías internas se realicen para aplicar mejora continua, preservan el principio de la información para contenga confidencialidad, integridad y accesibilidad, las solicitudes al cambio de incidentes en la seguridad de la información se evalúan para identificar los riesgos de SI y el impacto potencial sobre los controles y la política de seguridad de la información. Sin embargo, se encuentra una serie de no conformidades que se deben mejorar para el buen funcionamiento del proceso de gestión de seguridad de la información. Unas de estas no conformidades es la falta de comunicación al personal de la política de seguridad de la información. no se evidencia un objetivo establecido para la gestión de seguridad de la información, no se evidencia valoraciones del riesgo en intervalos planificados, no se evidencia que las auditorías internas sean usadas como oportunidad para la mejora ya que no mostraron documentos que soporten que se cumple con estos literales.

CONCLUSIÓN DE AUDITORÍA

La empresa Litigar punto Com debe de implementar todas las no conformidades para el proceso de gestión de seguridad de la información funcione correctamente es necesario que tenga un respectivo control y monitoreo junto con la capacitación al personal para junto con ellos se pueda cumplir con los objetivos del negocio

En constancia firman quienes intervinieron en la auditoría 23 días de marzo de 2019

AUDITOR LIDER: DIANA CAVIEDES	GERENTE DE LA EMPRESA: GABRIEL PARDO

Anexo 8

Proyecto	**FORMULACION ACCION DE MEJORA DEL PROCESO DE GESTIÓN DE SEGURIDAD DE LA**
Elaborado por	**DIANA MARCELA CAVIEDES NUBIA ESPERANZA ROA VANEGAS**
Fecha de elaboracion	**09-mar-19**
Fecha de seguimiento	**09-mar-19**

FASE	Descripcion del riesgo	Causa	Consecuencia	Categoria	Estado	Tipo de riesg	Impacto	Estrategia de acción
DISEÑO DEL SERVICIO	Inexistencia rol responsable de la gestion de la seguridad de la información	Directivas no dan importancia requerida a la Seguridad de la Información	No hay gestión de la SI	Administrativo	Identificado	Negativo	Alto	Asignar rol
	Perdida de la información de los clientes	No hay administración de la seguridad de la información	Pérdida de imagen, reputación y dinero	Técnico	Identificado	Negativo	Alto	Gestionar la seguridad de la información
	Accesos no autorizados a los sistemas de información de misión crítica de la compañía	No hay proceso de gestion de usuarios	Pérdida de confidencialidad, integridad y disponibilidad de información	Técnico	Identificado	Negativo	Alto	Gestionar la seguridad de la información
	No existe plan de recuperación de desastres	Directivas no dan importancia requerida a la Seguridad de la Información	No hay gestión de la SI	Técnico	Identificado	Negativo	Alto	Gestionar la seguridad de la información
	No estan identificadas las aplicaciones y la infraestructura asociada a las aplicaciones core del negocio	Directivas no dan importancia requerida a la Seguridad de la Información	No hay gestión de la SI	Técnico	Identificado	Negativo	Alto	Gestionar la seguridad de la información

Anexo 9

PLAN DE MEJORA						
AREA DE MEJORA	CAUSAS PRINCIPALES	OBJETIVO	ACCIONES DE MEJORA	PRIORIDAD	TIEMPOS (INICIAL - FINAL)	IMPACTO EN LA ORGANIZACIÓN
ALTA DIRECCIÓN	Las políticas y procedimientos de TI carecen de los respectivos controles para el cumplimiento del objetivo general de la compañía	Crear un control eficaz para el correcto funcionamiento de las políticas y procedimientos de TI	Establecer el respectivo proceso, basándose en la norma ISO 20000	ALTA		Alineación con los miembros del comité de seguridad de la información
ALTA DIRECCIÓN	Inexistencia de herramientas que permitan alertar a los empleados de la empresa sobre los riesgos a los que está expuesta la compañía si no se realiza un buen manejo de la información	Lograr que todos los empleados de Litigar punto com, cuenten con un nivel alto de conocimiento con respecto a la seguridad de la información	Establecer modelo de capacitación y periodidad de acuerdo con los diferentes roles de la compañía, lo cual deba ser requisito para todos y cada uno de los miembros de la compañía	ALTA		Medir el conocimiento a nivel de seguridad de todos los empleados de la compañía
ALTA DIRECCIÓN	Ausencia del DRP	Generar un plan de recuperación ante desastres	Implementar un plan de recuperación ante desastres, de manera preventiva	ALTA		Personal altamente calificado en las TI, para fortalecer los procesos de TI
ALTA DIRECCIÓN	No existe un mecanismo para el almacenamiento de forma segura de las contraseñas de los sistemas de información de misión critica	Garantizar el almacenamiento de contraseñas de los sistemas de información críticos	Implementar base de datos confiable y segura, donde reposen las contraseñas de misión crítica dentro de los sistemas de información	ALTA		Administrador directorio activo
ALTA DIRECCIÓN	Carencia de un mecanismo de registro y control de licenciamiento de software	Contar con un sistema de registro para el respectivo control de licencias de software	Uso de herramientas TI para hacer el seguimiento de licencias vencidas	ALTA		Personal administrativo
ALTA DIRECCIÓN	No se realiza de forma periódica mantenimiento correctivo del software	Definir cronograma alineado con las buenas prácticas, para la ejecución de mantenimiento correctivo del software	Estimar fechas de forma periódica para llevar a cabo trabajos de mantenimiento correctivo del software	ALTA		Personal con conocimiento de TI
ALTA DIRECCIÓN	De las no conformidades presentes, no se tiene ningún plan de seguimiento para darles solución.	Aplicar acciones correctivas de acuerdo a las no conformidades de las auditorias	Crera un plan de seguimiento para los no conformidades	ALTA		director del Área TI