ENTREGA 2 (SEMANA 5) - OPCION DE GRADO

Ingeniero Moisés Iván Rojas Marín – Código: 2022010014

Ingeniero Javier Ricardo Parra Lozada – Código: 1620650108

Facultad de Ingeniería, Diseño e Innovación, Institución Universitaria Politécnico Grancolombiano

Tercer Bloque / Opcion De Grado I -[grupo1]

Profesor Ricardo Gómez

1 de diciembre de 2020

Contenido

1. DESCRIPCIÓN DEL PROBLEMA:

La compañía Parra y Rojas Tech S.A.S es una empresa con prometedor crecimiento en los servicios tecnológicos críticos para el mercado actual, como lo son diseño e implementación de redes y soluciones de última milla, servicios en la nube y desarrollo de aplicaciones a la medida, pero a pesar de ofrecer una gama de servicios con gran innovación tecnológica, presenta unas fallas en la parte de seguridad de la información, más específicamente en la ausencia de mecanismos de seguridad que prevengan ataques a las propiedades de la información como lo es la confidencialidad, integridad y disponibilidad, dichos ataques pueden vulnerar las propiedades de la información tanto interna como la información propia del manejo comercial con los clientes y proveedores, dichas falencias nos puede llevar hasta incumplir compromisos legales y regulatorios a las que la empresa debe cumplir obligatoriamente.

Todos los aspectos anteriormente expuestos, nos puede llevar a perdidas económicamente fuertes, ya sea por incumplimiento de compromisos con los clientes o reprocesos presentados, también a perdidas reputacionales frente al mercado que indiscutiblemente también tendría a largo plazo pérdidas económicas cuantiosas.

1.1. RAZÓN REAL.

La compañía padece ausencia de procesos institucionalizados que garanticen la seguridad en los datos e información de clientes, los servicios prestados o productos desarrollados para ellos, lo que nos conlleva a no tener una total confianza.

1.2. SITUACIÓN DESEADA.

La compañía tiene implementado procesos que garantizan la seguridad en los datos y en la información dentro de los flujos de procesos de contratación, clientes, empleados, proyectos y contabilidad. Así teniendo continuidad de los procesos y del negocio propiamente, también ofreciendo completa confianza a los diferentes clientes de las variadas líneas de negocio de la organización.

1.3. PREGUNTA PROBLEMA.

¿La compañía puede mejorar sus procesos internos y comerciales, con la ayuda de la implementación de un sistema de seguridad de la información, que garantice la seguridad en sus procesos de negocio y de proyectos, mejorando así la calidad de estos, y evitando problemas de seguridad de la información tanto en sus procesos internos como externos?

1.4. RAZÓN DIFERENCIAL.

La organización no se ha preocupado por ahondar en temas de seguridad de la información, tanto en el ámbito interno, como en el manejo de los procesos comerciales con los clientes, y esto se debe a factores internos como lo son falta de concienciación en la importancia de incluir la seguridad de la información a los procesos internos, falta de un compromiso real de la gerencia para llevar a cabo proyectos de implementación de seguridad de la información, falta de personal capacitado para llevar a cabo dichos proyectos, y falta de capacitación al personal interno de la importancia de la seguridad de la información en sus actividades, entre otros.

2. OBJETIVOS

2.1. General.

Implementar mecanismos en procesos, claros, medibles, y gobernables en la compañía, en los cuales garantice la confidencialidad, integridad y disponibilidad de la información de clientes, servicios o productos de estos. La implementación de los procesos y sus mecanismos deben cumplir los siguientes aspectos:

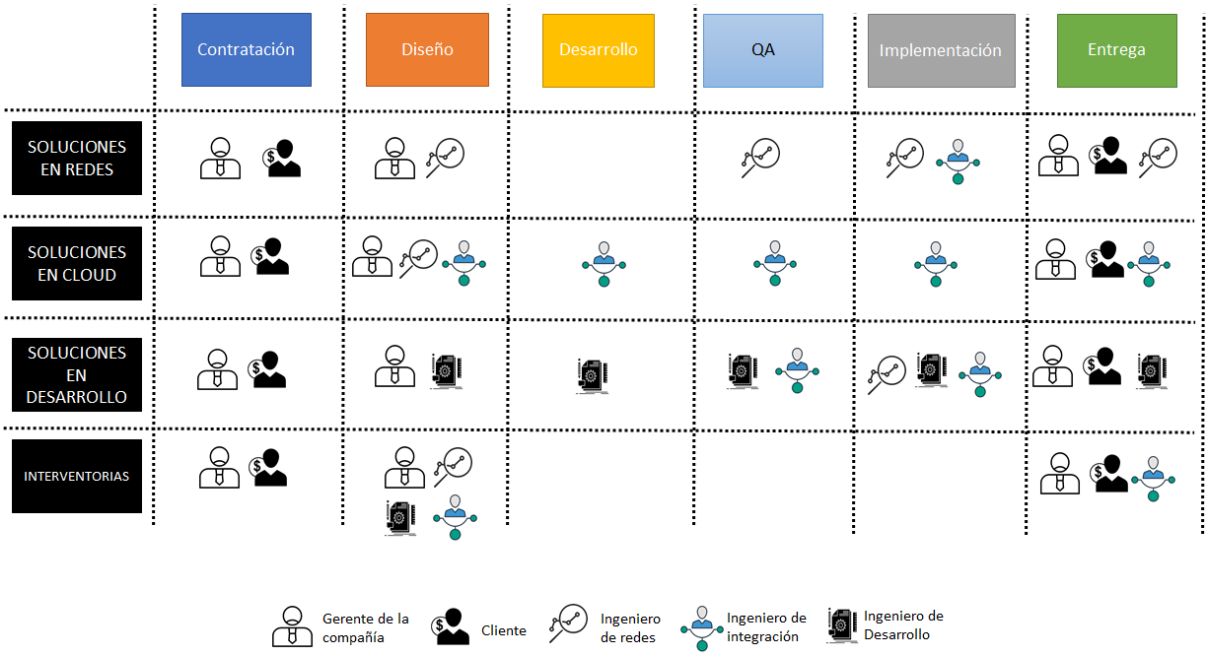
- El tiempo límite de planeación de la implementación no pueden ser superior a 4 semanas.
- El tiempo total de implantación de los procesos y sus mecanismos no puede superior a 16 semanas.
- El costo del total proyecto no puede superar el 16% del total de ganancia neta del año 2019 de la compañía.

2.2. Específicos.

- Crear la primera versión de la política de seguridad de la compañía.
- Generar un inventario de bienes de información dentro de cada proceso de la compañía.
- Generar matriz de riesgos de la información en la compañía.

3. IDENTIFICACIÓN DE LOS ACTORES:

Los Actores interesados en los procesos de la compañía, se plasman en el siguiente diagrama.



Definición de clientes:

Gerente de la compañía: Es quien desarrolla el proceso de contratación de servicios o desarrollo de productos con los clientes y hace levantamiento global y general de los requerimientos con ellos.

Cliente: Es quien hace el requerimiento de servicio o producto de desarrollo de software, lo recibe a cabalidad y paga por él.

Ingeniero en redes: Ingeniero especialista en diseño y tecnología en redes.

Ingeniero de desarrollo: Ingeniero especialista en diseño y desarrollo de software.

Ingeniero de integración: Ingeniero especialista en arquitectura de software, tecnologías y componentes de integración de productos de software e infraestructura.

De acuerdo con la descripción anterior, por medio de la siguiente tabla se describen las preocupaciones de cada gama de actores en la situación real del documento.

La compañía padece ausencia de procesos institucionalizados que garanticen la seguridad en los datos e información de clientes, los servicios prestados o productos desarrollados para ellos.		
Cliente	**Gerencia General**	**Ingenieros especialistas**
Temor de fuga de información sensible de cada cliente, manejada por la organización	Pérdidas económicas y reputacionales debido a fallas en los procesos internos y afectaciones	Retrabajos en tareas por cada uno de los proyectos con los clientes

Demora en entrega de proyectos por fallas de seguridad en los distintos procesos asociados		Pérdidas de información en los procesos de diseño.
		Pérdidas de información en los procesos de desarrollo.
		Pérdida de información en los procesos de implementación.

Para la identificación de clientes se va a usar la matriz de Influencia/Poder, de acuerdo con las siguientes definiciones.

		INVOLUCRAMIENTO ACTIVO	
		Influencia bajo	**Influencia alta**
AUTORIDAD	**Poder Alto**	Mantenerlos informados Nunca ignorados	Trabaja para él
	Poder Bajo	Mantenerlos informados Con mínimo esfuerzo	Trabaja con ellos

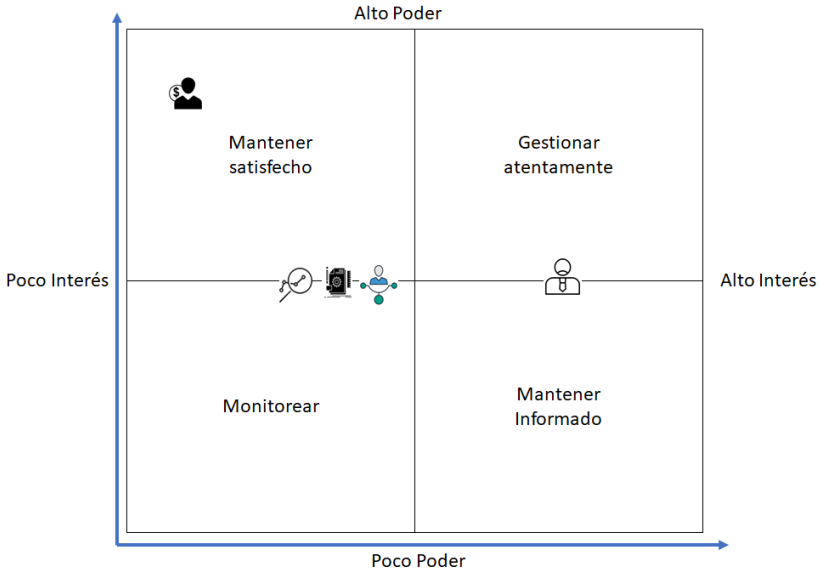
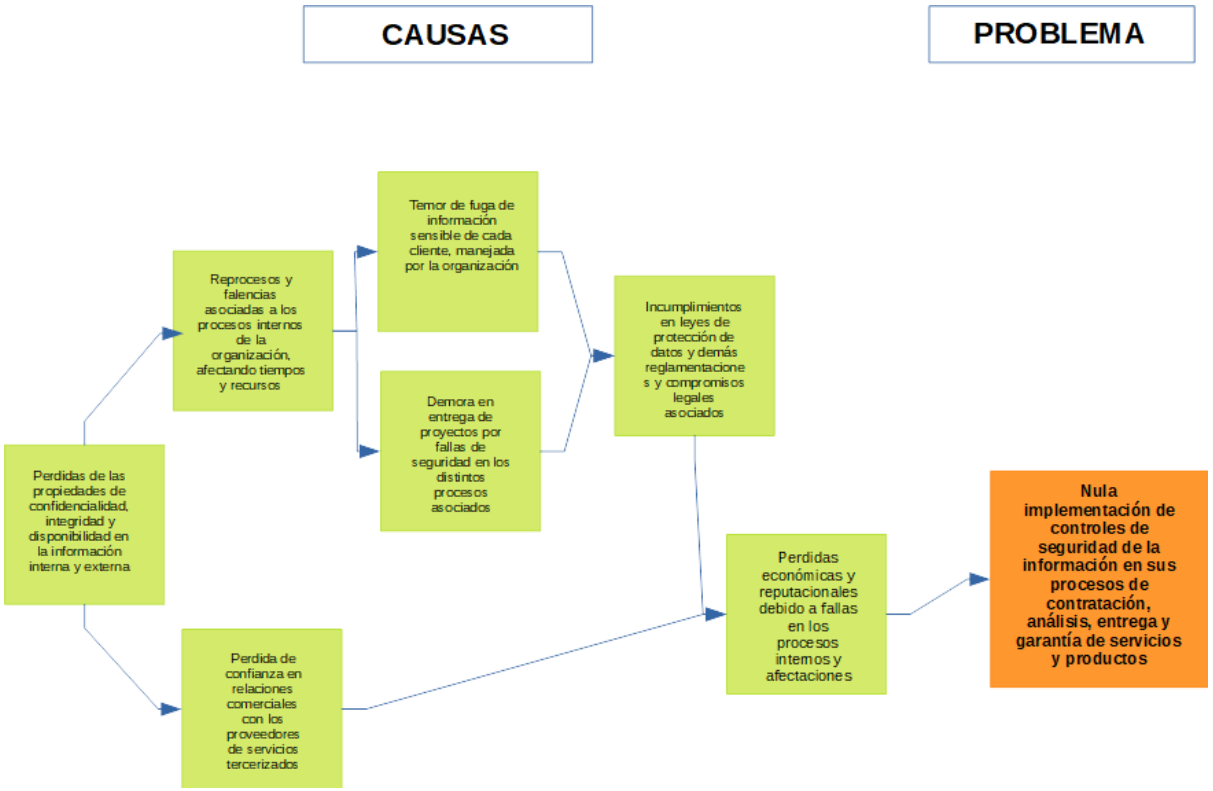


Ilustración 1 - Mapeo de usuarios

4. RED DE CAUSALES.

Ítem	Problema	Causa	Efecto
1	La compañía padece ausencia de procesos institucionalizados que garanticen la seguridad en los datos e información de clientes, los servicios prestados o productos desarrollados para ellos	Los procesos de la compañía son artesanales y muestran poca madurez	Los procesos son difícilmente repetibles o ofrecen una calidad cuestionable por las partes que ejecutan tareas en ellas
		No hay mecánicas de contingencia en caso de pérdida de información	Pérdida de tiempo en recuperación de datos. Incumplimiento en los tiempos de los procesos
		La información de cliente internos y externos puedes están o ser manipulada por personal no autorizado	Demandas por incumplimiento en de manejo de datos personales



5. EJECUCIÓN

La ejecución del proyecto que satisface la pregunta: ¿La compañía puede implementar procesos que garanticen la seguridad en datos en sus procesos de negocio y proyecto, mejorando la calidad de estos? Esta constituida en tres fases.

- Color amarillo, proceso de análisis y planeación.
- Color azul, proceso de contextualización, implementación y ejecución.
- Color verde, evaluación y entrega del proceso de implementación.

Item	Actividad	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20
1	Inicio del proceso																				
2	Invetnario de procesos y activos a proteger																				
3	Mecanismos generales de protección a procesos e información que manejen																				
4	Generación de la matriz de riesgo																				
5	Generación plan de capacitaciones																				
6	Presentación de propuestas de mejora																				
7	Ajustes a propuesta																				
8	Aprobación de Gerencia																				
9	Contextualización del plan de mejora y optimización de procesos																				
10	Optimización de roles enfocados a procesos																				
11	Implementación de controles a los activos de información en los procesos																				
12	Validación y prueba en las optimizaciones																				
13	Presentación de resultados																				

6. ANÁLISIS PROSPECTIVO

El análisis prospectivo se refiere como el estudio de las causas técnicas, científicas, económicas, tecnológicas, sociales y demás situaciones que el futuro podrían impactar en el desarrollo de las empresas.

En el siguiente análisis prospectivo realizado a la compañía Parra y Rojas Tech S.A.S, se pretende dar una evaluación detallada y precisa para identificar variables favorables y no favorables dentro y fuera de la compañía.

La compañía Parra y Rojas Tech S.A.S es una empresa con prometedor crecimiento en los servicios tecnológicos críticos para el mercado actual, como lo son diseño e implementación de redes y soluciones de última milla, servicios en la nube y desarrollo de aplicaciones a la medida

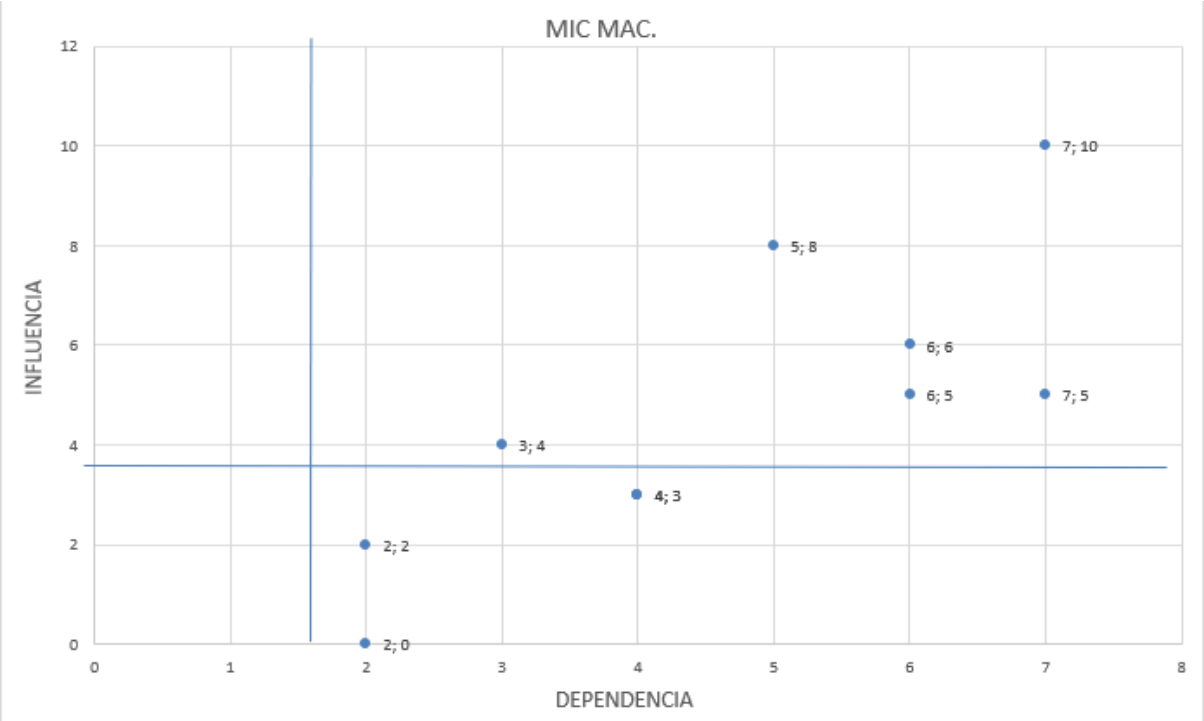
Primero, sacamos un listado de variables que son relevantes para la empresa en el estudio prospectivo, luego con calificación priorizamos las principales variables, hasta tener las principales que pueden influir en el estudio prospectivo:

VARIABLES						
#	**Nombre de variable**	**Factor**	**Descripción**	**DOFA**	**Magnitud del impacto**	**Indicador de la variable**
1	Nueva competencia en el sector tecnológico	ECONOMICO	Aumento de empresas que ingresan al mismo sector del mercado	Amenaza	Alto	# Clientes perdidos por la competencia/clientes totales *100
2	pérdida de clientes existentes	ECONOMICO	Pérdida de clientes por problemas de fuga y/o perdida de información	Debilidad	Alto	# Clientes perdidos /clientes totales *100
3	Aumento ganancias mejora procesos	ECONOMICO	Aumento de ganancias por implementar buenas prácticas seguridad	Oportunidad	Medio	% ganancias después de implementación / año
4	Perdida reputacional por fallos seguridad	ECONOMICO	Pérdida económica por deterioro de buen nombre debido a fallos de seguridad	Debilidad	Alto	% de pérdidas económicas por perdida de clientes
5	Sanciones por incumplimiento regulatorio	LEGAL	Sanciones económicas por incumplir marco regulatorio actual	Amenaza	Alto	% de pérdidas económicas por incumplimientos legales
6	Sensibilización interna sobre seguridad información	SOCIAL	Plan de capacitación sobre temas de seguridad	Oportunidad	Alto	# personas capacitadas/# total personal
7	Aumentar el teletrabajo en la compañía	TECNOLOGICO	Aumento de empleados en teletrabajo permanente	Oportunidad	Medio	# de trabajadores en teletrabajo/ # de trabajadores aptos para teletrabajo *100
8	Aumento ataques informáticos	TECNOLOGICO	Riesgo inherente al mercado de sufrir ataques informáticos	Amenaza	Alto	# ataques prevenidos/#ataques detectados *100
9	Aumento regulaciones privacidad y manejo de datos	LEGAL	Creación de más leyes de protección de datos de clientes y empleados	Amenaza	Alto	Cumplimiento nuevas regulaciones (SI/NO)
10	Implementación SGSI interno	LEGAL	Obligatoriedad de implementación SGSI por relaciones comerciales	Debilidad	Alto	% porcentaje avance implementación> 70% /año

A continuación, se procede a calcular la matriz de impactos cruzados con base en la 10 tendencias o variables claves escogidas para la empresa

	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	DEPENDENCIAS Totales
V1 Nueva competencia en el sector tecnologico		2	0	0	0	0	0	0	0	0	2
V2 Perdida de clientes existentes	0		0	3	1	0	0	1	0	0	5
V3 Aumento ganancias mejora procesos	0	0		0	0	1	1	0	1	3	6
V4 Perdida reputacional por fallos seguridad	0	3	0		0	0	0	3	0	0	6
V5 Sanciones por incumplimiento regulatorio	0	2	0	0		0	0	0	0	2	4
V6 Sensibilización interna sobre seguridad información	0	0	3	0	0		1	0	0	3	7
V7 Aumentar el teletrabajo en la compañía	0	0	1	0	0	1		0	0	0	2
V8 Aumento ataques informaticos	0	1	0	2	0	0	0		0	0	3
V9 Aumento regulaciones privacidad y manejo de datos	0	0	0	0	2	0	0	0		2	4
V10 Implementacion SGSI interno	0	0	2	0	0	3	0	0	2		7
INFLUENCIAS TOTALES	0	8	6	5	3	5	2	4	3	10	

Y como resultado, vemos el gráfico MIC-MAC, así podemos observar las distintas variables en la zona de poder y la zona de conflicto.



VARIABLE	ETIQUETA	Dependencia TOTALES	Influencias TOTALES
V1 Nueva competencia en el sector tecnológico	**1**	2	0
V2 Perdida de clientes existentes	**2**	5	8
V3 Aumento ganancias mejora procesos	**3**	6	6
V4 Perdida reputacional por fallos seguridad	**4**	6	5
V5 Sanciones por incumplimiento regulatorio	**5**	4	3
V6 Sensibilización interna sobre seguridad información	**6**	7	5
V7 Aumentar el teletrabajo en la compañía	**7**	2	2
V8 Aumento ataques informáticos	**8**	3	4
V9 Aumento regulaciones privacidad y manejo de datos	**9**	4	3
V10 Implementación SGSI interno	**10**	7	10
Promedio		4,6	4,6

Las variables a considerar son del cuadrante superior derecho, ubicado en la zona de conflicto, las cuales en el cuadro anterior están señaladas en azul, el cual debe ser el enfoque de la empresa referente al problema inicial planteado

Luego con estas variables en zona de conflicto, podemos plantear hipótesis a un futuro cercano:

V2 Perdida de clientes existentes, debido a la nula implementación de mecanismos de seguridad en los procesos internos y que incurren en demoras o incumplimientos en acuerdos comerciales:

- Hipótesis 1: perder el 2% de la base de clientes existente
- Hipótesis 2: perder el 4% de la base de clientes existente
- Hipótesis 3: perder el 7% de la base de clientes existente

V3 Aumento ganancias mejora procesos, gracias a la mejora de los diferentes procesos internos, aplicándole mecanismos y controles de seguridad, tenemos procesos mas claros y mas eficientes para beneficiar a los clientes:

- Hipótesis 1: Aumentar 1% de ganancias en los productos con procesos mejorados
- Hipótesis 2: Aumentar 3% de ganancias en los productos con procesos mejorados
- Hipótesis 3: Aumentar 6% de ganancias en los productos con procesos mejorados

V4 Perdida reputacional por fallos seguridad, significa que porcentaje de ganancias proyectadas pierde la entidad, debido al daño reputacional después de comprobar fallos de seguridad materializados

- Hipótesis 1: Perdida de 5% de ganancias por perdida reputacional
- Hipótesis 2: Perdida de 8% de ganancias por perdida reputacional
- Hipótesis 3: Perdida de 10 % de ganancias por perdida reputacional

V6 Sensibilización interna sobre seguridad información, se refiere al porcentaje de personal capacitado en temas de seguridad de la información aplicado en su rol dentro de la compañía

- Hipótesis 1: 60% de personal capacitado en la organización
- Hipótesis 2: 80% de personal capacitado en la organización

- Hipótesis 3: 90% de personal capacitado en la organización

V8 Aumento ataques informáticos, acá hablamos del número de ataques informáticos prevenidos hacia los recursos de la organización sobre el total detectados

- Hipótesis 1: 60% de ataques informáticos evitados
- Hipótesis 2: 80% de ataques informáticos evitados
- Hipótesis 3: 95% de ataques informáticos evitados

V10 Implementación SGSI interno, se refiere al porcentaje de implementación del SGSI en el primer año del proyecto

- Hipótesis 1: 60% de implementación total del proyecto del SGSI
- Hipótesis 2: 70% de implementación total del proyecto del SGSI
- Hipótesis 3: 80% de implementación total del proyecto del SGSI

Según estas hipótesis, podemos inferir que el estudio prospectivo nos lleva a mirar los beneficios de implementar controles y mecanismos encaminados a la seguridad de la información, como por ejemplo un proyecto de implementación de un SGSI, como gran eje central para evitar ataques informáticos, crear un plan complete de capacitación y sensibilización para los colaboradores, todas estas acciones nos ayudaría a la mejora de procesos que al final repercute en mejoras económicas gracias a dichas mejoras, y por ultimo prevendríamos tanto la pérdida de clientes y pérdidas económicas debido a perdidas reputacionales, las cuales serian muy complicadas para el desarrollo de la empresa.

7. GOBERNABILIDAD, VIABILIDAD Y PERTINENCIA

7.1. Gobernabilidad

El gobierno de proyectos es un sistema basado en procesos que permite a la gerencia de la empresa, su asamblea de accionistas, su junta directiva, y otras partes interesadas tener información oportuna, relevante, confiable y transparente sobre todas las inversiones empresariales realizadas a través de los proyectos, programas y portafolios.

La gobernanza del proyecto ocurre principalmente fuera de los límites tradicionales de un proyecto. En términos generales, involucra a la junta de una organización (o sus delegados) y al patrocinador del proyecto (un gerente ejecutivo) encargado de llevar a la organización a un desempeño superior al promedio, teniendo en cuenta el riesgo.

Según PMI, la gobernabilidad del proyecto debe actuar como eslabón que permite que la junta directiva y los diferentes stakeholders del proyecto intercambien información relevante y confiable del proyecto en sí.

Para lograr el éxito del desarrollo del proyecto, la gobernabilidad debe ir liderada por la parte gerencial de la organización, los cuales tendrán la función de supervisar y controlar las fases del proyecto, así mismo la toma de decisiones que pueden afectar positiva o negativamente la implementación del proyecto de seguridad de la información.

7.2. Viabilidad

7.2.1 Legal

La viabilidad legal, se refiere a las diferentes leyes y normativas que debemos cumplir atadas a la implementación del proyecto y que afecte la operación de la organización, como lo son las siguientes:

- LEY ESTATUTARIA 1266 DE 2008: Disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales
- LEY ESTATUTARIA 1581 DE 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- DECRETO 1377 DE 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- LEY 1273 DE 2009: Ley de Delitos Informáticos en Colombia
- DECRETO 2952 DE 2010: Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008
- DECRETO 886 DE 2014: Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012
- DECRETO 1083 DE 2015: Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012

7.2.2 Técnica

Para el desarrollo del proyecto, técnicamente hablando, la necesidad primaria sería contratación de una empresa tercera, experta en la implementación de sistemas de seguridad de la información, y en la planeación de proyectos de esta índole, estos dos requisitos deben ir unidos, ya que la empresa tercera, tendrá la responsabilidad de cumplir en los tiempos establecidos, las diferentes fases planteadas en el proyecto, tanto en el levantamiento de información inicial, la construcción de las diferentes matrices, planes de capacitación, políticas y demás herramientas que ayude a la compañía a cumplir con el objetivo planteado. Así mismo se propone la contratación de un experto en seguridad de la información, que haga el empalme del proyecto con la empresa consultora, y pueda seguir la evolución de sistema, una vez se finalice el proyecto planteado, para así tener actualizado el sistema de seguridad de la información de acuerdo con los objetivos estratégicos de la organización

7.2.3 Económica

El proyecto de implementación de mecanismos y controles de seguridad no puede superar el 16% del total de ganancia neta del año 2019 de la compañía, por ende debe distribuirse el proyecto en las siguientes partes:

Contratación de un tercero para inicio, ejecución y despliegue del proyecto, esto según el nivel de profundidad que requiera la empresa, debe incluir la adquisición de equipos para seguridad perimetral, así como equipos para tener algún tipo de “Defense in Depth” implementada.

También la actualización de software en seguridad tato para equipos terminales como para servidores.

A lo anterior se debe sumar el costo de creación e implementación de un plan completo de capacitación y sensibilización para el personal interno, y por último la adquisición de una persona que se encargue del sistema implementado

7.3. Pertinencia

Debido a los reportes de aumento de ciber ataques a empresas, el cual muestra por ejemplo que, en el 2017, Colombia fue el sexto país con mayor numero de ataques en Latinoamérica, se hace imprescindible contar con mecanismos de prevención y respuesta a la hora de la materialización de amenazas informáticas a las cuales se enfrentan las empresas hoy en día, ya que según cifras del 2018, gracias a dos millones de ciber ataques, se presentaron perdidas mundiales por 45.000 millones de dólares, lo cual puede llevar a una pyme a la bancarrota. Debido a todo lo expuesto anteriormente, el proyecto se hace de gran impacto e importancia, ya que podemos mejorar la seguridad de la información de la compañía, no solo de la interna propiamente, sino la que por los procesos comerciales, tratamos y administramos, y teniendo en cuenta el gran valor de la información para las empresas, un proyecto de estos es de obligatoria implementación en cualquier organización, sin importar el tamaño de esta.

8. BIBLIOGRAFÍA

Bibliografía

Figuerola, N. (Mayo de 2014). *Gobernabilidad de los Proyectos*. Obtenido de https://articulospm.files.wordpress.com/: https://articulospm.files.wordpress.com/2014/05/gobernabilidad-de-los-proyectos.pdf

GÓMEZ, M. A. (2016). *UNA MIRADA A LA GERENCIA ESTRATÉGICA DE PROYECTOS*. Obtenido de repository.eafit.edu.co: https://repository.eafit.edu.co/bitstream/handle/10784/11445/MariaAlejandra_SaldarriagaG%c3%b3mez_2016.pdf?sequence=2&isAllowed=y