Elaboración del plan director de implementación del SGSI basado en la ISO/IEC27001 para una empresa de Servicios y Soluciones Informáticas

Presentación de Trabajo Final de Master

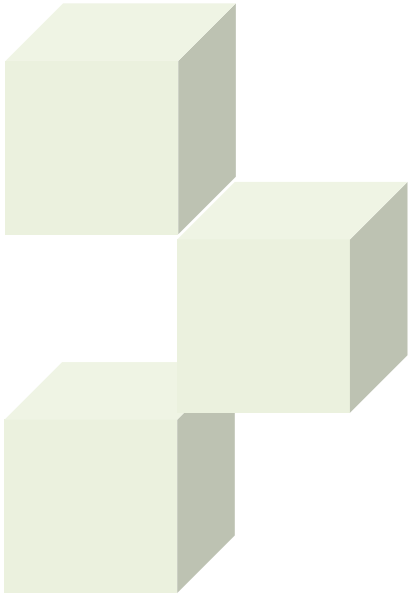
William Alexander Ortiz Jimenez

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Universitat Oberta de Catalunya

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Agenda



EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

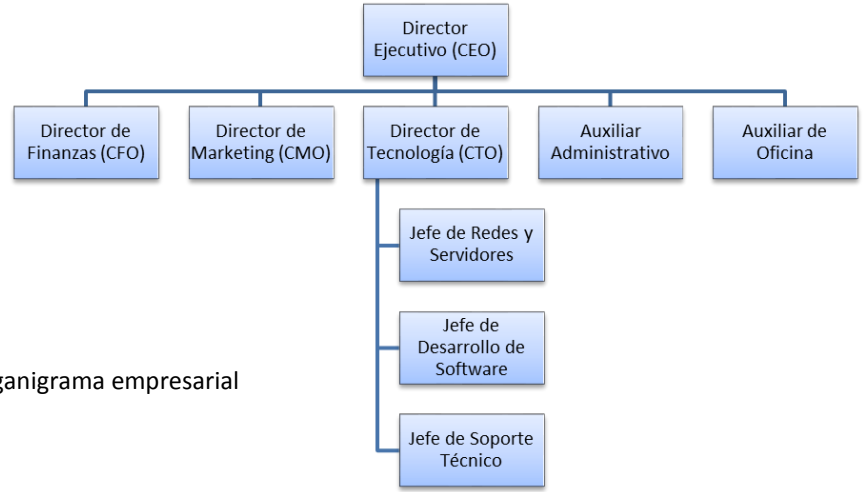
1. Resumen

El presente Trabajo Final de Master tiene como propósito presentar la implementación del Sistema de Gestión de la Seguridad de la Información de la empresa de servicios y soluciones informáticas EXPERTEC ubicada en Colombia en el Departamento del Cauca en la ciudad de Popayán, basado en la norma ISO/IEC 27001 y los controles del estándar ISO/IEC 27002 referente a las buenas prácticas.

Para la implementación del SGSI se estableció diferentes etapas iniciando con un análisis DAFO para contextualizar y comprender la situación actual de la empresa en referencia al ámbito de la seguridad de la información, posterior se realizó un análisis diferencial de la empresa para evaluar la norma ISO/IEC 27001 y los controles de la norma ISO/IEC 27002 en su estado inicial; así mismo, se establecieron los documentos para el cumplimiento normativo de la implementación del SGSI. Por otra parte, se utilizó la metodología de análisis y gestión de riesgos MAGERIT para orientar a la empresa en la gestión de riesgos a los que está expuesta. Una vez definido el análisis y gestión de riesgos se establecieron propuestas de proyectos para implementar mejoras y medidas de control adecuadas que permitan mitigar los riesgos encontrados. Finalizando, se estableció un proceso de auditoría para analizar el nivel de capacidad de madurez en la que avanzo el SGSI después de implementar las propuestas de proyectos planteados junto con los resultados obtenidos.

2. Contexto

EL proyecto del TFM fue realizado en una empresa de la ciudad de Popayán del país de Colombia clasificada como MiPyme. La empresa ofrece servicios y soluciones de implementación y configuración de redes estructuradas y servidores, desarrollo de software y aplicaciones móviles, soporte técnico a empresas en software y hardware.



Organigrama empresarial

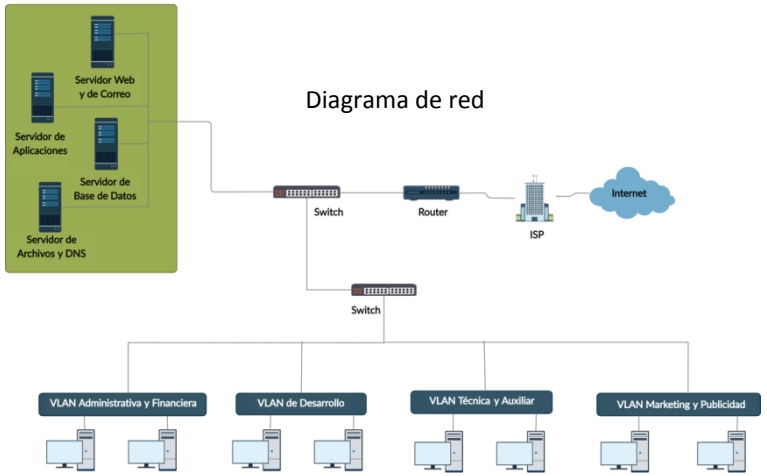


Diagrama de red

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Situación actual

Para entender la situación actual de la empresa en relación a la protección de los activos y la seguridad de la información se hizo uso de la matriz DAFO, la cual, permite realizar un diagnostico y gestión de las debilidades, amenazas, fortalezas y oportunidades.

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Situación actual

A su vez, se complementó con la estrategia CAME (Corregir, afrontar, mantener y explotar) para definir un plan estratégico sobre el análisis realizado en la empresa.

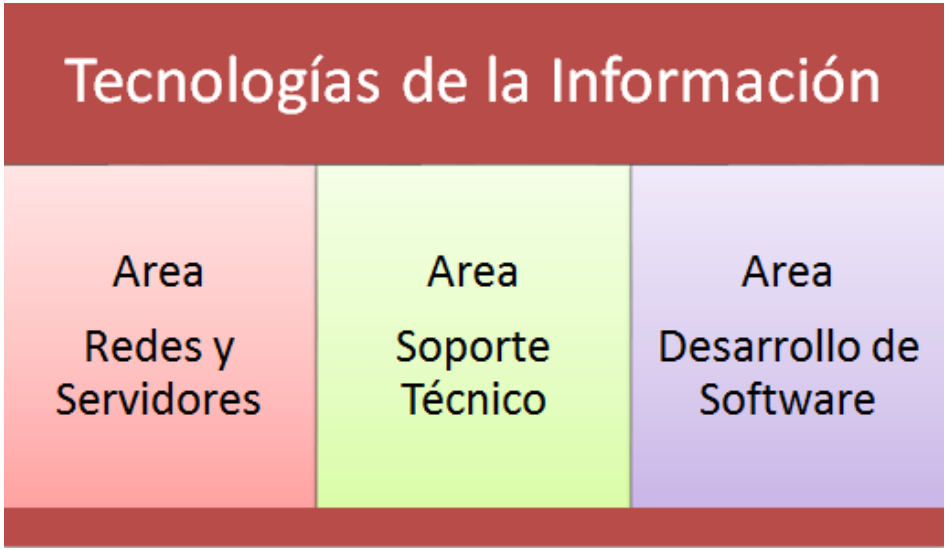
DAFO/CAME	Análisis Interno	Análisis Externo
Factores Negativos	Estrategias para **Corregir Debilidades** *- Generar sistemas de protección ante ataques de redes externas.* *- Implementar elementos redundantes de sistemas de alimentación UPS necesarios para el continuó funcionamiento de servidores y sistemas de información.* *- Implementar sistemas de protección de antivirus y antimalware en los dispositivos de almacenamiento donde se realizan los backups.* *- Generar métodos de identificación y autenticación a los equipos de cómputo del área de desarrollo.* *- Plan de concientización y capacitación sobre las políticas de seguridad a los funcionarios de la empresa.* *- Formación a los funcionarios sobre buenas prácticas y uso de los dispositivos tecnológicos y el Internet.*	Estrategias para **Afrontar Amenazas** *- Plan de soporte ante fallas de Internet, servicio de alojamiento y cloud.* *- Estrategias de asistencia efectiva y oportuna a las empresas que requieren el servicio de soporte técnico.* *- Monitoreo y protección constante de la infraestructura de red y servidores que contienen información crítica y sensible.* *- Actualización de sistemas operativos, antivirus y sistemas de información.* *- Emplear estrategias para la protección de los vectores de ataque identificados en el monitoreo.* *- Realización periódica de copias de seguridad de la información crítica y sensible.*
Factores Positivos	Estrategias para **Mantener Fortalezas** *- Capacitación y actualización en tendencias tecnológicas al personal de la empresa.* *- Certificación permanente de la empresa y el personal de acuerdo a los objetivos y modelo de negocio.* *- Estrategias para la continua inversión en tecnología.* *- Mejoramiento y actualización de equipos, dispositivos y software requerido en la empresa.* *- Generación de espacios y actividades para el fortalecimiento del trabajo colaborativo entre los funcionarios o personal.*	Estrategias para **Explotar Oportunidades** *- Establecer los controles y parámetros para el tratamiento de la seguridad de la información.* *- Obtener la certificación ISO/IEC 27001 mediante la implementación del SGSI.* *- Aplicar los procedimientos y controles para lograr los objetivos planteados en el SGSI y el mejoramiento continuo del negocio.* *- Evaluar las capacitaciones sobre la implementación y ejecución del SGSI al personal para retroalimentar y obtener una constante mejoría en la realización de los procesos.*

Matriz DAFO en estrategia CAME

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

3. Alcance del SGSI

Se aplicó a las áreas y sistemas que ejecutan los procesos más importantes de la empresa como son los activos y recursos de la estructura de redes y servidores, el área de soporte técnico y el área de desarrollo de software y aplicaciones.



EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

4. Objetivos del Plan Director

- Identificar los activos y recursos que se requieren proteger teniendo en cuenta su nivel de importancia y necesidad para el funcionamiento de los procesos de la empresa.
- Analizar la situación actual de la empresa teniendo en cuenta los factores críticos de seguridad, riesgos potenciales e impactos generados.
- Identificar y analizar amenazas y vulnerabilidades que incidan en los activos y recursos tanto en la infraestructura de redes, servidores, equipos de cómputo y elementos del soporte técnico tanto a nivel físico como lógico.
- Determinar lineamientos, estrategias y parámetros que permitan mitigar las amenazas y vulnerabilidades con el propósito de mitigar los riesgos presentes.
- Elaborar el plan director del sistema de gestión de seguridad de la información SGSI, abarcando las normativas y requerimientos de seguridad; funciones, roles y responsabilidades de los usuarios para el control y administración del SGSI; guías de buenas prácticas y planes de continuidad de negocio acorde a los procesos de la empresa; lo anterior, garantizando la confidencialidad, integridad y disponibilidad de la seguridad de la información en la empresa.

5. Análisis diferencial

Análisis GAP

Clausulas de la ISO/IEC 27001

- Contexto de la organización
- Soporte
- Operación
- Evaluación del desempeño
- Mejoramiento

Nivel	Estado	Valoración en porcentajes	Definición
L0	Inexistente	0%	Carencia total de procesos reconocibles. No existe gestión en la seguridad.
L1	Inicial	25%	No existen procesos concretos y tampoco plantillas o guías definidas. Este nivel es preliminar, el cual establece pautas y directivas para asegurar la seguridad de la información.
L2	Repetible	50%	Se siguen procedimientos similares en las mismas actividades o tareas que realizan las personas. No existe comunicación de procedimientos generales. Las responsabilidades asignadas recaen en cada persona. Existe un alto grado de confianza en el conocimiento de las personas.
L3	Establecido	75%	Se implementan, comunican y documentan procesos de forma más permanente y estable. La entidad tiene más participación en el desarrollo de los procesos por medio de un control y monitoreo establecido.
L4	Administrado	95%	Se mide el cumplimiento y evolución de los procesos mediante indicadores. Los procesos facilitan mejores prácticas. Se determinan medidas cuando los procesos no funcionan de manera efectiva.
L5	Mejorado	100%	Teniendo en cuenta los resultados obtenidos de los controles implantados se hace una revisión de los procesos que han tenido una mejora continua. Se dispone de herramientas para garantizar y mejorar la calidad y eficiencia.

Modelo de capacidad de madurez CMM

Análisis GAP

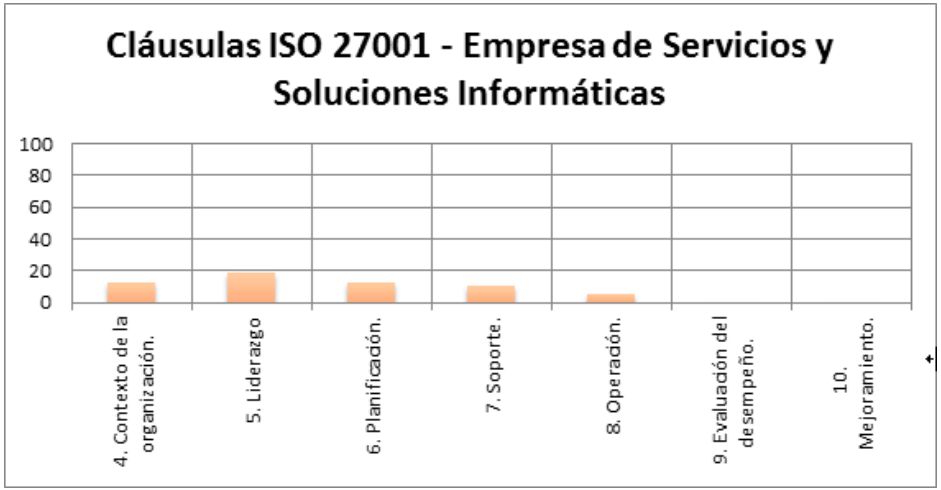
Dominios, objetivos de control y controles de la ISO/IEC 27002:2013

- 14 dominios
- 35 objetivos de control
- 114 controles

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Resultados del Análisis diferencial

Los requisitos o cláusulas de la norma ISO/IEC 27001 para un SGSI de la empresa se encuentran por debajo del 20% de cumplimiento. Lo que indica que el nivel de capacidad de madurez esta por debajo del nivel L1 (Inicial)



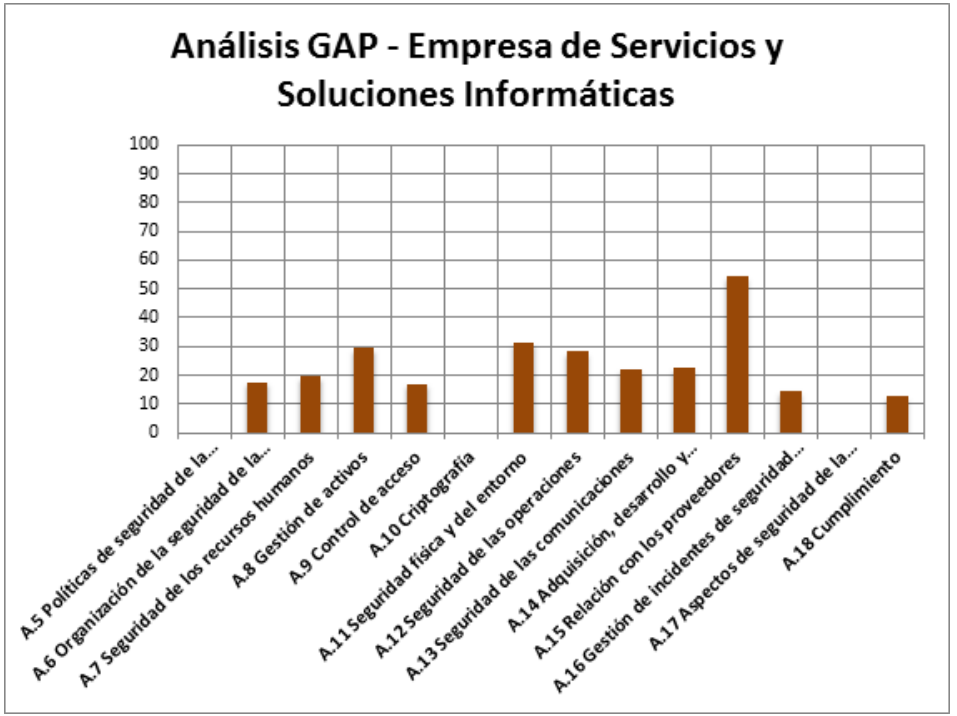
Resultados de análisis de las cláusulas de la ISO/IEC 27001

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Resultados del Análisis diferencial

La mayoría de los controles se encuentran en un nivel de madurez inexistente e inicial, lo que indica que no existe procesos fuertemente establecidos que permitan abordar los problemas o peligros de la seguridad de la información en las diferentes áreas de la empresa.

El control de Relación con los proveedores presenta un nivel de madurez repetible L2 siendo el único que contiene procedimientos más asertivos en relación a la seguridad y gestión de políticas, tratamientos y seguimientos de las relaciones y servicios prestados por los proveedores.



Resultados de análisis de los controles de la ISO/IEC 27002:2013

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

6. Documentación del SGSI

Para el cumplimiento normativo de la implementación del SGSI de la empresa se utilizó el siguiente formato adaptable a los siguientes documentos requeridos:

- Política de Seguridad.
- Procedimiento de Auditorías Internas.
- Gestión de Indicadores.
- Procedimiento Revisión por Dirección.
- Gestión de Roles y Responsabilidades.
- Metodología de Análisis de Riesgos.
- Declaración de Aplicabilidad.

EXPERTEC SERVICIOS Y SOLUCIONES INFORMÁTICAS	POLITICA, DOCUMENTO, PROCEDIMIENTO, ETC	Código: Versión: Fecha de aprobación: Página:

ESQUEMA
1. Introducción: definición de la pauta que se va a realizar
2. Objetivo: fin o propósito del documento
3. Alcance: a quien o quienes está dirigido el documento
4. Marco normativo y regulatorio: se indican las normas de guía o modelo en la construcción del documento.
5. Descripción: descripción del documento, política, metodología, procedimiento, etc.
6. Medios de divulgación: medios de comunicación por el cual se va a divulgar el documento

	Nombres y Apellidos	Cargo	Fecha	Firma
Elaborado				
Revisado				
Aprobado				

Algunos formatos de la documentación del SGSI

EXPERTEC	POLITICA DE SEGURIDAD	Código: DGSI-01
		Versión:1
		Fecha de aprobación: Marzo 2021
		Páginas:

ESQUEMA
1. Introducción En harás de mejorar la estrategia de Seguridad de la Información de la empresa EXPERTEC surge la necesidad de establecer una Política de Seguridad de la Información que permita buscar medidas adecuadas de protección de la información, precisando sus lineamientos, para garantizar el correcto control y reducir los riesgos asociados.
2. Objetivo Establecer la normatividad que permita preservar la información y los sistemas de la empresa, garantizando la integridad, confidencialidad y disponibilidad de la información y de los activos.
3. Alcance La política de seguridad está dirigida y aplicada a todas las áreas de la empresa, personal, proveedores y toda persona externa que tenga relación con los activos de la empresa.
4. Marco normativo y regulatorio Norma ISO/IEC 27001
5. Descripción Se han definido las siguiente políticas generales para dar cumplimiento por parte de todo el personal de la empresa: **5.1 Cumplimiento y sanciones** Todo el personal, contratista, colaborador y personal externo deben cumplir y acatar las políticas y procedimientos en cuestión de protección y seguridad de

EXPERTEC	GESTIÓN DE INDICADORES	Código: DGSI-03
		Versión:1
		Fecha de aprobación: Marzo 2021
		Páginas:

ESQUEMA
1. Introducción Es importante establecer indicadores que ayudan a medir la eficacia de los lineamientos definidos en el sistema de gestión de la seguridad, realizando un control con datos medidos de manera actualizada.
2. Objetivo Establecer los indicadores necesarios para la supervisión de los controles de seguridad.
3. Alcance Todas las áreas en las que se implemente por lo menos un control.
4. Marco normativo y regulatorio
5. Descripción La medición sistemática de los controles de seguridad y su temporalidad, permite tener una visión clara de la efectividad de los mismos. A continuación, se listan los componentes de cada indicador:

COMPONENTE	DESCRIPCIÓN
ID del indicador	Nomenclatura única definida por la empresa para identificar el indicador.
Nombre del indicador	Representa la medición que se va a realizar.
Descripción	Explicación del objetivo del indicador.
Control del seguridad	Control al cual se le realiza la medición.
Tipo	Efectiva, eficiencia o impacto.

EXPERTEC	ROLES Y RESPONSABILIDADES	Código: DGSI-05
		Versión:1
		Fecha de aprobación: Marzo 2021
		Páginas:

ESQUEMA
1. Introducción Dentro de la continuidad del negocio para obtener una certificación en la empresa es indispensable asignar y establecer los roles y responsabilidades al personal para poder cumplir con la correcta gestión de la seguridad de la información.
2. Objetivo Definir y establecer los roles y responsabilidades al personal de la empresa identificando las áreas de trabajo y las funciones asignadas.
3. Alcance Dirigido a todos los funcionarios de las áreas de la empresa incluyendo proveedores y asociados que intervienen en los procesos de la seguridad de la información y de los activos
4. Marco normativo y regulatorio Norma ISO/IEC 27001
5. Descripción A continuación se describen los roles y las responsabilidades de acuerdo al objetivo planteado y el alcance que se desea obtener: **5.1 Responsable de Seguridad** Es el encargado de planear, verificar, ejecutar y darle seguimiento a la implantación del SGSI. El rol es asumido por el responsable o Director de Tecnología o jefe de tecnología (CTO). Las responsabilidades de este rol son: • Ser parte de la elaboración, revisión y divulgación de las políticas, lineamientos, procedimientos y metodologías de la seguridad de la información de la empresa. • Gestionar, supervisar y evaluar el cumplimiento de las políticas

7. Análisis de riesgos

Para el análisis de riesgos se utilizó la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT V.3.0 con el propósito de orientar a la empresa en la gestión de los riesgos de seguridad (confidencialidad, integridad, disponibilidad)

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Inventario de activos

Los activos de la empresa se los clasificó según el ámbito, la cantidad y se estableció un factor de criticidad; el cual, se lo mide en una escala de alto, medio y bajo

Alto	El activo es altamente relevante para los procesos esenciales de la empresa y es indispensablemente disponible. La continuidad de la empresa se pone en peligro.
Medio	El activo es medianamente importante para los proceso de la empresa y su ausente disponibilidad retrasa algunos procesos. La continuidad de la empresa no se ve afectada
Bajo	El activo interviene en algunos procesos de la empresa que no están directamente relacionados con la empresa y su ausente disponibilidad causa algún contratiempo. La continuidad en ningún caso se ve afectada.

Factor de criticidad de activos

Inventario de activos de la empresa

Ámbito	Activo	Cantidad	Factor de criticidad *
CH	Servidores	4	Alto
	Equipos de sobremesa	5	Alto
	Laptops	4	Alto
	Smartphone	9	Medio
	Impresoras	2	Bajo
R	VLANs	4	Alto
	Puntos de acceso wifi	2	Medio
	Switch	2	Alto
	Router	2	Alto
P	Empleados	9	Medio
S	Entornos de producción	N/R	Alto
CS	Sistema Operativo Windows	9	Medio
	Software de servicio de correo	1	Alto
	Software de servicio web	1	Alto
	Software de servicio de aplicaciones	1	Alto
	Software de servicio de base de datos	1	Alto
	Software de servicio de archivos	1	Alto
	Software de servicio de DNS	1	Alto
	Software de entorno de desarrollo IDE	1	Alto
	Software de entorno marketing digital	1	Bajo
	Antivirus	9	Medio
	Herramientas Ofimáticas	9	Bajo
D	Información empresarial	13	Alto
	Información personal	9	Medio
	Contactos de clientes y proveedores	N/R	Alto
EA	Fibra óptica	1	Alto
	Sistema eléctrico	1	Alto
MEDIA	Dispositivos de almacenamiento externos	1	Medio

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Valoración de activos

La valoración de activos se estableció mediante la cuantificación de costos y se complementó con la dependencia de activos según el esquema que se indica.

Escala de valoración de activos

Categoría	Valoración	Rango de costos ($USD)
MB	Muy bajo	< $USD 500
B	Bajo	> $USD 500, <= $USD 3.000
M	Medio	> $USD 3.000, <= $USD 10.000
A	Alto	> $USD 10.000, <= $USD 55.000
MA	Muy alto	> $USD 55.000

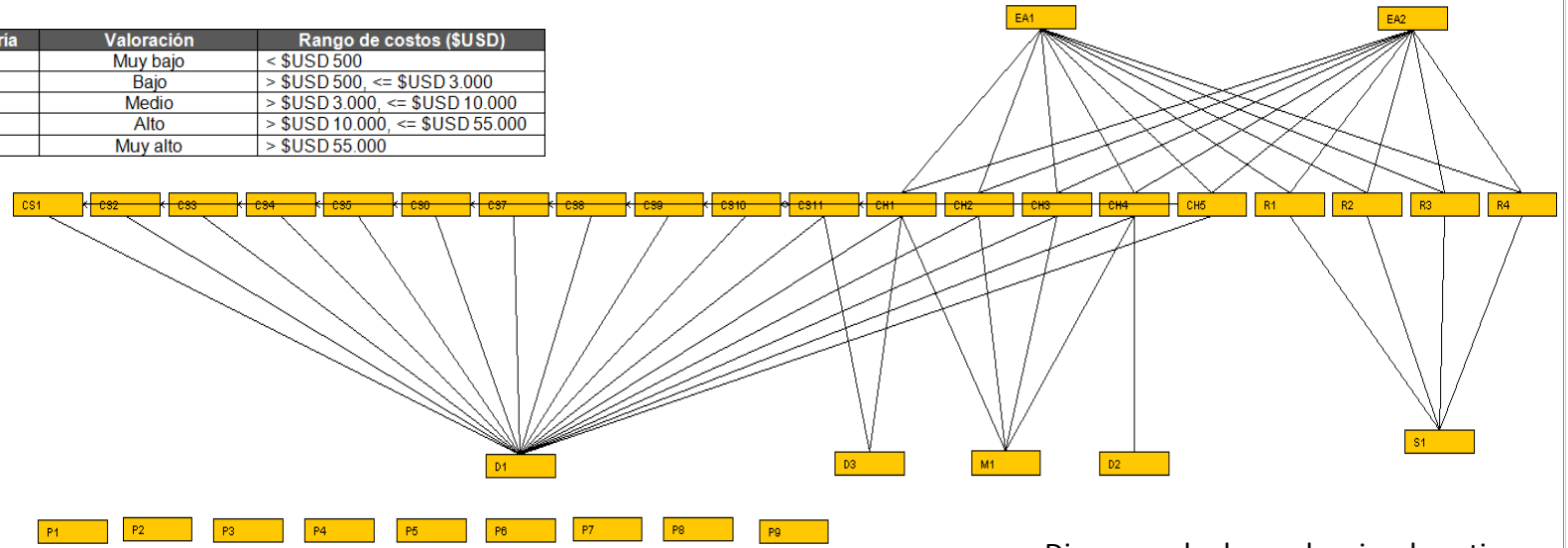


Diagrama de dependencias de activos

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Valoración de activos

Resultados de valoración de rangos de costos vs categoría de tipos de activos

Valoración	Categoría del tipo de activo
MB: Muy bajo	R, S, CS, MEDIA
B: Bajo	I, CH, CS, P, D, R, EA
M: Medio	CH, CS, R, S, D
A: Alto	P, D
MA: Muy alto	

Resultados:

Los resultados obtenidos por la valoración de activos indican que la mayoría se encuentran en los rangos de Muy bajo, Bajo y Medio, pertenecientes a los activos: Componentes Hardware y software, Red, Servicios y Datos. Los activos de Personal y Datos se encuentran en el rango de Alto y no existen activos en el rango de Muy alto.

Activo	Cantidad	Categoría de escalafón de valoración	Categoría de dependencias de activos
Servidores	4	M	R, S
Equipos de sobremesa	5	M	CH, CS
Laptops	4	M	CH, CS
Smartphones	9	B	CS, D, P
Impresoras	2	B	CH, CS, I
VLANs	4	M	R, EA
Puntos de acceso wifi	2	MB	R
Switch	2	MB	R
Router	1	MB	R
Director Ejecutivo (CEO)	1	M	P
Director de Finanzas (CFO)	1	B	P
Director de Tecnología (CTO)	1	B	P
Jefe de Redes Estructuradas y Servidores	1	B	P
Jefe de desarrollo de software	1	B	P
Jefe de soporte técnico	1	B	P
Director de Marketing (CMO)	1	B	P
Auxiliar o asistente administrativo	1	MB	P
Auxiliar de oficina	1	MB	P
Entornos de producción	1	MB	S

Valoración de activos según categoría de escalafón de costos y dependencias de activos

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

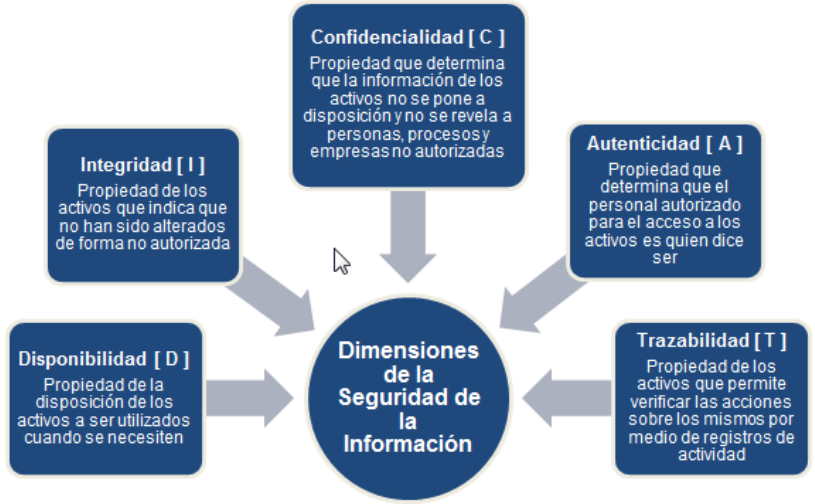
Dimensiones de seguridad

Teniendo en cuenta las cinco dimensiones se estableció una escala para realizar las valoraciones de criticidad teniendo en cuenta los siguientes criterios

Valoración	Criterio
10	Daño muy grave a la empresa
7-9	Daño grave a la empresa
4-6	Daño importante a la empresa
1-3	Daño menor a la empresa
0	Irrelevante para la empresa

Los activos se valoran de acuerdo a su grado de importancia según los siguientes criterios

Valoración de grado de Importancia	Criterio
MA	Muy alta
A	Alta
M	Media
B	Baja
D	Despreciable



EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Resumen de valoración

Este resumen permitió realizar un análisis de la valoración de los activos según el grado de importancia de los mismos como las valoraciones de los aspectos críticos de las dimensiones de la seguridad que afectaría a los activos de la empresa. Además, permitió generar acciones sobre los activos que tengan un valor alto y muy alto puesto que generan un daño grave y muy grave en el funcionamiento de la empresa.

Ámbito	Activo	Valor	Aspectos críticos				
			A	C	I	D	T
CH	Servidores	A	9	8	10	10	8
CH	Equipos de sobremesa	A	8	8	7	8	7
CH	Laptops	A	8	8	7	8	7
CH	Smartphones	M	6	5	5	6	5
CH	Impresoras	D	0	0	0	1	0
R	VLANs	MA	10	10	9	10	5
R	Puntos de acceso wifi	A	7	8	7	8	3
R	Switch	A	7	7	8	8	3
R	Router	A	9	9	9	10	3
P	Director Ejecutivo (CEO)	MA	10	10	9	7	3
P	Director de Finanzas (CFO)	MA	10	10	9	8	5
P	Director de Tecnología (CTO)	MA	10	10	9	10	5
P	Jefe de Redes Estructuradas y Servidores	A	9	9	9	9	6
P	Jefe de desarrollo de software	A	8	8	8	7	5
P	Jefe de soporte técnico	M	7	6	7	7	4
P	Director de Marketing (CMO)	M	6	7	5	5	2
P	Auxiliar o asistente administrativo	M	5	6	5	7	3
P	Auxiliar de oficina	B	4	4	3	4	1
S	Entornos de producción	A	7	7	8	8	4
CS	Sistema Operativo Windows	M	4	6	5	5	0
CS	Software de servicio web	A	7	7	9	10	6
CS	Software de servicio de aplicaciones	A	7	8	9	9	7
CS	Software de servicio de base de datos	A	7	9	9	9	6
CS	Software de servicio de archivos	M	7	6	7	7	4
CS	Software de servicio de DNS	M	5	4	5	6	2
CS	Software de entorno de desarrollo IDE	M	6	7	7	6	5
CS	Software de entorno marketing digital	B	4	3	3	4	3
CS	Antivirus	M	4	6	7	8	1
CS	Herramientas Ofimáticas	D	0	0	0	2	0
D	Información empresarial	MA	9	10	10	10	6
D	Información personal	B	0	2	0	0	0
D	Contactos de clientes y proveedores	M	6	9	9	8	3
EA	Fibra óptica	A	8	6	7	9	4
EA	Sistema eléctrico	MA	3	4	8	10	4
MEDIA	Dispositivos de almacenamiento externos	A	7	8	9	9	4

Valoración de activos

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Análisis de amenazas

Teniendo en cuenta el tipo de amenaza establecido en MAGERIT, se realizó una tabla resumen en donde se establecen los activos afectados, la escala de frecuencia con la que se produce una amenaza y el impacto de la amenaza en las dimensiones de la seguridad en escala de porcentajes.

Resultados:

Como resultados se tiene lo siguiente:

- Los desastres naturales (N): el impacto se ve afectado en la disponibilidad en un 70%
- Las amenazas de origen industrial (I): el impacto se ve afectado en la integridad y la disponibilidad oscilando entre el 60% y 80%

Amenazas en los activos y las Dimensiones de la seguridad

Tipo de Amenaza: N – Desastres Naturales							
Amenaza	Activos afectados	F*	Impacto de la amenaza (%)				
			A	C	I	D	T
[N.1] Fuego	CH1-CH5, R1-R4, M1, EA1,EA2					70%	
[N.2] Daños por agua	CH1-CH5, R1-R4, M1, EA1,EA2					70%	
[N.*] Desastres naturales	CH1-CH5, R1-R4, M1, EA1,EA2					70%	
Tipo de Amenaza: I – Origen Industrial							
Amenaza	Activos afectados	F*	Impacto de la amenaza (%)				
			A	C	I	D	T
[I.1] Fuego	CH1-CH5, R1-R4, M1, EA1,EA2	2				70%	
[I.2] Daños por agua	CH1-CH5, R1-R4, M1, EA1,EA2	2				70%	
[I.*] Desastres industriales	CH1-CH5, R1-R4, M1, EA1,EA2	1				70%	
[I.3] Contaminación mecánica	CH1-CH5, R1-R4, M1, EA1,EA2	3				80%	
[I.4] Contaminación electromagnética	CH1-CH5, R1-R4, M1, EA1,EA2	1				70%	
[I.5] Avería de origen físico o lógico	CH1-CH5, CS1-CS11, M1, EA1	4			60%	70%	
[I.6] Corte del suministro eléctrico	CH1-CH5, R1-R4, M1, EA1,EA2	2				80%	

Análisis de amenazas

Resultados:

- Los errores y fallos no intencionados: el impacto se ve afectado en la confidencialidad, integridad, disponibilidad y trazabilidad oscilando entre el 40% y 80%
- Los ataques intencionados: el impacto se ve afectado en la autenticidad, la confidencialidad, integridad, disponibilidad y trazabilidad oscilando entre el 40% y 100%

Amenazas en los activos y las Dimensiones de la seguridad

Tipo de Amenaza: E – Errores y fallos no intencionados							
Amenaza	Activos afectados	F*	Impacto de la amenaza (%)				
			A	C	I	D	T
[E.1] Errores de los usuarios	D1-D3, S1, CS1-CS11, M1	5		60%	60%	60%	
[E.2] Errores del administrador	CH1-CH5, CS1-CS11, D1-D3, R1-R4, S1, M1	3		70%	70%	70%	
[E.3] Errores de monitorización (log)	D1	2			40%		40%
[E.4] Errores de configuración	D1	3			70%		
Tipo de Amenaza: A – Ataques intencionados							
Amenaza	Activos afectados	F*	Impacto de la amenaza (%)				
			A	C	I	D	T
[A.3] Manipulación de los registros de actividad (log)	D1	3			50%		60%
[A.4] Manipulación de la configuración	D1	3		50%	60%	60%	
[A.5] Suplantación de la identidad del usuario	D1-D3, S1, CS1-CS11, R1-R4	4	100 %	100 %	100 %		
[A.6] Abuso de privilegios de acceso	D1-D3, S1, CS1-CS11, R1-R4	2		60%	70%	70%	
[A.7] Uso no previsto	CH1-CH5, CS1-CS11, EA1-EA2, R1-R4, S1, M1	2		40%	60%	60%	
[A.8] Difusión de software dañino	CS1-CS11	3		60%	80%	80%	
[A.9] [Re-]encaminamiento de mensajes	S1, CS1-CS11, R1-R4	2		40%			

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Impacto potencial

El impacto potencial permite medir el daño sobre el activo derivado de la materialización de una amenaza.

Para poder medir el impacto se utilizó una escala de niveles de impacto y una fórmula cuyo resultado se determina de la valoración de activos por el porcentaje de impacto de amenaza

Escala de niveles de impacto

Impacto	Rango del Impacto en %	Rango del Impacto en decimal	Rango del Impacto en valores	Valor
N: Nulo	0%	0	0	**0**
MB: Muy Bajo	>0%,<=10%	>0,<=0,1	>0,<=1	**1**
B: Bajo	>10%,<=20%	>0,1,<=0,2	>1,<=2	**2**
M: Medio	>20%,<=50%	>0,2,<=0,5	>2,<=5	**3**
A: Alto	>50%,<=80%	>0,5,<=0,8	>5,<=8	**4**
MA: Muy alto	>80%,<=100%	>0,8,<=1,0	>8,<=10	**5**

Fórmula

Impacto potencial = Valoración de activos X Porcentaje de impacto de amenaza

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Impacto potencial

Para establecer el impacto potencial en la tabla de cálculo y registro del impacto potencial se obtiene el rango del impacto en valores y se puede determinar el nivel de impacto (Nulo, Muy Bajo, Bajo, Medio, Alto, Muy alto) para los activos de la empresa.

Activo	Valoración de activos					Impacto de amenaza* (% / 100)					Impacto Potencial en valores				
	A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
Servidores	9	8	10	10	8	0	1,0	1,0	1,0	0	0	8	10	10	0
Equipos de sobremesa	8	8	7	8	7	0	0,8	0,8	0,8	0	0	6,4	5,6	6,4	0
Laptops	8	8	7	8	7	0	0,8	0,8	0,8	0	0	6,4	5,6	6,4	0
Smartphones	6	5	5	6	5	0	0,8	0,8	0,8	0	0	4	4	4,8	0
Impresoras	0	0	0	1	0	0	0,5	0,5	0,5	0	0	0	0	0,5	0
VLANs	10	10	9	10	5	1,0	1,0	1,0	1,0	0	10	10	9	10	0
Puntos de acceso wifi	7	8	7	8	3	0	0,7	0,7	0,7	0	0	5,6	4,9	5,6	0
Switch	7	7	8	8	3	0	0,7	0,7	0,7	0	0	4,9	5,6	5,6	0
Router	9	9	9	10	3	0	0,8	0,8	0,8	0	0	7,2	7,2	8	0
Director Ejecutivo (CEO)	10	10	9	7	3	0	1,0	0,8	0,8	0	0	6,4	7,2	5,6	0
Director de Finanzas (CFO)	10	10	9	8	5	0	0,8	0,8	0,8	0	0	8	7,2	6,4	0
Director de Tecnología (CTO)	10	10	9	10	5	0	0,8	0,8	1,0	0	0	8	7,2	10	0
Jefe de Redes Estructuradas y Servidores	9	9	9	9	6	0	0,7	0,7	0,7	0	0	6,3	6,3	6,3	0
Jefe de desarrollo de software	8	8	8	7	5	0	0,6	0,7	0,7	0	0	4,8	5,6	4,9	0
Jefe de soporte técnico	7	6	7	7	4	0	0,5	0,5	0,5	0	0	3	3,5	3,5	0
Director de Marketing (CMO)	6	7	5	5	2	0	0,5	0,5	0,5	0	0	3,5	2,5	2,5	0
Auxiliar o asistente administrativo	5	6	5	7	3	0	0,4	0,4	0,4	0	0	2,4	2	2,8	0

Cálculo y registro del Impacto Potencial

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Nivel de riesgo aceptable y residual

Para establecer el nivel de riesgo aceptable y residual se realizó un análisis teniendo en cuenta la frecuencia de ocurrencia en cada uno de los activos para realizar la valoración del riesgo.

Además, se estableció los niveles de riesgo a partir de un rango de valoración de riesgo, en donde, se define un umbral para los valores mayores a seis (>6) en los niveles Alto y Muy Alto; que conlleva a implementar controles que permitan reducir los niveles de riesgo en los activos identificados.

Fórmula

Valoración de riesgo = Valor de frecuencia de ocurrencia X Valor del Impacto Potencial

Frecuencia de ocurrencia

Valor	frecuencia de ocurrencia	Niveles de frecuencia de ocurrencia
0,01	Varios años	**MB:** Muy Bajo
0,1	Más de 2 años	**B:** Bajo
1	Anual	**N:** Normal
10	Mensual	**A:** Alto
100	Diaria	**MA:** Muy Alto

Niveles de riesgo

Niveles	Rango de valoración de riesgo
MB: Muy Bajo	>0,<=1
B: Bajo	>1,<=3
M: Medio	>3,<=6
A: Alto	>6,<=8
MA: Muy Alto	>8,<=10

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Nivel de riesgo aceptable y residual

Resultados

Como resultados según el análisis, de los 36 activos establecidos en la empresa; 19 se identificaron en los niveles Alto y Muy Alto por encima del umbral del riesgo afectando las dimensiones de seguridad (Confidencialidad, Integridad y Disponibilidad) mayormente; 11 se identificaron en el nivel Medio; y 6 se identificaron en los niveles Bajo y Muy Bajo. Cabe resaltar, que en algunos activos se ven afectados algunas dimensiones de la seguridad más que otras, por lo tanto los valores resultantes varían según su análisis.

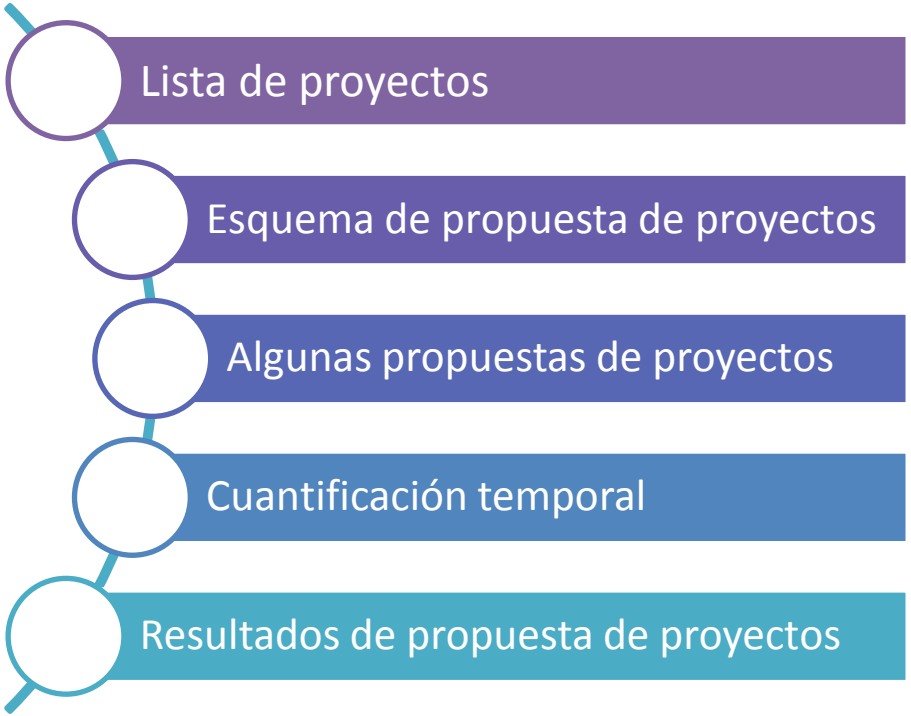
Valoración de riesgo según la frecuencia de ocurrencia y el impacto potencial

Activo	Frecuencia de ocurrencia (valor)	Impacto Potencial en valores					Valoración de riesgo				
		A	C	I	D	T	A	C	I	D	T
Servidores	1	0	8	10	10	0	0	8	10	10	0
Equipos de sobremesa	1	0	6,4	5,6	6,4	0	0	6,4	5,6	6,4	0
Laptops	1	0	6,4	5,6	6,4	0	0	6,4	5,6	6,4	0
Smartphones	1	0	4	4	4,8	0	0	4	4	4,8	0
Impresoras	1	0	0	0	0,5	0	0	0	0	0,5	0
VLANs	1	10	10	9	10	0	10	10	9	10	0
Puntos de acceso wifi	1	0	5,6	4,9	5,6	0	0	5,6	4,9	5,6	0
Switch	1	0	4,9	5,6	5,6	0	0	4,9	5,6	5,6	0
Router	1	0	7,2	7,2	8	0	0	7,2	7,2	8	0
Director Ejecutivo (CEO)	1	0	6,4	7,2	5,6	0	0	6,4	7,2	5,6	0

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

8. Propuesta de proyectos

En esta etapa se identificaron los proyectos para implementar en el SGSI en el marco del mejoramiento de los controles de seguridad y para reducir o mitigar los niveles de riesgos encontrados en la etapa de análisis de riesgos.



EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Lista de proyectos

Se listan los nombres de los proyectos que se tuvieron en cuenta para la propuesta:

P001 - Política de seguridad de la Información.
P002 - Gestión de redes y comunicaciones.
P003 - Seguridad y mantenimiento de los equipos y recursos.
P004 - Organización y formación al personal en seguridad de la información.
P005 - Implementación de un CPD auxiliar para soporte de servidores y servicios.
P006 - Organización y clasificación de la información.
P007 - Mejoramiento en los sistemas de gestión de usuarios.

Esquema de propuesta de proyectos

Se estableció un esquema general para identificar cada propuesta de proyecto

- **Nombre del Proyecto**
- **Código**
- **Objetivos de mejora**
- **Justificación**
- **Controles Identificados**
- **Activos afectados**
- **Puntos de control o medidores**
- **Responsable de ejecución del proyecto**
- **Presupuesto**
- **Plazos de consecución y fecha límite de cumplimiento**

Propuesta de proyectos para la implementación en el SGSI

Nombre del Proyecto:	Política de seguridad de la Información	**Código:**	P001
Objetivos de mejora:	• Definir y establecer la política de seguridad de la información en la empresa.		
Justificación:	Como propuesta inicial se debe elaborar la política de seguridad que permita orientar y servir de apoyo en la seguridad de la información de acuerdo con los propósitos de la empresa. Las políticas deben revisarse periódicamente (1 o 2 veces) cada año y se deben establecer en todos los niveles de la empresa.		
Controles Identificados:		**Activos afectados:**	
A.5.1.1 Políticas para la seguridad de la información A.5.1.2 Revisión de las políticas para la seguridad de la información		CH1-CH5, CS1-CS11, P1-P9, R1-R4, S1, D1-D3, EA1-EA2, M1	
Puntos de control o medidores:	• Documentos sobre la política de seguridad de la información aprobada por las directivas y el comité de seguridad. • Revisión de documentación de la política de seguridad. • Comunicación y publicación de la política de seguridad al personal de la empresa.		
Responsable de ejecución del proyecto:	Director de Tecnología (CTO)		
Presupuesto:	El presupuesto se plantea por jornadas laborales de 8 horas diarias de lunes a viernes. • Horas de trabajo semanal: 40 horas • Total horas por los 2 meses: 320 horas • Costo hora: $USD 8.28 • Costo Total por los 2 meses: $USD 2,649		
Plazos de consecución y fecha límite de cumplimiento:	El cumplimiento de los objetivos debe realizarse a corto plazo; por lo tanto, se establece un tiempo de 2 meses para su realización.		

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Algunas propuestas de proyectos

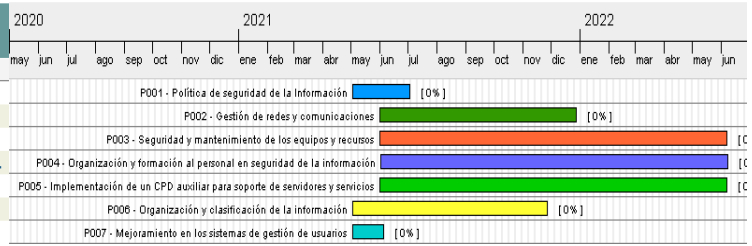
Nombre del Proyecto:	Gestión de redes y comunicaciones	**Código:**	P002
Objetivos de mejora:	• Aplicar controles para establecer las reglas de acceso de la información en las redes y servicios de la empresa. • Mejorar el uso y control de las redes de datos para garantizar la confidencialidad, integridad y disponibilidad en los servicios y recursos.		
Justificación:	El asegurar la protección de los recursos y servicios de la infraestructura de red y de comunicaciones de la empresa permite garantizar el intercambio de información interna y externa de forma más confiable y segura. Por lo tanto, se hace necesario establecer controles, monitoreo o seguimientos, asegurar servicios y definir acuerdos y políticas para el intercambio de información en las redes. Así mismo, se requiere realizar actualizaciones en los sistemas de información comprendidos en la red con el objetivo de optimizar los recursos y servicios dependiendo del crecimiento en la misma.		
Controles Identificados:		**Activos afectados:**	
A.9.1.2 Acceso a redes y a servicios en red A.13.1 Gestión de la seguridad de las redes A.13.2 Transferencia de información		CH1, CH2, CH3, R1-R4, S1	
Puntos de control o medidores:	• Verificación de la aplicación de los controles y de la optimización en el uso y gestión de las redes. • Monitoreo y registro de los estados de las redes, recursos y dispositivos que conforman la infraestructura de la redes dentro de la empresa. • Reportes generados del monitoreo y diagnóstico realizado a la infraestructura de red y los servicios.		
Responsable de ejecución del proyecto:	Jefe de Redes y Servidores.		
Presupuesto:	Para esta propuesta se tiene un presupuesto de $USD 3.000		
Plazos de consecución y fecha límite de cumplimiento:	Para la realización de la propuesta se tiene estipulado un periodo de mediano plazo de 6 meses para su ejecución.		

Nombre del Proyecto:	Implementación de un CPD auxiliar para soporte de servidores y servicios	**Código:**	P005
Objetivos de mejora:	• Implementar un centro de procesamiento de datos CPD auxiliar con el fin de brindar apoyo y soporte a los servidores principales en caso de que fallen por cualquier incidente presentado. • Dar continuidad al funcionamiento de los servicios y software instalados en los servidores principales.		
Justificación:	El centro de procesamiento de datos en la empresa se describe como el espacio físico donde se hospeda el equipo tecnológico y permite crear, procesar, almacenar y transferir la información de los servicios que ofrece la empresa; por ende, es de vital importancia generar las medidas de seguridad en el CPD e implementar métodos y técnicas alternativas que permitan salvaguardar la información y darle continuidad a todos los procesos que son indispensables para la empresa.		
Controles Identificados:		**Activos afectados:**	
A.12.3 Copias de seguridad A.12.5.1 Instalación de software en sistemas operativos A.12.6.1 Gestión de las vulnerabilidades técnicas A.13.1.2 Seguridad de los servicios de red A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas A.16.1 Gestión de incidentes y mejoras en la seguridad de la información A.17.1 Continuidad de Seguridad de la información		CH1, CS2-CS7, R1-R4, EA1, EA2	
Puntos de control o medidores:	• Instalación del CPD alterno (servidores, redes, infraestructura y software) • Configuraciones y registros del CPD alterno que sirva de respaldo de los servicios que brinda a la empresa y a los clientes. • Registros de las copias de seguridad realizadas a los servidores principales y actualizados en los servidores alternos del CPD. • Documentos donde se establecen los conductos y lineamientos para la gestión y control de redes y servicios de la empresa.		

Cuantificación temporal

Planificación de cada proyecto en términos de tiempo y/o fechas para la ejecución de cada uno esquematizado en el siguiente diagrama de Gantt:

Nombre	Fecha de ini...	Fecha de fin	Recursos
P001 - Política de seguridad de la Información	3/05/21	2/07/21	Director Ejecutivo (CEO),Director de Tecnología (CTO)
P002 - Gestión de redes y comunicaciones	1/06/21	27/12/21	Jefe de Redes y Servidores,Director de Tecnología (CTO)
P003 - Seguridad y mantenimiento de los equi...	1/06/21	6/06/22	Jefe de Soporte Técnico,Director de Tecnología (CTO)
P004 - Organización y formación al personal en...	2/06/21	7/06/22	Director de Tecnología (CTO),Jefe de Redes y Servidore...
P005 - Implementación de un CPD auxiliar par...	1/06/21	6/06/22	Director de Tecnología (CTO),Jefe de Redes y Servidores
P006 - Organización y clasificación de la inform...	3/05/21	26/11/21	Director de Tecnología (CTO),Director Ejecutivo (CEO)
P007 - Mejoramiento en los sistemas de gestió...	3/05/21	4/06/21	Jefe de Redes y Servidores,Director de Tecnología (CTO)

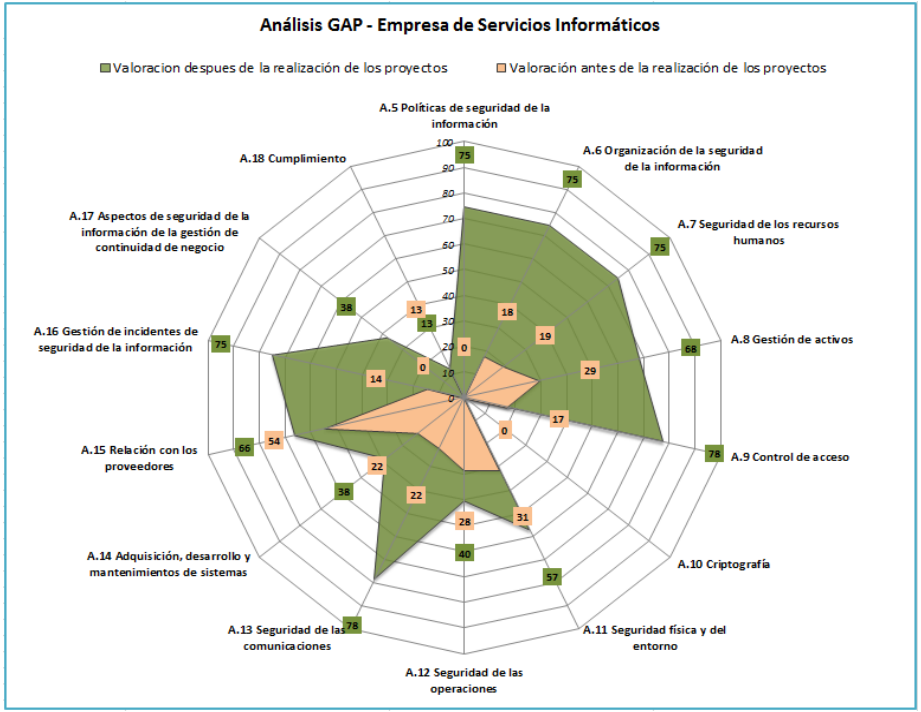


Resultados de propuesta de proyectos

Se realizó el análisis GAP de los controles (dominios y subdominios) de la ISO/IEC 27002 indicando la evolución en los controles identificados en cada proyecto.

En el diagrama se puede notar la evolución y/o crecimiento que tuvieron los dominios una vez se implementan cada uno de los proyectos. El avance se ha presentado en casi la mayoría de dominios o controles reflejando un crecimiento superior en un rango del 78 % aproximadamente con respecto al análisis diferencial inicial de la empresa.

Análisis GAP de la valoración después de la realización de los proyectos vs análisis GAP de la valoración antes de la realización de los proyectos



EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

9. Auditoría de cumplimiento

En esta etapa se tuvo en cuenta los requisitos para la elección del auditor interno y se establecieron los controles y los objetivos de control según el dominio que los contiene organizados en un periodo de 3 años.

Primer año	Segundo año	Tercer año
A.5 Políticas de seguridad de la información. A.6 Organización de la seguridad de la información. A.7 Seguridad de los recursos humanos. A.8 Gestión de activos. A.9 Control de acceso.	A.10 Criptografía. A.11 Seguridad física y del entorno. A.12 Seguridad de las operaciones. A.13 Seguridad de las comunicaciones. A.14 Adquisición, desarrollo y mantenimiento de los sistemas.	A.15 Relación con los proveedores. A.16 Gestión de incidentes de seguridad de la información. A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio. A.18 Cumplimiento.

Etapas de Auditoría de cumplimiento

Para dar cumplimiento a los procesos de auditoria se establecieron las siguientes etapas para su realización

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Evaluación de la madurez

Para la realización de la evaluación de la Madurez en el proceso de auditoría se empleó la tabla del Modelo de la Capacidad de Madurez.

Resumen modelo de capacidad de madurez CMM

Nivel	Estado	Valoración en porcentajes
L0	Inexistente	0%
L1	Inicial	25%
L2	Repetible	50%
L3	Establecido	75%
L4	Administrado	95%
L5	Mejorado	100%

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Evaluación de la madurez

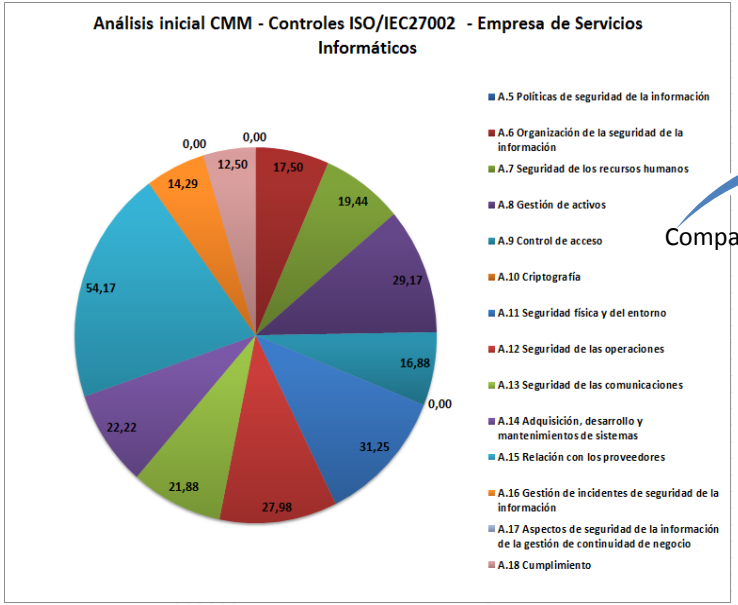
Se evaluó cada uno de los 114 controles del estándar ISO/IEC 27002 teniendo en cuenta el modelo de capacidad de madurez planteado en el inicio del proyecto para la realización del análisis diferencial.

PRIMER AÑO		
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.5 Políticas de seguridad de la información	**L3**	**75%**
5.1 Directrices de gestión de la seguridad de la información		*75%*
A.5.1.1 Políticas para la seguridad de la información		75%
A.5.1.2 Revisión de las políticas para la seguridad de la información		75%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.6 Organización de la seguridad de la información	**L3**	**75%**
A.6.1 Organización interna		75%
A.6.1.1 Roles y responsabilidades para la seguridad de la información		75%
A.6.1.2 Separación de deberes		75%
A.6.1.3 Contacto con las autoridades		75%
A.6.1.4 Contacto con grupos de interés especial		75%
A.6.1.5 Seguridad de la información en la gestión de proyectos.		75%
A.6.2 Dispositivos móviles y teletrabajo		*75%*
A.6.2.1 Política para dispositivos móviles		75%
A.6.2.2 Teletrabajo		75%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.7 Seguridad de los recursos humanos	**L3**	**75%**
A.7.1 Antes de asumir el empleo		*75%*
A.7.1.1 Selección		75%
A.7.1.2 Términos y condiciones del empleo		75%
A.7.2 Durante la ejecución del empleo		*75%*
A.7.2.1 Responsabilidades de la dirección		75%
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.		75%
A.7.2.3 Proceso disciplinario		75%
A.7.3 Terminación y cambio de empleo		*75%*
A.7.3.1 Terminación o cambio de responsabilidades de empleo		75%

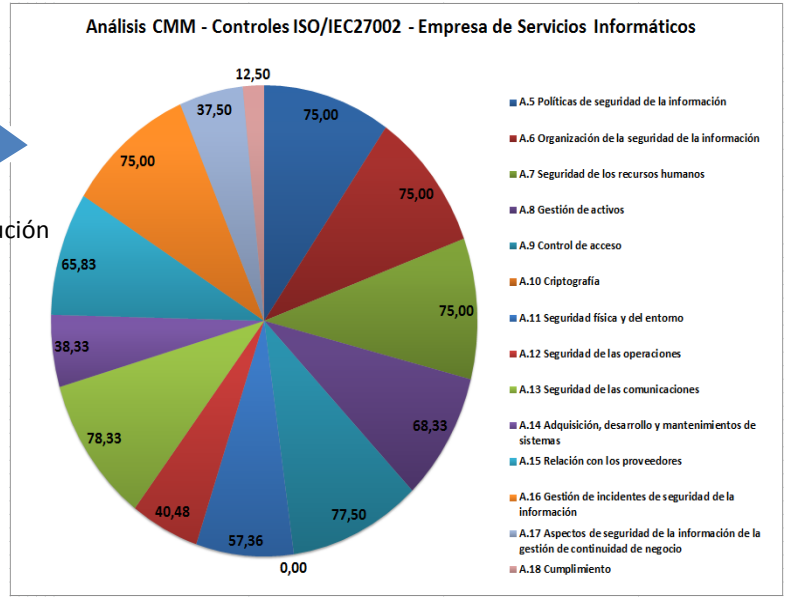
Análisis del proceso de auditoría de los controles de la ISO/IEC 27002 utilizando el CMM

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Resultados de auditoría



Comparación y evolución



Gráfica de **análisis inicial** de los controles de la ISO/IEC 27002 utilizando el CMM

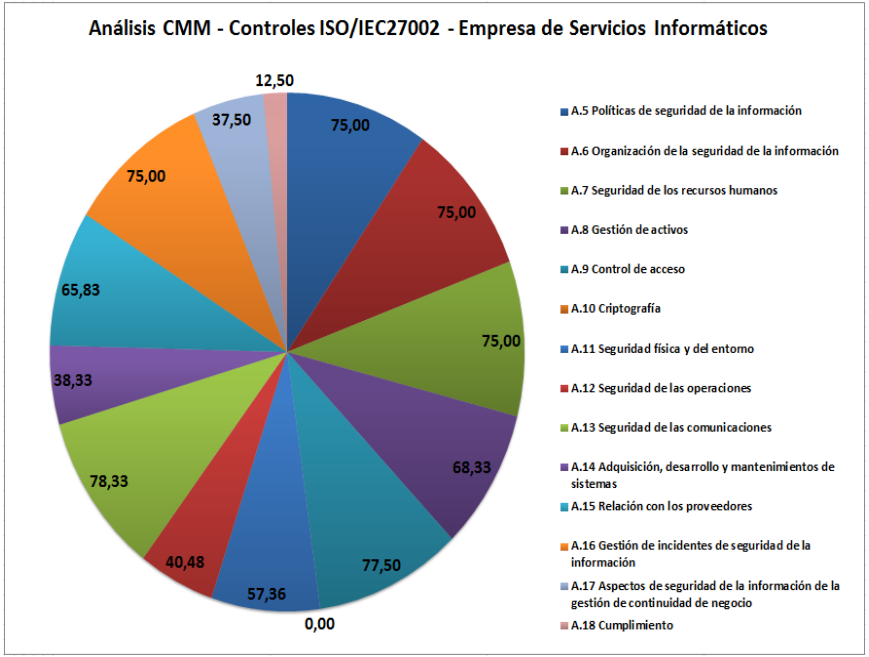
Gráfica de **análisis posterior** de los controles de la ISO/IEC 27002 utilizando el CMM

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Resultados de auditoría

Resultados

Existe una variación significativa de la mayoría de los controles a su análisis inicial. Los controles A5 Políticas de seguridad de la información, A6 Organización de la seguridad de la información, A7 Seguridad de los recursos humanos, A9 Control de acceso, A13 Seguridad de las comunicaciones, A16 Gestión de incidentes de seguridad de la información; tuvieron una mejora en 75% teniendo un nivel dentro del CMM del L3.



Gráfica de **análisis posterior** de los controles de la ISO/IEC 27002 utilizando el CMM

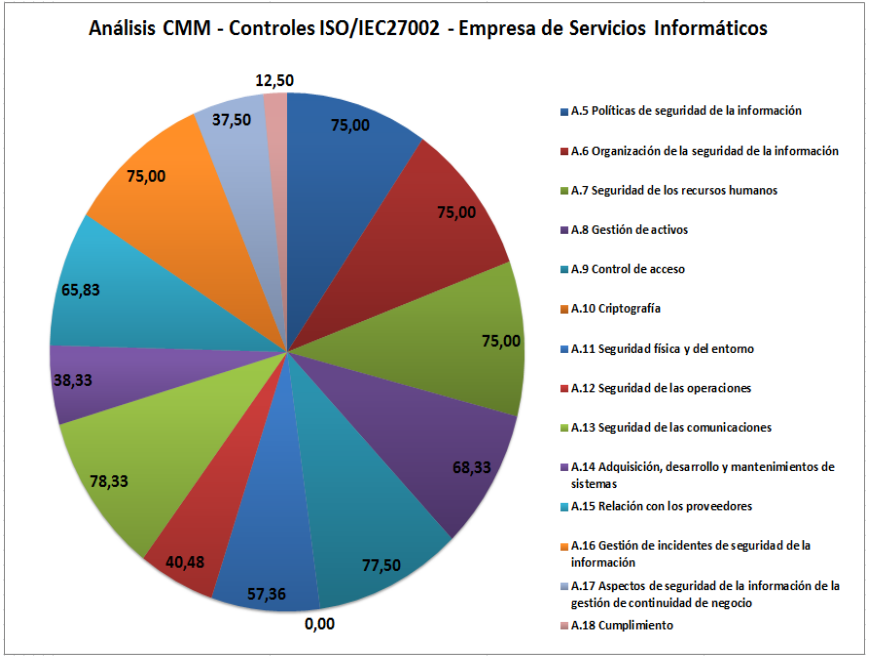
EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Resultados de auditoría

Resultados

Otros controles mejoraron entre un 25% y un 50%; como es el caso de los controles A8 Gestión de activos, A11 Seguridad física y del entorno, A17 Aspectos de seguridad de la información de la gestión de continuidad de negocio. Por último, los controles A10 Criptografía y A18 Cumplimiento, se mantuvieron y no presentaron mejorías.

Aunque los controles han tenido una mejora apreciable, es importante indicar que factores como la evolución de la tecnología y los procesos implementados en la empresa pueden determinar el surgimiento de nuevos inconvenientes que afectarían los resultados tratados, lo cual permitirá realizar nuevos análisis sobre los controles afectados.



Gráfica de **análisis posterior** de los controles de la ISO/IEC 27002 utilizando el CMM

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

Informe de auditoría

El informe de auditoría tendrá la siguiente información:

- Fecha de elaboración del informe
- Área auditada
- Responsable del área auditada
- Cargo del responsable del área auditada
- Email del responsable del área auditada
- Objetivo de la auditoría
- Alcance de la auditoría
- Fechas de la auditoría
- Total, días de duración de la auditoría
- Integrantes del equipo auditor
- Email de los integrantes del equipo auditor
- Actividades realizadas en la auditoría
    - Criterios para el muestreo
    - Actividades principales
    - Observaciones de la evaluación
    - Observaciones de la evaluación de requisitos de la especificación técnica, proceso o servicio.
- Observaciones
- Recomendaciones
- Nombre del auditor asignado al área auditada, cargo del auditor, firma del auditor.

EXPERTEC
SERVICIOS Y SOLUCIONES INFORMÁTICAS

10. Conclusiones

Para lograr cumplir con los objetivos planteados del Plan Director se han determinado las siguientes etapas dentro de la empresa resaltando de forma concluyente los resultados y las acciones realizadas en cada una de ellas:

- Se realizó en primera instancia un análisis DAFO complementado con una estrategia CAME con el propósito de contextualizar y entender la situación actual de la empresa en cuanto al ámbito de seguridad de la información se refiere.
- Posteriormente se realizó un análisis diferencial de la empresa teniendo en cuenta los estándares de la ISO/IEC 27001 y los controles de la norma ISO/IEC 27002 con el objetivo de evaluar las cláusulas de la ISO 27001 y los controles de la ISO 27002 utilizando como referencia y valoraciones el modelo de capacidad de madurez el cual arrojo los resultados de medición de cumplimiento de los estándares en la empresa.
- Además se establecieron los documentos obligatorios para el cumplimiento normativo de la implementación del SGSI, los cuales, se generaron unos formatos para la estructuración y organización de los documentos que permitieron alinear los parámetros y estrategias para la gestión de la seguridad de la información.

Conclusiones

- Se aplicó la metodología de Análisis y Riesgos de los Sistemas de Información MAGERIT para direccionar a la empresa en la gestión de riesgos realizando las siguientes actividades: inventario de activos de la empresa, valoración de los activos, valoración de las dimensiones de la seguridad de la información, análisis de amenazas presentes en los activos de la empresa, impacto potencial a materializarse una amenaza en los activos y valoración del nivel de riesgo potencial y residual según la frecuencia de ocurrencia y el impacto potencial. Las anteriores actividades permitieron identificar y analizar los activos que se encuentran en riesgo según los niveles establecidos y que afectan las dimensiones de la seguridad.
- Paso siguiente fue la propuesta de diferentes proyectos que permitieron realizar mejoras en los controles y reducir o mitigar los riesgos identificados en la etapa de análisis y riesgos. En la presentación de los proyectos se utilizó un esquema que abarco los puntos descriptivos de los proyectos con sus características relevantes para su planeación e implementación. De igual manera, se realizó un análisis y comparación GAP en donde se identificó la evolución referente al estado inicial de los controles del estándar ISO/IEC 27002 con respecto a la aplicación de las propuestas de los proyectos.
- Por último, se implementó un proceso de auditoría para estipular el nivel de capacidad de madurez en la que se encuentra el SGSI de la empresa. En este proceso se utilizó el CMM realizado en la primera etapa para realizar un diagnóstico acerca del avance que se obtuvo del análisis realizado inicialmente con respecto al análisis posterior.

Conclusiones

Mediante la implementación del plan director del SGSI se ha logrado establecer niveles de protección de los activos y recursos que se identificaron esenciales y prioritarios en la empresa; tales como la infraestructura de redes, servidores, equipos de cómputo, los elementos de soporte técnico, software utilizado, sistemas de información y servicios implementados.

Se ha logrado mitigar amenazas y vulnerabilidades que afectan los activos, recursos y procesos mediante la implementación del Plan Director del SGSI y los lineamientos, estrategias, documentos y normativas que se han establecido en los análisis y resultados de las etapas mencionadas anteriormente.

En definitiva, la implementación del Plan Director del SGSI ha logrado cumplir con los objetivos planteados para la gestión de riesgos en la empresa EXPERTEC consiguiendo aplicar los controles necesarios para la mitigación y reducción de los riesgos referentes a la seguridad de la información. No obstante, es importante aclarar que se deben mejorar tanto los controles priorizados como los controles que aún no se han logrado superar para obtener de esta forma que la empresa cumpla con los estándares necesarios y darle una calidad en la continuidad del negocio.

Agradecimientos

A todos los docentes, administrativos y compañeros de estudio de la Universitat Oberta de Catalunya que hicieron posible la realización del Master y su colaboración para que todo sea posible.