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

Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013 para la unidad de GST

Autor: María Fernanda Chaparro Ronderos

Director: Antonio José Segovia Henares

Junio de 2016

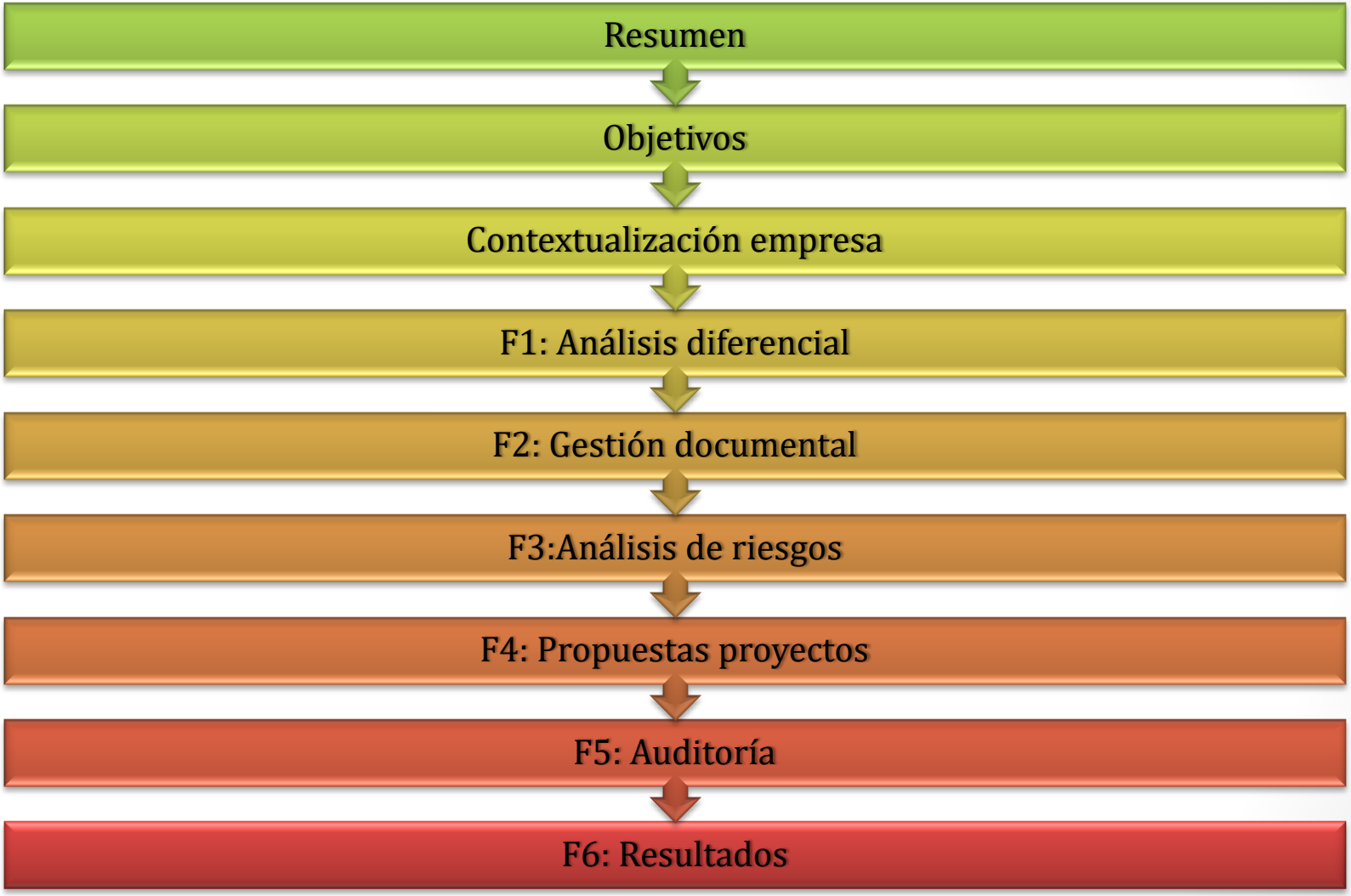
UOC Universitat Oberta de Catalunya www.uoc.edu

UAB Universitat Autònoma de Barcelona

Universitat Rovira i Virgili

UIB Universitat de les Illes Balears

Agenda



María Fernanda Chaparro Junio de 2016

Resumen

El proyecto pretende establecer las bases de un SGSI (Sistema de Gestión de la Seguridad de la Información) basados en la norma ISO 27001:2013, y en los controles del anexo A de la ISO 27002:2013, en la Unidad de Gerencia de Servicios Tecnológicos de una Universidad ubicada en Colombia, teniendo en cuenta que la unidad hasta ahora se encuentra implementando estrategias de seguridad de la información sobre algunos procesos.

María Fernanda Chaparro Junio de 2016

Objetivo general

- Integrar las estrategias de seguridad de la información, así como la documentación y políticas de la oficina de gerencia de Servicios Tecnológicos (GST), en un sistema de Gestión de la seguridad de la información, basados en la norma ISO/IEC 27001:2013, para mejorar en el corto, mediano y largo plazo los aspectos de seguridad de dicha oficina, relacionados con los dominios y las cláusulas que se encuentran en su estado inicial de maduración.

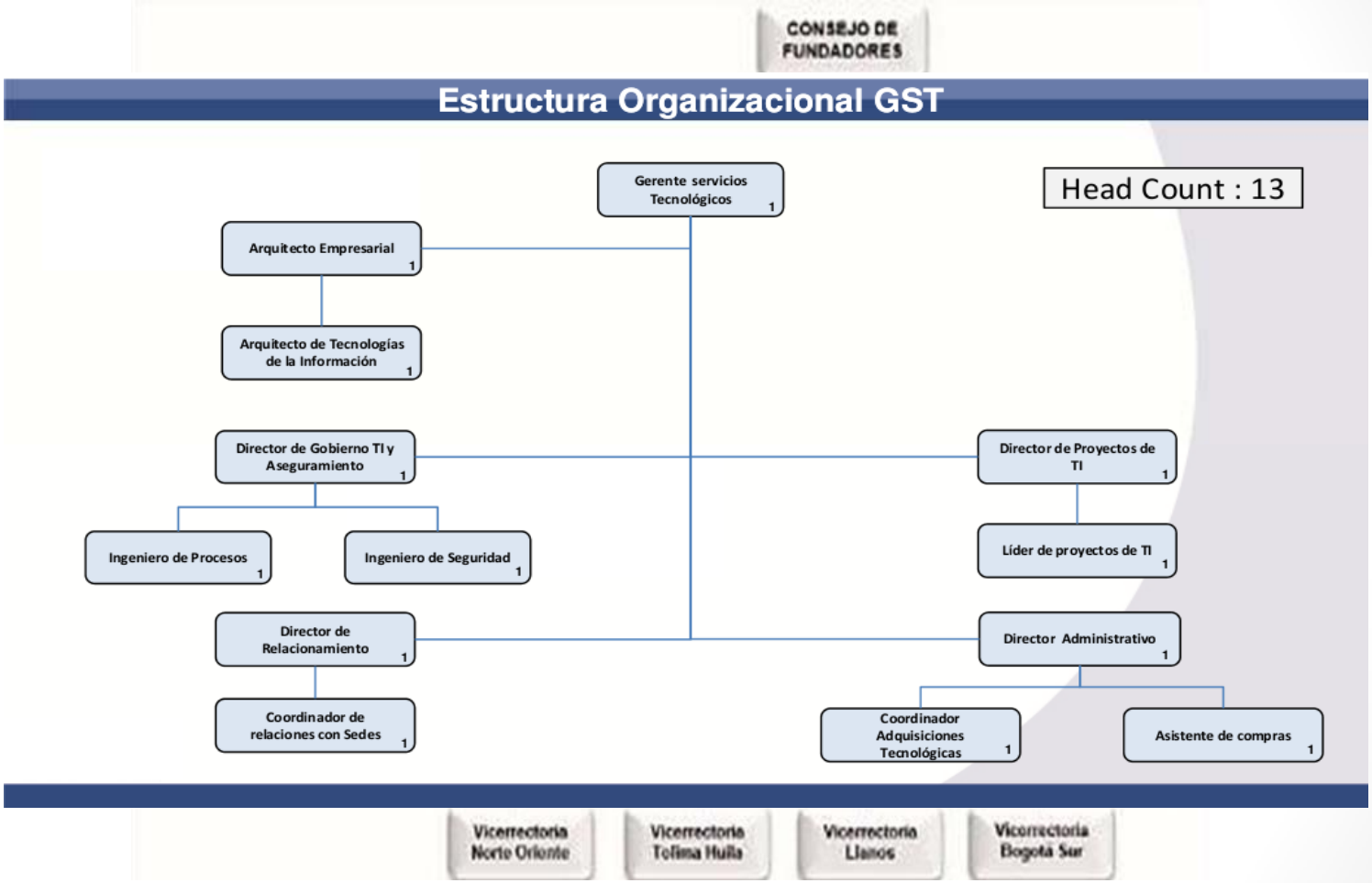
María Fernanda Chaparro Junio de 2016

Objetivos específicos

- Alinear los procesos de la oficina de GST para cumplir con los requisitos de la norma ISO 27001:2013.
- Generar los planes de continuidad de negocio, o reducir el número de incidentes de seguridad no tratados.
- Identificar los procesos que permitan realizar los controles y gestionar el SGSI, además de la creación de la documentación necesaria en los formatos de gestión documental con los que cuenta la Corporación universitaria XX.
- Generar la confianza en los directivos, funcionarios administrativos y académicos, con respecto a las aplicaciones, sistemas de información que se desarrollan y utilizan normalmente.
- Generar el plan de capacitación y concientización tanto de los directivos, como de los funcionarios administrativos y académicos, para lograr una mejor educación en el manejo de los activos de información.

María Fernanda Chaparro Junio de 2016

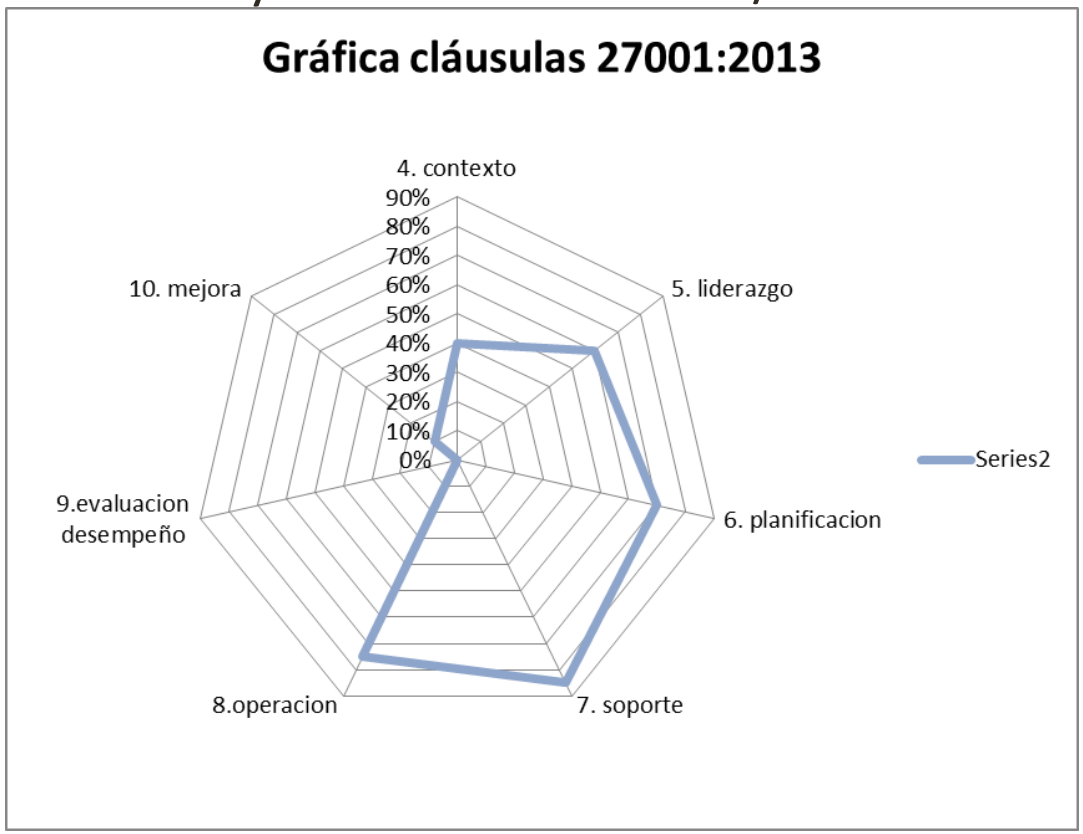
Contextualización empresa



María Fernanda Chaparro Junio de 2016

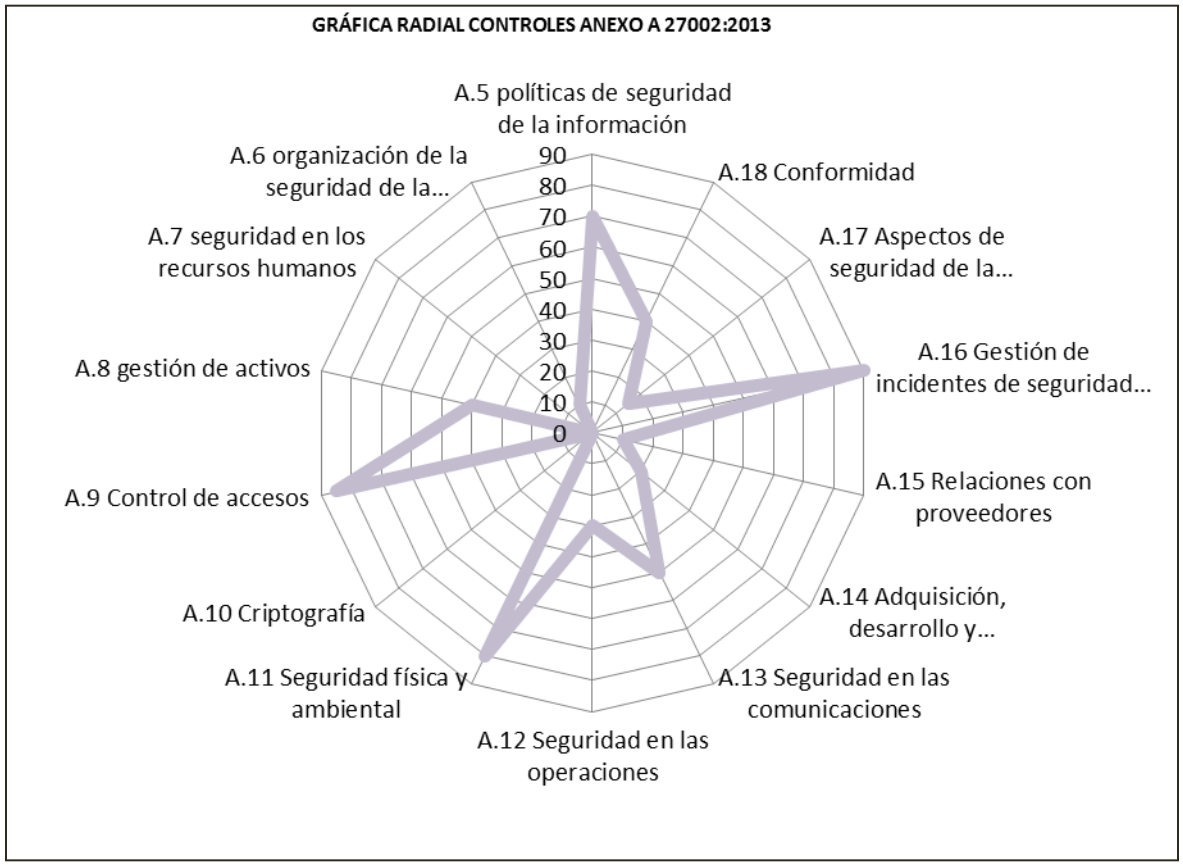
F1: Análisis diferencial

Antes de iniciar el proyecto se realiza un análisis diferencial del estado actual de la oficina de GST en relación a la seguridad de la información, tomando como referente de comparación la ISO/IEC 27001:2013 y el anexo A de la ISO/IEC 27002:2013.



María Fernanda Chaparro Junio de 2016

F1: Análisis diferencial



María Fernanda Chaparro Junio de 2016

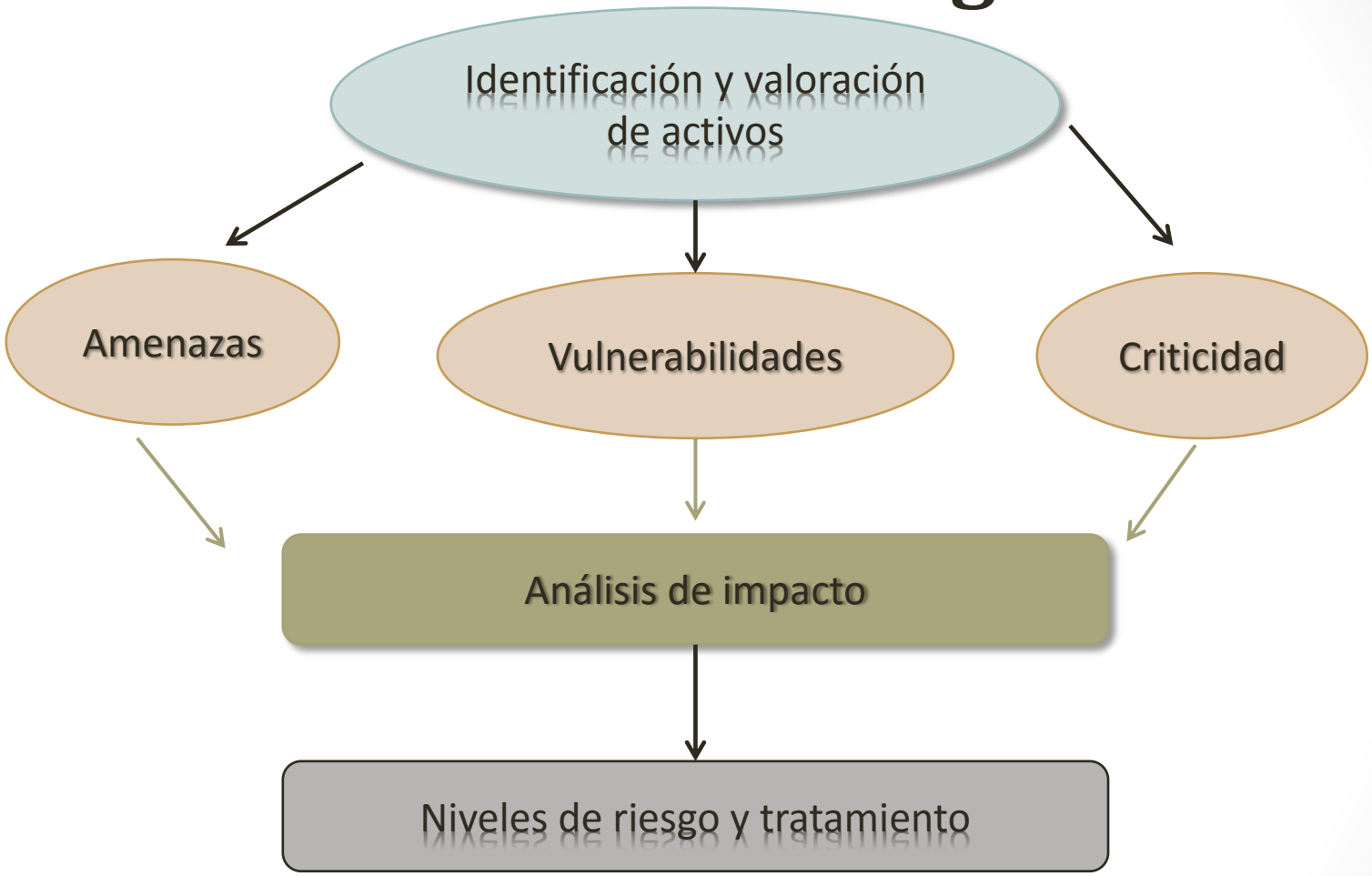
F2: Gestión documental

GESTION DOCUMENTAL

- **Política de seguridad de la información**
- ***Procedimiento de Auditorías Internas***
- **Procedimiento revisión por dirección**
- **Gestión de Indicadores**
- **Gestión de roles y responsabilidades**
- ***Declaración de aplicabilidad***
- ***Metodología de análisis de riesgos***

María Fernanda Chaparro Junio de 2016

F3: Análisis de riesgos



María Fernanda Chaparro Junio de 2016

F3: Análisis de riesgos

Activo	Amenaza	Frecuencia estimada	D	I	C	T	A	Valor activo	Impacto potencial
EQUIPOS	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,002739	50%					$ 90.000.000,00	$ 123.255,00
	[E.24] Caída del sistema por agotamiento	0,002739	80%					$ 90.000.000,00	$ 197.208,00
	[A.12] Análisis de tráfico	0,002739			90%			$ 90.000.000,00	$ 221.859,00
	[A.14] Interceptación de información (escucha)	0,03287			95%			$ 90.000.000,00	$ 2.810.385,00
	[A.24] Denegación de servicio	0,002739	95%					$ 90.000.000,00	$ 234.184,50
EDIFICIO (OFICINAS, RECEPCIÓN, SALA DE ESPERA, SALA DE REUNIÓN, BODEGA, ETC.)	[N.1] Fuego	0,002739	100%					$ 10.000.000.000,00	$ 27.390.000,00
	[N.2] daños por agua	0,002739	90%					$ 10.000.000.000,00	$ 24.651.000,00
	[N.3] inundación	0,002739	80%					$ 10.000.000.000,00	$ 21.912.000,00
	[N.4] Siniestro mayor	0,002739	100%					$ 10.000.000.000,00	$ 27.390.000,00
	[N.5]Fenómeno sísmico	0,002739	100%					$ 10.000.000.000,00	$ 27.390.000,00
	[I.1] Fuego	0,002739	100%					$ 10.000.000.000,00	$ 27.390.000,00
	[I.2] daños por agua	0,002739	90%					$ 10.000.000.000,00	$ 24.651.000,00
	[I.12] Sobrecarga eléctrica	0,002739	50%					$ 10.000.000.000,00	$ 13.695.000,00
	[I.6] Corte del suministro eléctrico	0,002739	60%					$ 10.000.000.000,00	$ 16.434.000,00
	[I.7] Condiciones inadecuadas de tempera	0,002739	50%	80%				$ 10.000.000.000,00	$ 21.912.000,00
	[E.18] Destrucción de información	0,002739	90%	90%				$ 10.000.000.000,00	$ 24.651.000,00
	[A.11] Acceso no autorizado	0,002739		95%	90%			$ 10.000.000.000,00	$ 26.020.500,00
	[A.15] Modificación deliberada de la info	0,002739	90%					$ 10.000.000.000,00	$ 24.651.000,00
	[A.18] Destrucción de información	0,002739	90%					$ 10.000.000.000,00	$ 24.651.000,00

Activo	Amenaza	Salvaguarda	Frecuencia estimada	D	I	C	T	A	Valor activo	Impacto Residual
EDIFICIO (OFICINAS, RECEPCIÓN, SALA DE ESPERA, SALA DE REUNIÓN, BODEGA, ETC.)	[N.1] Fuego	Sistema de deteccion y extinción de incendios; plan de recuperación de desastres;	0,002739	5%					$ 10.000.000.000,00	$ 1.369.500,00
	[N.2] daños por agua	Detectores de humedad; plan de continuidad del negocio	0,002739	10%					$ 10.000.000.000,00	$ 2.739.000,00
	[N.3] inundación	Detectores de humedad; plan de continuidad del negocio	0,002739	10%					$ 10.000.000.000,00	$ 2.739.000,00
	[N.4] Siniestro mayor	Póliza	0,002739	20%					$ 10.000.000.000,00	$ 5.478.000,00
	[N.5]Fenómeno sísmico	Póliza	0,002739	30%					$ 10.000.000.000,00	$ 8.217.000,00
	[I.1] Fuego	Sistema de deteccion y extinción de incendios; plan de recuperación de desastres; plan de continuidad del negocio	0,002739	5%					$ 10.000.000.000,00	$ 1.369.500,00
	[I.2] daños por agua	Póliza	0,002739	10%					$ 10.000.000.000,00	$ 2.739.000,00
	[I.12] Sobrecarga eléctrica	Circuitos de protección y transferencia	0,002739	10%					$ 10.000.000.000,00	$ 2.739.000,00
	[I.6] Corte del suministro eléctrico	Planta eléctrica y UPS;plan de recuperación de desastres	0,002739	5%					$ 10.000.000.000,00	$ 1.369.500,00
	[I.7] Condiciones inadecuadas de ter	Detectores de humedad y temperatura	0,002739	15%	15%				$ 10.000.000.000,00	$ 4.108.500,00
	[E.18] Destrucción de información	Copias de respaldo en otro lugar fisico	0,002739	10%	10%				$ 10.000.000.000,00	$ 2.739.000,00
	[A.11] Acceso no autorizado	Control de acceso biométrico	0,002739		5%	5%			$ 10.000.000.000,00	$ 1.369.500,00
	[A.15] Modificación deliberada de la	Control de acceso	0,002739	10%					$ 10.000.000.000,00	$ 2.739.000,00
	[A.18] Destrucción de información	Control de acceso biométrico, copias de respaldo en otro sitio	0,002739	5%					$ 10.000.000.000,00	$ 1.369.500,00
	[A.26] Ataque destructivo	Control de acceso/vigilancia	0,002739	10%					$ 10.000.000.000,00	$ 2.739.000,00

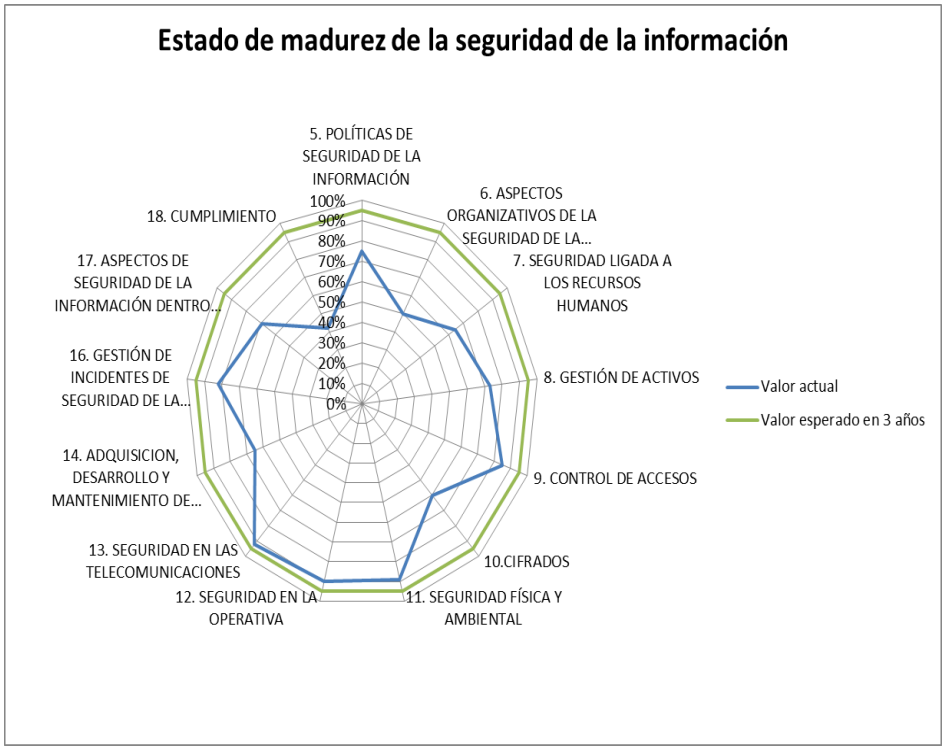
María Fernanda Chaparro Junio de 2016

F4: Propuestas proyectos

Proyecto	Riesgos identificados	Pilar	Acciones	impacto	Prioridad desarrollo
Plan de capacitación	[E.1] Errores de los usuarios.	Integridad	Cursos de capacitación Campaña publicitaria Concienciación	Alto Medio Alto	Medio
	[E.2] Errores del administrador.	Integridad			
	[E.7] Deficiencias en la organización.	disponibilidad			
	[E.18] Destrucción de información.	integridad			
	[E.19] Fugas de información.	confidencialidad			
Plan de continuidad del negocio	[I.1] Fuego	Disponibilidad	Generación plan de acción. Establecimiento grupos de respuesta. Estudio, diseño e implementación Centro de Datos alterno	Alto Medio Alto	Alto
	[I5] avería de origen físico o lógico.	Disponibilidad			
	[I.6] Corte del suministro eléctrico.	Disponibilidad			
	[I.12] Sobrecarga eléctrica.	Disponibilidad			
	[I13] fluctuación eléctrica.	Disponibilidad			
	[N.1] Fuego	Disponibilidad			
	[N.2] daños por agua.				
	[N.3] inundación.				
	[N.4] Siniestro mayor.				
	[N.5] Fenómeno sísmico.				
	[A.18] Destrucción de información.				
	[A.26] Ataque destructivo.				
Plan de mitigación de riesgos	[A.14] Interceptación de información (escucha).	Integridad, disponibilidad	Bloqueo de puertos de comunicación empleados por software. Inspección de tráfico, bloqueo de tráfico. Inspección y medición del tráfico para control de canal. Establecimiento de políticas de uso de software, políticas de intercambio de información y actualización de políticas de uso de TI.	Medio Medio Medio	Alto
	[A.18] Destrucción de información	Disponibilidad			
	[E.8] Difusión de software dañino	Disponibilidad, Integridad			

María Fernanda Chaparro Junio de 2016

F5: Auditoría de cumplimiento



No.	DOMINIO	valor actual	Valor en análisis diferencial
5	5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	75%	70%
6	6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	50%	10%
7	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	64%	0%
8	8. GESTIÓN DE ACTIVOS	73%	40%
9	9. CONTROL DE ACCESOS	85%	85%
10	10.CIFRADOS	60%	0%
11	11. SEGURIDAD FÍSICA Y AMBIENTAL	89%	80%
12	12. SEGURIDAD EN LA OPERATIVA	90%	30%
13	13. SEGURIDAD EN LAS TELECOMUNICACIONES	92%	50%
14	14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	69%	20%
16	16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	82%	90%
17	17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA CONTINUIDAD DEL NEGOCIO	69%	15%
18	18. CUMPLIMIENTO	42%	40%

Se realizó informe de auditoría interna, encontrándose once (11) no conformidades, clasificadas en cuatro (4) no conformidades menores y siete (7) mayores, las cuales evidencian fallas en cláusulas como liderazgo, evaluación del desempeño y mejora.

María Fernanda Chaparro Junio de 2016

F6: Resultados

- ✓Desarrollo Procedimiento de Auditorías Internas
- ✓Plan de continuidad del negocio
- ✓Plan de concienciación y capacitación
- ✓Resumen ejecutivo
- ✓Informe compañía
- ✓Estado cumplimiento controles

María Fernanda Chaparro Junio de 2016

¿Qué sigue?

- Capacitación y certificación personal en auditoría interna 27001:2013.
- Nuevo análisis de riesgos una vez terminado este ciclo.
- Reunión alta dirección para asignación de presupuesto para proyectos relacionados con el SGSI.