PROYECTO
Plan para la implementación de un SGSI Basado en ISO 27001: 2013

Presentación de resultados

UAB Universitat Autònoma de Barcelona

UOC www.uoc.edu

Universitat Rovira i Virgili

Sandra Murillo Guacas

Diciembre 2015

CONTENIDO

1. Resumen
2. Alcance del Sistema
3. Objetivos
4. Justificación
5. Plan de Seguridad de la Información

1 - Resumen

En este proyecto se realiza un análisis del estado actual de la Seguridad de la Información para una empresa Colombiana, de servicios de Auditoría y Consultoría Informática. El proceso misional de negocio es el desarrollo de software a la medida y el objetivo del proyecto es el análisis y el diseño de un Plan Director para la implementación del Sistema de Gestión de la Seguridad de la Información en esta empresa.

2 - Objetivos

General:

Elaborar un plan para la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013.

2 - Objetivos

Específicos:

- Identificar el contexto de la organización para establecer los riesgos potenciales en el ambiente informático
- Proponer controles para preservar la seguridad de la información durante el ciclo de vida del desarrollo de sistemas de información.
- Establecer controles para preservar la protección de datos durante las pruebas ejecutadas a los sistemas de información.
- Diseñar un plan de concientización sobre la importancia de la Seguridad de la información.
- Establecer los recursos requeridos para la implementación del plan Directo

3 - Contextualización - Descripción de la Empresa

- Visión: Ser en los próximos cinco años una organización reconocida a nivel nacional e internacional, ocupando un lugar preferencial en la prestación de Consultoría y Asesoría Informática en empresas nacionales e internacionales.

- Misión: Apoyar organizaciones públicas y privadas en la gestión de tecnologías informáticas con soluciones estratégicas, efectivas, herramientas tecnológicas innovadoras y talento humano competente.

3 - Contextualización - Descripción de la Empresa

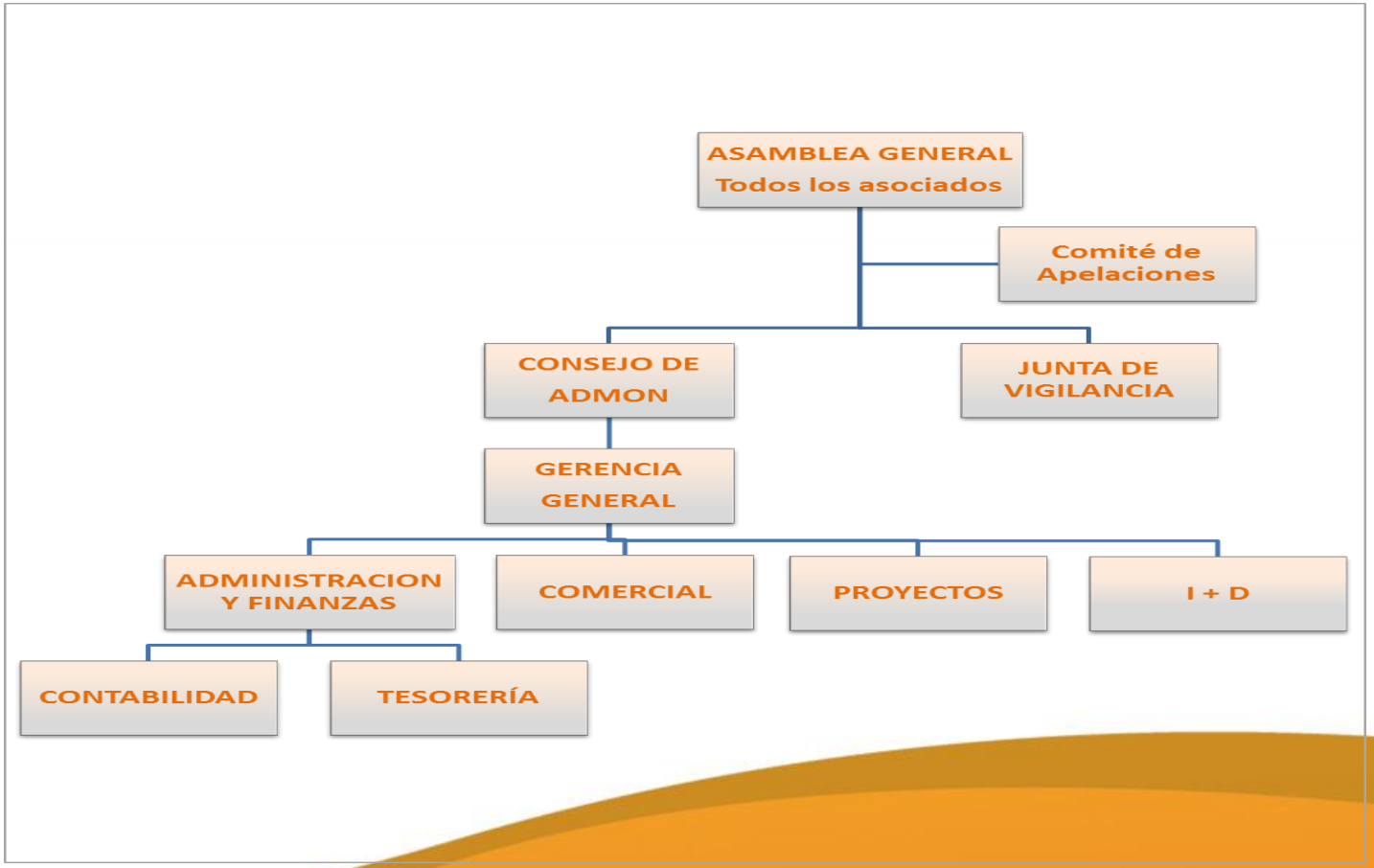
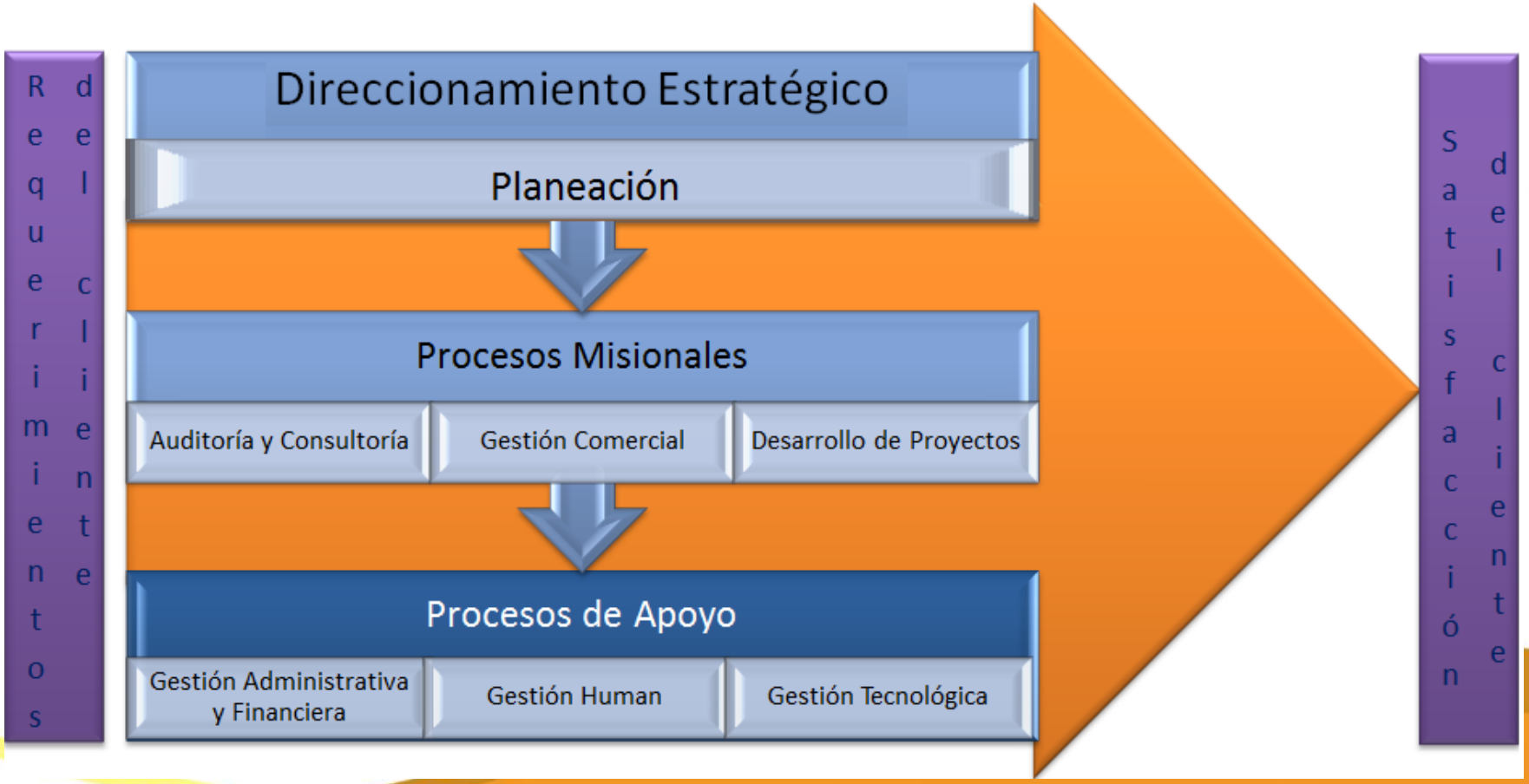


Diagrama Organizacional

3 - Contextualización - Descripción de la Empresa



La Empresa por Procesos

3 - Contextualización - Descripción de la Empresa

Diagrama de Red de la Empresa

4 - Plan de Seguridad de la Información

- El Plan de Seguridad de la Información se desarrolló en cinco etapas:
  - ETAPA 1: Análisis Diferencial
  - ETAPA 2: Sistema de Gestión Documental
  - ETAPA 3: Análisis de Riesgos
  - ETAPA 4: Propuesta de Proyectos
  - ETAPA 5: Auditoría de Cumplimiento

- Se tomó como marco de referencia.
  - La norma ISO/IEC 27001:2013 para el SGSI
  - La Metodología Magerit Versión 3.0 para el análisis de riesgos

ETAPA 1: Análisis Diferencial

Evaluación de Requisitos de la norma ISO/IEC27001:2013

ETAPA 1: Análisis Diferencial

DESCRIPCIÓN	% DE CUMPLIMIENTO	NIVEL DE MADUREZ
No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver	0%	No existente
Inicial- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ***ad hoc*** que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizada	20%	Inicial
Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los error es son muy probables	40%	Repetible
Definido-Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes	60%	Definido
Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmenta	80%	Administrado
Optimizado- Los procesos se han refinado hasta un nivel de mejo r práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida	100%	Optimizado

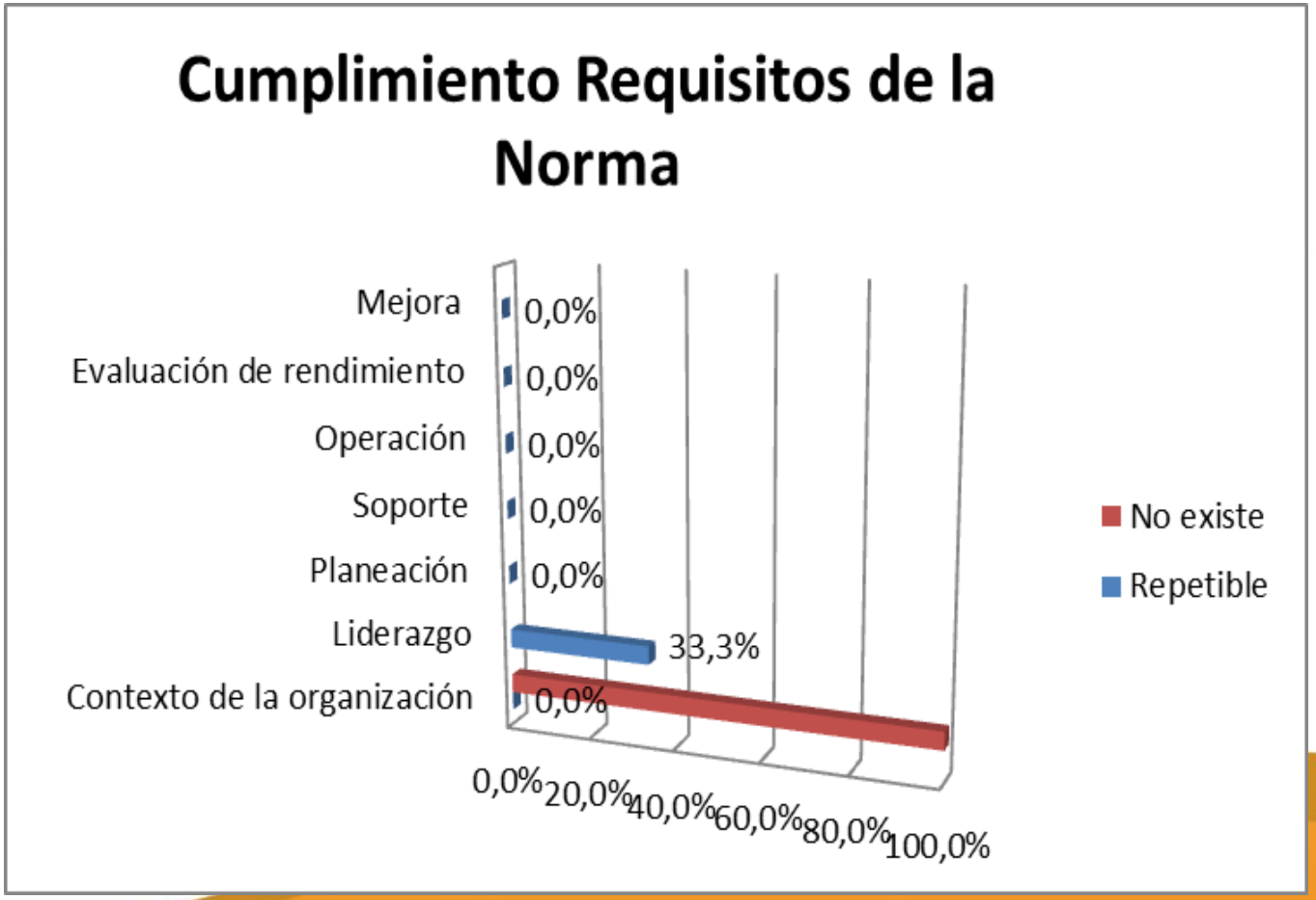
Niveles de madurez - COBIT V4.1

ETAPA 1: Análisis Diferencial

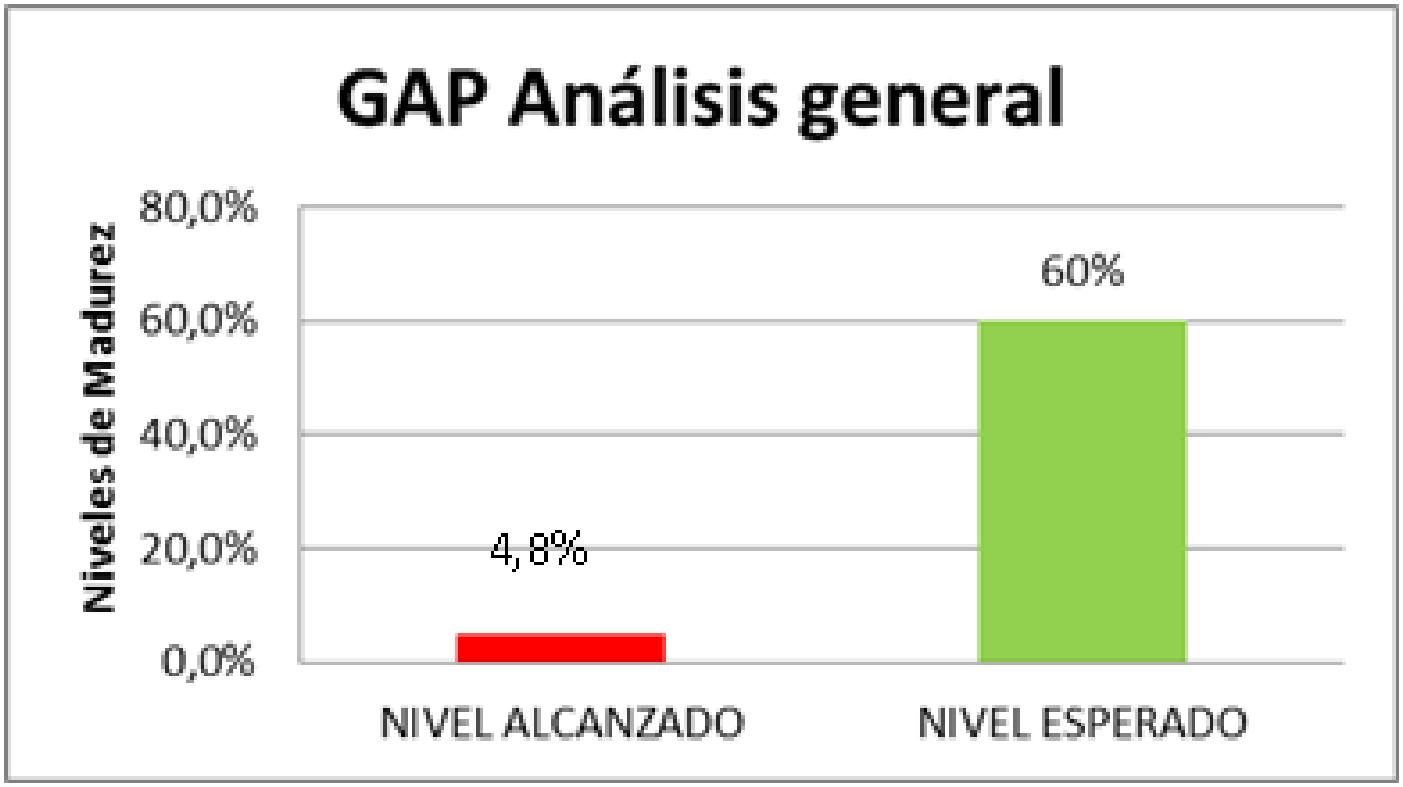
- Se realizó un análisis deferencial con respecto a la norma ISO/IEC27001:2013

Dominio		BRECHA		Puntaje Dominio	Puntaje Dominio	
		SI	NO			
4 Contexto de la organización	4.1 Entendiendo la organización y su contexto		X	0,0%	0,0%	No existe
	4.2 Entendiendo las necesidades y expectativas de las partes interesadas		X	0,0%		
	4.3 Determinando el alcance del sistema de gestión de seguridad de la información		X	0,0%		
	4.4 Sistema de gestión de seguridad de la información		X	0,0%		
5 Liderazgo	5.1 Liderazgo y compromiso	X		33,3%	33%	Repetible
	5.2 Política		X	0,0%		
	5.3 roles, responsabilidades y autoridades en la organización		X	0,0%		
6 Planificación	6.1 Acciones para tratar riesgos y oportu		X	0,0%	0,0%	No existe
	6.2 Objetivos de seguridad de la información y planes para lograrlos		X	0,0%		
7 Soporte	7.1 Recursos		X	0,0%	0,0%	No existe
	7.2 Competencia		X	0,0%		
	7.3 Toma de conciencia		X	0,0%		
	7.4 Comunicación		X	0,0%		
	7.5 Información documentada		X	0,0%		
8 Operación	8.1 Planificación y control operacional		X	0,0%	0,0%	No existe
	8.2 Valoración de riesgos de la seguridad de la información		X	0,0%		
	8.3 Tratamiento de riesgos de la seguridad de la información		X	0,0%		
9 Evaluación del de	9.1 Seguimiento, medición, análisis y eva		X	0,0%	0,0%	No existe
	9.2 Auditoría interna		X	0,0%		
	9.3 Revisión por la dirección		X	0,0%		
10 Mejora	10.1 No conformidades y acciones correc		X	0,0%	0,0%	No existe
	10.2 Mejora continua		X	0,0%		

ETAPA 1: Análisis Diferencial



ETAPA 1: Análisis Diferencial

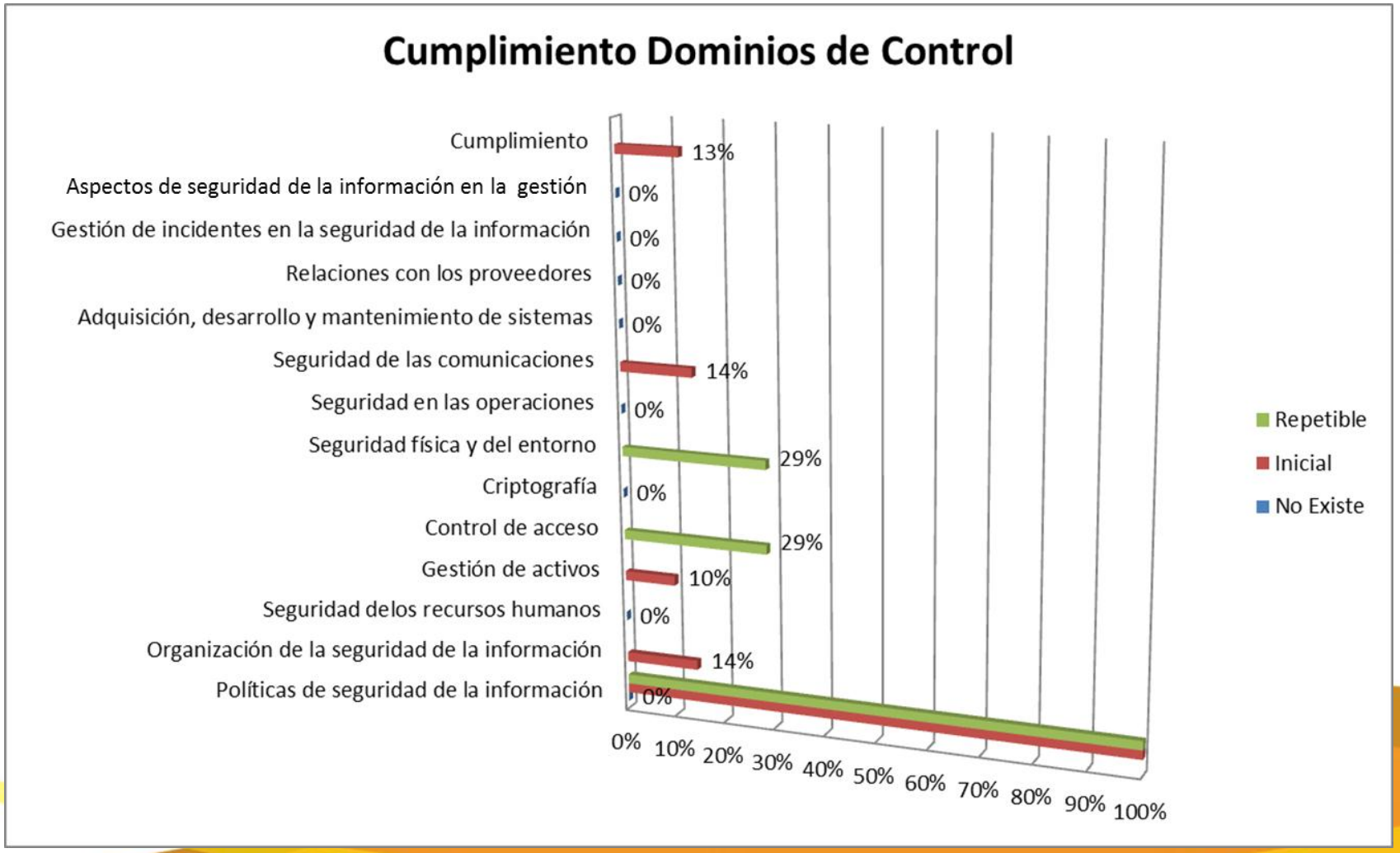


Evaluación de Cumplimiento de controles según la norma ISO/IEC27002:2013

ETAPA 1: Análisis Diferencial

CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA ISO/IEC 27002:2013			
DOMINIOS DE CONTROL		**Porcentaje de Cumplimiento**	
5	Políticas de seguridad de la información	0%	No existe
6	Organización de la seguridad de la información	14%	Inicial
7	Seguridad delos recursos humanos	0%	No existe
8	Gestión de activos	10%	Inicial
9	Control de acceso	29%	Repetible
10	Criptografía	0%	No existe
11	Seguridad física y del entorno	29%	Repetible
12	Seguridad en las operaciones	0%	No existe
13	Seguridad de las comunicaciones	14%	Inicial
14	Adquisición, desarrollo y mantenimiento de sistemas	0%	No existe
15	Relaciones con los proveedores	0%	No existe
16	Gestión de incidentes en la seguridad de la información	0%	No existe
17	Aspectos de seguridad de la información en la gestión de continuidad de negocio	0%	No existe
18	Cumplimiento	13%	Inicial

ETAPA 1: Análisis Diferencial



ETAPA 2: Sistema de Gestión Documental

ETAPA 2: Sistema de Gestión Documental

- Objetivo.

Establecer una estructura documental, normalizada y formal para el registro de los documentos generados por el Sistema de Gestión de Seguridad de la Información.

ETAPA 2: Sistema de Gestión Documental

ETAPA 3: Análisis de Riesgos

ETAPA 3: Análisis de Riesgos

Se desarrollaron 5 actividades en el análisis de riesgos establecidas en el documento Metodología de análisis de Riesgos:

- Inventario de Activos
- Valoración de Activos
- Análisis de Amenazas
- Impacto Potencial
- Nivel de Riesgo

ETAPA 3: Análisis de Riesgos

- Inventario de Activos

AMBITO	ID	ACTIVO
Instalaciones [L]	[L-01]	Oficina de Sistemas
Hardware [HW]	[HW-01]	Servidores
	[HW-03]	Estaciones de Trabajo
Aplicación [SW]	[SW-01]	Sistemas Operativos
	[SW-03]	Microsoft Office
	[SW-04]	Antivirus
	[SW-05]	Windows Server 2008 R2
	[SW-07]	Herramientas de desarrollo
	[SW-09]	Aplicativo Contable
	[SW-10]	Aplicativo Micronif
	[SW-11]	Sigcoop 8.0
Datos[D]	[D-01]	Datos de Clientes, Asociados, Empleados.
	[D-02]	Códigos fuente.
	[D-03]	Datos de gestión Administrativa, contable y financiera.
	[D-04]	Copias de Seguridad
	[D-05]	Logs

AMBITO	ID	ACTIVO
Red de Comunicación [COM]	[COM-01]	Dispositivos de Acceso a redes
	[COM-02]	Rourter
	[COM-04]	Red Telefónica
	[COM-05]	Red inalámbrica
Servicios [S]	[S-01]	Correo Electrónico
	[S-02]	Servicio Web
Equipamiento auxiliar [AUX]	[AUX-01]	Impresoras
	[AUX-02]	Regulador de Voltaje
	[AUX-03]	Aire Acondicionado
	[AUX-04]	Archivadores
Personal [P]	[P-01]	Responsable de TI
	[P-02]	Desarrolladores
	[P-03]	Demás personal de TI
	[P-04]	Personal de Administración
	[P-05]	Asociados

ETAPA 3: Análisis de Riesgos

- Valoración de Activos

AMBITO	ID	ACTIVO	ASPECTOS CRITICOS					TOTAL	IMPORTANCIA
			[A]	[C]	[I]	[D]	[T]		
Instalaciones [L]	[L-01]	Oficina de Sistemas	7	8	8	9	5	37	A
Hardware [HW]	[HW-01]	Servidores	5	9	9	8	6	37	A
	[HW-03]	Estaciones de Trabajo	3	2	1	1	1	8	B
Aplicación [SW]	[SW-01]	Sistemas Operativos	3	2	1	1	1	8	B
	[SW-03]	Microsoft Office	3	2	1	1	0	7	B
	[SW-04]	Antivirus	5	2	5	5	3	20	M
	[SW-05]	Windows Server 2008 R2	3	8	8	8	6	33	A
	[SW-07]	Herramientas de desarrollo	2	3	2	1	0	8	B
	[SW-09]	Aplicativo Contable	2	8	9	8	7	34	A
	[SW-10]	Aplicativo Micronif	5	9	5	5	3	27	A
	[SW-11]	Sigcoop 8.0	3	9	3	3	2	20	M

ETAPA 3: Análisis de Riesgos

- Análisis de Amenazas

AMENAZAS:		FRECUENCIA		ASPECTOS CRITICOS				
				[A]	[C]	[I]	[D]	[T]
[N.1]	Fuego	MP	1				100%	
[N.2]	Daños por agua	MP	1				70%	
[I.1]	Fuego	MP	1				100%	
[I.2]	Daños por agua	PF	0,1				50%	
[A.7]	Uso no previsto	N	1				20%	
[A.11]	Acceso no autorizado	PF	0,1		30%	30%		
[A.26]	Ataque destructivo	MP	0,01				100%	
Ámbito: Instalaciones	**Activo: [L-01] Oficina de Sistemas**	N	1,00	0,00	0,30	0,30	1,00	0,00

ETAPA 3: Análisis de Riesgos

- Impacto Potencial

Resultado del impacto Potencial

IP = Vr. Activo (por dimensión) * Vr. Amenaza.

ID	ACTIVO	VALORACIÓN ACTIVOS					IMPORTANCIA	VALORACIÓN AMENAZAS					IMPACTO POTENCIAL				
		[A]	[C]	[I]	[D]	[T]		[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[L-01]	Oficina de Sistemas	7	8	8	9	5	A	0%	30%	30%	100%	0%	0	2,4	2,4	9	0
[HW-01]	Servidor Principal	5	9	9	8	6	A	0%	100%	30%	100%	0%	0	9	2,7	8	0
[HW-02]	Servidor de Desarrollo y Pruebas	3	5	5	5	2	M	0%	100%	30%	100%	0%	0	5	1,5	5	0
[HW-03]	Estaciones de Trabajo No. 1, 2 y 3	3	2	1	1	1	B	0%	100%	30%	100%	0%	0	2	0,3	1	0
[HW-06]	Portátiles No. 1 y 2	3	2	1	1	1	B	0%	100%	30%	100%	0%	0	2	0,3	1	0
[SW-01]	Windows 7 Profesional	3	2	1	1	1	B	100%	100%	100%	100%	0%	3	2	1	1	0
[SW-02]	Windows 8.1	3	2	1	1	1	B	100%	100%	100%	100%	0%	3	2	1	1	0

ETAPA 3: Análisis de Riesgos

- Nivel de Riesgo

cálculo del Riesgo total

Riesgo = impacto potencial x frecuencia

ID	ACTIVO	FRECUENCIA		IMPACTO POTENCIAL					RIESGO				
				[A]	[C]	[I]	[D]	[T]	[A]	[C]	[I]	[D]	[T]
[L-01]	Oficina de Sistemas	N	1	0	2,4	2,4	9	0	0,00	2,40	2,40	9	0,00
[HW-01]	Servidor Principal	F	10	0	9	2,7	8	0	0,00	90	27	80	0,00
[HW-02]	Servidor de Desarrollo y Pruebas	F	10	0	5	1,5	5	0	0,00	50	15	50	0,00
[HW-03]	Estaciones de Trabajo No. 1, 2 y 3	F	10	0	2	0,3	1	0	0,00	20	3	10	0,00
[HW-06]	Portátiles No. 1 y 2	F	10	0	2	0,3	1	0	0,00	20	3	10	0,00

ETAPA 4: Propuesta de Proyectos

CODIGO:	NOMBRE PROYECTO:	DESCRIPCION:
PS-001	Legalización y controles de Software de Infraestructura y de Gestión	El propósito es establecer controles para mitigar los riesgos que se pueden presentar en los sistemas de información de la gestión administrativa, como cuentas de usuario con menor nivel de privilegios, renovación de licencia, actualizaciones, etc.
PS-002	Gestión de privilegios y Acceso a los aplicativos	Se pretende optimizar el acceso a los Sistemas de Información y asignar a quien corresponda los privilegios necesarios para su desempeño.
PS-003	Mejoramiento en el proceso de copias de seguridad	Disponer de los controles necesarios para asegurar que se realiza la protección de la información de manera adecuada y se respanda de acuerdo con las políticas de seguridad de información
PS-004	Gestión de log	Permitir a los administradores información oportuna sobre las tareas que realizan los usuarios en el sistema de información de tal manera que se puedan asignar responsabilidades en caso que se presenten eventos adversos.
PS-005	Garantizar la continuidad del servicio en caso de no disponibilidad de equipos de comunicaciones	Se propone establecer controles para minimizar el impacto de las amenazas que tienen como resultado interrupciones en los servicios que presta el área de TI a los usuarios.
PS-006	Garantizar la continuidad del servicio en caso de caída de las redes	Se propone establecer controles para minimizar el impacto de las amenazas que tienen como resultado interrupciones en los servicios que presta el área de TI a los usuarios.
PS-007	Mejoramiento en el Servicio de Correos	Se pretende implementar controles que mejoren el uso del correo electrónico institucional por parte de los funcionarios y que asignen responsabilidades sobre este servicio a quien corresponda.
PS-008	Continuidad de los procesos ante	Lograr implementar acciones que faciliten la disponibilidad de personal para
PS-009	Continuidad del SGSI ante la ausencia de personal relacionado	Definir las políticas que garanticen la continuidad del personal y la frecuencia de convocatoria al comité del SGSI de tal manera que no se vea comprometida su permanencia en la empresa.
PS-010	Política de seguridad de la información	La dirección de la organización debe cumplir con el requisito de definir la política de seguridad de la información como elemento fundamental para la implementación de un SGSI

ETAPA 4: Propuesta de Proyectos

CODIGO:	NOMBRE PROYECTO:	DESCRIPCION:
PS-011	Organización de la seguridad de la información	De acuerdo con la evaluación resultados para satisfacer los requerimientos de control necesitados en la mitigación de los riesgos que resultaron críticos, es necesario implementar los controles en los respectivos procesos para garantizar la protección de la información.
PS-012	Gestión de los activos	Entendiendo la importancia de los sistemas de información, la infraestructura de TI y los otros activos de información que deben estar disponibles a los usuarios es importante la definición de políticas de control para estos activos.
PS-013	Sistema de control de acceso físico	es indispensable implementar controles efectivos en las instalaciones en los ambientes de los sistemas de información.
PS-014	Sistema de control físico de los equipos	La protección de los activos físicos en los ambientes de los sistemas de información es indispensable y para ello se deben implementar controles efectivos.
PS-015	Políticas de relación con los proveedores	Cada día las empresas se ven mas amenazadas por la adopción de servicios de TI ofrecidos por terceros, por ello se deben mejorar los controles que preserven la seguridad de la información.
PS-016	Políticas de incidentes de seguridad de la información	La entrega de servicios de TI a los usuarios implica la percepción de valor positiva o negativa por parte de los usuarios. La seguridad de la información es uno de los aspectos que incide en esta percepción.
PS-017	Cumplimiento de normativa legal y de la organización	Las entidades reguladoras establecen para algunos tipos de empresa requisitos de control para la seguridad de la información que debe ser implementados para poder operar.
PS-018	Cumplimiento de auditorías al SGSI	Es necesario dentro de el Sistema de Gestión cumplir con la verificación de el seguimiento al SGSI.
PS-019	Plan de continuidad de negocio	La no disponibilidad de los recursos o la pérdida o destrucción de los alguno de ellos son riesgos que deben mitigarse. Para ello se deben establecer controles que garanticen la planeación y seguimiento a los planes de continuidad de negocio y recuperación de desastres.

ETAPA 4: Propuesta de Proyectos

Plan a Corto, mediano y largo plazo.

CODIGO	PROYECTO	TIEMPO EN MESES	AÑO 1	AÑO 2	AÑO 3
			2016	2017	2018
PS-010	Política de seguridad de la información	2			
PS-004	Gestión de log	1			
PS-003	Mejoramiento en el proceso de copias de seguridad	3			
PS-001	Legalización y controles de Software de Infraestructura	5			
PS-012	Clasificación de la informació	1			
PS-011	Organización de la seguridad de la información	2			
PS-013	Sistema de control de acceso	2			
PS-002	Gestión de privilegios y Acceso a los aplicativos	2			
PS-006	Garantizar la continuidad del servicio en caso de caída de las redes	1			
PS-017	Cumplimiento de normativa	2			
PS-007	Mejoramiento en el Servicio de Correos	2			

ETAPA 4: Propuesta de Proyectos

Plan a Corto, mediano y largo plazo.

CODIGO	PROYECTO	TIEMPO EN MESES	AÑO 1 2016	AÑO 2 2017	AÑO 3 2018
PS-008	Continuidad de los procesos ante la ausencia de personal	2			
PS-005	Garantizar la continuidad del servicio en caso de no disponibilidad de equipos de comunicaciones	3			
PS-009	Continuidad del SGSI ante la ausencia de personal relacionado	2			
PS-014	Sistema de control físico de los equipos	1			
PS-015	Políticas de relación con los proveedores	1			
PS-016	Políticas de incidentes de seguridad de la información	1			
PS-018	Cumplimiento de auditorías al SGSI	2			
PS-019	Plan de continuidad de negocio	3			

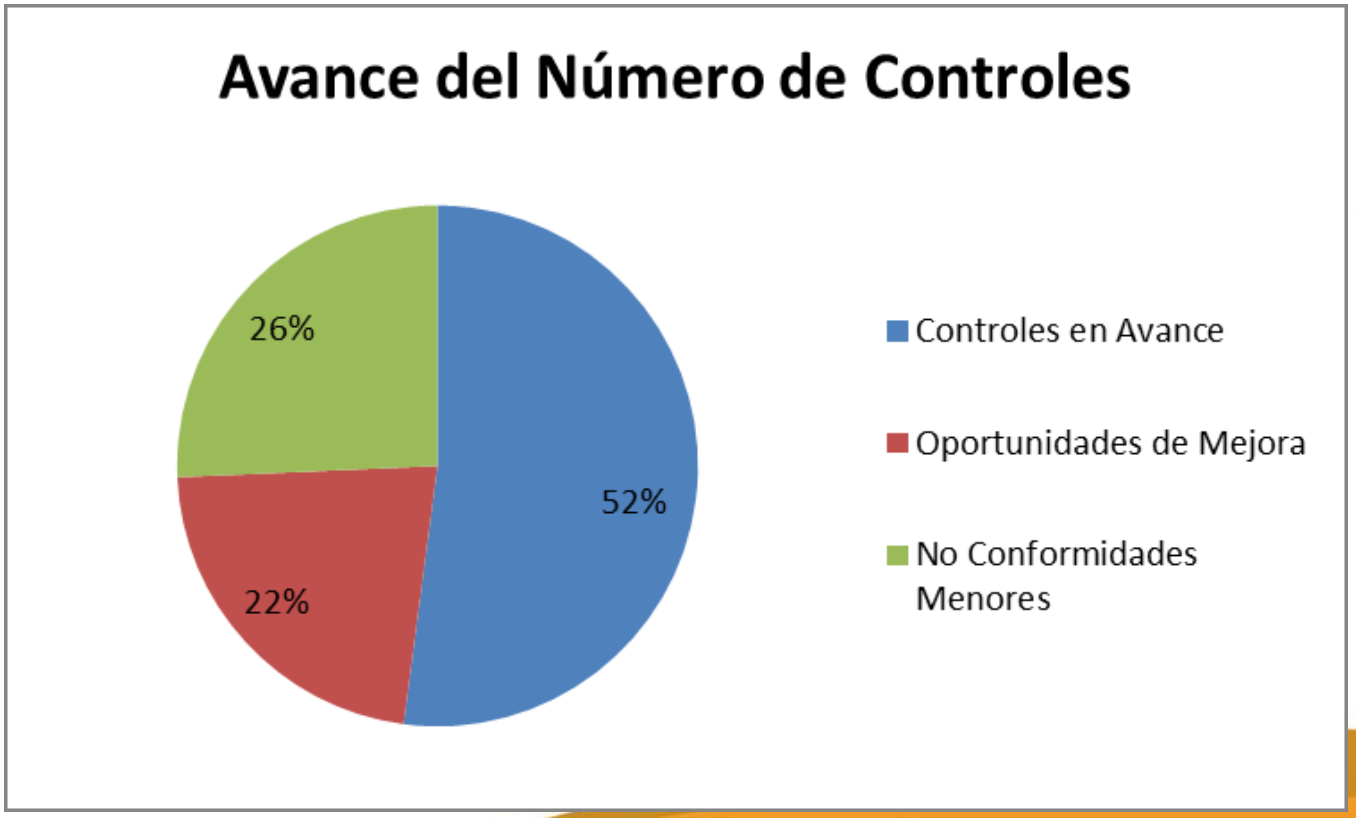
ETAPA 4: Propuesta de Proyectos

Evaluación del resultado de la ejecución de los proyectos

CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA ISO/IEC 27002:2013											
DOMINIOS DE CONTROL		Progreso 2016	Progreso 2017	Progreso 2018	Valor observado 2016	Valor observado 2017	Valor observado 2018	Lines Base	METAS		
									2016	2017	2018
5	Políticas de seguridad de la información	60%	0%	0%	60	0	0	0%	100	100	100
6	Organización de la seguridad de la información	86%	78%	100%	12	35	60	14%	14	45	60
7	Seguridad de los recursos humanos	0%	88%	92%	0	35	55	0%	0	40	60
8	Gestión de activos	50%	100%	100%	20	60	60	10%	40	60	60
9	Control de acceso	0%	0%	92%	0,4	0,4	55	29%	29	29	60
10	Criptografía	0%	0%	0%	0	0	0	0%	0	0	0
11	Seguridad física y del entorno	0%	66%	83%	0	30	50	29%	29	45	60
12	Seguridad en las operaciones	33%	100%	92%	10	60	55	0%	30	60	60
13	Seguridad de las comunicaciones	0%	100%	92%	0	60	55	14%	14	60	60
14	Adquisición, desarrollo y mantenimiento de sistemas	0%	100%	100%	0	60	60	0%	0	60	60
15	Relaciones con los proveedores	0%	0%	83%	0	0	50	0%	0	0	60
16	Gestión de incidentes en la seguridad de la información	0%	0%	75%	0	0	45	0%	0	0	60
17	Aspectos de seguridad de la información en la gestión de continuidad de negocio	0%	50%	92%	0	15	55	0%	0	30	60
18	Cumplimiento	50%	90%	100%	15	45	60	13%	30	50	60

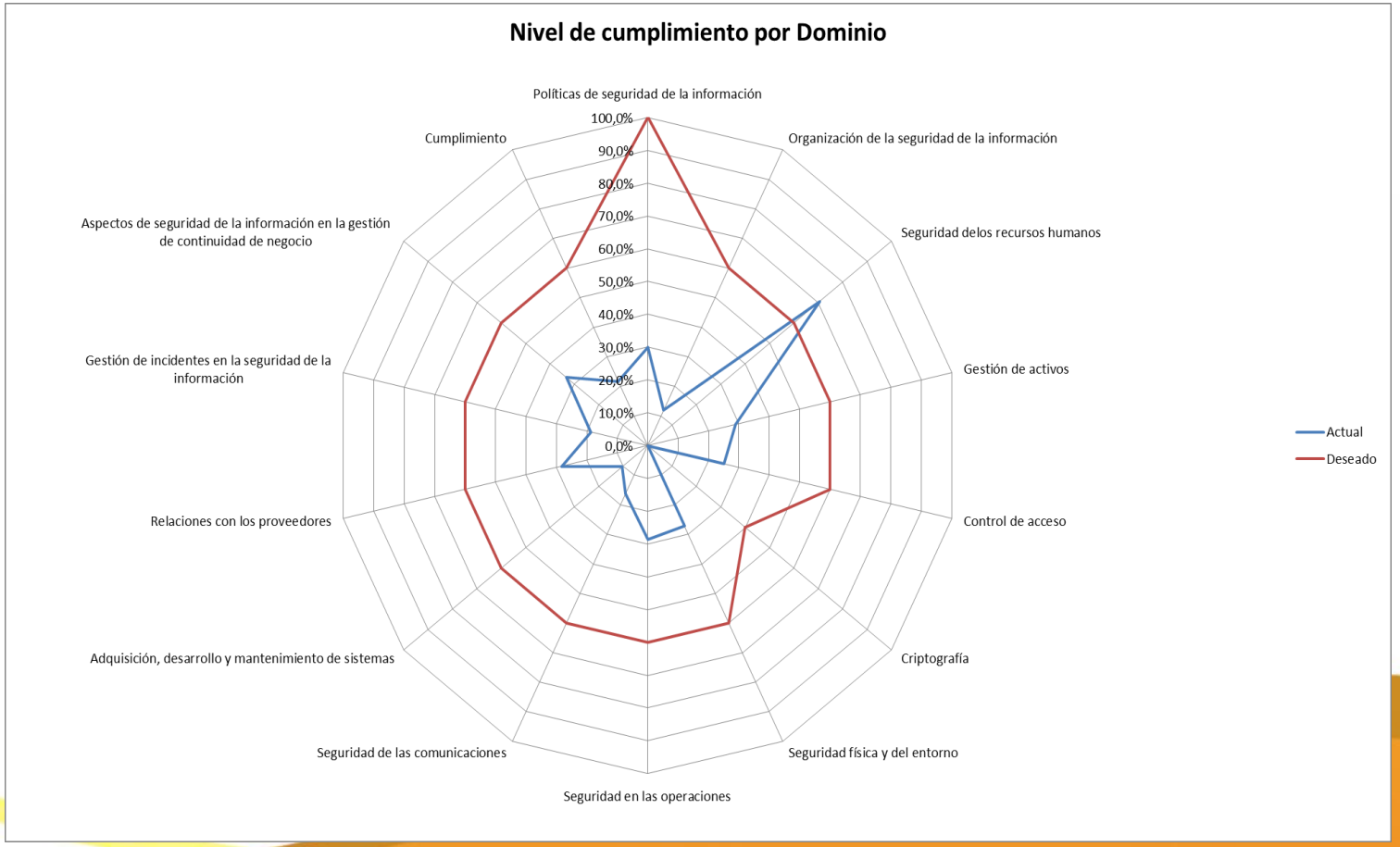
ETAPA 5: Auditoría de Cumplimiento

Avance de los controles



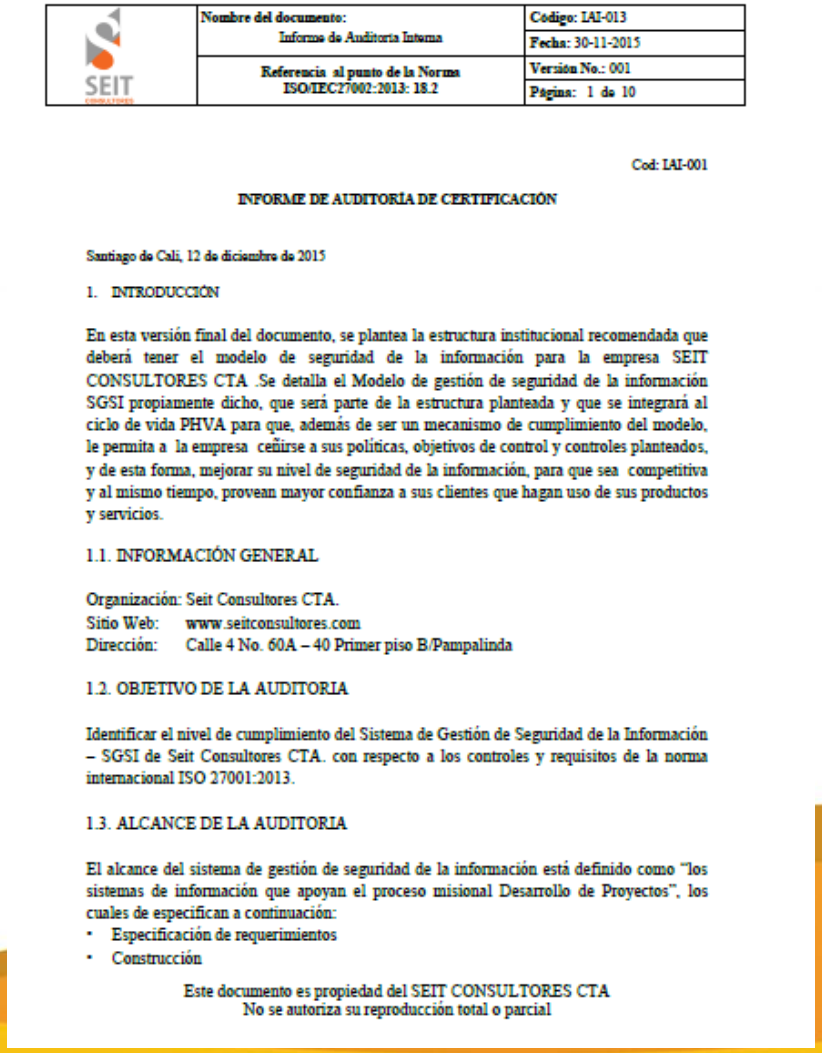
ETAPA 5: Auditoría de Cumplimiento

Niveles de cumplimiento antes y después de los proyectos



ETAPA 5: Auditoría de Cumplimiento

Informe de Auditoría



SEIT CONSULTORES	**Nombre del documento:** Informe de Auditoria Interna	**Código:** IAI-013
		Fecha: 30-11-2015
	Referencia al punto de la Norma ISO/IEC27002:2013: 18.2	**Versión No.:** 001
		Página: 1 de 10

Cod: IAI-001

INFORME DE AUDITORÍA DE CERTIFICACIÓN

Santiago de Cali, 12 de diciembre de 2015

1. INTRODUCCIÓN

En esta versión final del documento, se plantea la estructura institucional recomendada que deberá tener el modelo de seguridad de la información para la empresa SEIT CONSULTORES CTA .Se detalla el Modelo de gestión de seguridad de la información SGSI propiamente dicho, que será parte de la estructura planteada y que se integrará al ciclo de vida PHVA para que, además de ser un mecanismo de cumplimiento del modelo, le permita a la empresa ceñirse a sus políticas, objetivos de control y controles planteados, y de esta forma, mejorar su nivel de seguridad de la información, para que sea competitiva y al mismo tiempo, provean mayor confianza a sus clientes que hagan uso de sus productos y servicios.

1.1. INFORMACIÓN GENERAL

Organización: Seit Consultores CTA.
Sitio Web: www.seitconsultores.com
Dirección: Calle 4 No. 60A – 40 Primer piso B/Pampalinda

1.2. OBJETIVO DE LA AUDITORIA

Identificar el nivel de cumplimiento del Sistema de Gestión de Seguridad de la Información – SGSI de Seit Consultores CTA. con respecto a los controles y requisitos de la norma internacional ISO 27001:2013.

1.3. ALCANCE DE LA AUDITORIA

El alcance del sistema de gestión de seguridad de la información está definido como "los sistemas de información que apoyan el proceso misional Desarrollo de Proyectos", los cuales de especifican a continuación:

- Especificación de requerimientos
- Construcción

Este documento es propiedad del SEIT CONSULTORES CTA
No se autoriza su reproducción total o parcial

ETAPA 5: Auditoría de Cumplimiento

Informe de Auditoría

NORMA ISO 27001:2013		NC MAYOR	NC MENOR	OPORNUTIDAD DE MEJORA
5	Políticas de seguridad de la información	0	0	1
6	Organización de la seguridad de la in	0	3	3
7	Seguridad delos recursos humanos	0	0	1
8	Gestión de activos	0	3	3
9	Control de acceso	0	4	4
10	Criptografía	0	0	2
11	Seguridad física y del entorno	0	2	5
12	Seguridad en las operaciones	0	9	2
13	Seguridad de las comunicaciones	0	4	1
14	Adquisición, desarrollo y mantenimiento de sistemas	0	4	3
15	Relaciones con los proveedores	0	1	2
16	Gestión de incidentes en la seguridad de la información	0	2	3
17	Aspectos de seguridad de la información en la gestión de continuidad de negocio	0	2	0
18	Cumplimiento	0	3	2

ETAPA 5: Auditoría de Cumplimiento

CONCLUSIÓN FINAL

La auditoría encontró que no se está haciendo la revisión de los controles ya establecidos y que es insuficiente la documentación de los procesos. Determinando además que ciertos procedimientos resultan no adecuados para dar cumplimiento a lo exigido por la norma.

ETAPA 5: Auditoría de Cumplimiento

RECOMENDACIONES

- Es necesario que la empresa reajuste su cronograma en cuanto a la finalización de implementación de los controles y la fecha de posible certificación.

- También es necesario que la empresa destine los recursos planteados para la ejecución de los proyectos e implantación de los controles en especial aquellos de mayor incumplimiento como son la Seguridad en las operaciones, la seguridad de las comunicaciones y Adquisición, desarrollo y mantenimiento de sistemas. Y otros que podrían afectar directamente la obtención del certificado, como el dominio de Cumplimiento.

6 - Entregables

1. Memorias
2. Anexos
3. Resumen ejecutivo
4. Presentaciones

Gracias