"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los equipos"
Kevin Mitnick

CompanyLogo

Oficina de Seguridad de la Información

PROYECTO
Implementación del SGSI basado en ISO/IEC 27001:2013

Ricardo Pulgarín Gómez

Diciembre de 2014

interno

Agenda

Resumen

En el presente proyecto, se analiza una empresa Colombiana del sector agropecuario con más de 5000 empleados a nivel nacional. Se plantea a implementación de un sistema de gestión de seguridad de la información basado en los requerimientos de la norma ISO/IEC 27001:2013 y la planeación de la implementación de los controles de la ISO/IEC 27002:2013. La empresa solo tiene un oficial de seguridad informática y no cuenta con una estrategia de seguridad de la información. Se realiza toda la propuesta de implementación para sustentar la necesidad de implantar un SGSI a corto plazo.

La Empresa

Estructura de organización por procesos

La Empresa

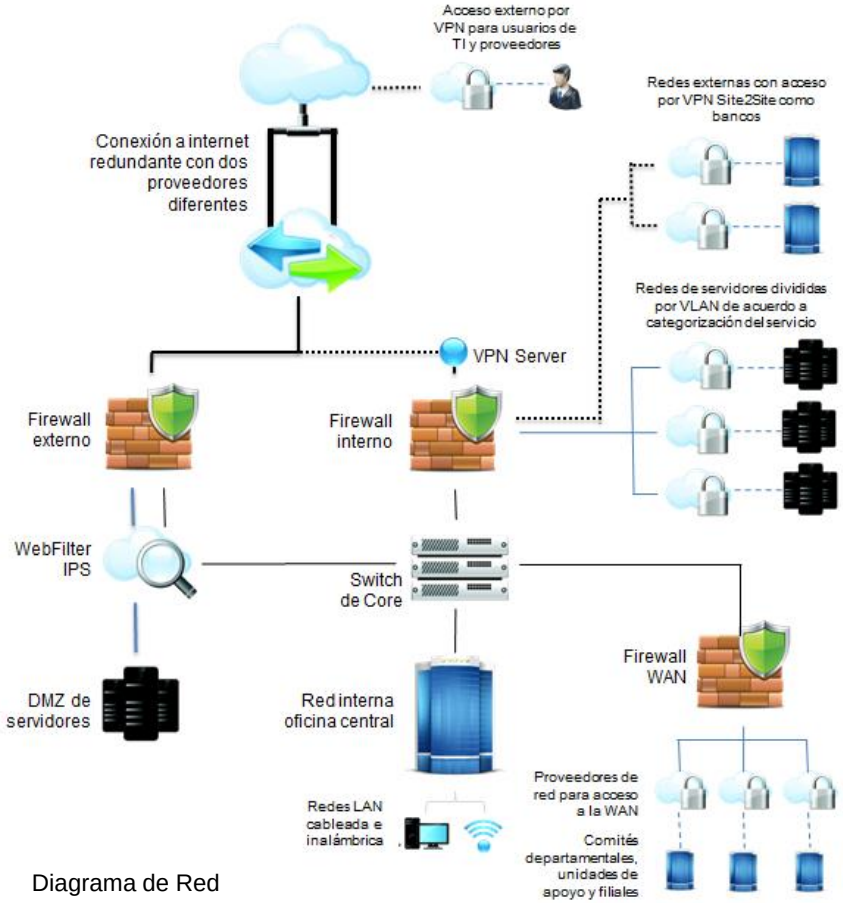


Diagrama de Red

Objetivos generales

- ✓ Crear un Sistema de Gestión de Seguridad de la Información.
- ✓ Integrar los requerimientos especificados en la norma ISO/IEC 27001:2013 al gobierno de TI.
- ✓ Implementar controles de la ISO/IEC 27002:2013 para reducir incidentes.
- ✓ Crear un programa de auditoría del SGSI.
- ✓ Generar confianza en los usuarios.

Justificación del SGSI

La necesidad de reducir la aparición de incidentes o la reacción adecuada y eficiente en caso que ocurran, minimizando así su impacto.

Política de seguridad de la información

La política existente carece de detalles y no contemplaba muchos controles

Estructura organizacional

No se tenían claros los roles ni las responsabilidades. Se requería concienciación de los funcionarios

Recursos necesarios

Esfuerzo en tiempo, personas y dinero no estaba incluido en el gobierno de TI

Controles de protección de los activos de información

Muchos activos carecían de salvaguardas y los sistemas de no estaban alineados a unas políticas de seguridad

Plan de Seguridad de la Información

- ✓ Definición de la política y objetivos de seguridad.
- ✓ Análisis diferencial de la empresa respecto a las de la ISO/IEC 27001:2013 e ISO/IEC 27002:2013.
- ✓ Análisis de riesgos.
- ✓ Selección de salvaguardas/controles de activos de información.
- ✓ Propuesta de proyectos de mejora.

FASE 1: Situación inicial

Objetivos del plan director

Se definieron 11 objetivos específicos para el plan de seguridad

Análisis diferencial

Se realizó la evaluación de estado de la compañía respecto a la norma ISO/IEC 27001 y a los controles recomendados de la ISO/IEC 27002

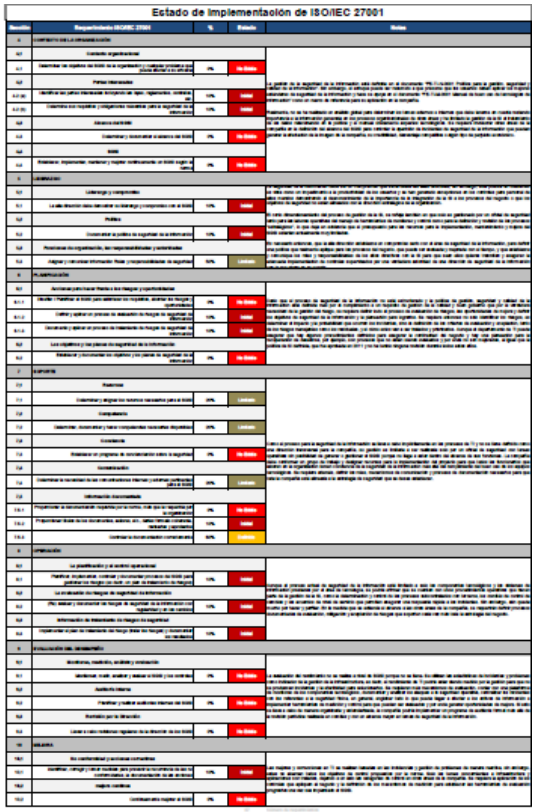
FASE 1: Situación inicial

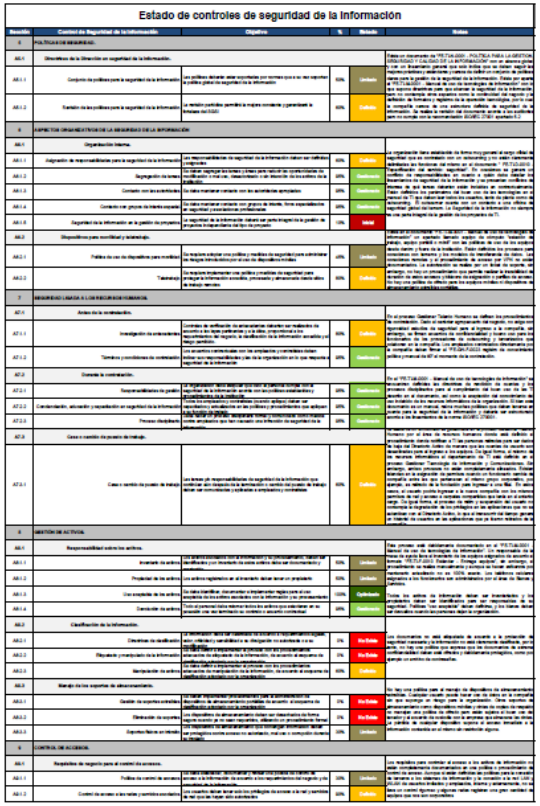
ESTADO		DESCRIPCIÓN	PROPORCIÓN DE CUMPLIMIENTO DE LOS REQUISITOS DEL SGSI	PROPORCIÓN DE CONTROLES POR ESTADO DE IMPLEMENTACIÓN
-	? Desconocido	Aún no ha sido validado	0%	0%
0	No Existe	Ausencia absoluta de una política reconocible, procedimiento, control, etc.	41%	4%
10	Inicial	El desarrollo apenas está iniciando y requerirá una trabajo significativo para cumplir con el requisito	41%	1%
50	Limitado	Progresando muy bien pero aún incompleto	15%	23%
90	Definido	El desarrollo está más o menos completo aunque se carece de detalle y/o aún no se ha implementado, impartido y promovido por la alta dirección	4%	39%
95	Gestionado	El desarrollo está completa, el proceso/control se ha implementado y recientemente comenzó a operar	0%	29%
100	Optimizado	El requisito está completamente cumplido, está funcionando completamente como se esperaba, está siendo monitoreado y mejorado constantemente, y hay evidencia sustancial para demostrarlo en una auditoría	0%	4%
-	No aplicable	TODOS los requisitos en el cuerpo principal de la norma ISO / IEC 27001 son obligatorios SI el SGSI es para ser certificado. De lo contrario, podrían ser ignorados.	0%	0%

Modelo de Madurez de la Capacidad (CMM)

FASE 1: Situación inicial

Anexo A. Análisis GAP de implementación ISOIEC 27001 e ISOIEC 27002





FASE 2: Sistema de Gestión Documental

- Anexo Documental I. GSO-Q-001 Política de Seguridad de la Información.pdf
- Anexo Documental I. GSO-Q-002 Políticas y Normas de Seguridad de la Información.pdf
- Anexo Documental II - Anexo A. GSO-F-001 Formato Programa anual de auditorías.pdf
- Anexo Documental II - Anexo B. GSO-F-002 Formato Plan de auditoria interna.pdf
- Anexo Documental II - Anexo C. GSO-F-003 Formato Informe de auditoría interna del SGSI.pdf
- Anexo Documental II. GSO-P-001 Procedimiento de Gestión de Auditorías Internas.pdf
- Anexo Documental III. GSO-P-002 Procedimiento de Gestión de Indicadores.pdf
- Anexo Documental IV. GSO-P-003 Procedimiento de Gestión de Roles y Responsabilidades.pdf
- Anexo Documental VI. GSO-I-002 Declaración de Aplicabilidad.pdf
- Anexo Documental VII. GSO-I-001 Metodología de Análisis de Riesgos.pdf

FASE 3: Análisis de Riesgos

- ✓ Definición del Nivel de Riesgo Aceptable y riesgo Residual
- ✓ Inventario de activos
- ✓ Valoración de los activos
- ✓ Análisis de amenazas
- ✓ Evaluación del Impacto potencial

Catálogo de activos

Datos	Equipamiento Auxiliar
Servicios de TI	Redes de comunicaciones
Software	Instalaciones
Hardware	Personal
	Soportes de Información

FASE 3: Análisis de Riesgos

Ejecución de la metodología MAGERIT

D5 Archivos del repositorio central				Valor del activo: A															
Código	Tipos de Activos afectados	Amenaza	Frecuencia	Criticidad					Impacto					Riesgo				
				[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[E.1]	[D] [K] [S] [SW] [Media]	Errores de los usuarios	EF	9	8	4			72%	64%	32%			72,00%	64,00%	32,00%		
[E.2]	[D] [K] [S] [SW] [HW] [COM] [Media]	Errores del administrador	MPF	10	1	1			80%	8%	8%			0,24%	0,02%	0,02%		
[E.3]	[D]	Errores de monitorización (log)	F					9					72%					1,15%
[E.4]	[D]	Errores de configuración	MPF		10					80%					0,24%			
[E.14]	[D] [SW] [COM]	Escapes de información	PF			10					80%					0,40%		
[E.15]	[D] [K] [S] [SW] [COM] [Media] [L]	Alteración accidental de la información	MF		8					64%					4,54%			
[E.18]	[D] [K] [S] [SW] [COM] [Media] [L]	Destrucción de información	EF	10					80%					80,00%				
[E.19]	[D] [K] [S] [SW] [COM] [Media] [L] [P]	Fugas de información	PF			8					64%					0,32%		
[A.3]	[D]	Manipulación de los registros de actividad (log)	MPF					9					72%					0,22%
[A.4]	[D]	Manipulación de la configuración	MPF		5	2	9			40%	16%	72%			0,12%	0,05%	0,22%	
[A.5]	[D] [K] [S] [SW] [COM]	Suplantación de la identidad del usuario	MPF		8	8	10			64%	64%	80%			0,19%	0,19%	0,24%	
[A.6]	[D] [K] [S] [SW] [HW] [COM]	Abuso de privilegios de acceso	F	5	5	8			40%	40%	64%			0,64%	0,64%	1,02%		
[A.11]	[D] [K] [S] [SW] [HW] [COM] [Media] [AUX] [L]	Acceso no autorizado	MPF		8	8				64%	64%				0,19%	0,19%		
[A.13]	[S] [D]	Repudio	F					10					80%					1,28%
[A.15]	[D] [K] [S] [SW] [COM] [Media] [L]	Modificación deliberada de la información	MF		8					64%					4,54%			
[A.18]	[D] [K] [S] [SW] [Media] [L]	Destrucción de información	EF	10					80%					80,00%				
[A.19]	[D] [K] [S] [SW] [COM] [Media] [L]	Divulgación de información	PF			6					48%					0,24%		
Totales por dominio:				10	10	10	10	10	80%	80%	80%	80%	80%	80,00%	64,00%	32,00%	0,24%	1,28%

FASE 3: Análisis de Riesgos

Se creó una plantilla para resumir el análisis de Riesgos de todos los activos

Ámbito	Código	Activo	Valor	Criticidad (valor más alto ponderado)					Impacto (calculado con valores ponderados)					Riesgo (calculado con valores ponderados)				
				[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[AUX] Equipamiento Auxiliar	AUX1	Equipamiento de aire acondicionado del datacenter	A	MA	D	D	D	D	A	MB	MB	MB	MB	M	MB	MB	MB	MB
[AUX] Equipamiento Auxiliar	AUX2	Equipamiento contraincendios del datacenter	A	MA	D	D	D	D	A	MB	MB	MB	MB	B	MB	MB	MB	MB
[AUX] Equipamiento Auxiliar	AUX3	Robot de cintas de backup	M	MA	D	MA	D	D	M	MB	MB	MB	MB	B	MB	MB	MB	MB
[AUX] Equipamiento Auxiliar	AUX4	Equipamiento de alimentación eléctrica dual	M	MA	M	D	D	D	M	B	MB	MB	MB	MB	MB	MB	MB	MB
[AUX] Equipamiento Auxiliar	AUX5	Racks	MB	MA	D	D	D	D	MB	MB	MB	MB	MB	MB	MB	MB	MB	MB
[AUX] Equipamiento Auxiliar	AUX6	Cableado	MB	MA	D	A	D	D	MB	MB	MB	MB	MB	MB	MB	MB	MB	MB
[COM] Redes de comunicaciones	COM1	Red telefónica	A	B	M	M	MA	D	MB	B	MB	MB	MB	MB	MB	MB	MB	MB
[COM] Redes de comunicaciones	COM2	Red de datos Local (LAN)	A	MA	M	A	A	D	A	M	MB	MB	MB	M	M	B	B	MB
[COM] Redes de comunicaciones	COM3	Red de datos Corporativa (WAN)	MA	MA	M	B	A	D	MA	M	MB	MB	MB	MA	MB	M	MB	MB
[COM] Redes de comunicaciones	COM4	Red inalámbrica (WLAN)	M	MA	M	A	A	D	M	B	MB	MB	MB	MA	MB	A	A	MB
[COM] Redes de comunicaciones	COM5	Canal de Internet	M	MA	M	A	A	D	M	B	MB	MB	MB	M	MB	A	MB	MB
[D] Datos	D1	Datos de los usuarios para validación de credenciales	M	MA	MA	MA	MA	MA	M	M	MB	MB	MB	A	A	A	A	M
[D] Datos	D2	Registros de pagos a asociados	MA	MA	MA	MA	MA	A	MA	MA	MB	MB	MB	M	M	B	MB	MB
[D] Datos	D3	Mapas geográficos	MA	MA	A	MA	MA	A	MA	A	MB	MB	MB	B	MB	MB	MB	MB
[D] Datos	D4	Correos electrónicos	MA	MA	A	A	M	A	MA	A	MB	MB	MB	M	B	M	B	B
[D] Datos	D5	Archivos del repositorio central	A	MA	MA	MA	MA	MA	A	A	MB	MB	MB	MA	MA	MA	B	A
[D] Datos	D6	Registros de actividades de software	B	MA	MA	MA	MA	MA	B	B	MB	MB	MB	MB	MB	MB	MB	M
[HW] Hardware	HW1	Servidor	A	MA	M	M	D	D	A	B	MB	MB	MB	A	B	B	MB	MB
[HW] Hardware	HW2	Computador personal	MB	MA	M	A	D	D	MB	MB	MB	MB	MB	MB	MB	B	MB	MB
[HW] Hardware	HW3	Computador portátil	MB	MA	M	MA	D	D	MB	MB	MB	MB	MB	MB	MB	MB	MB	MB
[HW] Hardware	HW4	Móviles	MB	MA	M	MA	D	D	MB	MB	MB	MB	MB	MB	MB	MB	MB	MB
[HW] Hardware	HW5	Impresoras	MB	MA	M	MA	D	D	MB	MB	MB	MB	MB	B	MB	MB	MB	MB
[HW] Hardware	HW6	Equipamiento de red	M	MA	M	MA	D	D	M	B	MB	MB	MB	M	MB	M	MB	MB
[HW] Hardware	HW7	Central telefónica	B	MA	M	MA	D	D	B	MB	MB	MB	MB	B	MB	B	MB	MB
[L] Instalaciones	L1	Edificio	MA	MA	B	M	D	D	MA	MB	MB	MB	MB	B	MB	B	MB	MB
[MEDIA] Soportes de información	MEDIA1	Cintas de backup	M	MA	M	MA	D	D	M	B	MB	MB	MB	M	MB	M	MB	MB
[P] Personal	P1	Usuarios externos	M	A	M	A	D	D	M	B	MB	MB	MB	MB	MB	MB	MB	MB
[P] Personal	P2	Usuarios internos	M	A	M	A	D	D	M	B	MB	MB	MB	MB	MB	MB	MB	MB
[P] Personal	P3	Operadores	M	A	M	A	D	D	M	B	MB	MB	MB	M	MB	MB	MB	MB
[P] Personal	P4	Administradores de Infraestructura	A	A	M	A	D	D	A	B	MB	MB	MB	A	MB	B	MB	MB
[P] Personal	P5	Coordinadores	A	A	M	A	D	D	A	B	MB	MB	MB	B	MB	B	MB	MB
[P] Personal	P6	Directivos	MA	A	M	A	D	D	A	M	MB	MB	MB	M	MB	B	MB	MB
[P] Personal	P7	Contratistas	B	A	M	A	D	D	B	MB	MB	MB	MB	MB	MB	MB	MB	MB
[P] Personal	P8	Representantes de proveedores	MB	A	M	A	D	D	MB	MB	MB	MB	MB	MB	MB	MB	MB	MB
[S] Servicios	S1	Servicio de Internet	A	MA	M	M	A	M	A	M	MB	MB	MB	MA	M	B	MB	MB
[S] Servicios	S2	Repositorio de Archivos	M	MA	A	A	A	A	M	M	MB	MB	MB	M	M	M	B	M
[S] Servicios	S3	Páginas web	M	MA	M	M	A	M	M	B	MB	MB	MB	M	M	B	MB	MB
[S] Servicios	S4	Correo electrónico	A	MA	M	M	A	M	A	M	MB	MB	MB	MA	M	B	MB	MB
[S] Servicios	S5	DNS	M	MA	M	M	A	M	M	B	MB	MB	MB	B	MB	MB	MB	MB
[S] Servicios	S6	DHCP	M	MA	M	M	A	M	M	B	MB	MB	MB	MB	MB	MB	MB	MB
[SW] Software	SW1	Aplicativos de Ofimática	MB	MA	M	D	D	D	MB	MB	MB	MB	MB	MB	MB	MB	MB	MB
[SW] Software	SW2	Clientes de correo electrónico	MB	MA	M	D	D	D	MB	MB	MB	MB	MB	MB	MB	MB	MB	MB
[SW] Software	SW3	Sistema de gestión de base de datos	M	MA	MA	B	D	D	M	M	MB	MB	MB	B	MB	MB	MB	MB
[SW] Software	SW4	Sistemas operativos	B	MA	MA	B	D	D	B	B	MB	MB	MB	A	A	B	MB	MB
[SW] Software	SW5	Gestor de máquinas virtuales	M	MA	MA	B	D	D	M	M	MB	MB	MB	MB	MB	MB	MB	MB
[SW] Software	SW6	Sistema de gestión de backups	M	MA	MA	B	D	D	M	M	MB	MB	MB	B	B	MB	MB	MB
[SW] Software	SW7	Sistema de referenciación geográfica	MA	A	A	B	D	D	A	A	MB	MB	MB	B	MB	MB	MB	MB
[SW] Software	SW8	Sistema de gestión de pagos a asociados	A	A	A	B	D	D	A	A	MB	MB	MB	MB	MB	MB	MB	MB

FASE 3: Análisis de Riesgos

Los activos de información con las fallas más altas inducen la creación de proyectos enfocados en mitigar el riesgo

Ámbito	Código	Activo	Riesgo (calculado con valores ponderados)				
			[D	[I	[C	[A	[T
[COM] Redes de comunicaciones	COM3	Red de datos Corporativa (WAN)	MA	MB	M	MB	MB
[COM] Redes de comunicaciones	COM4	Red Inalámbrica (WLAN)	MA	MB	A	A	MB
[D] Datos	D1	Datos de los usuarios para validación de credenciales	A	A	A	A	M
[D] Datos	D5	Archivos del repositorio central	MA	MA	MA	B	A
[HW] Hardware	HW1	Servidor	A	B	B	MB	MB
[P] Personal	P4	Administradores de infraestructura	A	MB	B	MB	MB
[S] Servicios	S1	Servicio de Internet	MA	M	B	MB	MB
[S] Servicios	S4	Correo electrónico	MA	M	B	MB	MB
[SW] Software	SW4	Sistemas operativos	A	A	B	MB	MB

Se documentaron 29 recomendaciones de mejora de acuerdo al análisis de riesgos realizado y el nivel de riesgo aceptable definido por la organización para el plan de implementación, iniciando con los tratamientos de riesgos Altos y Muy Alto.

FASE 4: Propuestas de Proyectos

Código y Nombre		Impacto	Prioridad	Objetivo General	Fecha de ejecución
PRJ 01	Mejoramiento de los canales de internet	Alto	Baja	Acondicionar los canales de red de datos de la WAN e Internet con las velocidades adecuadas para la operación del negocio.	Enero
PRJ 02	Optimización de la red inalámbrica	Alto	Alta	Corregir las fallas de funcionamiento e implementar los mecanismos de control que aseguren su buen uso.	Enero - Julio
PRJ 03	Optimización del servicio de carpetas compartidas	Medio	Media	Mejorar las prácticas de seguridad de la información en el servicio de carpetas compartidas.	Enero - Mayo

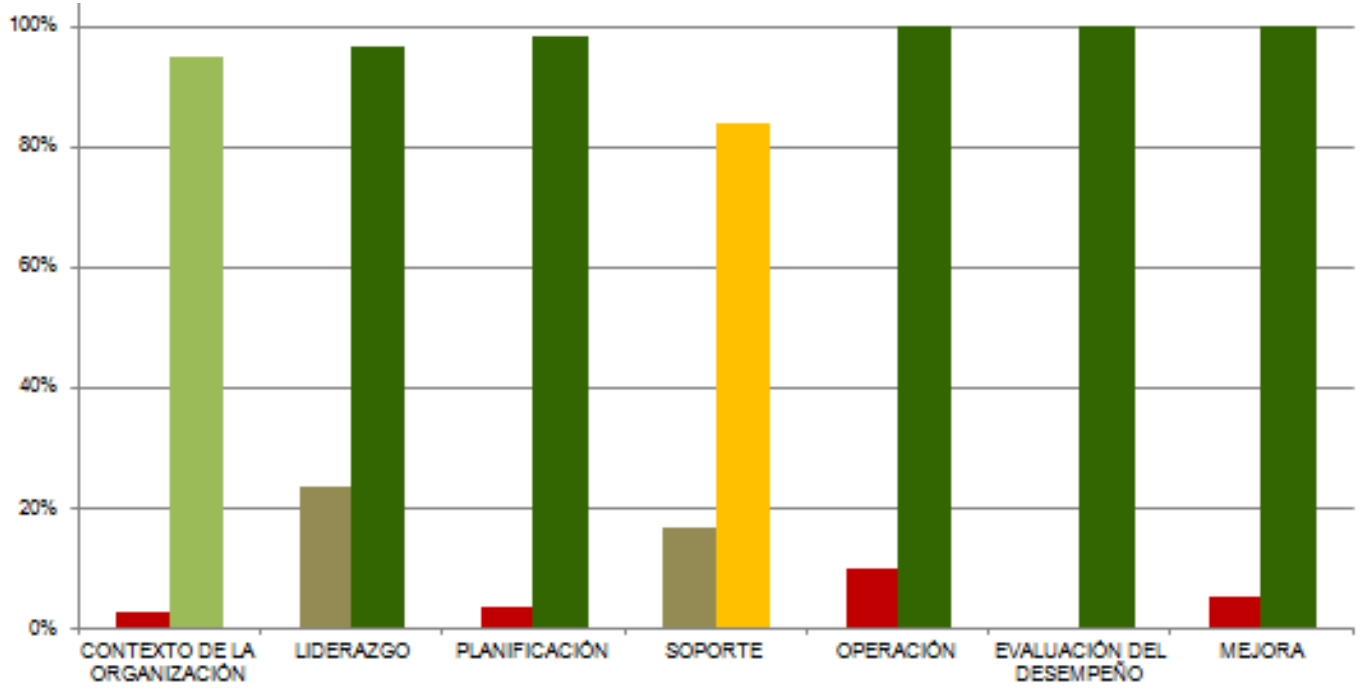
FASE 4: Propuestas de Proyectos

Código y Nombre		Impacto	Prioridad	Objetivo General	Fecha de ejecución
PRJ 04	Optimización del servicio de correo electrónico	Alto	Alta	Mejorar el servicio de correo electrónico	Enero - Julio
PRJ 05	Depuración de los Directorios de Autenticación de usuarios	Bajo	Media	Mejorar las prácticas de seguridad de la información en los servicios de Directorios de autenticación LDAP y Active Directory	Enero - Mayo
PRJ 06	Mejoramiento de los servidores	Alto	Media	Actualizar el hardware y sistemas operativos de los servidores	Enero - Noviembre
PRJ 07	Conformación de equipos de apoyo de administradores de infraestructura	Medio	Alta	Creación de los equipos de apoyo de los administradores de infraestructura	Enero - Febrero

FASE 4: Propuestas de Proyectos

Código y Nombre		Impacto	Prioridad	Objetivo General	Fecha de ejecución
PRJ 08	Aseguramiento de los equipos de usuario	Medio	Media	Mejorar las prácticas de seguridad de la información en los equipos de usuario asignados	Enero - Abril
PRJ 09	Alta disponibilidad de los servicios críticos para la Institución	Medio	Alta	Tener alta disponibilidad de los servicios críticos para la operación del negocio	Enero - Mayo
PRJ 10	Implementación de mejores prácticas de seguridad de la información relacionada con datacenters	Bajo	Baja	Mejorar las prácticas de seguridad de la información en la administración del centro de cómputo	Junio

FASE 5: Auditoría de Cumplimiento

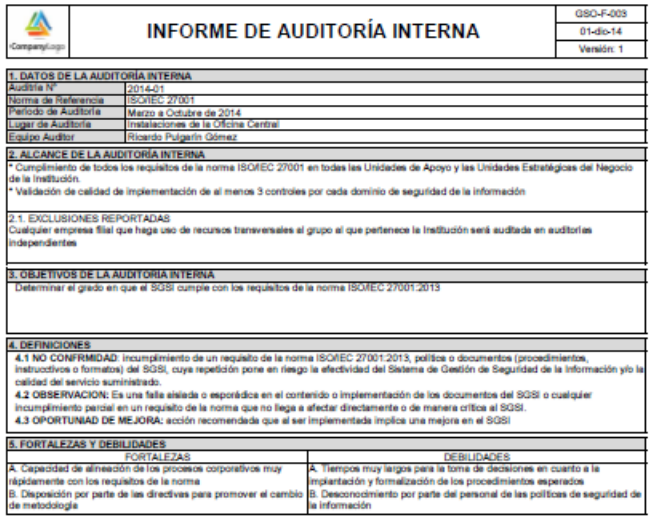


Comparación de porcentaje de implementación de controles antes y después del proyecto

FASE 5: Auditoría de Cumplimiento

Se generó un documento con el resultado de la auditoría interna. Se documentaron 15 No Conformidades

Anexo Documental II - Anexo C. GSO-F-003 Formato Informe de auditoría interna del SGSI



	INFORME DE AUDITORÍA INTERNA	GSO-F-003
CompanyLogo		01-dic-14
		Versión: 1

1. DATOS DE LA AUDITORÍA INTERNA	
Auditría N°	2014-01
Norma de Referencia	ISO/IEC 27001
Periodo de Auditoría	Marzo a Octubre de 2014
Lugar de Auditoría	Instalaciones de la Oficina Central
Equipo Auditor	Ricardo Pulgarín Gómez

2. ALCANCE DE LA AUDITORÍA INTERNA

* Cumplimiento de todos los requisitos de la norma ISO/IEC 27001 en todas las Unidades de Apoyo y las Unidades Estratégicas del Negocio de la Institución.
* Validación de calidad de implementación de al menos 3 controles por cada dominio de seguridad de la información

2.1. EXCLUSIONES REPORTADAS

Cualquier empresa filial que haga uso de recursos transversales al grupo al que pertenece la Institución será auditada en auditorías independientes

3. OBJETIVOS DE LA AUDITORÍA INTERNA

Determinar el grado en que el SGSI cumple con los requisitos de la norma ISO/IEC 27001:2013

4. DEFINICIONES

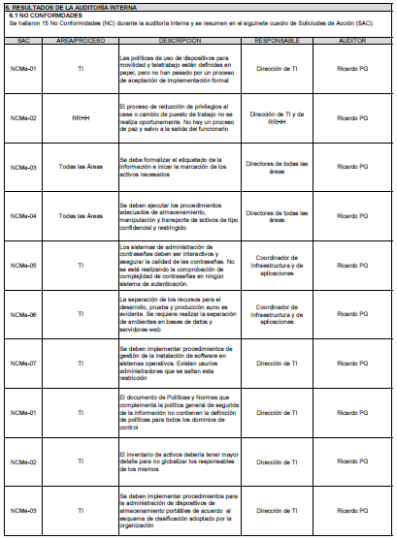
4.1 NO CONFIRMIDAD: Incumplimiento de un requisito de la norma ISO/IEC 27001:2013, política o documentos (procedimientos, instructivos o formatos) del SGSI, cuya repetición pone en riesgo la efectividad del Sistema de Gestión de Seguridad de la Información y/o la calidad del servicio suministrado.

4.2 OBSERVACION: Es una falla aislada o esporádica en el contenido o implementación de los documentos del SGSI o cualquier incumplimiento parcial en un requisito de la norma que no llega a afectar directamente o de manera crítica al SGSI.

4.3 OPORTUNIAD DE MEJORA: acción recomendada que al ser implementada implica una mejora en el SGSI

5. FORTALEZAS Y DEBILIDADES

FORTALEZAS	DEBILIDADES
A. Capacidad de alineación de los procesos corporativos muy rápidamente con los requisitos de la norma B. Disposición por parte de las directivas para promover el cambio de metodología	A. Tiempos muy largos para la toma de decisiones en cuanto a la implantación y formalización de los procedimientos esperados B. Desconocimiento por parte del personal de las políticas de seguridad de la información



6. RESULTADOS DE LA AUDITORÍA INTERNA

6.1 NO CONFORMIDADES

Se hallaron 15 No Conformidades (NC) durante la auditoría interna y se resumen en el siguiente cuadro de Solicitudes de Acción (SAC):

SAC	AREA/PROCESO	DESCRIPCION	RESPONSABLE	AUDITOR
NCMe-01	TI	Las políticas de uso de dispositivos para movilidad y teletrabajo están definidas en papel, pero no han pasado por un proceso de aceptación de implementación formal	Dirección de TI	Ricardo PG
NCMe-02	RRHH	El proceso de reducción de privilegios al cese o cambio de puesto de trabajo no se realiza oportunamente. No hay un proceso de pacy salvo a la salida del funcionario	Dirección de TI y de RRHH	Ricardo PG
NCMe-03	Todas las Áreas	Se debe formalizar el etiquetado de la información e iniciar la marcación de los activos necesarios	Directores de todas las áreas	Ricardo PG
NCMe-04	Todas las Áreas	Se deben ejecutar los procedimientos adecuados de almacenamiento, manipulación y transporte de activos de tipo confidencial y restringido	Directores de todas las áreas	Ricardo PG
NCMe-05	TI	Los sistemas de administración de contraseñas deben ser interactivos y asegurar la calidad de las contraseñas. No se está realizando la comprobación de complejidad de contraseñas en ningún sistema de autenticación	Coordinador de Infraestructura y de aplicaciones	Ricardo PG
NCMe-06	TI	La separación de los recursos para el desarrollo, prueba y producción aunq es evidente. Se requiere realizar la separación de ambientes en bases de datos y servidores web	Coordinador de Infraestructura y de aplicaciones	Ricardo PG
NCMe-07	TI	Se deben implementar procedimientos de gestión de la instalación de software en sistemas operativos. Existen usurios administradores que se saltan esta restricción	Dirección de TI	Ricardo PG
NCMe-01	TI	El documento de Políticas y Normas que complementa la política general de seguridad de la información no contienen la definición de políticas para todos los dominios de control	Dirección de TI	Ricardo PG
NCMe-02	TI	El inventario de activos debería tener mayor detalle para no globalizar los responsables de los mismos	Dirección de TI	Ricardo PG
NCMe-03	TI	Se deben implementar procedimientos para la administración de dispositivos de almacenamiento portátiles de acuerdo al esquema de clasificación adoptado por la organización	Dirección de TI	Ricardo PG

FASE 6: Informes de resultados

- ✓ Resumen ejecutivo
- ✓ Resumen de implementación de controles
- ✓ Informe de resultados
- ✓ Programa de concienciación a los usuarios

¡Gracias!