Elaboración de un Plan de Implementación de la ISO/IEC 27001:2005

Tutor: Antonio José Segovia

TABLA DE CONTENIDO

1. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

1.1 INTRODUCCION

Debido a los avances en las tecnologías, en los sistemas de información, las telecomunicaciones y la evolución de la sociedad de la información, las organizaciones se ven expuestas a riesgos que deben ser mitigados, tratados o trasferidos, por lo tanto la implementación de un sistema de gestión de seguridad de la información (SGSI), basados en la norma ISO 27001:2005, ISO 27002:2005, va a permitir a la entidad financiera proteger y asegurar el activo más importante: "la información", ayudar a la continuidad del negocio y controlar las debilidades detectadas en el negocio. Un SGSI Ayuda a conseguir los objetivos de la organización y reducir paulatinamente los riesgos a los que la organización se enfrente.
El siguiente trabajo fue realizado en una entidad financiera, de la ciudad de Cali, a la cual se realizó un diagnóstico inicial o análisis GAP, evaluando el nivel de cumplimiento de los requerimientos y controles enunciados en la norma ISO/IEC 27001:2005 e ISO/IEC 27002:2005, con el fin de trabajar en los aspectos más débiles y fortalecer los demás, en proceso de mejoramiento continuo.

1.2 CONOCIENDO LA ISO – 27001 / ISO – 27002 [1]

ISO 27001: Contiene los requisitos para la implantación de un sistema de gestión de seguridad de la información y define la forma de gestionar la seguridad de la información en cualquier tipo de organización. Un sistema de gestión de este tipo, igual que las normas ISO 9001o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada), es una norma en la que se pueden certificar las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005.

ISO 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios:
Estas normas están asociadas con otras normas de la familia ISO, tales como 27005, 27003, 27031, 9001, 14001 entre otras.

1.2.1 CUADRO COMPARATIVO ISO-27001:2005 VS ISO-27001:2013

ISO 27001:2013	ISO 27001:2005
4. Contexto de la Organización	
4.1 Conocimiento de la Organización y de su contexto	

[1] http://www.iso27000.es/iso27000.html

4.2 Comprensión de las necesidades y expectativas de las partes interesadas	
4.3 Determinación del alcance del SGSI	4.2.1 Establecimiento del SGSI
4.4 Sistema de Gestión de Seguridad de la Información	4.1 Requisitos Generales
5. Liderazgo	
5.1 Liderazgo y Compromiso	5.1 Compromiso de la Dirección
5.2 Política	4.2.1 Establecimiento del SGSI
5.3 Roles, Responsabilidades y Autoridades en la Organización	
6. Planificación	
6.1 Acciones para tratar Riesgos y Oportunidades	4.2.1 Establecimiento del SGSI 4.2.2 Implementación y operación del SGSI 4.2.3 Seguimiento y revisión del SGSI
6.1.1 Generalidades	
6.1.2 Evaluación de Riesgos de la Seguridad de la Información	
6.1.3 Tratamiento de Riesgos de la Seguridad de la Información	
6.2 Objetivos de Seguridad de información y Planeas para Lograrlos.	
6.1 Acciones para tratar Riesgos y Oportunidades	
7. Soporte	
7.1 Recursos	5.2.1 Provisión de Recursos
7.2 Competencia	5.2.2 Formación, toma de conciencia y competencia
7.3 Toma de Conciencia	
7.4 Comunicación	
7.5 Información Documentada	4.3.1 Generalidades 4.3.2 Control de Documentos 4.3.3 Control de Registros
7.5.1 Generalidades	
7.5.2 Creación y Actualización	
7.5.3 Control de la información documentada	
8. Operación	
8.1 Planificación y Control Operacional	4.2.1 Establecimiento del SGSI 4.2.2 Implementación y operación del SGSI 4.2.3 Seguimiento y revisión del SGSI
8.2 Evaluación de riesgos de la Seguridad de la Información	
8.3 Tratamiento de Riesgos de la Seguridad de la Información	
9. Evaluación del Desempeño	
9.1 Seguimiento, Medición, Análisis y Evaluación	
9.2 Auditorías Internas	6. Auditorías Internas
9.3 Revisión por la Dirección	7.1 Generalidades 7.2 Información para la revisión
10. Mejora	
10.1 No Conformidades y Acciones Correctivas	4.2.4 Mantenimiento y mejora del SGSI 8.2 Acción Correctiva 8.3 Acción Preventiva
10.2 Mejora Continua	8.1 Mejora Continua

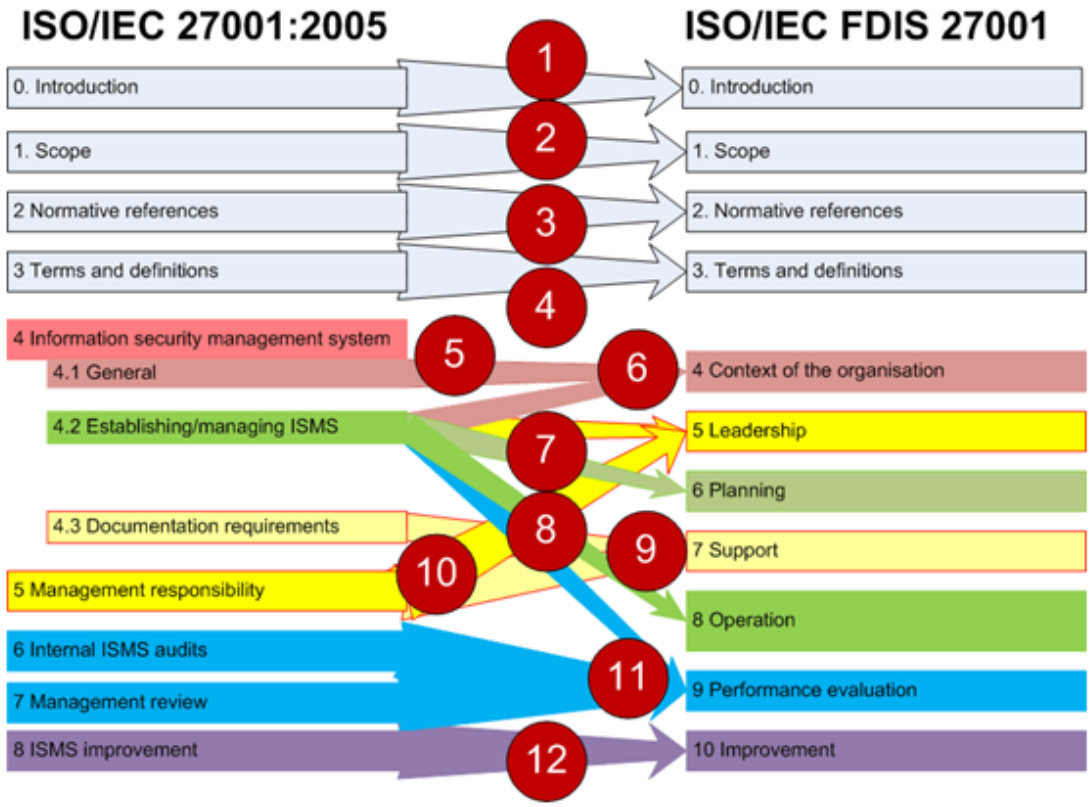


Figura 1. Cuadro comparativo

1.2.2 CUADRO COMPARATIVO ISO–27002:2005 VS ISO–27002:2013

ISO 27002:2013	ISO 27002:2005
A.5. Políticas de la Seguridad de la Información	
A.5.1. Orientación de la dirección para la Gestión de Seguridad de la Información.	
A.5.1.1. Políticas para la Seguridad de la Información	A.5.1.1. Información de documento de Política de Seguridad
A.5.1.2. Revisión de las Políticas para seguridad de la información	A.5.1.2. Revisión de la Política de Seguridad de la Información
A.6. Organización de la Seguridad de la Información	
A.6.1. Organización Interna	
A.6.1.1. Seguridad e la información Roles y Responsabilidades	A.6.1.3. Asignación de responsabilidades de seguridad de la información
	A.8.1.1. Roles y Responsabilidades
A.6.1.2. Separación de deberes - Funciones	A.10.1.3. Segregación de Funciones
A.6.1.3. Contacto con las autoridades	A.6.1.4. Contacto con las autoridades
A.6.1.4. Contacto con grupos de interés Especial	A.6.1.7. Contacto con grupos de Interés

A.6.1.5. Seguridad de la información en gestión de Proyectos	
A.6.2. Dispositivos Móviles y Teletrabajo	
A.6.2.1. Política para dispositivos móviles	A.11.7.1. Información móvil y las comunicaciones
A.6.2.2. Teletrabajo	A.11.7.2. Teletrabajo
A.7. Seguridad de los Recursos Humanos	
A.7.1. Antes de Asumir el empleo	
A.7.1.1. Selección	A.8.1.1. Selección
A.7.1.2. Términos y condiciones del empleo	A.8.1.2. Términos y condiciones de empleo
A.7.2. Durante la ejecución del Empleo	
A.7.2.1. Responsabilidades de la Dirección	A.8.2.1. Responsabilidades de la Dirección
A.7.2.2. Toma de Conciencia, educación y formación en la Seguridad de la información	A.8.2.2. Toma de Conciencia, educación y formación en la Seguridad de la información
A.7.2.3. Proceso Disciplinario	A.8.2.3. Procesos Disciplinario
A.7.3. Terminación y Cambio de Empleo	
A.7.3.1. Terminación o Cambio de responsabilidades de empleo	A.8.3.1. Responsabilidades de terminación
A.8. Gestión de Activos	
A.8.1. Responsabilidad por los activos	
A.8.1.1. Inventario de activos	A.7.1.1 Inventario de Activos
A.8.1.2. Propiedad de los Activos	A.7.1.2. Propiedad de los Activos
A.8.1.3. Uso aceptable de los Activos	A.7.1.3. Uso aceptable de los activos
A.8.1.4. Devolución de los Activos	A.8.3.2. Devolución de los activos
A.8.2. Clasificación de la información	
A.8.2.1. Clasificación de la información	A.7.2.1. Directrices de Clasificación
A.8.2.2. Etiquetado de la información	A.7.2.2. Etiquetado y manejo de la información
A.8.2.3. Manejo de Activos	A.10.7.3. Procedimientos de tratamiento de la información
A.8.3. Manejo de medios de soporte	
A.8.3.1. Gestión de medios de soporte removibles	A.10.7.1. Gestión de soportes extraíbles
A.8.3.2. Disposición de los medios de soporte	A.10.7.2. Eliminación de los medios de comunicación
A.8.3.3. Transferencia de medios de soporte físico	A.10.8.3 Medios físicos en Tránsito
A.9. Control de Acceso	
A.9.1. Requisitos del negocio para control de acceso	
A.9.1.1. Política de control de acceso	A.11.1.1. Política de control de acceso
A.9.1.2. Acceso a redes y a servicios en red	A.11.4.1. Política sobre el uso de los servicios de red
A.9.2. Gestión de acceso de usuarios.	
A.9.2.1. Registro y cancelación de registro de	A.8.3.3. Eliminación de los derechos de acceso

usuarios	
A.9.2.2. Suministro de acceso de usuarios	A.11.2.2. Gestión de Privilegios
A.9.2.3. Gestión de derechos de acceso privilegiado	
A.9.2.4. Gestión de Información de Autenticación secreta de usuarios	A.11.2.3. Gestión de Contraseñas de Usuario
A.9.2.5. Revisión de los derechos de acceso de usuarios	A.11.2.4. Revisión de los derechos de acceso de usuarios
A.9.2.6. Cancelación o ajuste de los derechos de acceso	A.8.3.3. Eliminación de los derechos de acceso
A.9.3. Responsabilidades de los usuarios	
A.9.3.1. Uso de información de autenticación secreta	A.11.3.1. Uso de Contraseña
A.9.4. Control de Acceso a Sistemas y Aplicaciones	
A.9.4.1. Restricción de acceso a información	A.11.6.1. Información restricción de acceso
A.9.4.2. Procedimiento de conexión segura	A.11.5.1. Procedimientos de inicio de sesión seguros A.11.5.5. Sesión de tiempo de espera A.11.5.6. Limitación del tiempo de conexión
A.9.4.3. Sistema de gestión de contraseñas	A.11.5.3. Sistema de Gestión de Contraseña
A.9.4.4. Uso de Programas utilitarios privilegiados	A.11.5.4. Uso de utilidades del sistema
A.9.4.5. Control de Acceso a Códigos fuente de programas	A.12.4.3. Control de acceso al código fuente del programa
A.10. Criptografía	
A.10.1. Controles Criptográficos	
A.10.1.1. Política sobre el uso de controles criptográficos	A.12.3.1. Política sobre el uso de controles criptográficos
A.10.1.2. Gestión de Claves	A.12.3.2. Gestión de Claves
A.11. Seguridad Física y del Ambiente	
A.11.1. Áreas Seguras	
A.11.1.1. Perímetro de seguridad física	A.9.1..1. Perímetro de Seguridad Física
A.11.1.2. Controles físicos de entrada	A.9.1.2. Controles de entrada físicas
A.11.1.3. Seguridad de oficinas, salones e instalaciones	A.9.1.3. Seguridad de oficinas, recintos e instalaciones
A.11.1.4. Protección contra amenazas externas y ambientales	A.9.1.4. Protección contra amenazas externas y ambientales
A.11.1.5. Trabajo en áreas seguras	A.9.1.5. Trabajo en áreas seguras
A.11.1.6. Áreas de despacho y carga	A.9.1.6 Áreas de Acceso público, de entrega y carga
A.11.2. Equipos	
A.11.2.1. Ubicación y protección de los equipos	A.9.2.1. Ubicación y protección de los equipos
A.11.2.2. Servicios públicos de soporte	A.9.2.2. Suministro de energía
A.11.2.3. Seguridad del cableado	A.9.2.3. Seguridad del cableado
A.11.2.4. Mantenimiento de equipos	A.9.2.4. Mantenimiento de equipos
A.11.2.5. Retiro de activos	A.9.2.7. Retiro de activos

A.11.2.6. Seguridad de equipos y activos fuera del predio	A.9.2.5. Seguridad de los equipos fuera de las instalaciones
A.11.2.7. Disposición segura o reutilización de equipos	A.9.2.6. Seguridad en la reutilización o eliminación de equipos
A.11.2.8. Equipos sin supervisión de los usuarios	A.11.3.2. Equipo de usuario desatendido
A.11.2.9. Política de escritorio limpio y pantalla limpia	A.11.3.3. Política de escritorio despejado y pantalla despejada
A.12. Seguridad de las Operaciones	
A.12.1. Procedimientos Operacionales y responsabilidades	
A.12.1.1. Procedimientos de operación documentados	A.10.1.1. Documentación de los procesos de operación
A.12.1.2. Gestión de Cambios	A.10.1.2. Gestión del Cambio
A.12.1.3. Gestión de Capacidad	A.10.3.1. Gestión de Capacidad
A.12.1.4. Separación de los ambientes de desarrollo, ensayo y operación	A.10.1.4. Separación de las instalaciones de desarrollo, prueba y operación
A.12.2. Protección contra códigos maliciosos	
A.12.2.1. Controles contra códigos maliciosos	A.10.4.1. Controles contra códigos maliciosos
A.12.3. Copias de Respaldo.	
A.12.3.1. Copias de respaldo de la información	A.10.5.1. Información de respaldo
A.12.4. Registro y seguimiento	
A.12.4.1. Registro de eventos	A.10.10.1. Registro de auditorías
A.12.4.2. Protección de la información de registro	A.10.10.3. Protección de la información del registro
A.12.4.3. Registros del administrador y del operador	A.10.10.3. Protección de la información del registro
A.12.4.4. Sincronización de relojes	A.10.10.4. Registros del Administrador y del Operador
A.12.5. Control de Software Operacional	A.10.10.6. Sincronización de relojes
A.12.5.1. Instalación de software en Sistemas Operativos	
A.12.6. Gestión de la vulnerabilidad técnica	A.12.4.1. Control del Software Operativo
A.12.6.1. Gestión de las vulnerabilidades técnicas	
A.12.6.2. Restricciones sobre la instalación de Software	A.12.6.1. Control de las vulnerabilidades técnicas
A.12.7. Consideraciones sobre auditorias de sistemas de información	
A.12.7.1. Controles sobre auditorias de sistemas de información	
A.13. Seguridad de las comunicaciones	A.15.3.1. Controles de auditoría de los sistemas de información
A.13.1. Gestión de la seguridad de redes	
A.13.1.1. Controles de redes	
A.13.1.2. Seguridad de los servicios de red	A.10.6.1. Controles de red
A.13.1.3. Separación en las redes	A.10.6.2. Seguridad de los servicios de red

A.13.2. Transferencia de información	A.11.4.5. Separación en las redes
A.13.2.1. Políticas y procedimientos de transferencia de información	
A.13.2.2. Acuerdos sobre transferencia de información	A.10.8.1. Políticas y Procedimientos de intercambio de información
A.13.2.3. Mensajes Electrónicos	A.10.8.2. Acuerdos de intercambio
A.14. Adquisición, desarrollo y mantenimiento de sistemas	
A.14.1. Requisitos de seguridad de los sistemas de información	
A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	A.12.1.1. Análisis y especificación de los requisitos de seguridad
A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas	A.10.9.1. Comercio electrónico A.10.9.3. Información pública
A.14.1.3. Protección de transacciones de servicios de aplicaciones	A.10.9.2. Transacciones en línea
A.14.2. Seguridad en los procesos de desarrollo y de soporte	
A.14.2.1. Política de desarrollo seguro	
A.14.2.2. Procedimientos de control de cambios en sistemas	A.12.5.1. Procedimientos de control de cambios
A.14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	A.12.5.2. Revisión técnica de las aplicaciones después de los cambios en el sistema operativo
A.14.2.4. Restricciones sobre cambios en los paquetes de Software	A.12.5.3. Restricciones en los cambios en los paquetes de software
A.14.2.5. Principios de construcción de sistemas seguros	
A.14.2.6. Ambiente de desarrollo seguro	
A.14.2.7. Desarrollo contratado externamente	A.12.5.5. Desarrollo de Software contratado externamente
A.14.2.8. Pruebas de seguridad de sistemas	
A.14.2.9. Pruebas de aceptación de sistemas	A.10.3.2. Aceptación de Sistemas
A.15. Relaciones con los proveedores	
A.15.1. Seguridad de la información en las relaciones con los proveedores	
A.15.1.1. Política de seguridad de la información para las relaciones con proveedores	A.6.2.3. Consideraciones de la Seguridad en los acuerdos con terceras partes
A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	A.6.2.3. Consideraciones de la Seguridad en los acuerdos con terceras partes
A.15.1.3. Cadena de suministro de tecnología de información y comunicación	
A.15.2. Gestión de la prestación de servicios de proveedores	
A.15.2.1. Seguimiento y revisión de los servicios de los proveedores	
A.15.2.2. Gestión de cambios en los servicios de los proveedores	
A.16. Gestión de incidentes de seguridad de la	A.10.2.2. Monitoreo y revisión de los servicios

información	de terceros
A.16.1. Gestión de incidentes y mejoras en la seguridad de la información	A.10.2.3. Gestión de cambios en los servicios de terceros
A.16.1.1. Responsabilidades y procedimientos	
A.16.1.2. Informe de eventos de seguridad de la información	
A.16.1.3. Informe de debilidades de seguridad de la información	A.13.2.1. Responsabilidades y Procedimientos
A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	A.13.1.1. Reporte sobre los eventos de seguridad de información
A.16.1.5. Respuesta a incidentes de seguridad de la información	A.13.1.2. Reporte sobre las debilidades de la seguridad.
A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información	
A.16.1.7. Recolección de Evidencia	
A.17. Aspectos de seguridad de la información de la gestión de continuidad del negocio	A.13.2.2. Aprendiendo de los incidentes de seguridad de la información
A.17.1. Continuidad de la seguridad de la información	A.13.2.3. Recolección de evidencia
A.17.1.1. Planificación de la continuidad de la seguridad de la información	
A.17.1.2. Implementación de la continuidad de la seguridad de la información	
A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	A.14.1.2. Continuidad del negocio y evaluación de riesgos
A.17.2. Redundancias	
A.17.2.1. Disponibilidad de instalaciones de procesamiento de información	A.14.1.5. Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio
A.18. Cumplimiento	
A.18.1. Cumplimiento de requisitos legales y contractuales	
A.18.1.1. Identificación de los requisitos de legislación y contractuales aplicables	A.15.1.1. Identificación de la legislación aplicable
A.18.1.2. Derechos de propiedad intelectual	A.15.1.2. Derechos de Propiedad Intelectual
A.18.1.3. Protección de los registros	A.15.1.3. Protección de los registros de la organización
A.18.1.4. Privacidad y protección de información identificable personalmente	A.15.1.4. Protección de los datos y privacidad de la información personal
A.18.1.5. Reglamentación de controles criptográficos	A.15.1.6. Reglamentación de los controles criptográficos
A.18.2. Revisiones de seguridad de la información	
A.18.2.1. Revisión independiente de la seguridad de la información	A.6.1.8. Revisión independiente de la Seguridad de la Información
A.18.2.2. Cumplimiento con las políticas y normas de seguridad	A.15.2.1. Cumplimiento con las políticas y normas de seguridad
A.18.2.3. Revisión del cumplimiento técnico	A.15.2.2. Comprobación de cumplimiento Técnico

1.2.3 CAMBIOS NORMA ISO 27002 CONTROLES ELIMINADOS

Control	Descripción 2005	Cambia 2013 Por	Incluye los controles de la ISO 27001:2005
A.6.1.1	Compromiso de la dirección con la seguridad de la información.	Seguridad de la Información Roles y Responsabilidades	**A.6.1.3** Asignación de responsabilidades para la seguridad de la información. **A.8.1.1** Roles y responsabilidades
A.6.1.2	Coordinación de la seguridad de la información.	Separación de deberes	**A.10.1.3** Separación de Funciones
A.6.1.3	Asignación de responsabilidades para la seguridad de la información.	Contacto con autoridades	**A.6.1.6** Contacto con las autoridades
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información.	Contacto con grupos de interés especial	**A.6.1.7** Contacto con grupos de interés especial
A.6.1.5	Acuerdos sobre la Confidencialidad	Seguridad de la información en la gestión de proyectos	
A.6.2.1	Identificación de riesgos relacionados con partes externas	Política de dispositivo móvil	**A.11.7.1** Computación y comunicaciones móviles.
A.6.2.2	Consideraciones de la seguridad cuando se trata con los clientes	Teletrabajo	**A.11.7.2** Trabajo remoto.
A.10.2.1	Prestación del servicio	N.A.	
A.10.7.4	Seguridad de la documentación del sistema.	N.A.	
A.10.8.5	Sistemas de información del negocio.	N.A.	
A.10.10.2	Monitoreo del uso del sistema	N.A.	
A.10.10.5	Registro de fallas	N.A.	
Control	Descripción 2005	Cambia 2013 Por	Incluye los controles de la ISO 27001:2005
A.11.4.2	Autenticación de usuarios para conexiones externas.	N.A.	
A.11.4.3	Identificación de los equipos en las redes.	N.A.	
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	N.A.	

A.11.4.6	Control de conexión a las redes.	N.A.	
A.11.6.2	Aislamiento de sistemas sensibles.	N.A.	
A.12.2.1	Validación de los datos de entrada.	Controles contra códigos maliciosos.	A.10.4.1 Controles contra códigos maliciosos.
A.12.2.2	Control de procesamiento interno.	N.A.	
A.12.2.3	Integridad del mensaje.	N.A.	
A.12.2.4	Validación de datos de salida	N.A.	
A.12.5.4	Fuga de información	N.A.	
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de Información.	N.A.	
A.15.3.2	Protección de las herramientas de auditoría de sistemas de información	N.A.	
A.6.1.5	Seguridad de la información en la gestión de proyectos		

1.2.4 CAMBIOS NORMA ISO 27002 NUEVOS CONTROLES

Control	Descripción 2013	Absorbe los controles de la ISO 27001:2005
A.6.1.5	Seguridad de la información en la gestión de proyectos	
A.12.6.2	Restricciones en la instalación de software	
A.14.2.1	Política de desarrollo de seguridad	
A.14.2.5	Principios de construcción de sistemas de seguros	
A.14.2.6	Ambiente de desarrollo seguro	
A.14.2.8	Pruebas de seguridad de sistemas	
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	**A.6.2.3** Consideraciones de la seguridad en los acuerdos con terceras partes
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	

A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	
A.16.1.5	Respuesta a incidentes de seguridad de la información	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	

1.3 CONTEXTUALIZACION

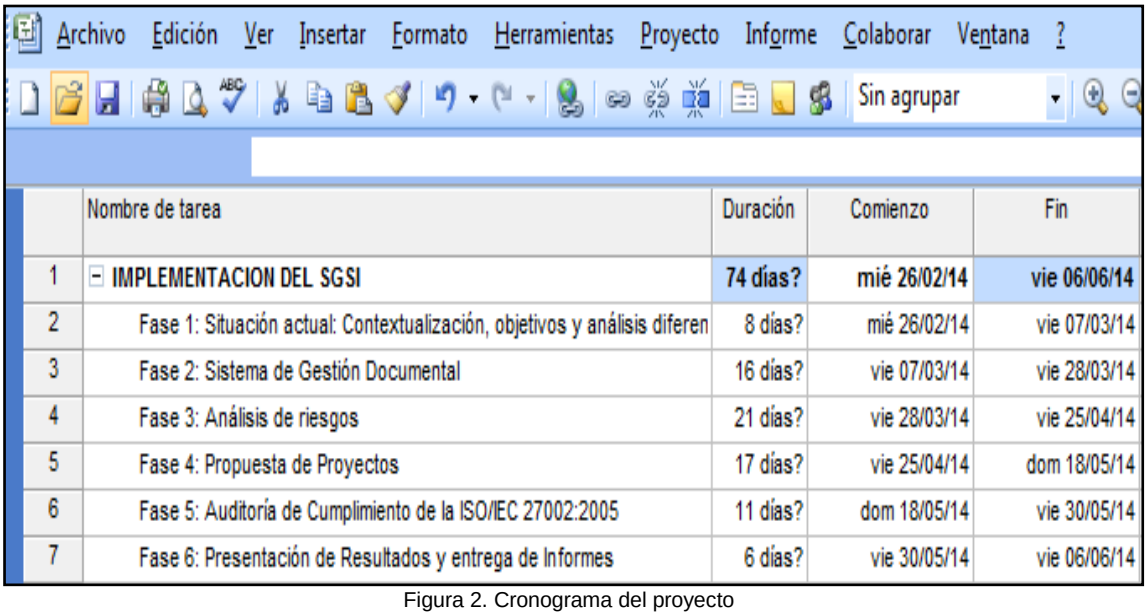
La empresa seleccionada para realizar el plan de Implementación de la norma ISO/IEC 27001:2005, es una entidad financiera, que denominaremos "AHORRAYA" dedicada a brindar soluciones financieras. Esta compañía se encuentra regulada y vigilada por la superintendencia Financiera de Colombia y en materia de protección de datos por la superintendencia de industria y Comercio.
Su estructura física está compuesta por 1 edificio principal ubicado en la ciudad de Cali donde se encuentra el centro de datos principal, 5 edificios administrativos distribuidos de la siguiente forma: Bogotá, aquí se encuentra ubicado el centro de datos alterno (CDA), Medellín, Barranquilla, Eje Cafetero y Palmira, en esta última ciudad se encuentra ubicado el sitio alterno de operaciones (SAO), cuenta además con 95 oficinas comerciales ubicadas en todo el país.
La organización cuenta con más de 1200 colaboradores, de los cuales 80 están asignados a las áreas de infraestructura, desarrollo de software, telecomunicaciones, continuidad del negocio y seguridad de la información.
Actualmente aunque la organización cuenta con una serie de herramientas de seguridad informáticas, personal calificado y adopta las mejores prácticas en esta materia, aún tiene muchas brechas en los siguientes aspectos:

- No se cuenta con una política de seguridad de la información.
- No existe un proceso formal para la administración y gestión de riesgos.
- El proceso para el desarrollo y mantenimiento del software tiene muchas falencias, huecos de seguridad, no se tiene clara una metodología de desarrollo de software seguro.
- No se tiene una metodología para gestionar los incidentes de seguridad.

Por lo tanto nuestro plan de implementación del SGSI, está orientado a los procesos más críticos de la organización los cuales son: Tecnología, Medios virtuales (Oficina Virtual) y el área de continuidad del negocio.

1.3.1 CRONOGRAMA PROYECTO

A continuación se detalla el cronograma estimado para la implementación:



	Nombre de tarea	Duración	Comienzo	Fin
1	IMPLEMENTACION DEL SGSI	74 días?	mié 26/02/14	vie 06/06/14
2	Fase 1: Situación actual: Contextualización, objetivos y análisis diferen	8 días?	mié 26/02/14	vie 07/03/14
3	Fase 2: Sistema de Gestión Documental	16 días?	vie 07/03/14	vie 28/03/14
4	Fase 3: Análisis de riesgos	21 días?	vie 28/03/14	vie 25/04/14
5	Fase 4: Propuesta de Proyectos	17 días?	vie 25/04/14	dom 18/05/14
6	Fase 5: Auditoría de Cumplimiento de la ISO/IEC 27002:2005	11 días?	dom 18/05/14	vie 30/05/14
7	Fase 6: Presentación de Resultados y entrega de Informes	6 días?	vie 30/05/14	vie 06/06/14

Figura 2. Cronograma del proyecto

1.3.2 ORGANIGRAMA ORGANIZACION

A continuación se detalla el organigrama de la compañía:

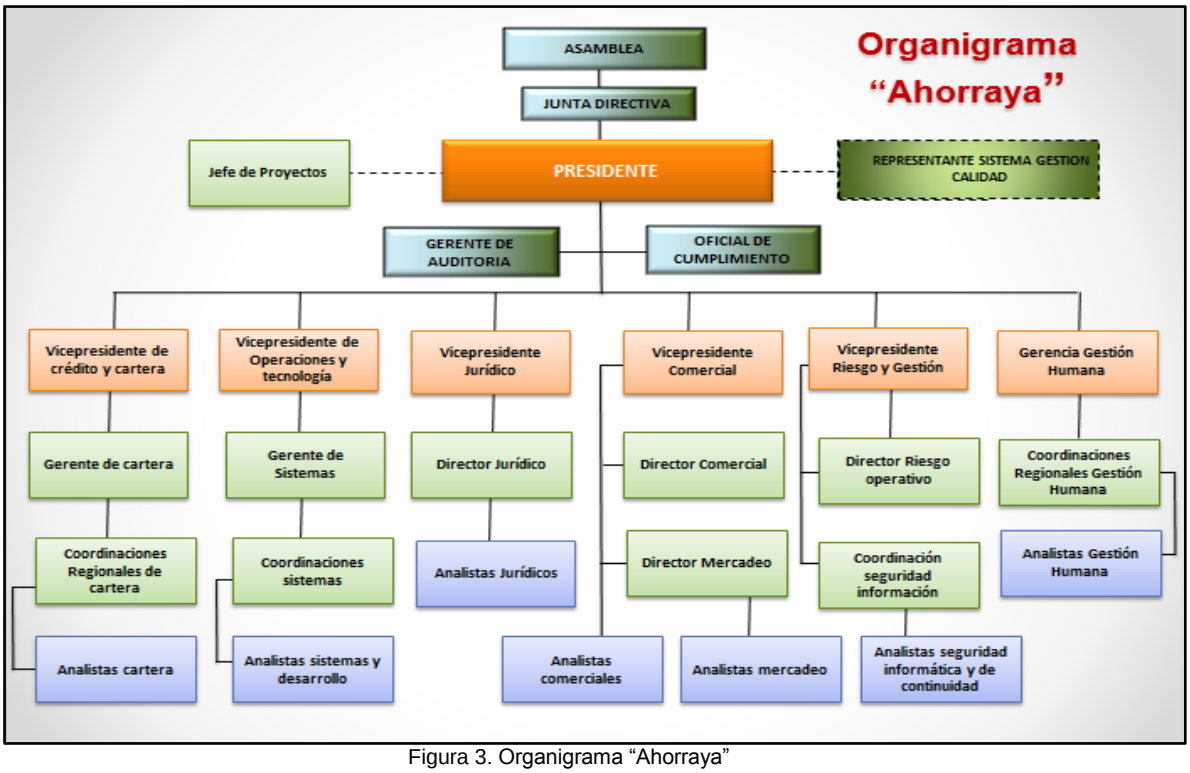


Figura 3. Organigrama "Ahorraya"

1.3.3 DIAGRAGRAMA DE RED

A continuación se detalla la red de la compañía:

El esquema de conexión de Telefónica en el centro de cómputo principal es el siguiente:

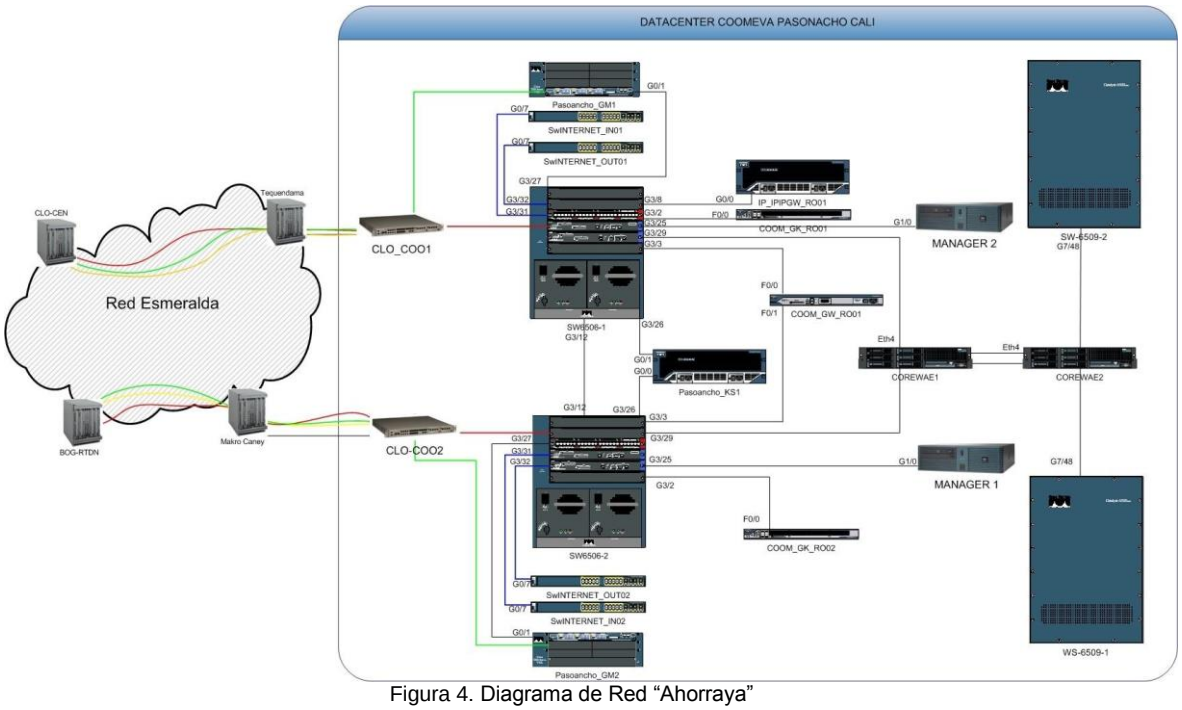


Figura 4. Diagrama de Red “Ahorraya”

Diagrama de red principal:

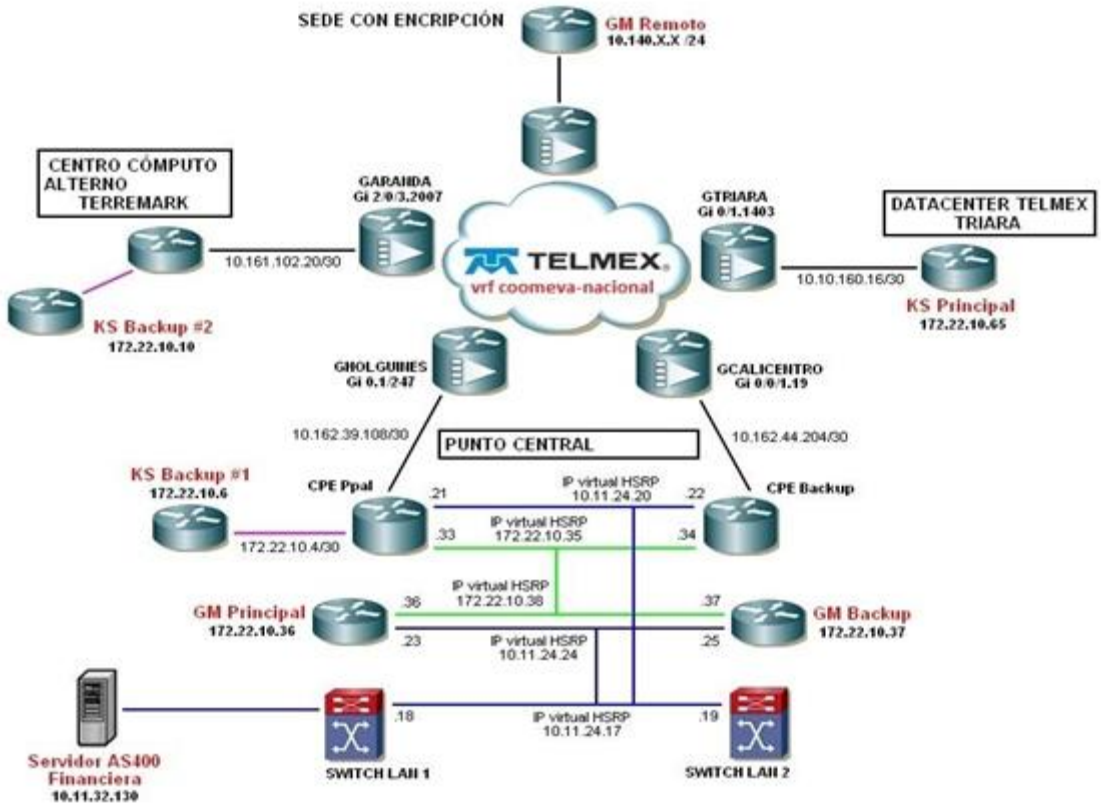


Figura 5. Diagrama de Red principal “Ahorraya”

1.4 OBJETIVO PLAN DIRECTOR

- Establecer una política de seguridad de la información, dirigida a colaboradores, clientes, terceros y proveedores, alineada con los objetivos estratégicos del negocio.

- Asegurar la implementación de las medidas de seguridad comprendidas en la presente Política, identificando los recursos y las partidas presupuestarias correspondientes.
- Definir un modelo de administración de riesgos, que permita tener un adecuado control sobre los incidentes de seguridad, que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- Proteger los activos de información del Banco y los recursos tecnológicos utilizados en su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales; con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Asegurar los procesos y activos de información que intervienen en la oficina Virtual de Ahorraya.
- Definir una metodología para el desarrollo seguro de software en Ahorraya.
- Mantener un programa de capacitación, diseñado a generar concientización y cultura en seguridad de la información a todos los colaboradores
- Proteger de forma adecuada la información para asegurar la continuidad del negocio, además de minimizar los posibles daños a la organización y maximizar el ROI y las oportunidades de negocio.
- Obtener el compromiso de la alta dirección para la implementación de la estrategia de seguridad de la información corporativa.
- Definir y administrar los indicadores que soportan la estrategia de seguridad de la información.
- Cumplir en todo momento con legislación vigente, las circulares externas definidas por los órganos de control y todo aquello relacionado con la protección de datos y sociedad de la información, así como cualquier otra que afecte a la seguridad de los activos de la Organización.

1.5 ANALISIS DIFERENCIAL

El Análisis GAP tiene como objetivo general evaluar el nivel de cumplimiento de los requerimientos y controles enunciados en la norma ISO/IEC 27001:2005 e ISO/IEC 27002:2005.

El diagnóstico de las norma tiene como objetivo dar una visión general del cumplimiento de los requerimientos necesarios para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). En particular, se busca identificar vacíos existentes en la entidad Financiera, con respecto a los controles y objetivos de control establecidos en la norma ISO 27001:2005 y en el anexo A de la misma ISO 27002:2005.

Análisis de información y valoración de madurez. Una vez obtenida la información, se procede a analizarla para estimar el nivel de madurez de cada cláusula, tanto a nivel los requerimientos del Sistema de Gestión de Seguridad de la Información, como de los controles definidos en el Anexo A de la norma. Los niveles de madurez y porcentajes utilizados para la evaluación son[2]:

[2] Basado en los niveles establecidos por CobIT. Tomado de Information Security Governance. Guidance for Boards of Directors and Executive Management, 2nd Edition. ISACA

Nivel de Madurez	%	Descripción
No Aplica	N/A	No aplica
Inexistente	0	No se aplican controles
Inicial / Ad Hoc	20	Se reconoce la necesidad de seguridad de la información. La implementación del control depende de cada individuo
Repetible	40	Los procesos y los controles siguen un patrón regular
Definido	60	Los procesos y los controles se documentan y se comunican
Administrado	80	Los controles se monitorean y se miden
Optimizado	100	Las buenas prácticas se siguen y automatizan

1.5.1 REQUERIMIENTOS SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Esta parte de la norma de obligatorio cumplimiento (cláusulas 4 a 8), define los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), dentro del contexto de las necesidades específicas del negocio.

La información obtenida durante la revisión documental muestra que en la entidad Financiera hasta el momento no se tiene establecido formalmente un Sistema de gestión de seguridad de la información que cumpla con los requerimientos metodológicos establecidos por la norma ISO 27001:2005. Sin embargo el hecho que la organización cuente con un sistema de gestión de Calidad certificado y en un nivel de madurez gestionado permite que muchos de los requerimientos exigidos se cumplan parcialmente.

Cláusula	Madurez
4. Sistema de Gestión de Seguridad de la Información	Inicial
5. Responsabilidad de la Dirección	Definido
6. Auditorías Internas	Repetible
7. Revisión de la Dirección	Definido
8. Mejora del SGSI	Definido

Los principales avances se identificaron en cuanto la responsabilidad y compromiso de la Dirección, que se ven reflejados en el apoyo y disposición que está dando al proyecto de IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) y, mejoras del sistema de gestión y revisiones por parte de

la alta dirección: debido a la afinidad que estas cláusulas tienen con el sistema de gestión de Calidad, sin embargo falta la orientación o enfoque propio del SGSI.

Las principales carencias identificadas corresponden a aspectos que aún no se han definido o formalizado al interior de la empresa, tales como el alcance del SGSI, el análisis de riegos de seguridad sistemático específico para todos los activos de información, la revisión del SGSI por parte de la Dirección, la gestión de los incidentes de seguridad, las características de documentación y los elementos asociados a las acciones correctivas y preventivas. Por esto, es importante identificar y establecer los procedimientos y demás documentación faltante exigida por la norma como parte de un SGSI.

A continuación se presentan las principales fortalezas y debilidades por cada clausula:

Fortalezas
• Existe un proyecto cuyo objeto es contratar una empresa consultora para apoyar la definición e implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), soportado en las mejores prácticas en esta materia dadas por la norma ISO-27001 y complementada por las normas ISO-27002.
• La organización tiene implementados sistemas de Administración de Riesgo Operativo (SARO) y Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo SARLAFT. Estos sistemas permiten y facilitan la incorporación de la cultura de gestión de riesgo en la organización, pilar importante del SGSI. • La organización ha desarrollado políticas de seguridad dando cumplimiento a los requerimientos exigidos por la Superintendencia Financiera de Colombia en la circular externa 042 de 2012.
• Adicionalmente la organización cuenta con un Sistema de Gestión de Calidad ISO 9001:2008 certificado y gestionado, que es perfectamente compatible con los Sistemas de Gestión ISO, facilitando así la implementación de un SGSI.
• Dentro de los ejercicios de auditoría se contemplan elementos relacionados con la seguridad de la información especialmente dando alcance a los requerimientos del SGC y el cumplimiento de los requerimientos regulatorios de la SFC.
• Se han desarrollado iniciativas de concientización en temas relacionados a la seguridad de la información.
• La organización cuenta con una plataforma documental de Gestión Integrada, donde se estandarizan y publican los procedimientos y procesos del sistema de Gestión de Calidad, se controlan versiones, publicaciones y acceso a los documentos por parte de los usuarios.
• Existen los listados maestros de registros de cada proceso, con los tiempos de retención definidos.

Oportunidades de mejora
• Si bien el proyecto es claro en su objetivo, es importante que la organización defina de manera formal el alcance del SGSI.
• La organización además de definir la política del SGSI, debe también definir el enfoque de análisis de riesgos de la organización.
• Revisión y unificación de procedimientos y políticas del sistema de gestión de calidad (SGC) con los requerimientos exigidos por el sistema de gestión de

seguridad de la información y así obtener un solo sistema de gestión integrado ahorrando esfuerzos en implementación y gestión

Nivel de madurez: Inicial

1.5.2 RESPONSIBILIDADES DE LA DIRECCIÓN

Fortalezas
• La Alta dirección es participe activa en el desarrollo del proyecto implementación del Sistema de Gestión de la Seguridad de la Información.
• Se ha destinado recursos tanto económicos como de Talento humano para la implementación del SGSI.
• Actualmente ya existen revisiones por parte de la alta dirección contempladas para el Sistema de Gestión de Calidad

Oportunidades de mejora
• Es importante que la Alta dirección defina para la metodología de análisis de riesgos que soportará el SGSI, el nivel de riesgo aceptable.
• Así mismo dentro de las revisiones de la dirección que actualmente se llevan a cabo para el SGC, incorporar los elementos necesarios para dar cumplimiento a las revisiones de la dirección que permitan cumplir los requerimientos del SGSI
• La Alta Dirección debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI

Nivel de madurez: definido

1.5.3 AUDITORIAS INTERNAS DEL SGSI

Fortalezas
• Actualmente la compañía lleva a cabo procesos de auditoría interna a sus procesos y procedimientos establecidos en el SGC. • Adicionalmente lleva a cabo Auditorias de tercera parte para el mantenimiento y certificación del SGC
• El proceso de Auditoria del SGC es maduro, facilitando así la incorporación de los elementos exigidos por el SGSI.

Oportunidades de mejora
• Es importante fortalecer el área de control interno para que tenga las competencias necesarias para abordar las auditorias del SGSI.
• Así mismo dentro de las revisiones de la dirección que actualmente se llevan a cabo para el SGC, incorporar los elementos necesarios para dar cumplimiento a las revisiones de la dirección que permitan cumplir los requerimientos del SGSI.

Nivel de madurez: Repetible.

1.5.4 REVISIÓN DEL SGSI POR LA DIRECCIÓN

Fortalezas
• El SGC tiene asignado un representante y un proceso para la revisión del sistema por parte de la Alta Dirección. Al seguir los lineamientos del Estándar ISO9001 permite fácilmente la integración de este procedimiento con lo requerido en la norma ISO27001

Oportunidades de mejora
• Así mismo dentro de las revisiones de la dirección que actualmente se llevan a cabo para el SGC, incorporar los elementos necesarios para dar cumplimiento a las revisiones de la dirección que permitan cumplir los requerimientos del SGSI.

Nivel de madurez: Definido

1.5.5 MEJORA DEL SGSI

Fortalezas
• El SGC tiene definidos procesos documentados para la eliminación de las causas de no conformidades identificadas y potenciales. Requisitos exigidos en los numerales 8.5 Mejora Continua y 8.1 Mejora del SGSI, correspondientes al SGC y SGSI respectivamente.

Oportunidades de mejora
• La correspondencia entre las normas ISO9001 e ISO27001 facilita la implementación de los requerimientos exigidos en el SGSI.

Nivel de madurez: Definido.

A continuación se detalla en la siguiente gráfica, con el nivel de madurez de acuerdo a lo definido en los requisitos de la norma ISO-27001

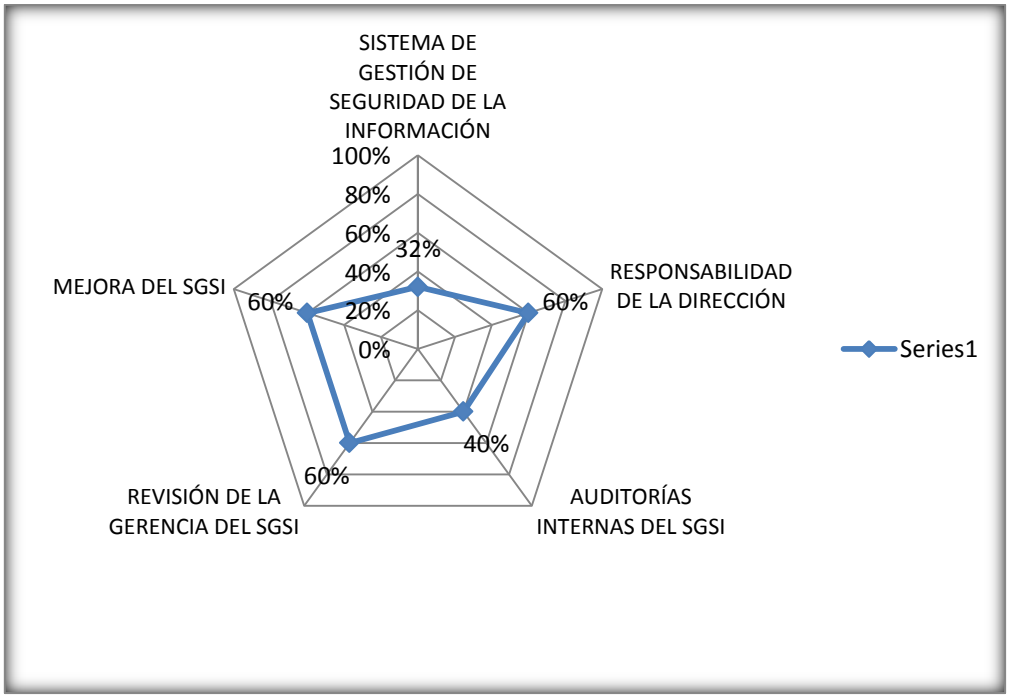


Figura 6. Estado Actual de Requerimientos del SGSI

CONTROLES DEL ANEXO A DE LA NORMA

El Anexo A de la norma ISO/IEC 27001:2005 define los controles mínimos a considerar para gestionar la seguridad de la información de manera adecuada. Desde el punto de vista de la certificación, cualquier exclusión de controles necesita justificarse y debe suministrarse evidencia de que los riesgos asociados han sido

aceptados apropiadamente por las personas responsables. La figura 4 muestra el nivel de madurez general por dominio de controles.

Dominio	Madurez
A.5 Política de seguridad de la información	Inicial
A.6 Organización de la seguridad de la información	Definido
A.7 Gestión de activos de información	Gestionado
A.8 Seguridad en los recursos humanos	Definido
A.9 Seguridad Física y Ambiental	Repetible
A.10 Gestión de las Comunicaciones y Operaciones	Repetible
A.11 Control de Acceso	Repetible
A.12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	Inicial
A.13 Gestión de Incidentes de Seguridad	Repetible
A.14 Gestión de la Continuidad del Negocio	Gestionado
A.15 Cumplimiento	Repetible

A continuación se presentan las principales fortalezas y debilidades por cada dominio.

1.5.6 POLÍTICA DE SEGURIDAD DE INFORMACIÓN

Fortalezas
• Existe un manual interno de seguridad de la información, donde se tienen definidas políticas de seguridad.

Oportunidades de mejora
• Definir y formalizar la política del SGSI
• No hay definida una periodicidad para la revisión del documento de políticas para garantizar que contemple las necesidades y cambios de la Organización.

Nivel de madurez: Inicial

1.5.7 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Fortalezas
• La Presidencia ha mostrado un interés explícito en fortalecer la seguridad de la información, asignación recursos para el desarrollo del mismo.
• Se tiene definido un rol específico encargado de la seguridad información • Se cuenta con un Comité de Riesgo del Banco
• La Organización desarrollo recientemente un documento importante de acuerdo de confidencialidad, para contrataciones de personal, como de terceros que se viene aplicando en todos los procesos de contratación.

Oportunidades de mejora
• Formalizar la creación de un Comité de Seguridad de información
• Es importante fortalecer los vínculos con organizaciones académicas, asociaciones y demás grupos de interés, con el objetivo de contar con una fuente

Oportunidades de mejora
actualizada de conocimiento y soporte para posibles eventos o incidentes.
• Aunque se han realizado algunas tareas de verificación por parte de Auditoría interna sobre algunos controles puntuales, enfocados principalmente sobre gestión de accesos, no se tiene implementada una función de revisión y verificación la gestión de la seguridad de la información.
• En el momento no se cuenta con un análisis de riesgos estructurado que permita determinar los escenarios de exposición a los que se puede ver enfrentada la información de la Organización al momento de contratar con terceros.

Nivel de madurez: Definido.

1.5.8 GESTIÓN DE ACTIVOS DE INFORMACIÓN

Fortalezas
• Existe una matriz de inventario de activos de información donde se identifican y clasifican los activos según su sensibilidad y criticidad.
• Existen procedimientos y definiciones de clasificación de la información de acuerdo a su sensibilidad • Actualmente la información física se encuentra debidamente rotulada según su sensibilidad y criticidad.
• Si, existe un documento llamado políticas de control acceso y manejo de la información, donde se contempla el uso del correo electrónico, internet, y software libre. • Se cuenta con políticas generales para el manejo de la red, documentos del escritorio, navegación de internet.

Oportunidades de mejora
• Aunque existe un inventario de activos de información, actualmente no están tipificados de manera que puedan clasificar para el análisis de riesgos..
• Establecer indicadores de gestión que permitan identificar el grado de cumplimiento de dichas políticas.

Nivel de madurez: Gestionado

1.5.9 SEGURIDAD DEL RECURSO HUMANO

Fortalezas
• La organización cuenta con un proceso de selección de personal maduro que contempla algunos requerimientos básicos sobre verificación de antecedentes judiciales, verificación de referencias, consulta en la CIFIN , visita domiciliaria y estudio de seguridad con Incocrédito.
• Los empleados firman otro SI de seguridad que se anexa en su contrato laboral. Esta aplica para todos los empleados, tanto temporales como permanentes.
• Se tiene definido un procedimiento de investigación disciplinaria que contempla un comité disciplinario donde se analiza la situación, se recopilan pruebas y se emite las responsabilidades para que la Alta Dirección tome las decisiones pertinentes.
• Adicionalmente se cuenta con un proceso para la terminación del contrato que contempla la notificación oportuna del cese de actividades a las áreas de

Fortalezas
tecnología para la revocación de permisos hacia los sistemas de información.
• Se han desarrollado iniciativas en pro de la sensibilización de la seguridad de la información, tales cursos virtuales, capacitaciones presenciales y envió de información a través del correo electrónico.
• Existe un procedimiento de Capacitación y creación de cultura en seguridad de la información que contempla la capacitación a los nuevos colaboradores.

Oportunidades de mejora
• Se cuenta con un reglamento interno de trabajo y un código de ética que hace referencia al cumplimiento de las políticas corporativas en general; sin embargo, no hay una definición explícita relacionada con las responsabilidades de los usuarios internos frente a la seguridad de la información.
• Aunque se tienen en cuenta algunos controles de seguridad cuando una persona ingresa a la empresa, no hay una verificación de estos mismos controles frente a la contratación de terceros.
• La Organización cuenta con un proceso de inducción cuando una persona ingresa a la empresa, sin embargo no existen indicadores de gestión que permita evaluar el nivel de concientización frente a los requerimientos de seguridad de la información.
• Aunque se cuenta con las diferentes iniciativas de sensibilización, la Organización no cuenta con un plan formal de capacitación de seguridad de información vigente
• En los perfiles de cargo no se definen las responsabilidades que los empleados tienen frente a la seguridad de la información.

Nivel de madurez: Definido**.**

1.5.10 SEGURIDAD FÍSICA Y AMBIENTAL

Fortalezas
• La Organización tiene agencias y puntos de servicio a nivel nacional cuya seguridad física se rige a partir de los lineamientos establecidos por la Coordinación Nacional de seguridad Bancaria.
• Esta implementada la cultura del uso unificado y permanente del carné por parte de los funcionarios de la Organización.
• El Área de Sistemas controlan los procesos de mantenimiento de equipos dentro de la organización, al igual que las autorizaciones de ingreso a las instalaciones por parte del área de seguridad Bancaria.
• El centro de cómputo cuenta con controles de acceso robustos (tarjetas de proximidad en 3 niveles de acceso) y procedimientos de autorización de ingreso formalizados. Además del centro de cómputo y las áreas de bóveda y caja de las oficinas, se tienen identificadas áreas de seguridad para la Mesa de dinero, Auditoría y cumplimiento.
• Se tienen implementados aires acondicionados para el centro de cómputo y todas las oficinas, especialmente para los equipos de comunicaciones.
• Existen controles de intrusión a las áreas seguras y oficinas tales como sistemas de alarma y monitoreo 24hrs junto con sistemas de videograbación y guardas de seguridad.

Oportunidades de mejora
• A pesar que se tienen controles ambientales en el centro de cómputo la capacidad de los aires acondicionados no es la adecuada para soportar los equipos actualmente instalados.
• Se evidencio que en el centro de cómputo se observaron acumulación de elementos inflamables como cartón y papel

Nivel de madurez: Repetible.

1.5.11 GESTIÓN DE COMUNICACIONES Y OPERACIONES

Fortalezas
• Los Procesos generales del área de TI, están basados en marcos de referencia y buenas prácticas como COBIT, ITIL e ISO 20000, todos los procedimientos tiene indicadores de gestión.
• Existen procedimientos orientados al control de cambios en los sistemas de información, dichos procedimientos contemplan alcances, identificación de sistemas impactados, medidas correctivas, contingencias, entre otras.
• Mensualmente se mide la capacidad de las maquinas que son críticas, tales como el AS400.
• Existen procedimientos para el respaldo de información crítica de la organización. Las cintas de respaldo se custodian mediante contrato de custodia de cintas.
• Para el manejo de Medios removibles se cuenta con un procedimiento para la solicitud de la habilitación de dispositivos de almacenamiento.
• En cuanto a los Controles de RED existe cifrado en la red WAN desde los enrutadores, Firewall e IPS, certificados para el acceso de redes inalámbricas.
• En relación a la gestión de vulnerabilidades se tiene establecido el escaneo mediante Qualys, semanalmente se escanean los dispositivos críticos en busca de vulnerabilidades. • Se realiza de forma periódica la instalación de parches administrados a través de la plataforma WUSUS.
• La organización cuenta con una solución endpoint contra el código malicioso que cuenta con Antivirus, antispam, anti malware, (McAfee), esta solución se encuentra instalada en todos los equipos de la organización.

Oportunidades de mejora
• A pesar que existen procedimientos para el respaldo de información, no existe formalmente una política para el respaldo de información, que contemple procedimientos formales para las pruebas de medios de almacenamiento, directrices sobre la clasificación de la información y el establecimiento de controles de cifrado sobre los mismos medios.
• En algunas oficinas no existen la condiciones mínimas de seguridad para las áreas de comunicaciones.(Algunos switches se encuentran mal ubicados y sin protección).
• Aunque se hace un monitoreo permanente sobre los sistemas y plataformas, no se tiene implementado un proceso formal de gestión de logs, aunque los sistemas y plataformas tecnológicas generan estos registros.
• Aunque hay un acuerdo de confidencialidad con los proveedores, la Organización no establece condiciones sobre el destino final que debe tener la información

Oportunidades de mejora
entregada cuando deje de ser útil para el propósito que tenía inicialmente.

Nivel de madurez: Repetible

1.5.12 CONTROL DE ACCESO

Fortalezas
• Existe una política y un proceso formal para la creación de usuarios en los diferentes sistemas y plataformas tecnológicas de la Organización de acuerdo con los cargos de los usuarios.
• Está definido un procedimiento para el bloqueo y/o eliminación de usuarios, que es ejecutado por gestión humana toda vez que un colaborador se retira de la organización.
• Las contraseñas empleadas para el acceso a los sistemas de información y plataformas cuentan con requerimientos de seguridad
• El proceso de gestión de usuarios es revisado periódicamente por parte de la de la Auditoría Interna.
• Las conexiones remotas se controlan a través de VPNs mediante las herramientas de Chekpoint.

Oportunidades de mejora
• Existen algunos sistemas de información que no soportan los requerimientos de manejo de contraseñas establecidos por el Banco. Sin embargo se espera solucionar esta situación mediante el desarrollo de un proyecto de gestión de identidades.
• La Organización tiene una política de bloqueo de estaciones y otra adicional de bloqueo después de 5 minutos definida por el banco
• Algunas redes de las oficinas comerciales no cuenta con mecanismos de segmentación para la protección contra accesos no autorizados a servicios o sistemas de información.
• No se cuenta con una política formal para el manejo de equipos móviles para mitigar riesgos asociados a este tipo de equipos.

Nivel de madurez: Repetible.

1.5.13 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Fortalezas
• Existe un procedimiento formal de gestión de cambios de software dentro del proceso de Administración de sistemas de información, que contempla procedimientos de análisis de requerimientos, desarrollo, pruebas y puesta en producción.
• Se han implementado ambientes independientes de desarrollo/pruebas y producción para los sistemas de la Organización. Existen procedimientos definidos para el paso a producción y creación de ambientes de pruebas.
• El proceso de desarrollo de software contempla la certificación de pruebas y mapa de pruebas. hay una firma que se llama Green SQA quien certifica el desarrollo y las pruebas hechas, y solo así se acepta el paso a producción del sistema.

Oportunidades de mejora
• Actualmente los requerimientos para los sistemas nuevos y existentes se enfocan en necesidades operativas y técnicas, pero no siempre contemplan elementos de seguridad de la información durante su desarrollo ni sobre controles para proteger los datos que manejan.
• La infraestructura tecnológica de la Organización no cuenta con controles de cifrado de información crítica en tránsito ni en reposo.
• No existe una política formal que regule el paso de información de los ambientes de producción a pruebas.

Nivel de madure: Inicial.

1.5.14 GESTIÓN DE INCIDENTES DE SEGURIDAD

Fortalezas
• No Existe un procedimiento formal para la gestión de incidentes, estos se gestionan de acuerdo a la categorización y se asignan los responsables para gestionarlos y responder ante el evento.
• Dentro del área de Seguridad Bancaria se tiene establecido los procedimientos relacionados con la recolección de evidencia, cadena de custodia, investigación, verificación de pruebas, e informe de incidente.

Oportunidades de mejora
• Diseñar un procedimiento formal para el reporte y gestión de incidentes de seguridad de la información en la entidad, que involucre a todos los empleados, se defina responsabilidades, se establezca líneas claras de comunicación y actividades para manejo de evidencias y aprendizaje de situaciones ocurridas.

1.5.15 GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

Fortalezas
• La organización cuenta con un BCP completo, con un nivel de madurez CMMI en "Gestionado".
• Existe BIA, con capitulo relacionado a recurso humano, físico, procesos. Es un proceso maduro.
• Se han hacen pruebas regulares. Se puede evidenciar trazabilidad de las pruebas realizadas
• Se tienen estrategias de Tecnología. Los procesos están documentados. Existen DRP. El Sitio alterno soporta todos los procesos críticos. Se está trabajando en alianza con empresas del grupo para dar soporte en caso de contingencia. Se está trabajado en equipos de alta disponibilidad.

Oportunidades de mejora
• Dentro de la estrategia de concientización sensibilizar y socializar los planes de continuidad
• Ejercitar y probar los planes de continuidad de negocio.

Nivel de madurez: Gestionado

1.5.16 CUMPLIMIENTO

Fortalezas
• La Organización cuenta con un área de asistencia jurídica para garantizar que sus actividades cumplan y no vayan en contra de las leyes y regulaciones aplicables.
• Todos los requerimientos de los entes reguladores del Banco se canalizan a través de Auditoría interna, y el Área Jurídica presta soporte y apoyo para el cumplimiento de dichos requerimientos.
• Auditoría interna verifica el cumplimiento de propiedad intelectual en relación a licenciamiento de software

Oportunidades de mejora
• La existencia de procedimientos de auditoría del SGC permite fácilmente la incorporación de requerimientos del SGSI en relación al cumplimiento.

Nivel de madurez: Repetible

Figura 7. Nivel de Maduración Dominios Anexo A

- Los resultados presentados son una visión general objetiva del estado actual de seguridad de la gestión de información respecto al estándar ISO/IEC 27001:2005 y la ISO/IEC27002:2005. El estado deseado debe estar alineado con los objetivos y estrategias definidas por la Organización, y adicionalmente, debe garantizar una respuesta efectiva al cumplimiento de requerimientos legales y regulatorios aplicables al negocio.
- Quizá una de las razones para que la entidad Financiera esté ubicado en niveles de madurez Repetible y Definido en los requerimientos del SGSI e implementación de controles respectivamente, es que actualmente el Banco cuenta con un Sistema de Gestión de Calidad certificado y, a los continuos

esfuerzos que la organización hace para mejorar sus procesos y procedimientos.

En el archivo en Excel denominado GAP_AHORRAYA_Detalle GAP ISO 27001-27002, se detalla un análisis GAP a nivel de los controles definidos en las normas ISO 27001:2005 - ISO 27002:2005.

1.6 RESULTADOS

Al finalizar el Plan para la Implementación de la ISO/IEC 27001:2005, obtendremos los siguientes resultados:

- Contar con un sistema de gestión permite ordenar las actividades de la organización y dirigirlas hacia el objetivo que la empresa busca.
- Lograr alcanzar todos los puntos establecidos en los objetivos propuestos.
- Contar con una política de seguridad de la información, que permita alinear las normas y procedimientos definidos por la organización.
- Gestionar el sistema de gestión de seguridad de la información, de acuerdo a lo definido en las normas ISO 27001 - ISO 27002.
- Cerrar los hallazgos encontrados en las auditorías internas realizadas al SGSI.
- Certificarse en la Norma ISO-27001:2005
- Administrar de forma eficiente los riesgos detectados en la organización y mitigarlos adecuadamente antes de que lleguen a ser un problema.
- Conseguir que el 100% del personal que labora en AHORRAYA, reporten los incidentes de seguridad de la información, con el fin de prevenir eventos que puedan afectar la continuidad del negocio.
- Afianzar los procesos, procedimientos y controles definidos en la continuidad del negocio
- Lograr Concientizar a todos los colaboradores de AHORRAYA, en seguridad de la información.