PLAN DE IMPLEMENTACIÓN SGSI BASADO EN LA NORMA ISO 27001:2013

ISAGXXX 2014

TFM MISTIC UOC 2014-2015

ROBIN J.SALCEDO B.

Agenda de la presentación

PLAN DE IMPLEMENTACIÓN SGSI ISO 27001:2013
TFM MISTIC 2014-2015

- Alcance del proyecto
- Contextualización y Entendimiento Organización ISAGXXX
- Fases del proyecto
- Metodología Técnica
- Análisis Diferencial
- Sistema Documental SGSI
- Gestión de Activos y Riegos
- Proyectos Propuestos de Seguridad
- Roadmap Seguridad Información
- Auditoria de Cumplimiento
- Recomendaciones y Conclusiones
- Cierre del Proyecto Final

Definiciones

- **Activo Crítico**: Instalaciones, sistemas o equipo eléctrico que si es destruido, degradado o puesto indisponible, afecte la confiablidad u operatividad del sistema eléctrico.
- **Análisis Diferencial:** Es un análisis que mide cómo una organización está llevando a cabo su desempeño con respecto a una serie de criterios establecidos en base a normas o procedimientos internos, controles seleccionados, las mejores prácticas de competencia, etc. El resultado de este análisis establece la diferencia entre el desempeño actual y el esperado, con un informe presentado con indicaciones sobre dónde están las deficiencias y "qué" falta para cumplir con cada requisito de la norma.
- **Auditoria:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Normas Aplicables: ISO 27002:2013, ISO 27005. iso 27001:2013.**

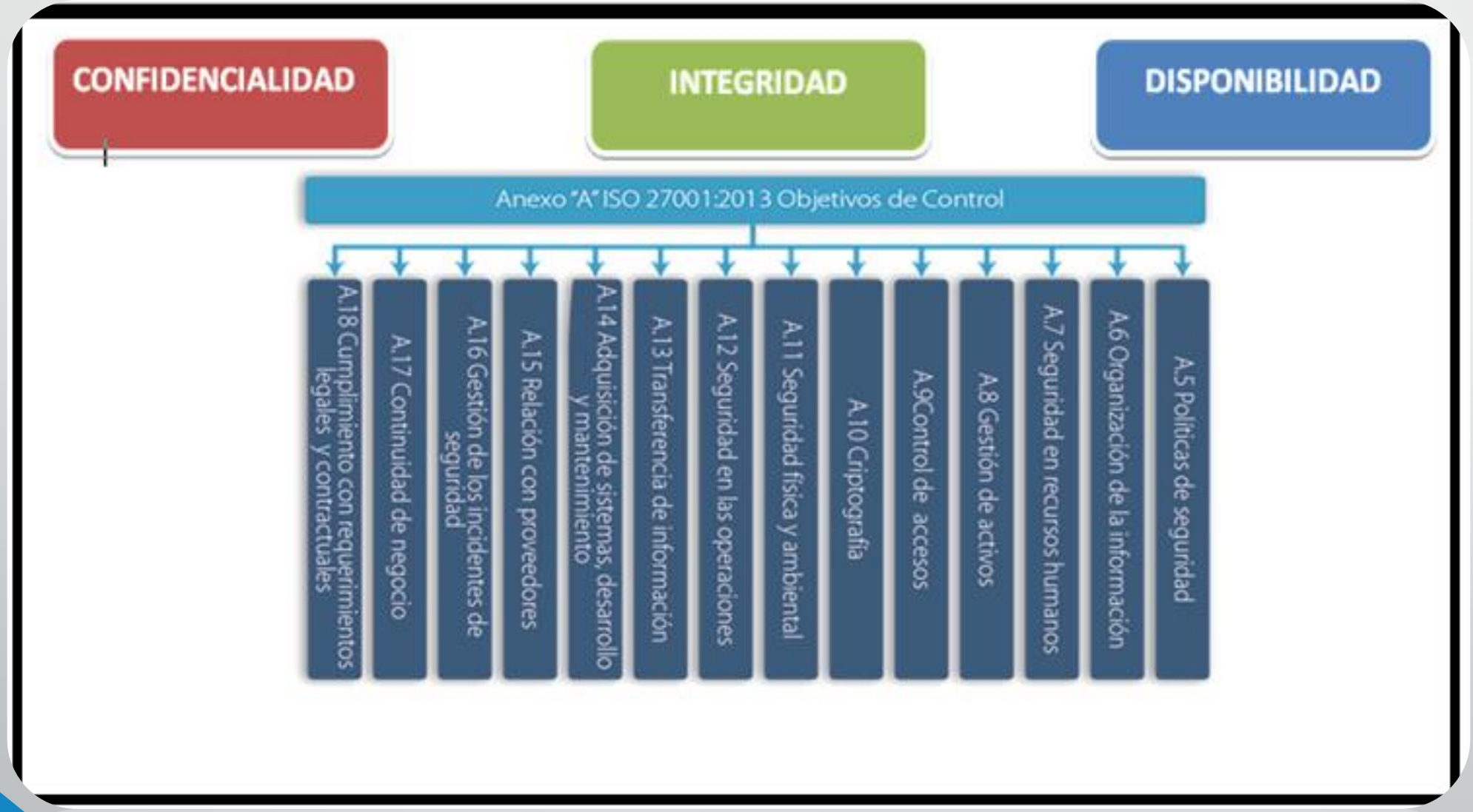
Alcance del Proyecto

Desarrollar, definir y ejecutar el plan de implementación del SGSI basado en la norma ISO 27001:2013 para el proceso critico de generación de energía y sus activos correlacionados con la gestión tecnológica, gestión de mantenimiento, sistemas SCADA de la organización ISAGXXX.

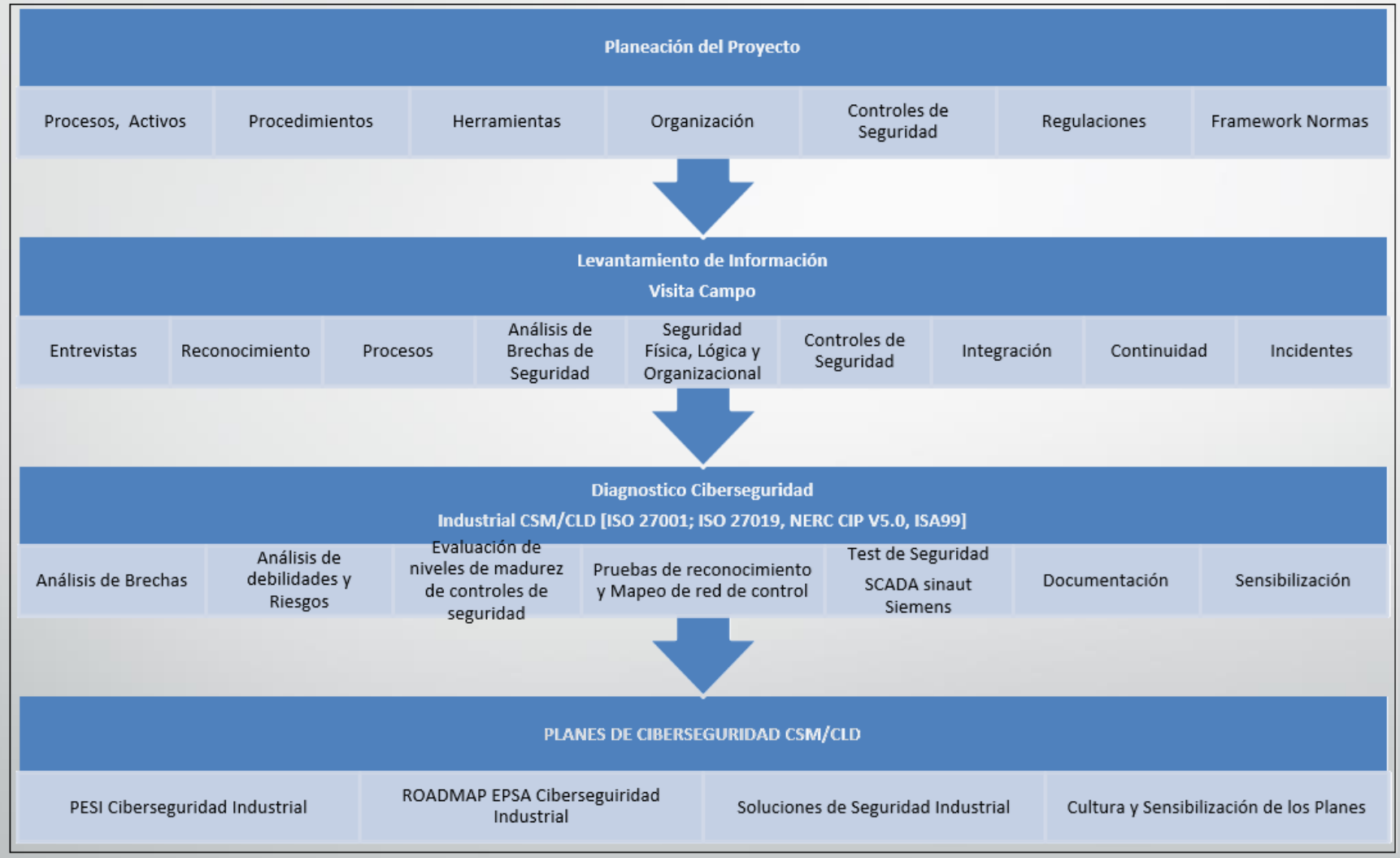
Alcance especifico del Proyecto:

- Entendimiento de la organización ISAGXXX.
- Levantamiento de Información de los Procesos de Operación, Tecnología y Mantenimiento.
- Desarrollo de entrevistas con el personal de Operación, Coordinación, Proveedores y Dirección de los Centros de Control. [*Reconocimiento del sistema SCADA, plataformas, arquitecturas, etc.*]
- Evaluación y Análisis Diferencial del estado actual de controles de seguridad aplicado a las plataformas Tecnológicas que soportan los sistemas de control, sistemas SCADA y los procesos de operación, de acuerdo a los requerimientos de la norma ISO 27002:2013.
- Definir, identificar y clasificar los activos de información que hacen parte del proceso critico de la generación de energía.
- Evaluación y gestión de los riesgos de seguridad de la información.
- Definir un modelo de gestión documental para al SGSI de la organización,
- Definir los planes de acción y el Roadmap de Ciberseguidad a corto, mediano y largo plazo para ISAGXXX, entre los años 2014 hasta el años 2017.
- Desarrollar auditorias de cumplimiento al SGSI.
- Gestión del SGSI.

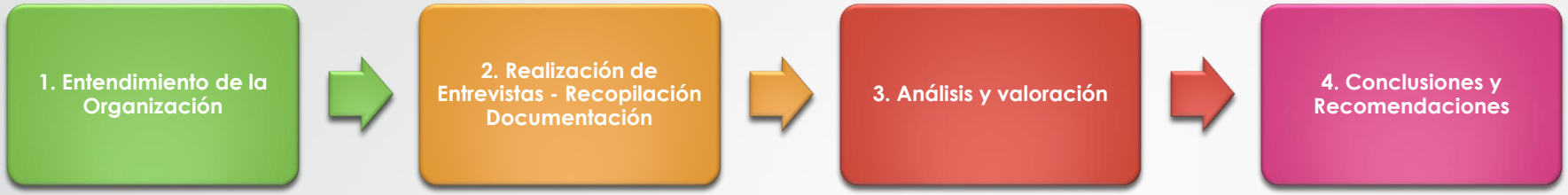
Marco Normativo del SGSI



Fases del Proyecto



Fases del Proyecto



1. Procesos
2. Estructura Organizacional
3. Operación
4. Responsables
5. Redes de Control
6. Sistema de Gestión de
7. Calidad/Ambiental/ Tecnología
8. Actividades de cumplimiento
9. Con Estándares de seguridad
10. Procedimientos de Operación
11. Guías/Instructivos
12. Documentación de Seguridad aplicada a los procesos de operación.
13. Gestión de Tecnología
14. Gestión de comunicaciones
15. Gestión de Proveedores
16. Gestión de Procesos
17. Arquitecturas CLD y SLM
18. Gestión de Operación

1. Cronograma de Entrevistas Con los responsables de las
2. Actividades de seguridad,
3. Soporte TIC, operación, MTO De los centros de control .
4. Revisión de la documentación Que soporta los procedimientos De seguridad y da cumplimiento.
5. Framework Ciberseguridad
6. Marco Normativo
7. Visitas a Campos y/o Inspección Física.
8. Evaluación del status de los
9. Controles de seguridad existentes o inexistentes, aplicados a las tecnologías de operación, gestión de operación y las plataformas TIC que soportan el sistema SCADA.

1. Análisis de los niveles de
2. Madurez de los controles de
3. Seguridad y ciberseguridad.
4. Evaluación de las escalas de
5. Madurez
6. Obtención del nivel de planeación, Implementación, operación y Mantenimiento de los controles De seguridad.
7. Valoración de escalas de Seguridad con relación al Framework normativo.
8. Ponderación del valor de control.
9. Análisis de Brecha de Seguridad
10. Gestión de Activos
11. Gestión Documental del SGSI
12. Gestión de Riesgos

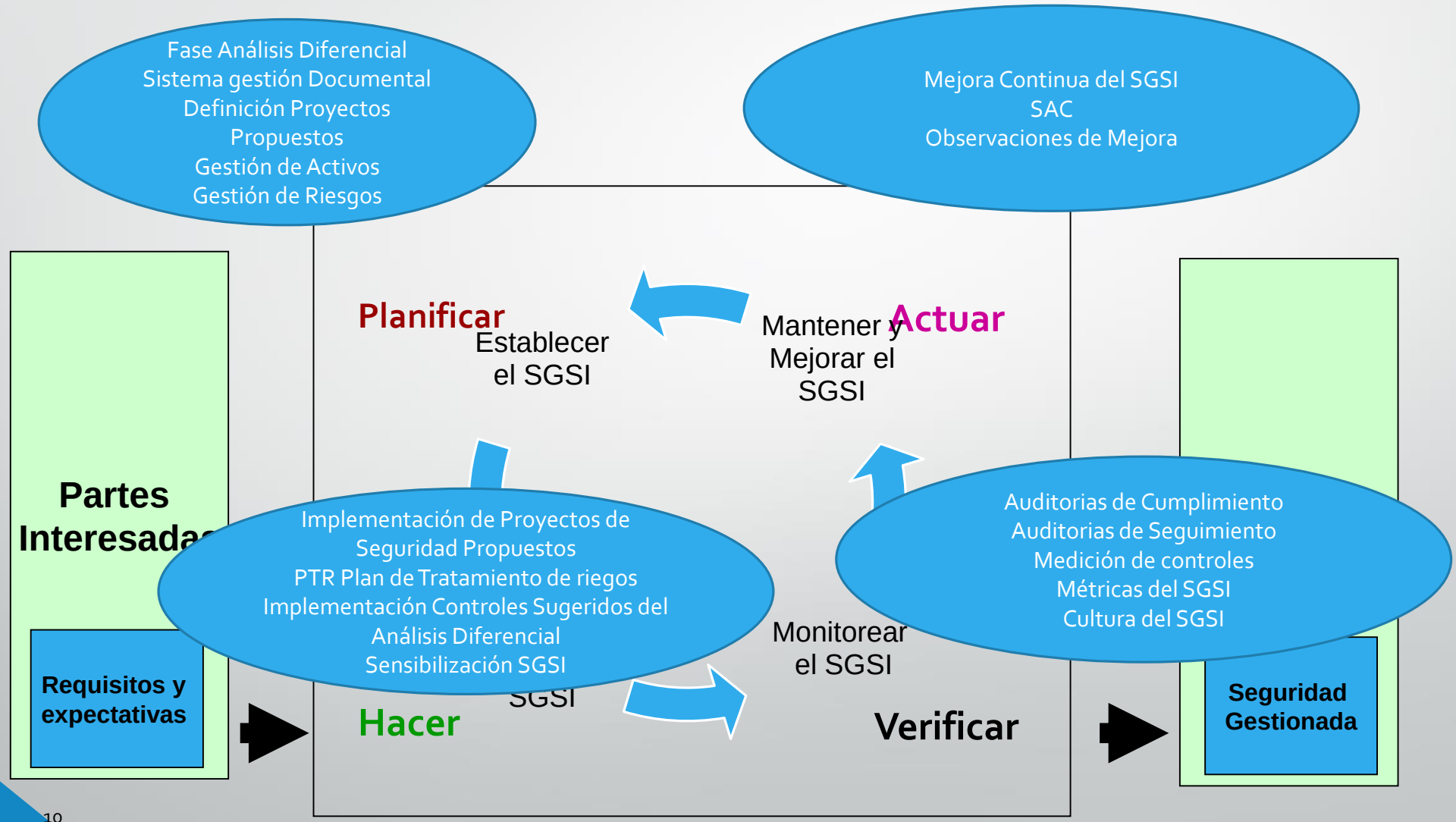
1. Planes de Acción en Seguridad y seguridad
2. Estrategia de seguridad focalizadas a las plataformas de operación de ISAGXXX.
3. Recomendaciones
4. PESI 2014
5. Auditoria de Cumplimiento
6. Cierre del Proyecto

Equipo de Trabajo Interdisciplinario ISAGXXX

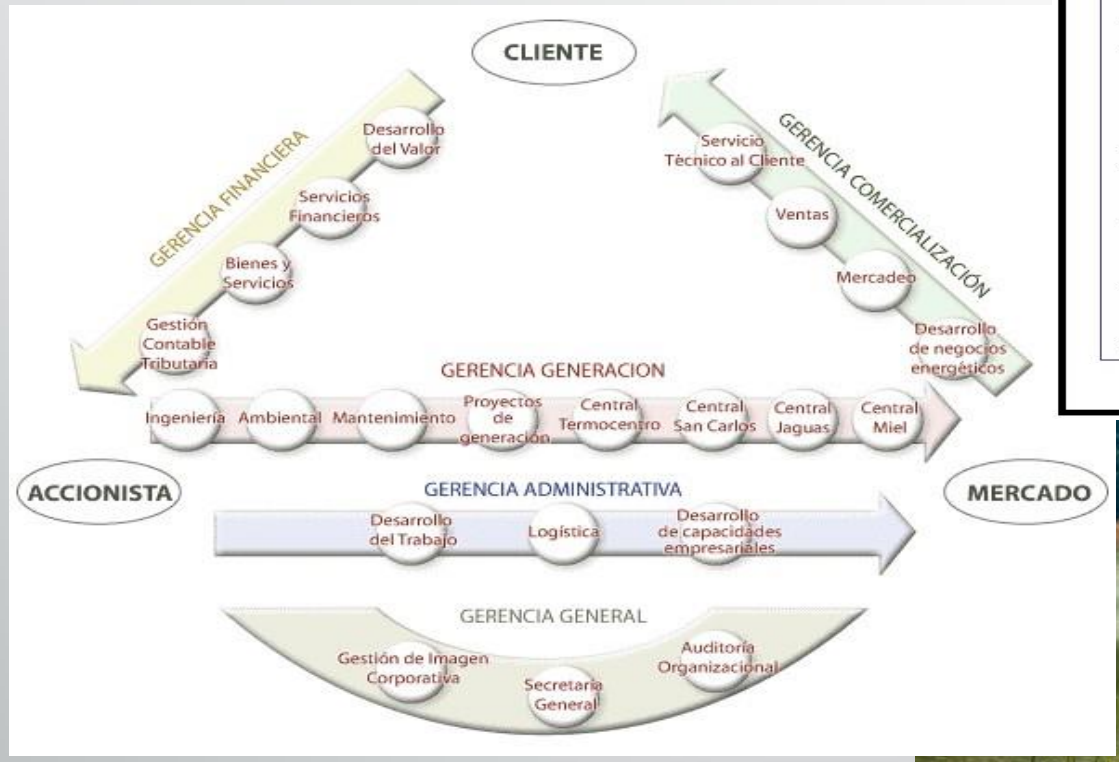
Gestión de Operación Generación y Distribución	Gerentes de Operación Coordinadores de Operación Operadores
Teleprocesos, telemedición, telecontrol	Personal de Mantenimiento de la aplicación SCADA Coordinadores de teleprocesos, telemedición y telecontrol
Gestión de Telecomunicaciones	•Coordinación de gestión de telecomunicaciones •Analistas de gestión de telecomunicaciones
Gestión Tecnológica	Coordinadores de Gestión tecnológica Personal de ISAGXXX Analista de gestión tecnológica, SAU, Gestores de Tecnología
Auditoria CELSIA - ISAGXXX	•Equipo de auditoria •Equipo de Auditoria ISAGXXX
Seguridad Física	•Coordinación de seguridad Física •Personal de Seguridad Física •Guardias de Seguridad
Gestión de Procesos	•Gestores de Procesos •Analista de Calidad y Gestión Documental

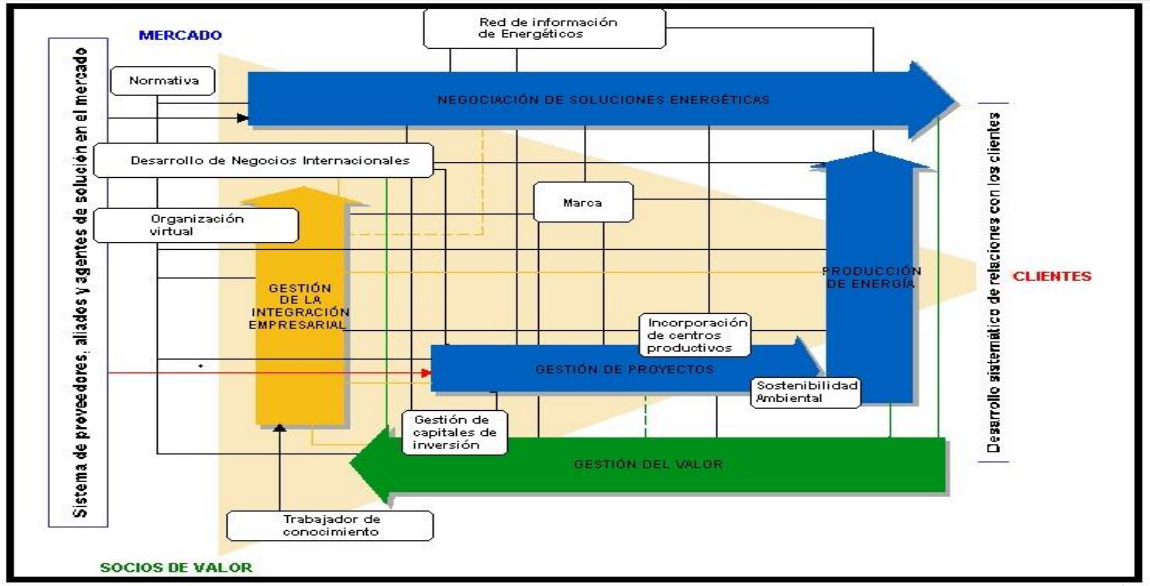
Metodología Técnica

Ciclo PHVA (Planificar /Hacer /Verificar /Actuar) Implementación del SGSI



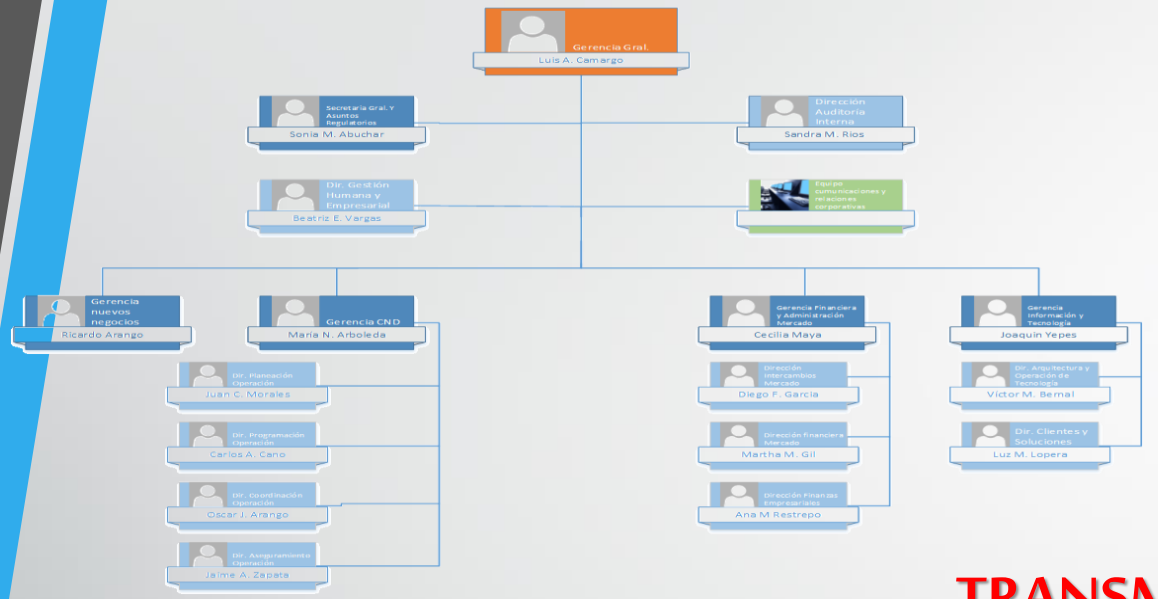
Contexto, Entendimiento Organizacional





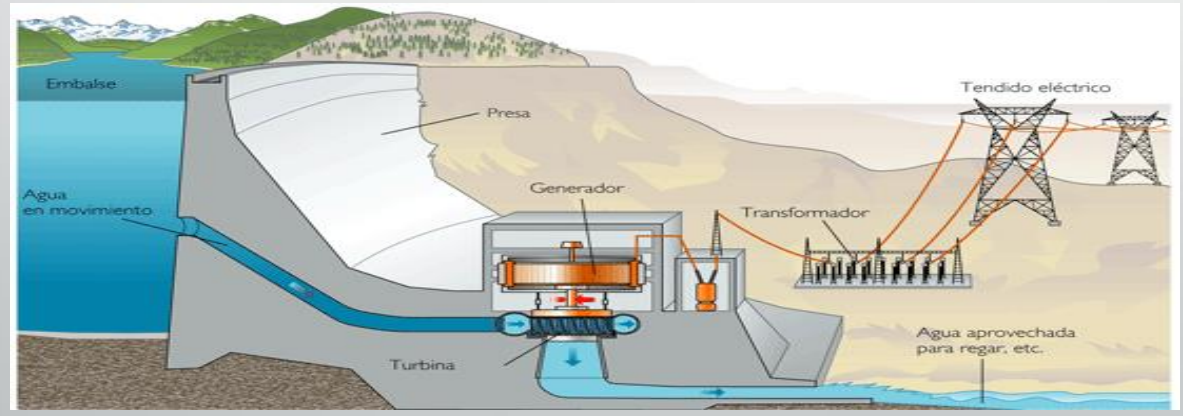
ISAGXXX desarrolla la capacidad de generación, produce y comercializa energía con el propósito de satisfacer las necesidades de sus clientes y crear valor empresarial. La gestión se desarrolla con ética, enfoque al cliente, sentido económico y responsabilidad social y ambiental.

Contexto, Entendimiento Organizacional



TRANSMISIÓN

GENERACIÓN



DISTRIBUCIÓN

UOC
www.uoc.edu

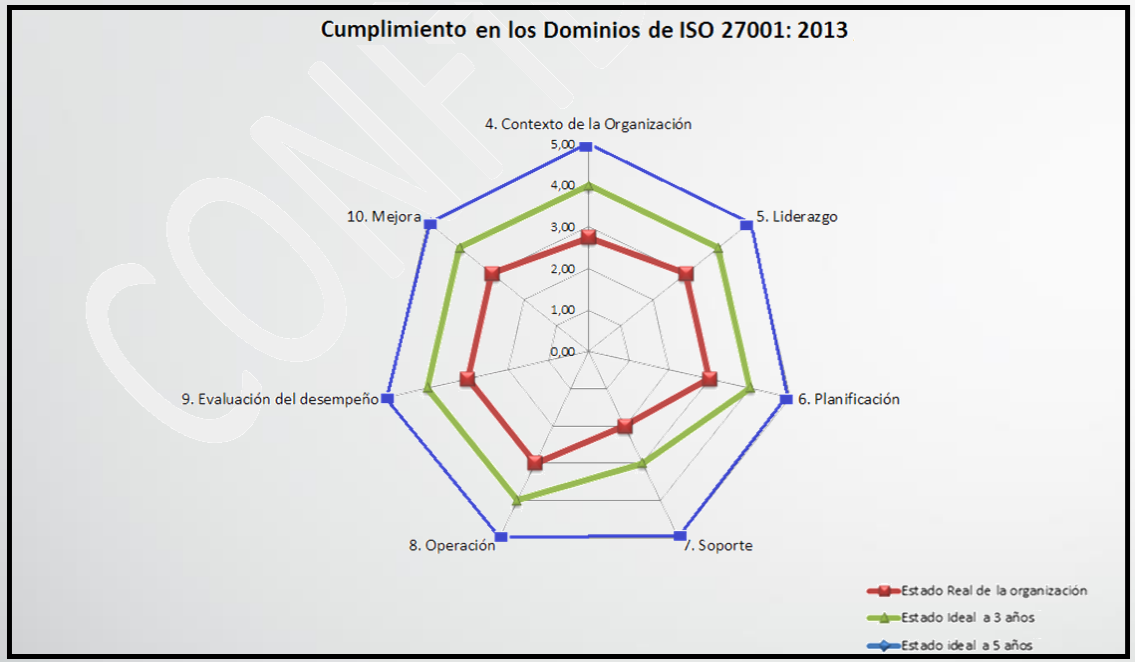
UAB
Universitat Autònoma de Barcelona

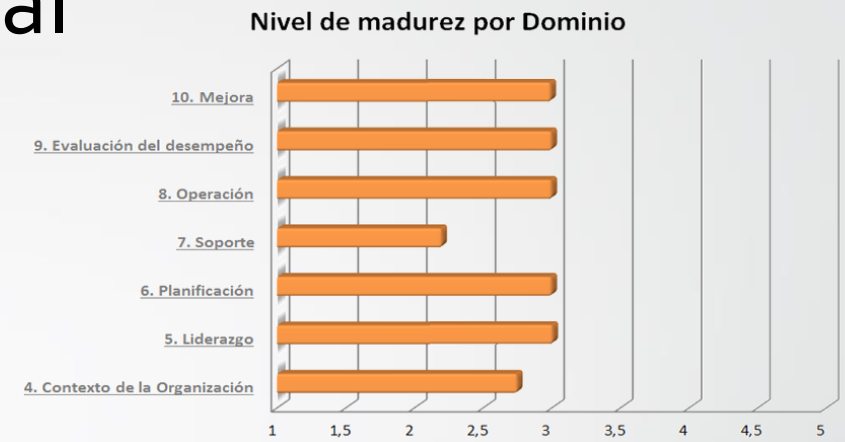
Universitat Rovira i Virgili

ANALISIS DIFERENCIAL ISO 27001:2013 METODOLOGIA COBIT/CMM

MODELO DE MADUREZ CONTROLES DE SEGURIDAD		
Escala	**%**	**Descripción**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	1	Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva.
Repetible	2	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Definido	3	Los procesos y los controles se documentan y se comunican. Es poco probable la detección de desviaciones.
Gestionado	4	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	5	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

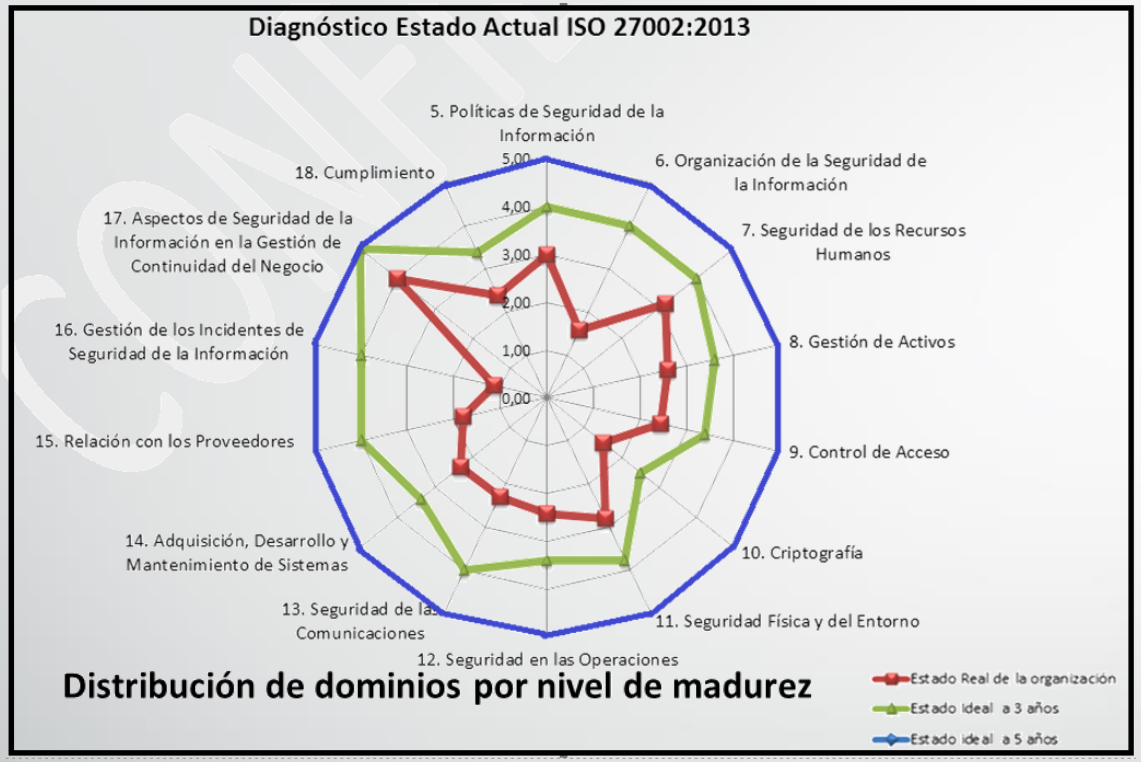
Fase 1: Análisis Diferencial Actual ISO 27001:2013

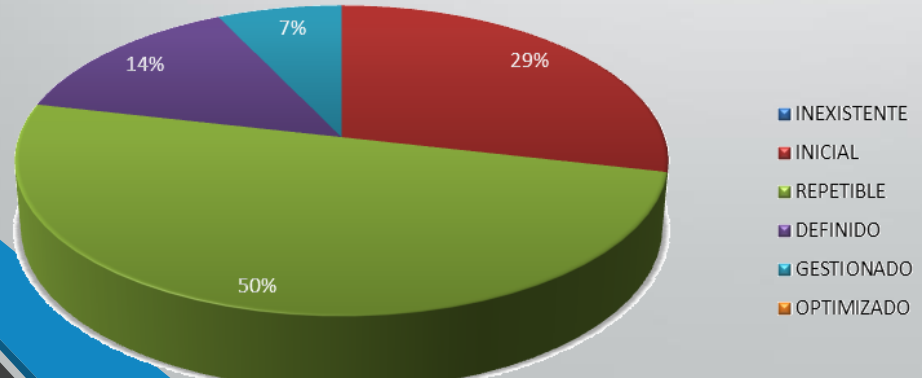




PUNTAJE – DOMINIO		
DOMINIO	Porcentaje	Calificación
4. Contexto de la Organización	2,75	Repetible
5. Liderazgo	3,00	Repetible
6. Planificación	3,00	Definido
7. Soporte	2,00	Repetible
8. Operación	3,00	Definido
9. Evaluación del desempeño	3,00	Definido
10. Mejora	3,00	Repetible
PROMEDIO	2,82	Repetible

Fase1: Análisis Diferencial Actual ISO 27002:2013





PUNTAJE - DOMINIO		
DOMINIO	Porcentaje	Calificación
5. Políticas de Seguridad de la Información	3,00	Definido
6. Organización de la Seguridad de la Información	1,57	Inicial
7. Seguridad de los Recursos Humanos	3,17	Definido
8. Gestión de Activos	2,60	Repetible
9. Control de Acceso	2,43	Repetible
10. Criptografía	1,50	Inicial
11. Seguridad Física y del Entorno	2,80	Repetible
12. Seguridad en las Operaciones	2,43	Repetible
13. Seguridad de las Comunicaciones	2,29	Repetible
14. Adquisición, Desarrollo y Mantenimiento de Sistemas .	2,31	Repetible
15. Relación con los Proveedores	1,80	Inicial
16. Gestión de los Incidentes de Seguridad de la Información	1,14	Inicial
17. Aspectos de Seguridad de la Información en la Gestión de Continuidad del Negocio	4,00	Gestionado
18. Cumplimiento	2,38	Repetible
PROMEDIO	2,39	Repetible

Hallazgos Críticos

ASPECTOS A MEJORAR

A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de Seguridad de la información se deben de revisar y actualizar periódicamente. Se debe dejar registro de esta actividad.

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Incluir la seguridad de la información en la gestión de proyectos. Independiente del tipo de proyecto.

Se deben definir políticas e implementar controles para los dispositivos móviles y teletrabajo

ASPECTOS A MEJORAR

6. PLANIFICACIÓN

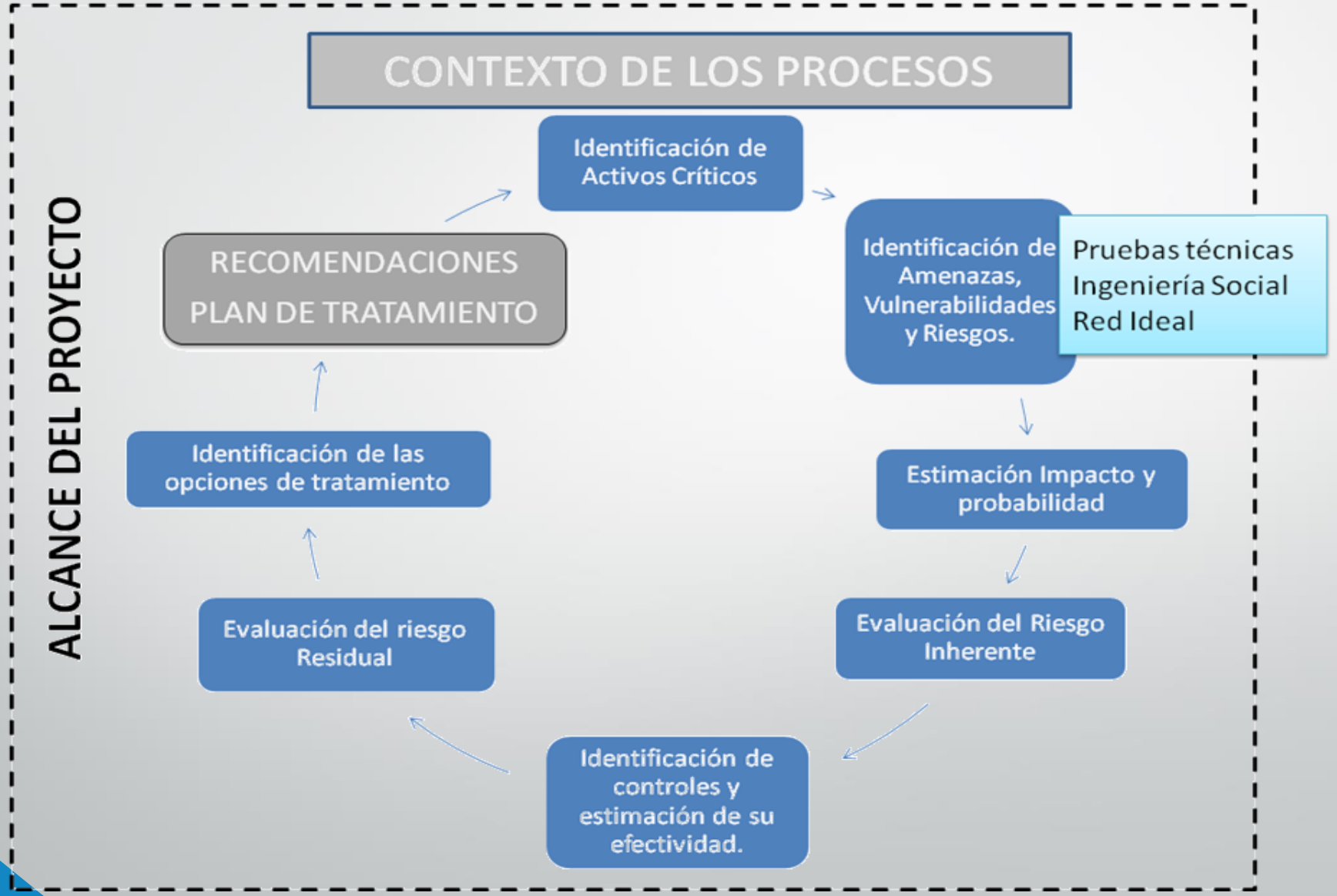
Definir y establecer los objetivos de seguridad de la información y planes para lograrlo

7. SOPORTE

Definir las competencias necesarias para la adecuada gestión de las actividades relacionadas con el SGSI y generar planes de acción para que los responsables cuenten con ellas.

Fase 2: Sistema de Gestión Documental SGSI Planes de Acción

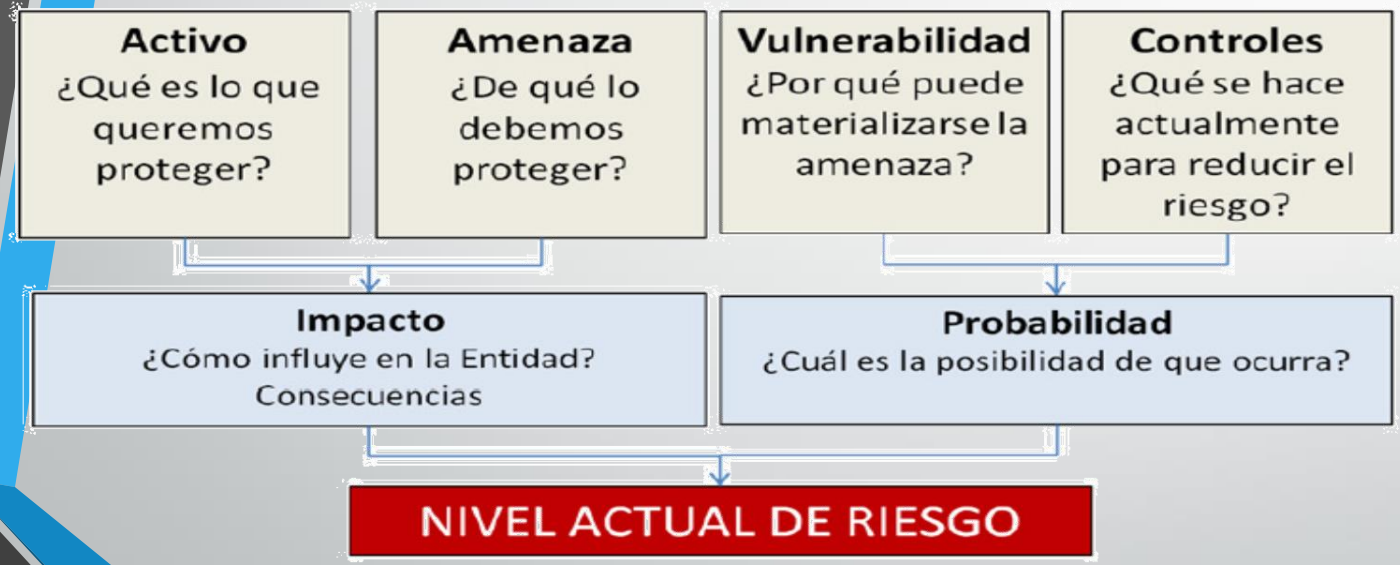
Fase 3: Gestión de Riesgos

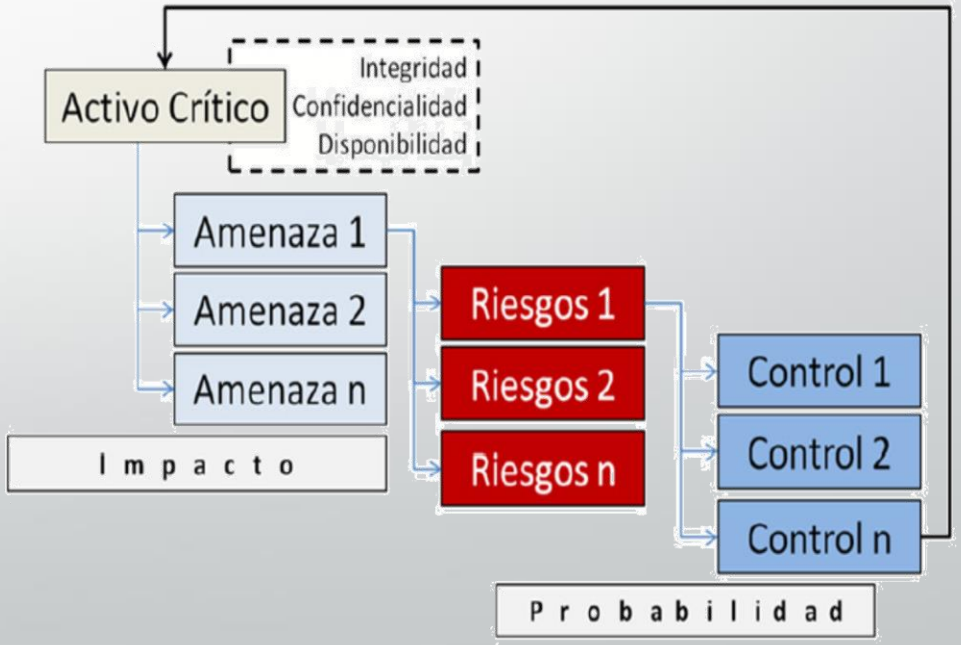


Fase 3: Gestión de Riesgos

Introducción al proyecto SGSI
Por que se esta realizando la actividad?

Explicación de la Metodología
Como se evalúa los riesgos?





Fase 3: Gestión de Riesgos

ISAGXXX

ACTIVOS CRÍTICOS ISAGXXXX

del ivo	Nombre Activo	Descripción y Observaciones	Proceso dueño del	Proceso que identifica el	Tipo	Fecha ingreso de	Fecha salida de	Estado del	Físico	Perímetro	Electrónico	Propietario Definido	Custodio Definido	Usuario definido	Personal	Financiera	Confidencialidad	Integridad	Disponibilidad	CRITICIDAD
R01	Informes de inspección	Solicitudes que llegan de las gerencias de producto o de las sucursales con el informe de la inspeccion, direccion del cliente, linderos,	Inspección de riesgos Generales	Inspección de riesgos Generales	Información	18-nov-14		Activo	Sucursales	Oficina Cerrada	Almacenado en la NAS	Oficina de administración de riesgos	Gerencia de tecnologia de la información	Oficina de administración de riesgos	No	No	PRIVADA	ALTO	ALTO	ALTO
R02	Información de posibles asegurados	Información de posibles asegurados	Inspección de riesgos Generales	Inspección de riesgos Generales	Información	18-nov-14		Activo	No	N.A.	Almacenado en SISE	Oficina de administración de riesgos	Gerencia de tecnologia de la información	Oficina de administración de riesgos	No	No	PRIVADA	ALTO	ALTO	ALTO
R04	Datos de la poliza	Las inspecciones del riesgo llegan de las gerentes de producto, sucursales y del area de riesgo (aquellos donde se necesita renovar las polizas o inspeccionarla por politicas de suscripción)	Inspección de riesgos Generales	Inspección de riesgos Generales	Información	18-nov-14		Activo	No	N.A.	Almacenado en SISE	Sucursal, gerente de producto y oficina de administracion	Sucursal, gerente de producto y oficina de administracion de riesgos, Gerencia	Sucursal, gerente de producto y oficina de administracion de riesgos	No	No	USO INTERNO	ALTO	ALTO	ALTO
R01	Informe de inspección: fisico o electronico	Informe de estudio e inspección para Riesgos especiales en polizas muy particulares (por ejemplo, polizas de almacenamiento de papel, fabricas de pinturas, productos quimicos, etc.)	Inspección de riesgos Generales	Inspección de riesgos Generales	Información	18-nov-14		Activo	Expediente de la póliza	Oficina Cerrada	Almacenado en la NAS	Sucursal, gerente de producto y oficina de administracion	Sucursal, gerente de producto y oficina de administracion de riesgos Gerencia	Sucursal, gerente de producto y oficina de administracion de riesgos	No	No	PRIVADA	ALTO	ALTO	ALTO
R01	Profesional lo especializado técnico	Profesional técnico con gran experiencia, quien realiza los estudios de riesgos técnicos.	Inspección de riesgos Generales	Inspección de riesgos Generales	Personas	18-nov-14		Activo	N.A.	N.A.	N.A.	N.A.	N.A.	Oficina de administracion de riesgos	No	No	PRIVADA	SIN CLASIFICAR	ALTO	ALTO
R01	Banco de inspecciones	Repositorio banco de inspecciones almacenado en la NAS (se almacena la información de riesgos facultativos y no	Inspección de riesgos Generales	Inspección de riesgos Generales	Información	18-nov-14		Activo	No	N.A.	Si	Oficina de administracion de riesgos	Gerencia de tecnologia de la información	Oficina de administracion de riesgos	No	No	PRIVADA	ALTO	ALTO	ALTO
R07	Equipos deingeniería	Camara termografica, medidor laser hilt, detector de gases, filmadora SONY, camara fotografica FUJY y GPS.	Inspección de riesgos Generales	Inspección de riesgos Generales	Hardware	18-nov-14		Activo	Almacenado en la oficina de	Especial	N.A.	Oficina de administracion de riesgos	Oficina de administracion de riesgos	Oficina de administracion de riesgos	No	No	PRIVADA	ALTO	ALTO	ALTO
R08	Sistema de información de los equipos de ingeniería	Programas o sistemas operativos de los equipos de ingeniería.	Inspección de riesgos Generales	Inspección de riesgos Generales	Software	18-nov-14		Activo	N.A.	N.A.	N.A.	Oficina de administracion de riesgos	Oficina de administracion de riesgos	Oficina de administracion de riesgos	No	No	PRIVADA	ALTO	ALTO	ALTO
R09	Recomendaciones para el cliente y el folio completo	Información enviado por correo electrónico que es una parte del informe de inspección.	Inspección de riesgos Generales	Inspección de riesgos Generales	Información	18-nov-14		Activo	N.A.	N.A.	Correo electrónico	Sucursal, cliente y oficina de administracion	Sucursal y oficina de administracion de riesgos	Sucursal, cliente y oficina de administracion de riesgos	No	No	PRIVADA	ALTO	ALTO	ALTO
F46	Sistemas SCADA	Archivo generado por la subgerencia de caja a traves del sistema SISE y se carga en un portal bancario para el envio de pagos electrónicos.	Proceso Caja	Proceso Caja	Información	18-nov-14		Activo	No	N.A.	SISE	Subgerente de Caja, Banca y Coaseguros	Subgerencia de Caja, Banca y Coaseguro	Subgerencia de Caja, Profesional de caja, Gerente de Operaciones y Vicepresidencia	No	Si	PRIVADA	ALTO	ALTO	ALTO
E51	Cheques, pagares y	Activo modificado por el comité de seguridad Custodia total de caja, el cual se almacena en	Proceso Caja	Proceso Caja	Información	18-nov-14		Activo	Caja fuerte Área de	Oficina	SISE	Subgerente de Caja, Banca y	Subgerencia de Caja, Banca y	Subgerencia de Caja, Gerencia	No	Si	PRIVADA	ALTO	ALTO	ALTO

Fase 3: Gestión de Riesgos

FACTOR DE RIESGO	ID	AMENAZA
INFRAESTRUCTURA FÍSICA	A01	Mala distribución del área o diseño del puesto de
	A02	Falta de orden y aseo
	A03	restringidas)
	A04	Incendio, inundacion o contaminación (aire y polvo)
	A05	Instalaciones y estructuras deficientes e inadecuadas (Fallas en edificios, oficinas y áreas de trabajo)
EVENTO EXTERNO	A06	Actos delictivos. (Agresión, asaltos, vandalismo o atentados, secuestro, extorción, fraude o robo, etc)
	A07	Desastres Naturales (Geologica y climatica)
	A08	aire acondicionado) o enlaces de comunicaciones (Internet)
TECNOLOGICA	A10	Hacking (Cracking de contraseñas o llaves, Deconfiguración o Suplantación de sitios Web, Distribucion de Spam, Eavesdrooping, DoS, Ejecucion de pruebas maliciosas o escaneos, etc)
	A11	Distribución de virus, Troyano, gusano o código malicioso de computador
	A12	Acceso lógico no autorizado (sistemas o redes)
	A13	Sobrecarga de sistema (Mal desempeño de las aplicaciones)
	A14	Incumplimiento de ciclos de mantenimiento
	A15	Malfuncionamiento de computadores o equipos de red (Deterioro y fallas técnicas de HW y SW)
	A16	Malfuncionamiento de las aplicaciones o software de sistemas
	A17	Incumplimiento de las politicas de manejo de equipos y medios tecnológicos (Instalación de software no autorizado, Uso de SW no licenciado, Pirateria o robo de SW, Descarga o envio de contenido
	A18	hardware

ID_Vuln	VULNERABILIDADES
V01	Instalaciones y estructura deficiente o antigua
v02	Susceptibilidad a temperatura, humedad, polvo y suciedad
v03	Inadecuado control de acceso lógico y/o físico a los activos de información.
v04	Incumplimiento en los procedimientos de control de visitantes e ingreso a las areas restringidas.
V05	Dependencia de servicios de terceros
V06	Inexistencia de respaldo y/o custodia de los activos de información
V07	Planes de continuidad parcialmente implementados. (Inadecuada prevención y gestión de desastres como incendios, terremotos, inundaciones en otros)
V08	Falta de abastecimiento de los servicios públicos básicos: energía, agua, gas, aire acondicionado.
V09	Ausencia de controles de cifrado en las comunicaciones
V10	Falta de protección contra virus y código malicioso.
V11	Monitoreo, segmentación y controles de red Incompletos
V12	Ausencia de mecanismos de control y monitoreo de red
V13	Ausencia de pistas de auditoría
V14	Ausencia de auditorías regulares
V15	Falta de mantenimientos predictivos, preventivos y correctivos constantes y/o respuesta inadecuada de mantenimiento del servicio
V16	Planes de renovacion tecnologica inexistentes o deficientes
V17	Ausencia o falla en los procedimientos de control de cambios.

ID	RIESGOS O CONSECUENCIA
R01	Alteración de Información no autorizada
R02	Fuga o divulgación de información confidencial
R03	Interrupción del servicio
R04	Pérdida de credibilidad, competitividad o imagen de la entidad.
R05	Información para la toma de decisiones errada o inoportuna.
R06	Daño o pérdida de activos.
R07	Sanciones económicas o legales
R08	Fraude / Robo

Fase 3: Gestión de Riesgos

Mapa De riesgos:	Matriz de riesgos definida por ISAGXXX Compañía de Seguros que permite visualizar en un Diagrama de calor los escenarios de riesgos con escala de prioridades tras haber referido los factores impacto y probabilidad.
Matriz de activos críticos:	Matriz con la información que describe los activos de información valorados como Críticos de acuerdo a la valoración de Confidencialidad, Integridad y Disponibilidad, a los cuales se les realizó el proceso de valoración de riesgos.
Matriz Rsg:	Matriz consolidada que contiene las amenazas, riesgos y controles asociados a cada activo de información analizado en la evaluación de riesgos .
Gráfica Distribución Amenazas	Gráfica de Distribución de Amenazas identificadas en la valoración de riesgos
Gráfica Top 10 Amenazas	Gráfica de las 10 amenazas mas referenciadas por los funcionarios entrevistados
Gráfica Distribución Riesgos	Gráfica de Distribución de Riesgos identificados en la valoración de riesgos
Distribución Cnt_por_efectibidad:	Tabla de distribución de controles teniendo en cuenta la efectibidad individual de los controles.
Gráfica Ausencia de controles:	Gráfica que consolida la lista de controles mas referenciados como inexistentes en ISAGXXX
Gráfica controles Débiles:	Gráfica que consolida la lista de controles mas referenciados como existentes con una efectibidad menor al 40% en ISAGXXX
Gráfica Controles Fuertes:	Gráfica que consolida la lista de controles mas referenciados como existentes con una efectibidad mayor al 80% en ISAGXXX
Gráfica Distribución RI:	Gráfica que consolidad de la distribución del Riesgo Inherente
Gráfica Distribución RR:	Gráfica que consolidad de la distribución del Riesgo Residual
Gráfica RI vs RR:	Gráfica que compara la distribucion de los Riesgos Ineherente y Residual teniendo en cuenta los valores establecidos en el mapa de riesgos (Mapa de Calor)
Grf_Amenazas_RR_Alto y crítico:	Gráfica de Distribución de Amenazas identificadas para los escenarios de riesgos donde el Riesgo Residual tiene valores Alto y crítico (Niveles en los cuales se les debe realizar tratamiento de los riesgos según el criterio de aceptacion de los riesgos)
Criterios clasificación Activos:	Criterios y niveles utilizados para la clasificacion de activos teniendo en cuenta la Confidencialidad, Integridad y Disponibilidad.
Formato Entrevista Rsg:	Formato entrevista de riesgos utilizado en las entrevistas de levantamiento de información para el análisis de Riesgos.
BD Controles:	Base de datos de los controles contemplados para el análisis de riesgos, con los criterios de relevancia de cada control que permite calcular la efectibidad de los controles.
Criterios Clasificación Rsg:	Criterios y niveles utilizados para la valoración de Impacto y probabilidad .

Fase 3: Gestión de Riesgos

ISAGXXXX

MATRIZ DE RIESGOS ISAGXXX

RIESGOS

ID Act	Nombre Activo	Descripción y Observaciones Activo	MacroProc	Proceso al que pertenece el activo	Tipo Activo	Amenazas	Probabilidad	Riesgo	Impacto	Riesgo Inherente	Para Riesgo Inherente	Riesgo Residual Calculado	Para Riesgo Residual Calculado	ID Cont	Control	Existe Un Es	Efectividad	Tipo de cont	Automatización	Obligatoriedad	Relevo Calcu
E-IR01	Informar de inspección	Solicitudes que llegan de las gerencias de productos de los recursos con el informe de la inspección, dirección del cliente, liderar.	Inspección de riesgos Generales	Inspección de riesgos Generales	Información		B	R01. Alteración de información no autorizada	A	ALTO	3	ALTO	2,102803738	C28	Controles de acceso física a las zonas restringidas(recepcion en zona de entrada, tarjetas de aproximación de accesos,sistemas biométricos, puertas cerradas con llave, puertas de acceso tipo esclusa,organizador)	E	40	Preventivo	Automática	Mandatoria	
							B	R02. Fuga divulgación de información confidencial	A	ALTO	3	ALTO	2,102803738	c29	Instalar y mantener un CCTV que grabe y almacene las imágenes y que debe estar conectado con el sistema de alarma	E	30	Detectivo	Automática	Mandatoria	
							B	R06. Daño a pérdida de activos	M	MODERADO	2	MODERADO	1,401869159	c33	Políticas y procedimientos establecidos de control de accesos físicos (politicas para mantener las puertas de las zonas restringidas,trackes cerradas con llave, procedimiento de autorización y acompañamiento de ingreso de visitantes a personal de reparto.	E	60	Preventivo	Manual	Mandatoria	
														c44	Control de entrada y salida de equipos en porterias. Las salidas deben estar debidamente autorizadas y registradas	E	50	Detectivo	Manual	Mandatoria	
														c131	Procesos de reporte y manejo de incidentes	NE	0	Detectivo	Manual	Mandatoria	
														c156	Estudios de vulnerabilidades, pruebas de penetracion internas y externas periodicas	NE	0	Detectivo	Manual	Discrecional	
														c19	Plan de Capacitación y entrenamiento en temas de seguridad de la información	NE	0	Preventivo	Manual	Mandatoria	
														C35	Identificación permanente del personal y carnet de visitantes	E	50	Detectivo	Manual	Mandatoria	
														C37	Gabinetes cerradas y seguras	E	20	Preventivo	Manual	Discrecional	
							B	R06. Daño a pérdida de activos	M	MODERADO	2	MODERADO	1,538461538	C38	Sistemas de Detección de humo (se recomienda instalar los sistemas en las ductos de aire acondicionado)	NE	0	Detectivo	Automática	Mandatoria	
						A04. Incendio, inundacion o contaminación (aire y polvo)	B	R04. Pérdida de credibilidad, competitividad o imagen de la	A	ALTO	3	ALTO	2,307692308	C39	Sistemas de detección y extinción de incendios (extintores de distintos tipos de fuego, puertas, ventanas y paredes en materiales antifuegos, rociadores y alarmas de fuego, dispositivos de agua)	NE	0	Detectivo	Automática	Mandatoria	
														C40	Controles de inundacion y filtraciones de agua (Tuberias fuera del contacto de datos, desagues en el exterior, impermeabilizaciones periodicas a la terraza del edificio)	NE	0	Detectivo	Automática	Discrecional	
														C78	Buenas prácticas de Backups (Frecuencia, Tipo de Backups, Rotación, pruebas, custodia, niveles de autorización, etc.)	E	80	Preventivo	Automática	Mandatoria	
						A08. Desastres Naturales (Geologicos y climaticos)	B	R03. Interrupción del servicio	B	BAJO	1	BAJO	0,551282051	C50	Se debe contar con un sistema eléctrico de emergencia que alimente los equipos críticos, sistemas de control de accesos, alarmas, rociadores , puertas, etc. durante una falla eléctrica	E	80	Preventivo	Automática	Mandatoria	
							B	R07. Sanciones económicas o legales	M	MODERADO	2	MODERADO	1,102564103	C71	Implementación de OLA (Acuerdos de nivel de la operación a nivel interno entre las áreas y TI). Definición de acuerdos de nivel de operación internos entre las unidades de negocio y TI	NE	0	Preventivo	Manual	Mandatoria	
														C68	Registros y analisis de fallas reportadas para ser usuarios a programas de monitoreo.	E	50	Detectivo	Manual	Mandatoria	
						A12. Accesos lógicos no autorizados (sistemas o redes)	B	R03. Interrupción del servicio	B	BAJO	1	BAJO	0,503225806	C90	Politicas de control de accesos definidas, aprobadas y documentadas	E	70	Preventivo	Manual	Mandatoria	
							B	R05. Información para la toma de decisiones errada o inoportuna	A	ALTO	3	MODERADO	1,509677419	c91	Procesos formales de solicitudes, autorización y asignación de cuentas	E	60	Preventivo	Automática	Mandatoria	
							B	R07. Sanciones económicas o	M	MODERADO	2	MODERADO	1,006451613	c92	Procedimientos de revisiones y eliminaciones de cuentas de usuarios que salen de la organización.	E	20	Detectivo	Manual	Mandatoria	
														C93	Eliminación de cuentas con permisos de administración locales. No deben existir cuentas administradores locales, para evitar que se instalen programas perjudiciales sin los debidos	E	90	Preventivo	Manual	Mandatoria	
														C96	Validación periódica de roles y perfiles	NE	0	Detectivo	Manual	Discrecional	
														C97	Políticas de contraseñas (cambios periódicos, complejidad, expiración, no repetir contraseñas recientes, UnicaID, consistencia, privacidad, etc.)	E	90	Preventivo	Automática	Mandatoria	
														C99	Bloqueos de sesiones por inactivación	E	90	Preventivo	Automática	Mandatoria	
														C100	Política de pantallas y escritorios limpios	E	20	Preventivo	Manual	Mandatoria	
														C104	Integración de cuentas con Directorio activo y manejo de políticas de grupos por sitios. (Implementación de políticas de grupos controladas desde el controlador de dominio, para que los miembros del dominio reciban propiedades de controles centrales)	NE	0	Detectivo	Automática	Discrecional	
														C111	Existencia de listas de personal autorizado para acceder la información, Producto de la clasificación de información se crea una lista del personal autorizado y los permisos con sus	NE	0	Detectivo	Manual	Discrecional	
						A23. Errores en la ejecución de las Actividades de mejoramiento y seguimiento.	M	R02. Fuga divulgación de información confidencial	A	ALTO	3	MODERADO	1,827906977	C15	Manual de funciones y funciones documentado	E	60	Preventivo	Manual	Mandatoria	
							M	R04. Pérdida de credibilidad, competitividad o imagen de la	A	ALTO	3	MODERADO	1,827906977	C17	Responsabilidades en cuanto a la seguridad de la información establecidas en el contrato de vinculación.	E	20	Preventivo	Manual	Mandatoria	
							M	R05. Información para la toma de decisiones errada o inoportuna	A	ALTO	3	MODERADO	1,827906977	C18	Medidas de desempeño y cumplimiento hacia el empleado o contratista.	NE	0	Detectivo	Manual	Discrecional	
							M	R06. Daño a pérdida de activos	M	MODERADO	2	MODERADO	1,218604651	C19	Plan de Capacitación y entrenamiento en temas de seguridad de la información	E	40	Preventivo	Manual	Mandatoria	
							M	R08. Fraude o robo	M	MODERADO	2	MODERADO	1,218604651	C20	Plan de Capacitación para el desempeño de las actividades de los funcionarios.	E	70	Preventivo	Manual	Mandatoria	
														C25	Rotación de funciones	NE	0	Preventivo	Manual	Discrecional	
														C24	Evaluaciones de carga laboral. Realización periódica de evaluaciones de carga laboral para establecer capacidades de oficinas	NE	0	Detectivo	Manual	Discrecional	
														C06	Acuerdos de confidencialidad.	E	90	Preventivo	Manual	Mandatoria	

Fase 3: Gestión de Riesgos

MAPA DE RIESGOS

PROBABILIDAD DE OCURRENCIA					
Muy Alta	1	2	3	4	Riesgo Inherente Extremo
Alta	1	2	3	Riesgo Inherente Alto	4
Moderada	1	2	Riesgo Inherente Moderado	3	4
Baja	1	Riesgo Inherente Bajo	2	3	4
Muy Baja	1	1	2	3	4
	Inferior	Menor	Importante	Mayor	Superior

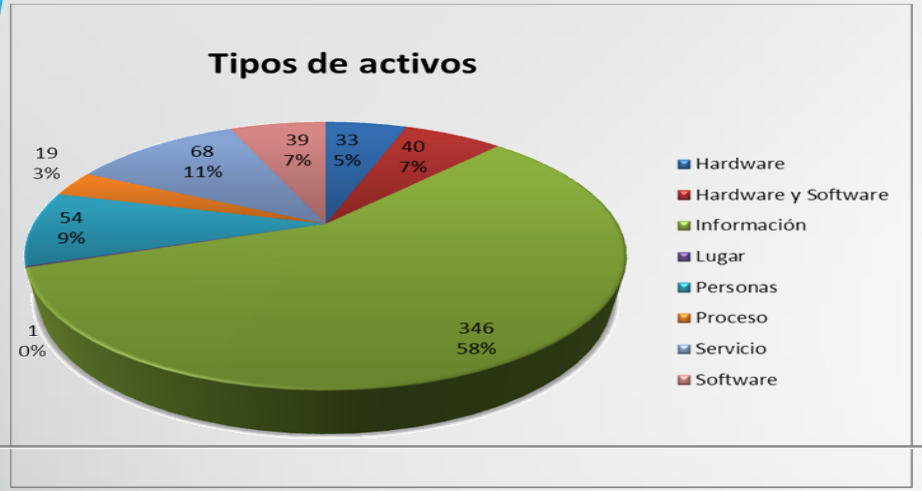
MAGNITUD DEL IMPACTO

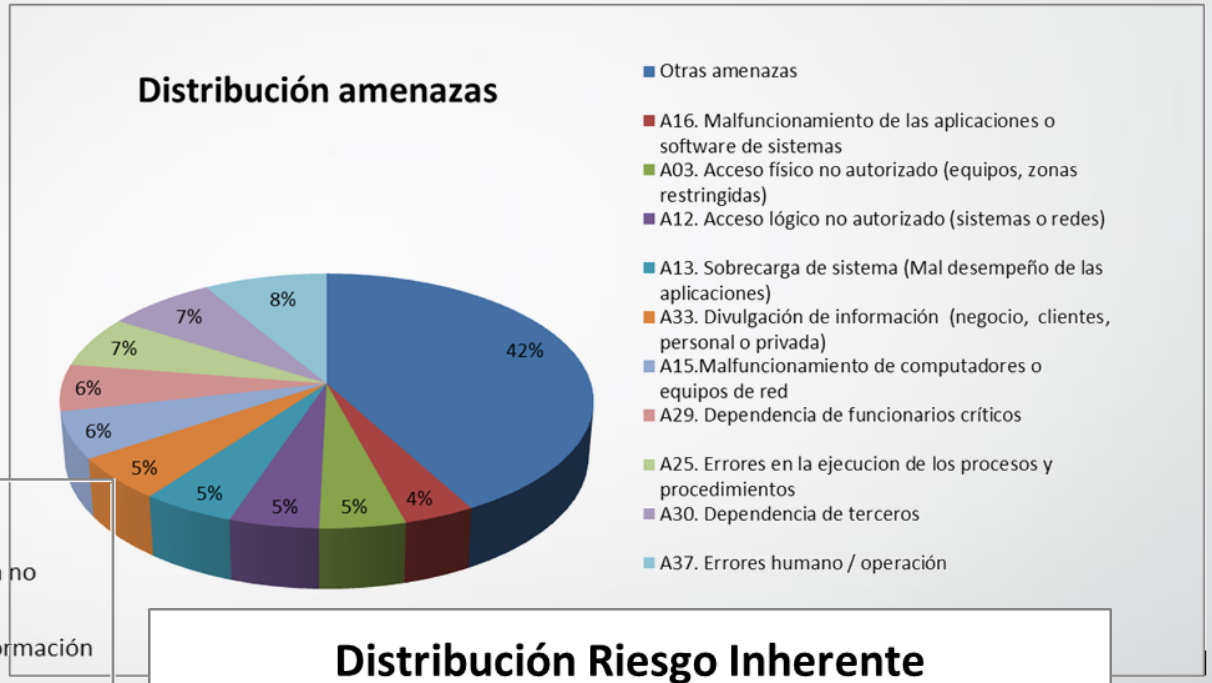
MATRIZ DE OPCIONES DE TRATAMIENTO

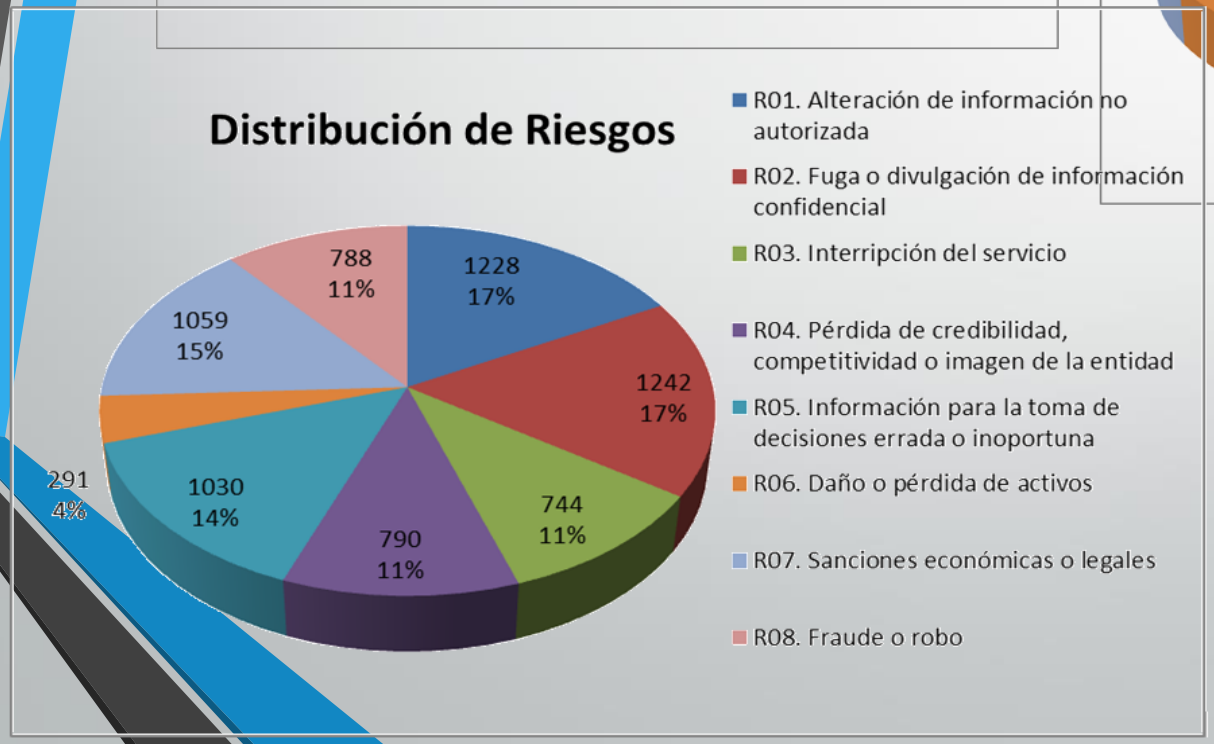
PROBABILIDAD DE OCURRENCIA					
Muy Alta	Retener los riesgos	Reducir o controlar el impacto y/o probabilidad	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos
Alta	Retener los riesgos	Reducir o controlar el impacto y/o probabilidad	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos
Moderada	Retener los riesgos	Reducir o controlar el impacto y/o probabilidad	Reducir o controlar el impacto y/o probabilidad	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos
Baja	Retener los riesgos	Retener los riesgos	Reducir o controlar el impacto y/o probabilidad	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos
Muy Baja	Retener los riesgos	Retener los riesgos	Reducir o controlar el impacto y/o probabilidad	Reducir o controlar el impacto y/o probabilidad.	Reducir o controlar el impacto y/o probabilidad. Transferir lo riesgos
	Inferior	Menor	Importante	Mayor	Superior

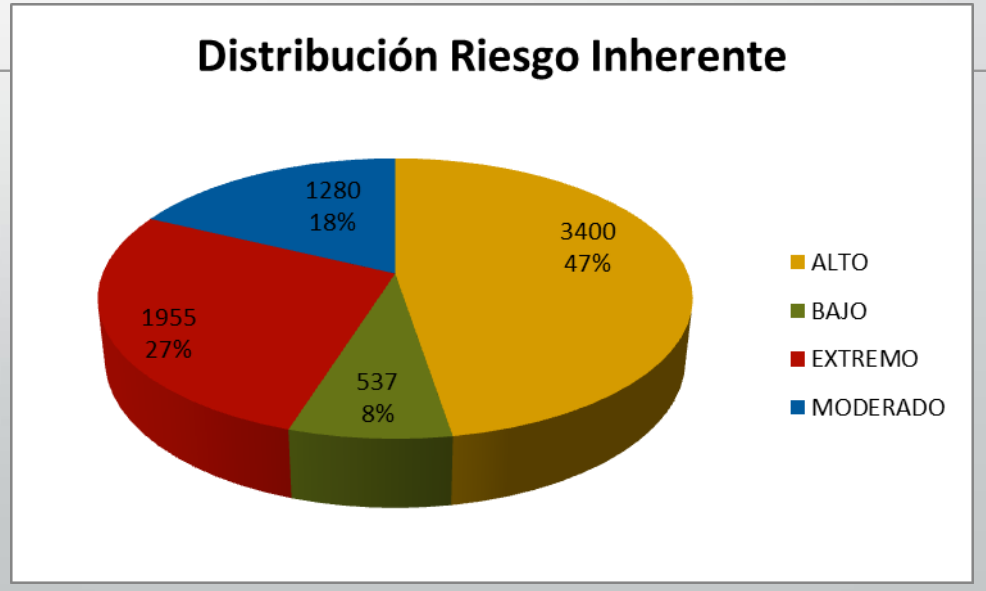
MAGNITUD DEL IMPACTO

Fase 3: Resultados Gestión de Riesgos









Fase 4: Proyectos de Seguridad Propuestos PTR- Planes de Tratamiento del Riesgo

1.Modelo de gobierno de seguridad de la información

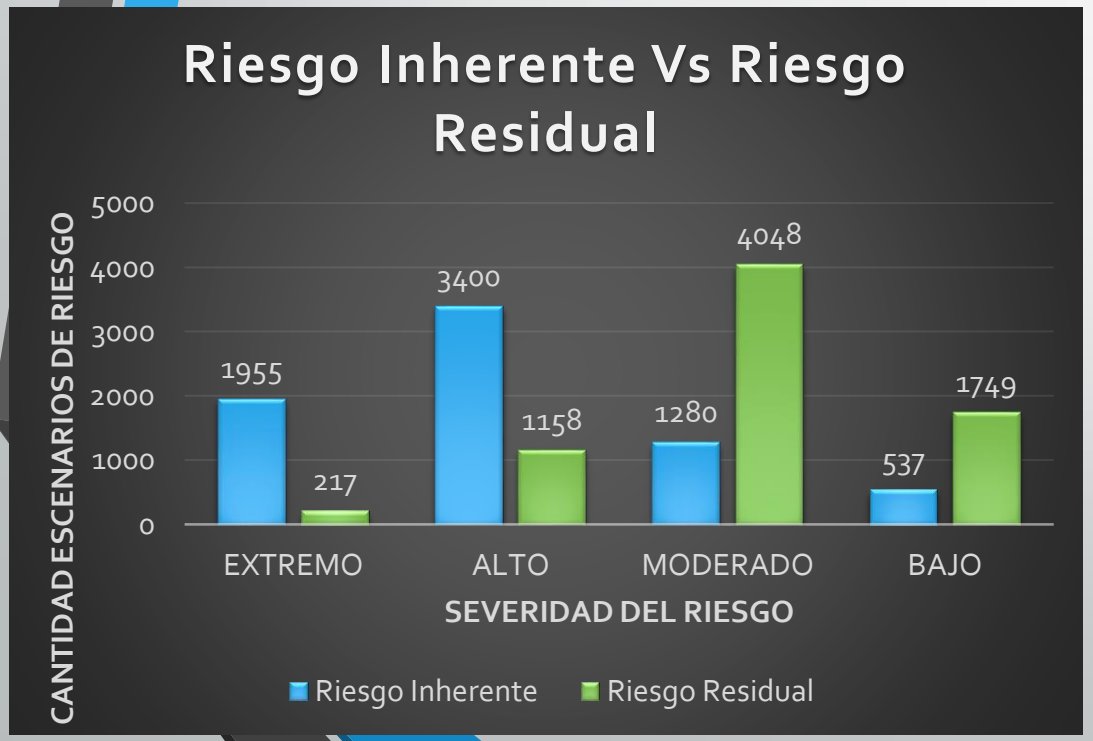
PLANES DE ACCIÓN E IMPLEMENTACIÓN DE TECNOLOGIA

ID	% completa	INICIATIVA	DESCRIPCIÓN	JUSTIFICACIÓN	BENEFICIOS	PRIORID	TIPO	TIEMPO	INDICADOR	RANGO DE COSTO APROX (EXPRESADO
1.1	0%	Documentar una política asociada con el uso de dispositivos móviles y medios removibles	La regulación corporativa frente al uso de dispositivos móviles debe estar claramente definida, considerando aspectos asociados con el uso, nivel de riesgo asociado, delimitación de las funciones en el entorno laboral y conectividad. Adicionalmente debe contemplar la posibilidad de que ISAGXXX desarrolle su tienda de aplicaciones propia con el software autorizado para instalar. Respecto al uso de medios removibles se considera necesario incluir aspectos como: El contenido de todo medio re-utilizable, previamente a ser desechado deberá procesarse para hacerlo irrecuperable. Cuando sea necesario se deberá requerir autorización para retirar medios de la organización dejando la correspondiente constancia escrita. Todo medio deberá ser almacenado en un ambiente protegido y seguro, de acuerdo con las especificaciones del fabricante. Si el tiempo de guarda de la información almacenada fuera mayor que el tiempo de vida de los medios de soporte deberán adoptarse previsiones para evitar pérdidas por degradación física. Los dispositivos de soporte de medios removibles en los sistemas solamente deberán ser habilitados cuando existan razones operativas que lo justifiquen. Los medios que contienen información confidencial deberán ser almacenados y eliminados de manera segura y efectiva, ya sea mediante destrucción o borrado de datos para ser utilizados por otra aplicación dentro de la organización o entregados en donación.	Debido a que ISAGXXX cuenta con lineamientos basicos respecto al uso de dispositivos móviles, se hace necesario implementar una politica robusta que permita ejercer control y gestión frente al amplio margen de vulnerabilidades y riesgos asociados con entornos basados en movilidad y uso de medios removibles, tales como fuga de información, propagación de malware y uso inapropiado de la tecnología en general.	Alineado completamente con los objetivos del negocio	ALTA	SERVICIO	0 a 6 Meses	Disminución del uso de dispositivos móviles y removibles no autorizados en el entorno laboral. Disminución de consumo de recursos de red por conexiones hacia dispositivos inalámbricos Disminución de incidentes por perdida de información almacenada sin autorización en dispositivos móviles y medios removibles no autorizados. Disminución de incidentes por propagación de malware y software malicioso en general.	0 a 5000
			La organización debe mantener control permanente							

Fase 4: Proyectos de Seguridad Propuestos PTR- Planes de Tratamiento del Riesgo

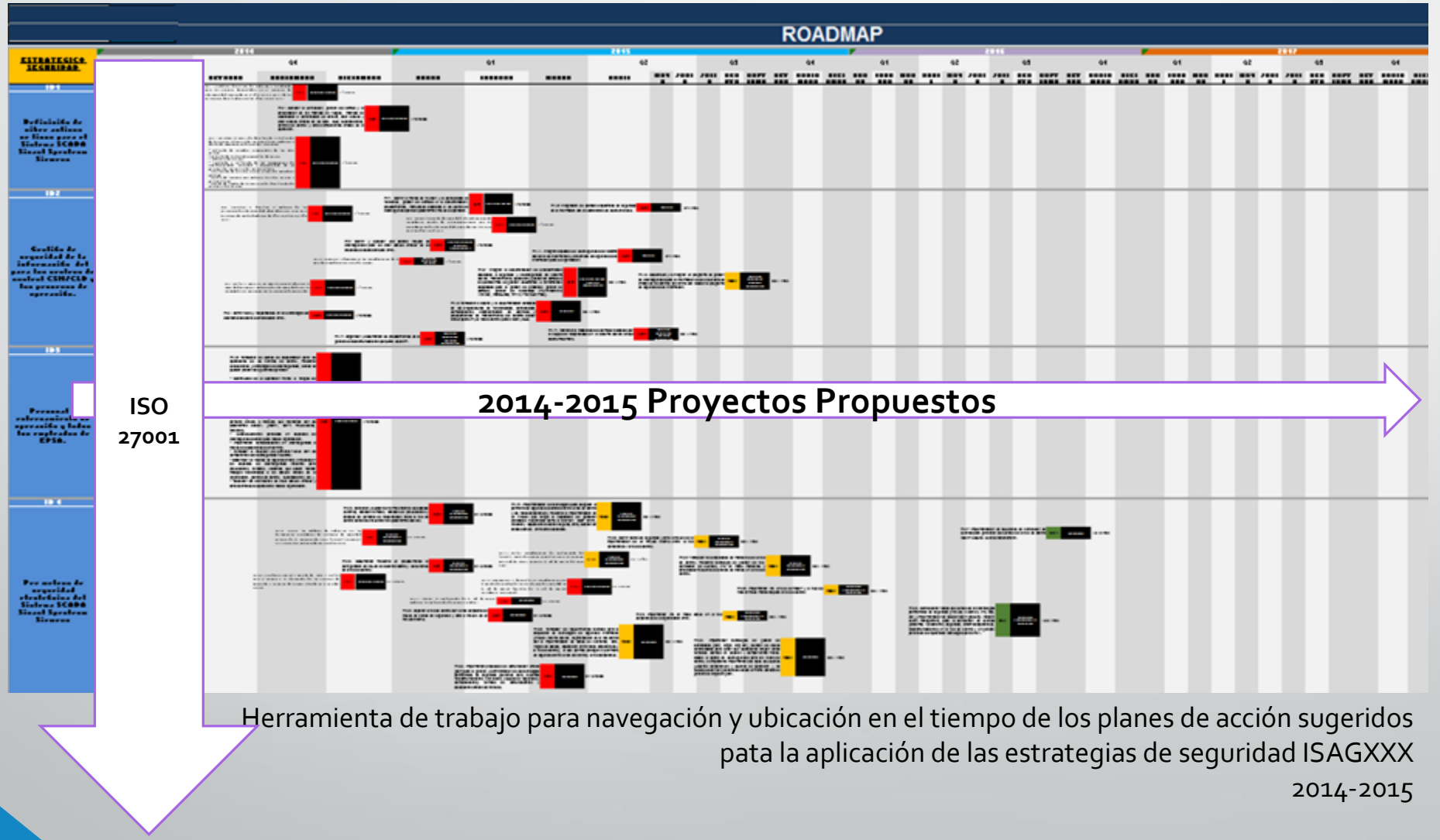
Herramienta de trabajo para navegación y gestión efectiva de los planes de acción sugeridos pata la aplicación de las estrategias de seguridad ISAGXXX

2014-2015



ACTIVIDAD	2014 SEP	2014 OCT	2014 NOV	2014 DIC	2015 ENE	2015 FEB
7.2.1 Fortalecer el área de Seguridad de la Información	CORTO PLAZO					
7.2.2 Lineamientos de seguridad de la Información						
7.2.3 Clasificación de la información						
7.2.6 Fortalecer niveles de seguridad sobre equipos Informáticos (Hardening)						
7.2.8 Proceso de gestión de incidentes						
7.2.5 Fortalecer controles de seguridad física			MEDIANO PLAZO			
7.2.9 Aislamiento y protección lógico de red						
7.2.10 Implementación de un sistema DLP (Data Leak Prevention)						
7.2.12 Esquema de alta disponibilidad en los canales de internet						
7.2.13 Baseline de seguridad para equipos					LARGO PLAZO	
7.2.15 Establecimientos de zonas críticas con controles físicos y medioambientales adecuados.						
7.2.4 Concientizar periódicamente en temas de Seguridad de la Información	ACTIVIDADES PERMANENTES					
7.2.7 Auditoría y seguimiento a terceros						
7.2.11 Acuerdos de Confidencialidad						
7.2.14 Evaluaciones de desempeño y carga laboral a empleados y contratistas						

ROADMAP SEGURIDAD DE LA INFORMACIÓN ISAGXXX 2014-2015



Herramienta de trabajo para navegación y ubicación en el tiempo de los planes de acción sugeridos pata la aplicación de las estrategias de seguridad ISAGXXX 2014-2015

Planes De Acción
Corto Plazo 2014

- Validar las políticas de seguridad sugeridas. Estas políticas deben ser avaladas, formalizadas y difundidas a todos los funcionarios, responsables e interesados en mantener prácticas adecuadas en el manejo seguro de la información.
- Implementar un sistema de bandas e inspección de paquetes en la entrada del edificio de Casa matriz.
- Implementar un sistema automatizado de control de ingreso y retiro de elementos administrados por personal de ISAGXXX.
- Definir OLA´s o Acuerdos de Nivel de Operación internos entre las unidades de negocio.
- Incluir en los planes de auditoría las actividades y procesos realizados por terceros.
- Incluir la disponibilidad de proveedores Backups.
- Promover la disponibilidad y adecuada capacitación de Funcionario Backup.
- Establecer y comunicar los procesos disciplinarios por faltas a seguridad de la información.
- Establecimiento y renovación de acuerdos de confidencialidad a empleados y contratistas.
- Desarrollar, divulgar y realizar pruebas a planes de recuperación de la infraestructura tecnológica.
- Configuración de servidores y equipos de comunicación con lineamientos básicos de seguridad
- Incluir esquemas de alta disponibilidad para los sistemas Core de la Organización.

Planes De Acción Mediano Plazo 2015

- Implementar tecnologías de monitoreo a nivel de red, equipos de comunicaciones, IPS, firewall en el perímetro de seguridad electrónica entre la red corporativa y la red de control.
- Integrar mediante las herramientas de gestión documental de la organización, todos los procedimientos e instructivos de la gestión de los proveedores, grupo analista del sistema SCADA, información de procesos, gestión tecnológica, gestión de la operación y gestión de las telecomunicaciones.
- Desarrollar pruebas de ciberseguridad periódicas a las plataformas SCADA de la organización.
- Fortalecer la gestión de accesos y niveles de seguridad a los recursos compartidos identificados en servidores críticos, para el acceso a información de la operación.
- Fortalecer los RFP o requerimientos técnicos de la solución SCADA que se encuentra en proceso de modernización para el año 2017, en base a los siguientes criterios en materia de ciberseguridad:

- Gestión de Mínimo Privilegios
- Ciclo de vida de gestión del software para la aplicación SCADA
- Gestión de Cambios integrada
- Integración de gestión de roles y perfiles con el Directorio activo.
- Cumplimiento normativo NERC y otros aspectos de ciberseguridad.

- Desarrollar estudios de viabilidad para la incorporación de tecnologías de ciberseguridad para los centros de control, tales como [IPS, FIREWALL, SIEM, Aplications Control en ambientes SCADA].

Planes De Acción Largo Plazo 2015

- Adquirir soluciones de seguridad que permitan fortalecer las siguientes necesidades en materia de seguridad.

IPS/IDS Scada / Gestión y correlación de Eventos / SIEM – Correlación y gestión de eventos de seguridad

Sing On – Gestión de Identidades / Aplications Control – Control de aplicaciones en las estaciones de operación SCADA

SOC – Outsorcing de Seguridad Gestionada / Soluciones para gestión documental integrada

Fase 5:Auditoria de Cumplimiento 2014 ISO 27001:2013

- Para obtener la certificación.
- Revisar conformidad con la norma (ISO/IEC 27001)
- Revisar grado de puesta en práctica del sistema
- Revisar la eficacia y adecuación en el cumplimiento de:
  - Política de seguridad
  - Objetivos de seguridad
- Identificar las fallas y debilidades en la seguridad
- Proporcionar una oportunidad para mejorar el SGSI,
- Cumplir requisitos contractuales.
- Cumplir requisitos regulatorios.
- Identificación de SAC mayores, menores y oportunidades de mejora.
- Programas de auditorias y gestión del SGSI.
- Compromiso por parte de la Dirección.

SOLICITUD DE ACCION CORRECTIVA MAYOR/MENOR/INFORMATIVA

No SAC: 1	Auditor: Robin Salcedo	Fecha:17/04/2012
Procedimiento: Pruebas, Mantenimiento y Reevaluación de Planes de Continuidad.		Área/Dpto/Función: Gestión de Continuidad
Referencia ISO 27001: A-14.1.5		Tipo Conformidad: **Mayor**

Detalles de la no conformidad: se identifica la ausencia de procedimientos asociados con la planificación, implementación, revisión y monitoreo de planes y programas relacionados con pruebas y mantenimiento del plan de continuidad, no se está implementando un plan de emergencia para probar planes de continuidad en los datacenter CUNI y SANTA BARBARA, no se tiene una prueba parcial del plan y no se identifican los mecanismos para identificar roles y responsables.

La naturaleza de la no conformidad con relación al dominio de Gestión Continuidad surge de la ausencia total de control de seguridad al requerimiento A-14.1.5 de la norma ISO 27001.

Situación Real Evidenciada:

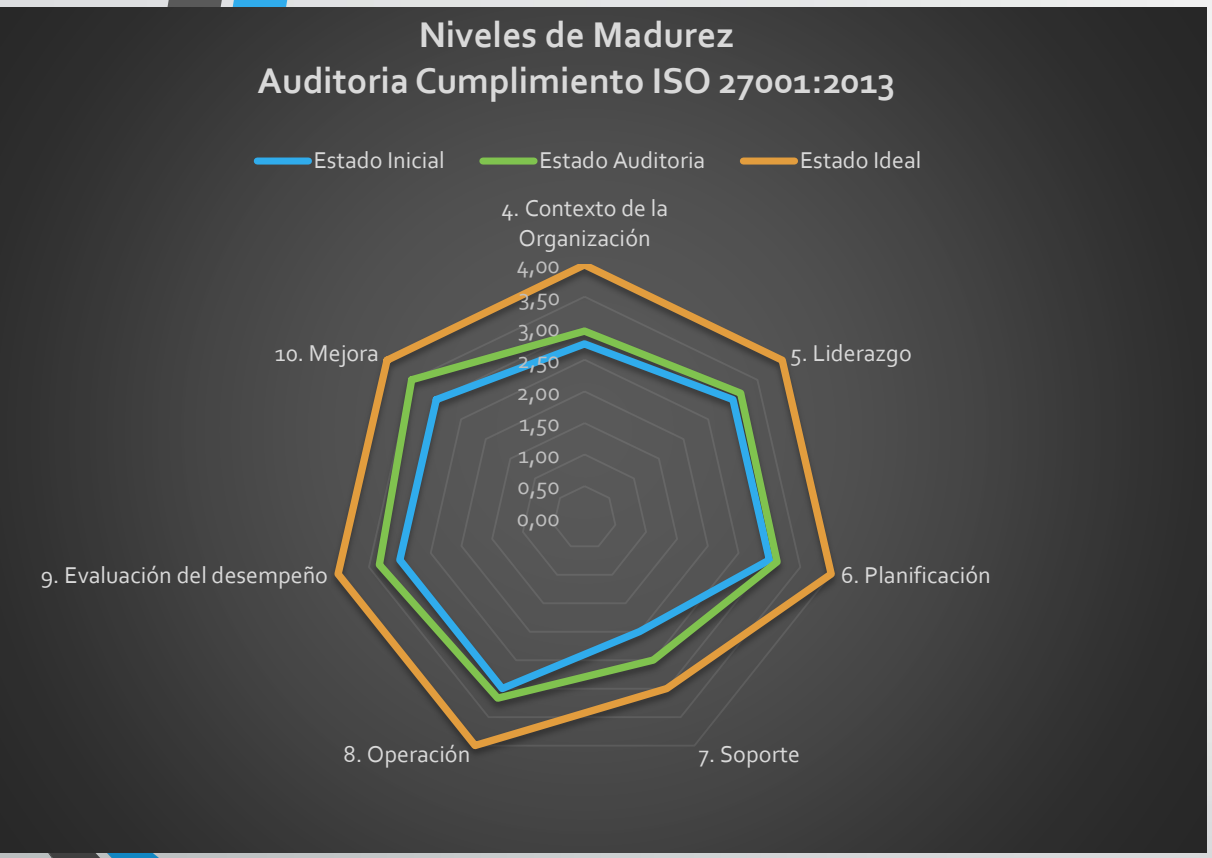
En la inspección física del Datacenter CUNI, no se identifica un mapa de evacuación en las áreas de trabajo y luego de una serie de consultas y preguntas al operador de turno, no se tiene conocimiento de los planes de evacuación del Datacenter.

Plan de Acción: Es necesario desarrollar los planes de pruebas y realizar una prueba parcial a cada uno de los datacenter (CUNI y SANTA BARBARA), poner a prueba el plan de continuidad en cada uno de los datacenter, adicionalmente probar los planes de emergencia, planes de mantenimiento, comités de evacuación y completar el ciclo de gestión del plan de continuidad de acuerdo a los 4 procesos del SGSI.

- Se deben asignar responsables para la realización de planes.
- Creación de programas de mantenimiento y pruebas a los planes.
- Acelerar las revisiones por parte del comité de continuidad y la dirección.
- Realizar y actualizar los informes asociados al plan de continuidad.
- Aprobación rápida del plan de continuidad para los dos Datacenter.
- Mapear los nombres de procedimientos, guías, formatos, informes relacionados con el plan de continuidad con relación a los requisitos exigidos por la norma en el dominio de continuidad del negocio vs el dominio de Gestión de Continuidad de la norma ISO 27001.

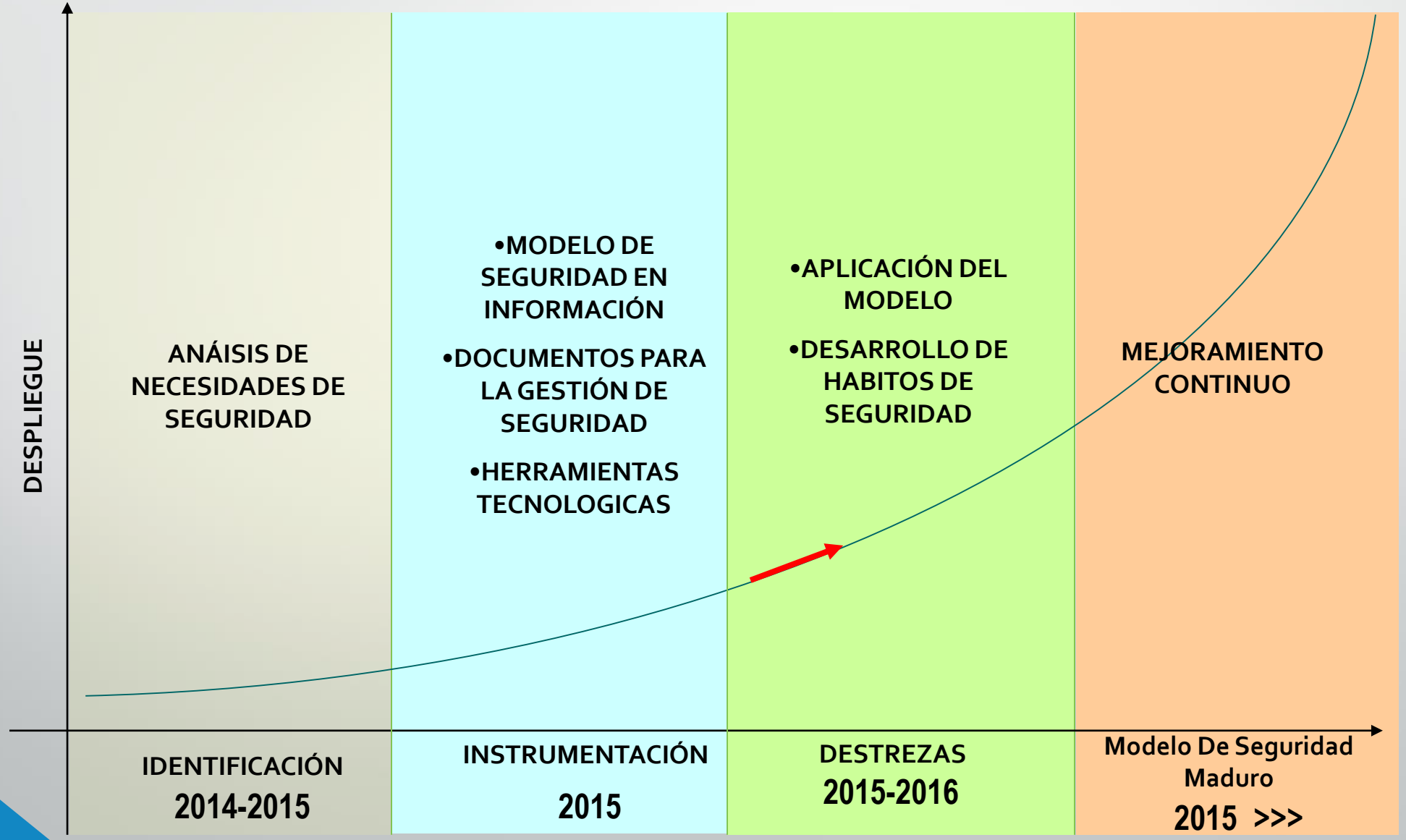
Firmado: Representante de la compañía	SAC Mayor propuesto fecha de cierre:	Firmado Auditor Robin Salcedo

Fase 5:Auditoria de Cumplimiento 2014 ISO 27002:2013



Resultados de la Auditoria de Cumplimiento 'Auditoria Interna' ; Diferencial en la evolución de los niveles de madurez entre La situación actual, la implementación de planes de acción A corto plazo, nivel de madurez de la auditoria Vs nivel de madurez ideal a largo plazo.

Mejora Continua del SGSI

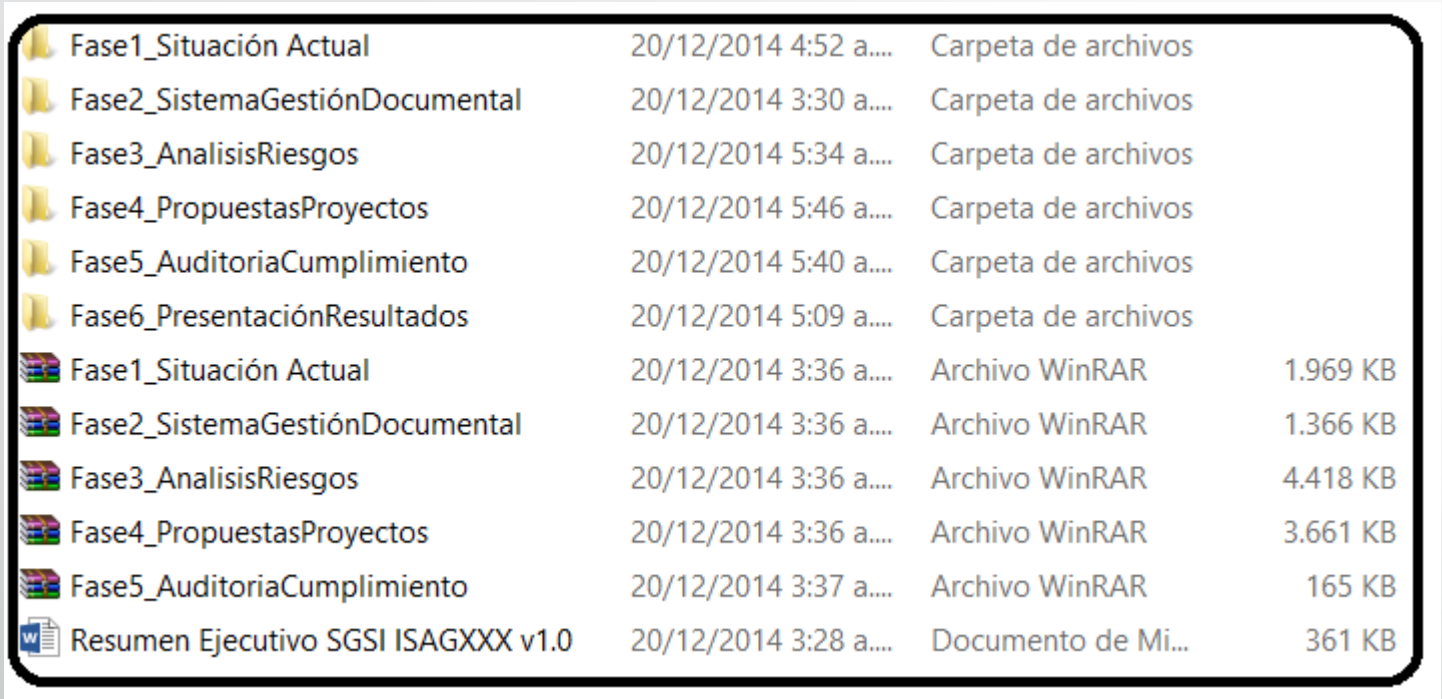


Factores Claves de Éxitos / Recomendaciones

- ✓ Apoyo de la alta dirección
- ✓ Participación integral de todas las áreas de la organización.
- ✓ Compromiso de los dueños y lideres de cada proceso en el mantenimiento y actualización de la matriz de activos y valoración de riesgos .
- ✓ Concientización, sensibilización y capacitación para que todos los funcionarios de la compañía conozcan sus roles y responsabilidades en el mantenimiento del sistema de gestión de seguridad de la información SGSI.

La actualización de la matriz de activos de información se debe realizar cada vez que existe un cambio significativo en los procesos o en la estructura organizacional de la compañía y los responsables de esta actividad son los dueños o lideres de cada proceso.

Memorias y Anexos del Proyecto SGSI ISAGXXX



Fase1_Situación Actual	20/12/2014 4:52 a....	Carpeta de archivos	
Fase2_SistemaGestiónDocumental	20/12/2014 3:30 a....	Carpeta de archivos	
Fase3_AnalisisRiesgos	20/12/2014 5:34 a....	Carpeta de archivos	
Fase4_PropuestasProyectos	20/12/2014 5:46 a....	Carpeta de archivos	
Fase5_AuditoriaCumplimiento	20/12/2014 5:40 a....	Carpeta de archivos	
Fase6_PresentaciónResultados	20/12/2014 5:09 a....	Carpeta de archivos	
Fase1_Situación Actual	20/12/2014 3:36 a....	Archivo WinRAR	1.969 KB
Fase2_SistemaGestiónDocumental	20/12/2014 3:36 a....	Archivo WinRAR	1.366 KB
Fase3_AnalisisRiesgos	20/12/2014 3:36 a....	Archivo WinRAR	4.418 KB
Fase4_PropuestasProyectos	20/12/2014 3:36 a....	Archivo WinRAR	3.661 KB
Fase5_AuditoriaCumplimiento	20/12/2014 3:37 a....	Archivo WinRAR	165 KB
Resumen Ejecutivo SGSI ISAGXXX v1.0	20/12/2014 3:28 a....	Documento de Mi...	361 KB

PREGUNTAS

ISAGXXX 2014

TFM MISTIC UOC 2014-2015

ROBIN J.SALCEDO B