



**IX JORNADA
de SEGURIDAD
INFORMATICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Establecimiento de las estrategias para las verificaciones integrales que cierran el primer ciclo de cinco o seis años en Seguridad de la Información en Colombia

Iván E. Guerra M.

CGRCP-IT: Certified IT Governance, Risk, Compliance Professional

Schlumberger DEXA Systems

Imatiz@Dexasystems.com





**IX JORNADA
de SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Agenda

Mensajes principales

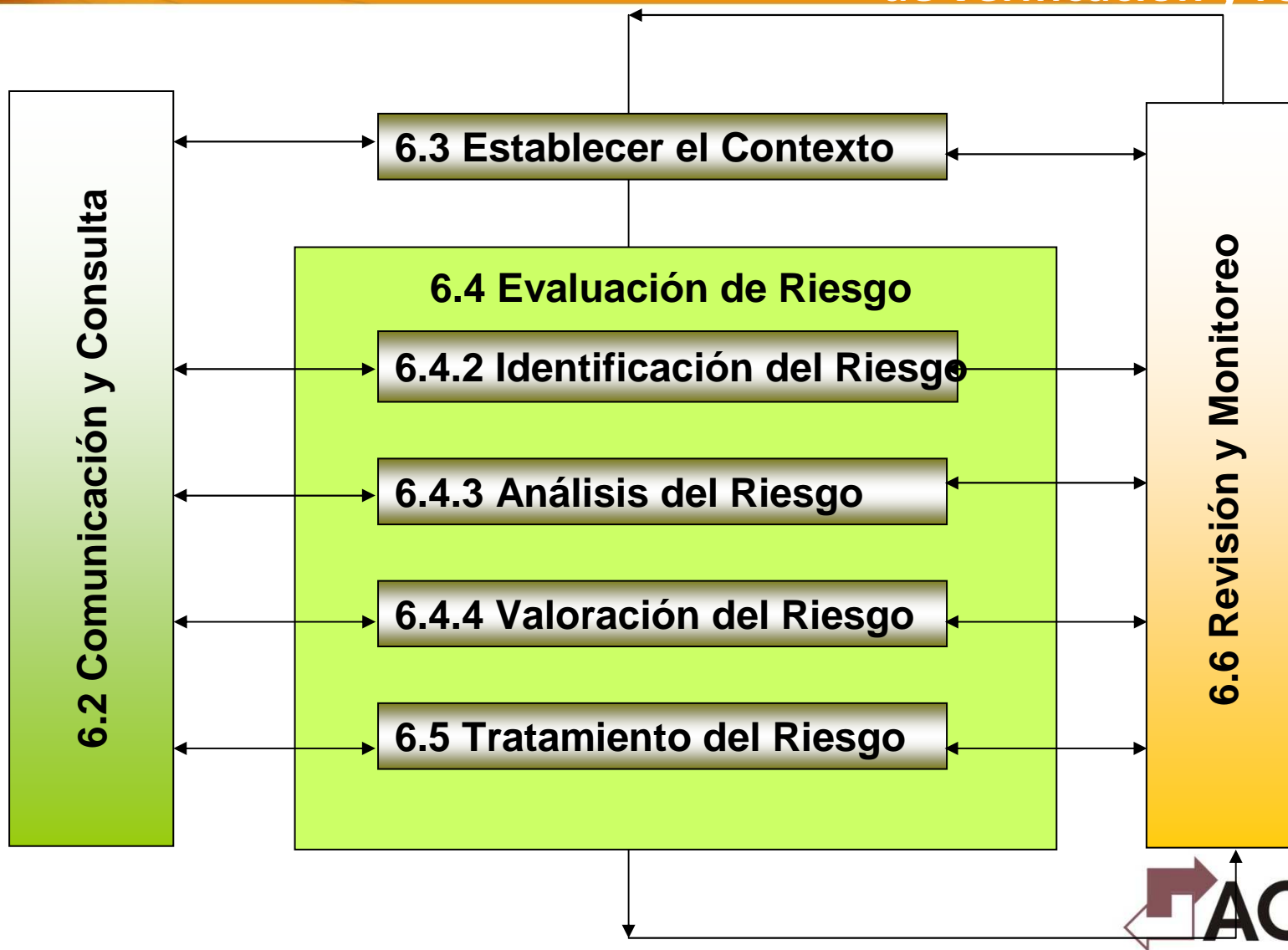
- Antecedentes de los escenarios de Control Interno en seguridad de la Información
- Consecuencias de la ejecución de dichos escenarios en las empresas.
- Un enfoque para desarrollar un programa de Control Interno en Seguridad de la Información.
- Aplicación en un caso real
- Conclusiones





**IX JORNADA
de SEGURIDAD
de INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

El Proceso de Seguridad de la Información se cierra con la fase de verificación y reporte



Fuente Draft ISO/DIS 31000



**IX JORNADAS
de SEGURIDAD
INFORMATICA**
Monitoreo y Evolución
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Las áreas de control de las instituciones se están preparando en seguridad de la información para realizar una función integral



Muros

Información

Fosos
profundos con
Defensas

Defensas

Para prevenir

Acceso no autorizado

Modificación no autorizada

No disponibilidad

“ Seguridad de la Información ”





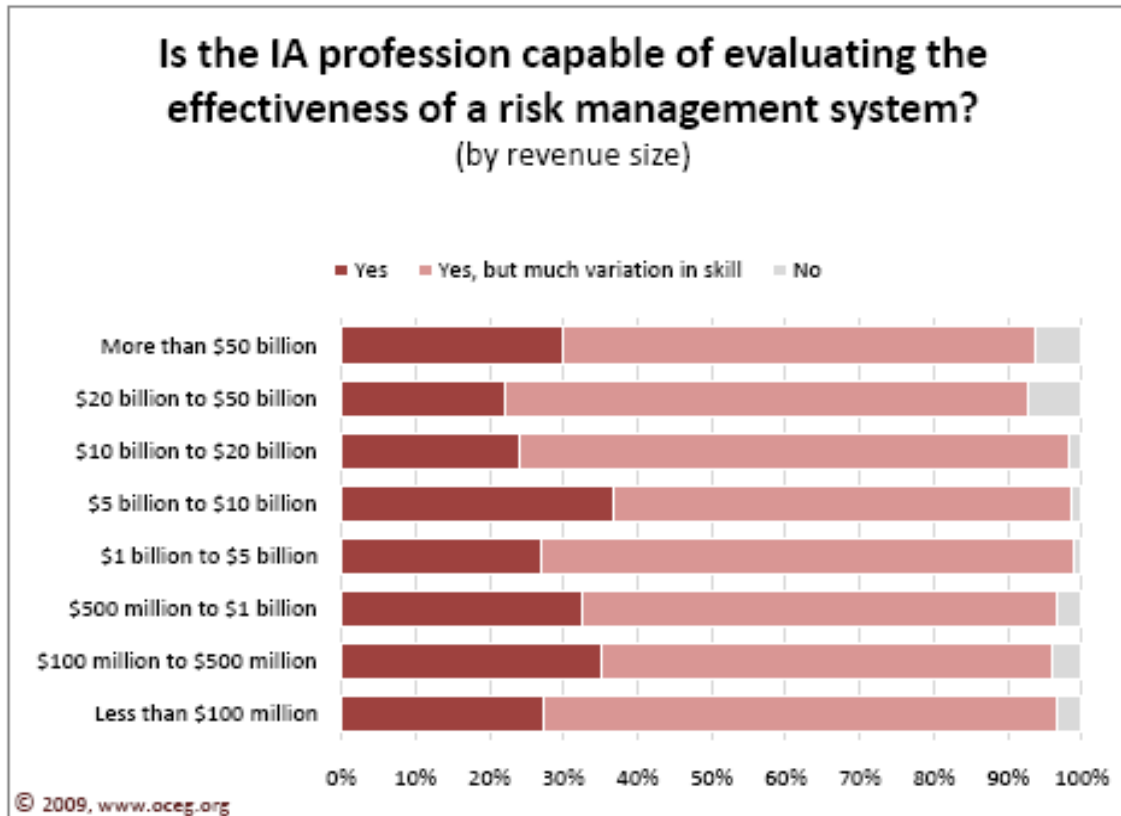
IX FORO NACIONAL DE SEGURIDAD INFORMATICA
Monitoreo y Protección de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Las organizaciones han invertido en la protección de la información y quieren ver si están listas para verificar su cumplimiento con los objetivos

Capacidad de la Profesión por Ingreso de las empresas



Fuente OCEG One-Minute Poll (OMP)
Questions about Internal Audit (IA)
n = 1015





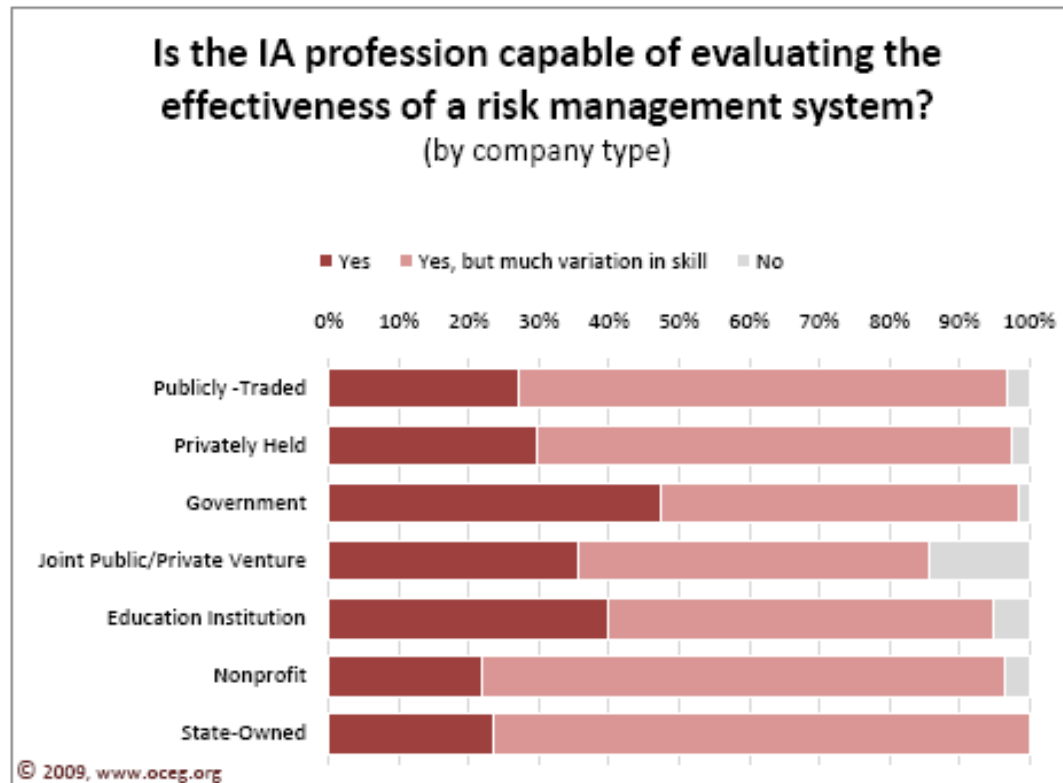
IX Jornada de Seguridad Informática
Monitoreo y Evolución de la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Las organizaciones han invertido en la protección de la información y quieren ver si están listas para verificar su cumplimiento con los objetivos

Capacidad de la Profesión por tipo de Industria



Fuente OCEG One-Minute Poll (OMP)
Questions about Internal Audit (IA)
n = 1015



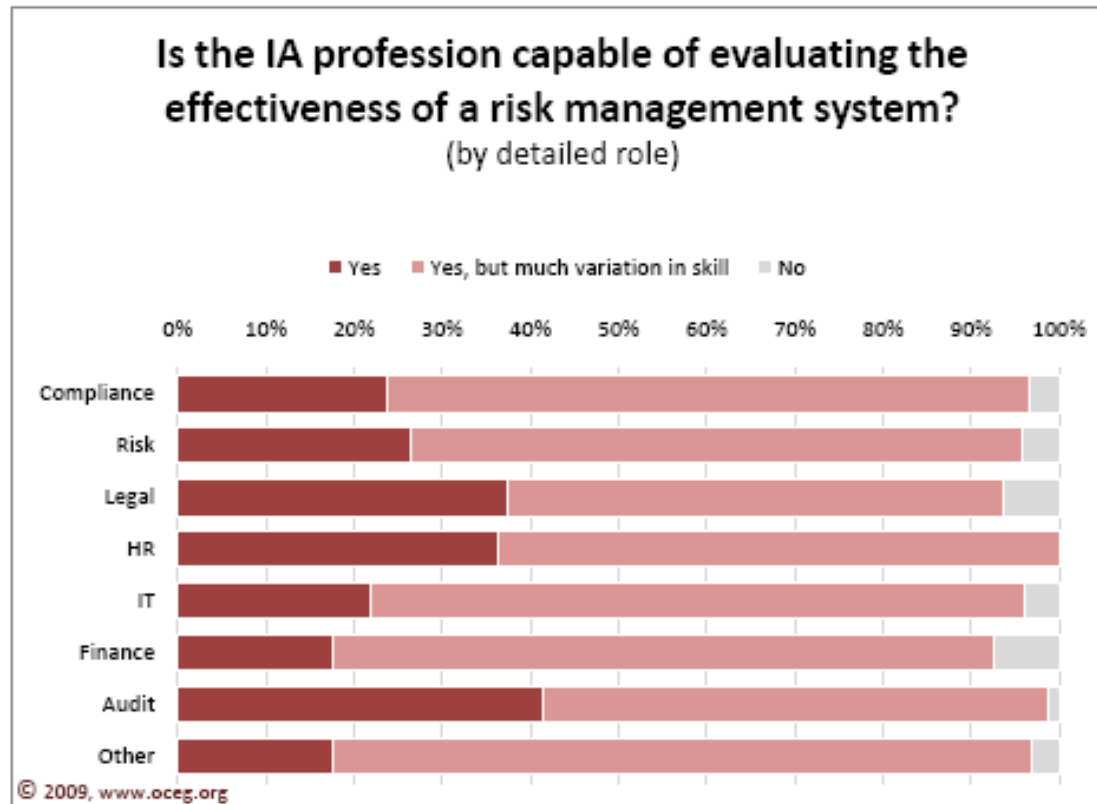


Las organizaciones han invertido en la protección de la información y quieren ver si están listas para verificar su cumplimiento con los objetivos

Capacidad de la Profesión por role ejecutado



Fuente OCEG One-Minute Poll (OMP)
Questions about Internal Audit (IA)
n = 1015



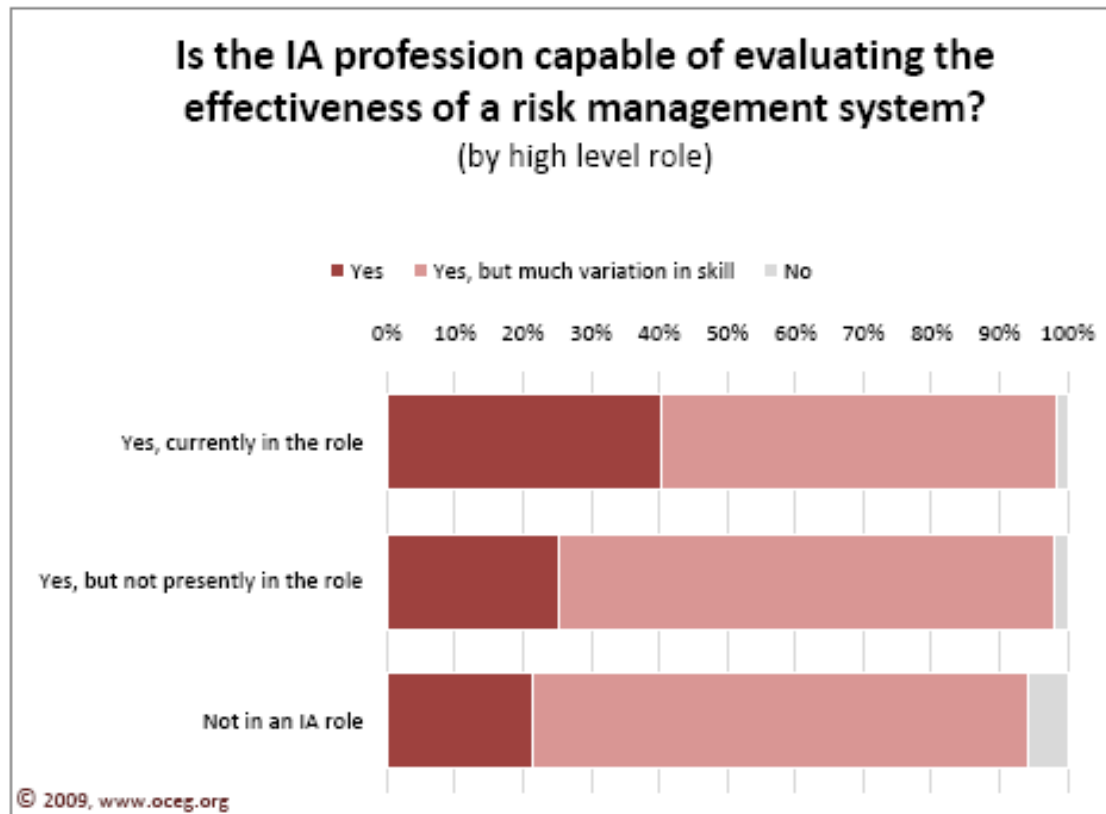


Las organizaciones han invertido en la protección de la información y quieren ver si están listas para verificar su cumplimiento con los objetivos

Capacidad de la Profesión por definición dentro de sus funciones



Fuente OCEG One-Minute Poll (OMP)
Questions about Internal Audit (IA)
n = 1015



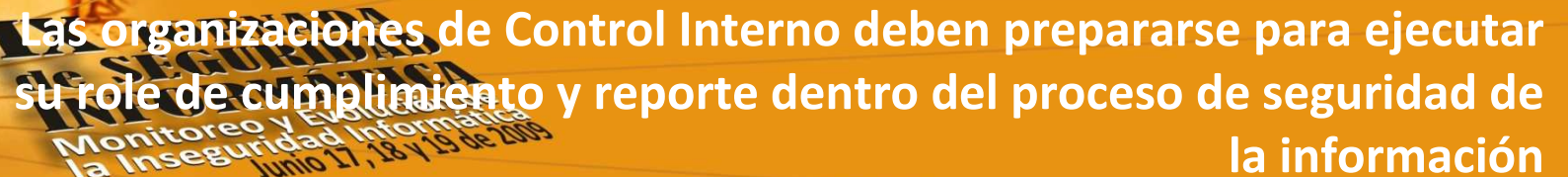


- **El proceso de Seguridad de la Información** no entendido ni ejecutado como un todo integral donde se llevan a cabo cada componente de Gobierno, Riesgo y Cumplimiento. Cada aspecto es un silo.
- **La organización de seguridad de la información** con mucho poder donde se olvida que parte de su responsabilidad es verificar el aspecto de cumplimiento.
- **Gobierno en seguridad de la información:**
 - Incompleto
 - Viciado por falta de conocimiento e intereses.
 - No retro alimentado y estancado en riesgos y definiciones de épocas anteriores.
 - No conectado a los procesos del negocio y a los de tecnología de la información.
- **Riesgos en seguridad de la información:**
 - Sin gestionar.
 - Manejo no preventivo.
 - Desconectados con los procesos de Tecnología que son emblema de Gobierno de TI como Control de Cambios.



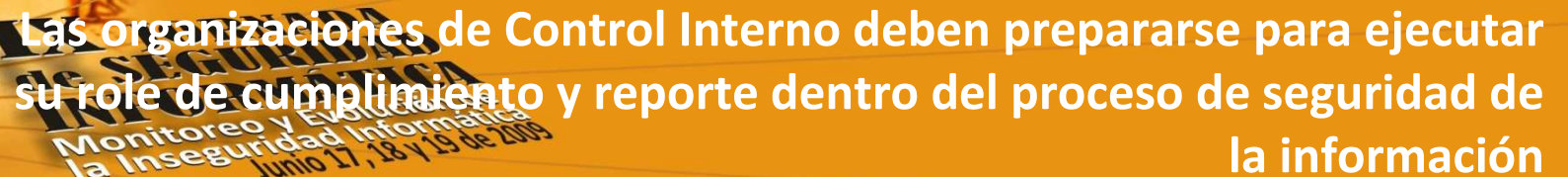
- **Cumplimiento en Seguridad de la Información**

- Áreas de Control con poco conocimiento en seguridad de la información y mejores prácticas.
- Áreas de control sin estándares de revisión en seguridad de la información.
- Áreas de control con metodologías que no incluyen seguridad de la información. Usualmente incluyen control de acceso y registros
- Áreas de control que desconocen las prácticas de la organización que lleva a esfuerzos duplicados en la evaluación de controles.
- Áreas que no tienen la función de Control Interno ejecutando labores de Auditoría, ganando espacio e imagen que no le corresponde.
- Auditorías que pierden efectividad por desconocimiento de las prácticas y su integridad.
- Áreas de control sin herramientas de gestión de riesgo.
- Falta de un programa de Auditoría en seguridad de la información que verifique
 - Alineamiento de la organización de seguridad de la información con los objetivos de negocio y mejores prácticas.
 - Cumplimiento de la Política de Seguridad de la Información.



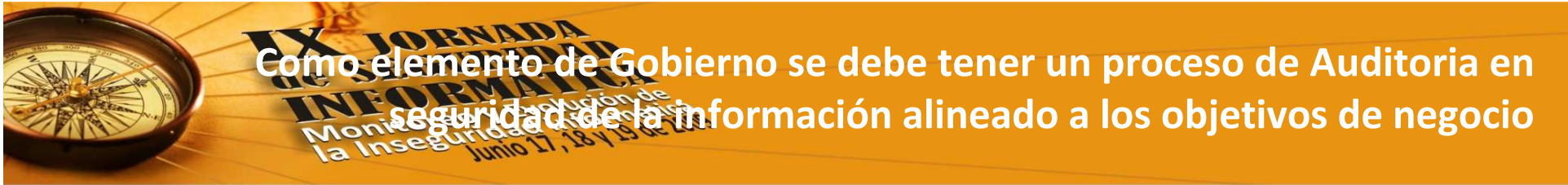
Las organizaciones de Control Interno deben prepararse para ejecutar su role de cumplimiento y reporte dentro del proceso de seguridad de la información

- Verificar el nivel de Cumplimiento de la Política de Seguridad de la información
- Verificar el nivel de penetración y seguimiento al área de seguridad de la información.
- Proveer un método estándar que empodere a la Organización de Auditoria en el ejercicio de su rol.
- Evaluar la vigencia y actualidad del Modelo de Seguridad de la Información
- Afianzar la cultura de seguridad de la información de la Organización para que se aplique y se cumpla en cada uno de los procesos de negocio, con participación directa de los propietarios de la información.



Las organizaciones de Control Interno deben prepararse para ejecutar su role de cumplimiento y reporte dentro del proceso de seguridad de la información

- Verificar el nivel de Cumplimiento de la Política de Seguridad de la información
- Verificar el nivel de penetración y seguimiento al área de seguridad de la información.
- Proveer un método estándar que empodere a la Organización de Auditoria en el ejercicio de su rol.
- Evaluar la vigencia y actualidad del Modelo de Seguridad de la Información
- Afianzar la cultura de seguridad de la información de la Organización para que se aplique y se cumpla en cada uno de los procesos de negocio, con participación directa de los propietarios de la información.



Como elemento de Gobierno se debe tener un proceso de Auditoria en seguridad de la informacion alineado a los objetivos de negocio

Proceso Administración de la Auditoria en seguridad de la información

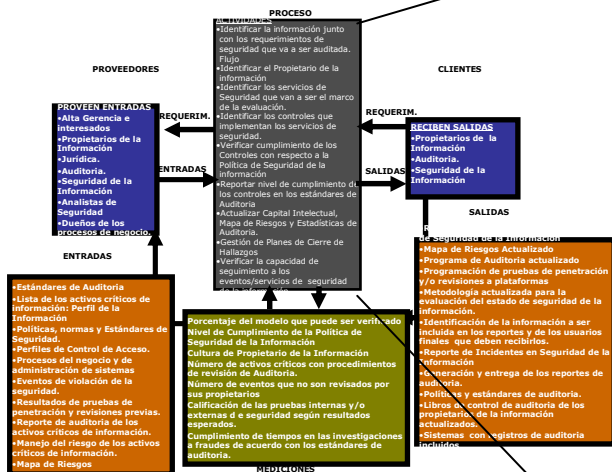
Misión: Hacer cumplir la Política de Seguridad de la Información

PROCESO

ACTIVIDADES

Identificar la información junto con los requerimientos de seguridad que va a ser auditada. Flujo

- Identificar el Propietario de la información
- Identificar los servicios de Seguridad que van a ser el marco de la evaluación.
- Identificar los controles que implementan los servicios de seguridad.
- Verificar cumplimiento de los Controles con respecto a la Política de Seguridad de la información
- Reportar nivel de cumplimiento de los controles en los estándares de Auditoria.
- Actualizar Capital Intelectual, Mapa de Riesgos y Estadísticas de Auditoria.
- Gestión de Planes de Cierre de Hallazgos
- Verificar la capacidad de seguimiento a los eventos/servicios de seguridad de la información.





**IX JORNADA
de SEGURIDAD
de INFORMATICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Con una organización responsable

Gerencia de Auditoria en Seguridad de la Información

Analistas de Proyectos de Auditoria en
Seguridad de la información

Analistas de Auditoria de Procesos de Administración
de sistemas Puede ser de la Organización de
Auditoria de Sistemas

Analistas de Servicios Estratégicos

Analistas de Servicios Administrativos

Analistas de Servicios Operativos

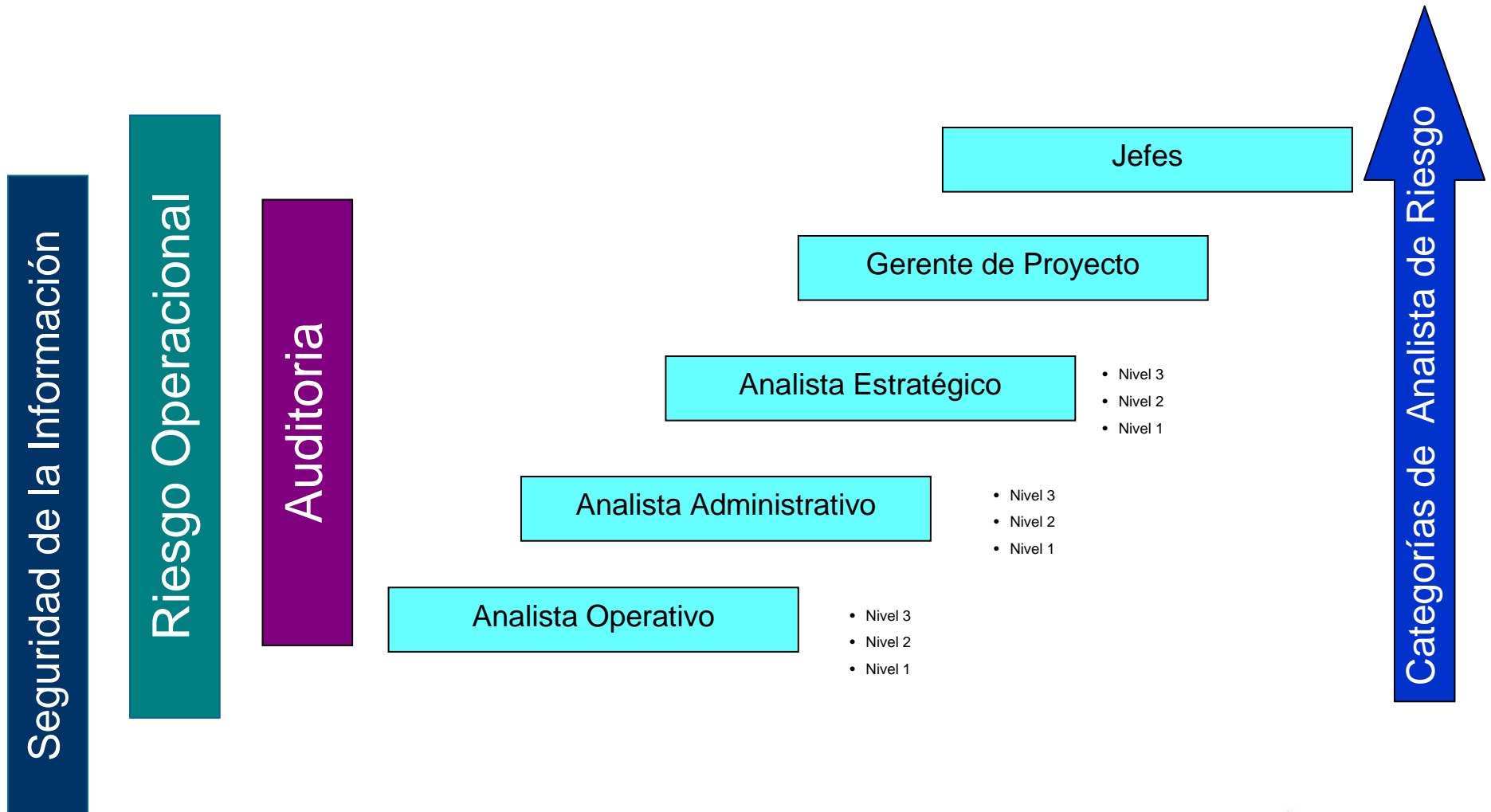
Analista Mejores prácticas

S



**IX JORNADA
de SEGURIDAD
de INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

Con un plan de carrera





- Procedimientos
- Estándares
- Organización
- Herramientas



- Revisión de cumplimiento a la Organización de Seguridad de la información.
- Revisión de cumplimiento a un Propietario de la Información.
- Revisión de cumplimiento de una Plataforma de Operación.
- Revisión de cumplimiento de una Aplicación
- Revisión de Cumplimiento a un proceso de negocio incluido Tecnología de la Información.
- Revisión de Cumplimiento de la Red Privada.
- Revisión de Cumplimiento con las conexiones a redes externas.
- Revisión de Cumplimiento con canales como Internet y los servicios que se están entregando.
- Revisión de Cumplimiento de Seguridad de la Información en el ciclo de vida de un servicio, una aplicación, un sistema o un producto.
- Revisión de Cumplimiento a un Proveedor
- Revisión de cumplimiento en los procesos de administración de sistemas como control de Cambio, Manejo de Inventario, Manejo de Incidentes, Manejo de problemas entre otros.
- Revisión de Cumplimiento a Seguridad Física respecto a proteger la información.
- Revisión del Proceso de manejo de Riesgo en Seguridad de la Información.





Estándares

- Roles a incluir en una revisión de Seguridad de la Información.
- Roles a incluir en una revisión integral de Procesos, Financiera y de Seguridad de la Información y la manera que se deben interrelacionar para tener sinergia y efectividad.
- Características del Líder de la revisión.
- Herramientas a utilizar.
- Protocolos a cumplir previo, durante y post revisión.
- Criterios que deben cumplir proveedores que ejecuten servicios para Auditoria.
- Establecimiento y desarrollo de Roles y Plan de carrera para funcionarios de Auditoria que van a desempeñar tareas de cumplimiento en seguridad de la información.



Cada funcionario de Auditoria debe tener una base en seguridad de la información para el ejercicio de su función

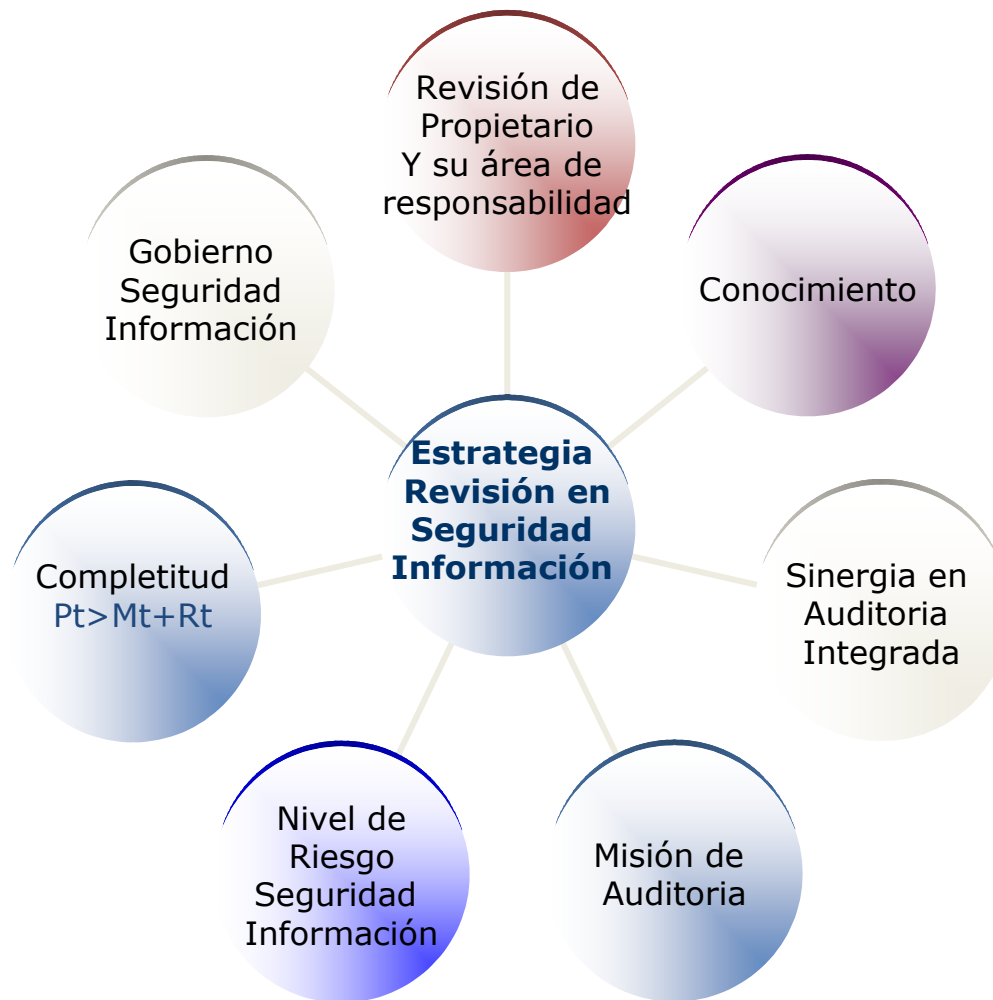
- Dominio completo de la metodología de manejo de riesgo en el uso de la información de la
- Dominio completo de la Política de Seguridad de la Información.
- Dominio de normas fundamentales en seguridad de la información
- Dominio completo de la Organización de Seguridad de la información y sus roles.
- Dominio completo del ISO27001.
- Dominio de mejores prácticas como COBIT, COSO.
- Los funcionarios de Auditoria especializados en Seguridad de la Información deben cumplir lo anterior y otras más en el camino de su especialidad y de tener certificaciones como Auditor del ISO27001, CISSP y otras reconocidas en Seguridad de la información.



- Política oficial de Seguridad de la Información.
- Programa de Auditoria en Seguridad de la Información.
- Mapa de Riesgos en Seguridad de la Información
- Normas que han sido oficializadas y pueden ser objetivo de revisión de Cumplimiento de parte de Auditoria. De lo contrario son guías.
- Procedimientos establecidos y oficiales de seguridad de la información.
- Herramienta de apoyo:
 - A la auditoria, como hallazgos, recomendaciones, flujos de información, seguimiento a recomendaciones, mejoras al modelo de seguridad de la información.
 - Gestión de Riesgo
 - Verifiquen el nivel cumplimiento de la Política y mejores prácticas.
- Mejores prácticas como el ISO27001, ISO/IEC 17799 2005 y futuras, y COBIT.
- Proveedores externos que puedan suplir alguna falta de habilidad o conocimiento como Hackers éticos o especialistas de plataforma, evitando que sean Juez y Parte.



Una vez definidos los componentes del Método se debe plantear la estrategia de revisión que sea ganadora en tiempo, en resultados y en claridad.





- Ser dueño del proceso de Seguridad de la Información.
- Ser dueño de la Información, que es usualmente un área de negocio o la misma tecnología
- Ser dueño de un proceso que coincide con la anterior definición.
- Ser dueño de una aplicación que soporta uno o más procesos de negocio, establecido por el dueño del proceso.
- Ser dueño de una plataforma con una responsabilidad de administrador delegada por Tecnología de la Información
- Ser dueño de un servicio de negocio que se provee por un canal, que igualmente debe tener un propietario cuyo nivel de protección establecido se debe mantener.
- Ser dueño de un proveedor o tercera parte que está utilizando información de la Institución para ejecutar los servicios que ha tercerizado el propietario.
- Ser dueño del proceso de manejo de riesgo de la Institución



- La función de un dueño y como usualmente se encuentra en la Política de Seguridad de la información se puede ver en tres grandes componentes:
 - P de Proteger la información de la que es dueño.
 - M de Monitorear el buen uso de dicha información
 - R de Reaccionar ante eventos no autorizados en el uso de su información.



El Gobierno en Seguridad de la Información a revisar se debe seleccionar con base en el alcance de la responsabilidad del dueño objeto de la revisión

En lo posible se debe seleccionar los elementos oficiales y declarados como revisables por la organización. En caso de no ser oficiales los resultados de los elementos caen en recomendaciones y no en rompimiento de la Política de Seguridad de la información

- Políticas individuales.
- Normas.
- Estándares de Plataforma
- Procedimientos
- Roles y Responsabilidades en Seguridad de la Información.
- Herramientas de Seguridad de la Información.
- Perfil de la Información junto con su clasificación, requerimientos de seguridad y controles mínimos.

Y deben ser revisados en su objetivo principal: Proteger la información de la institución.



Dentro de cada Organización sus funcionarios deben tener una responsabilidad en la protección de la información y es la que se debe inspeccionar



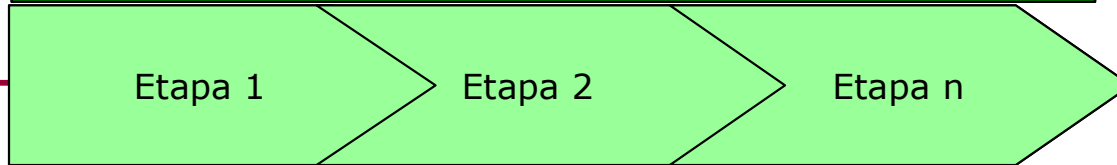
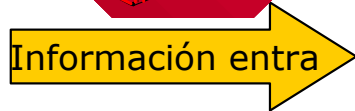
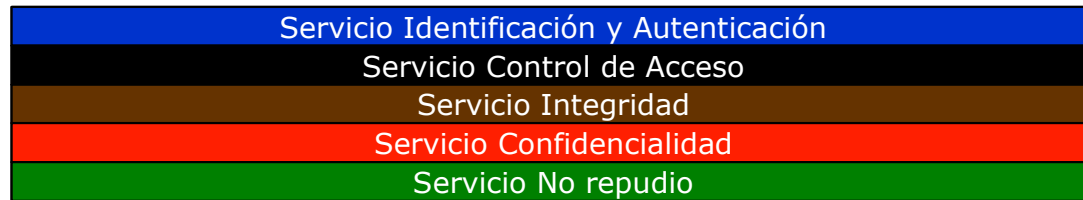
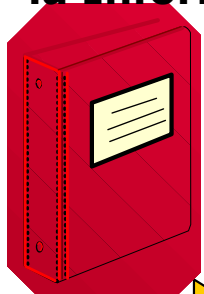


La orientación de la revisión debe ser la protección de la información punto a punto, que se efectúa por medio de la implantación de los servicios de Seguridad

Política de Seguridad de la Información

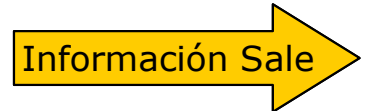
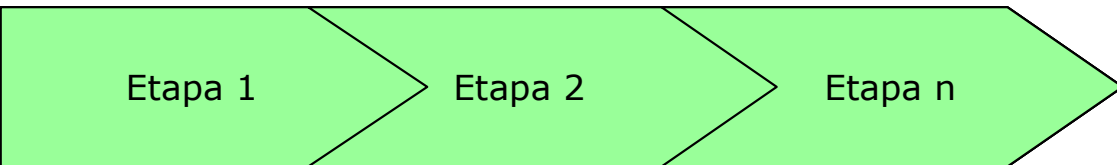
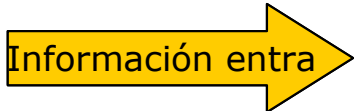
Tesorería - LA

Flujo 1



Flujo 2

Servicios de Seguridad de la Información
Acorde con su criticidad

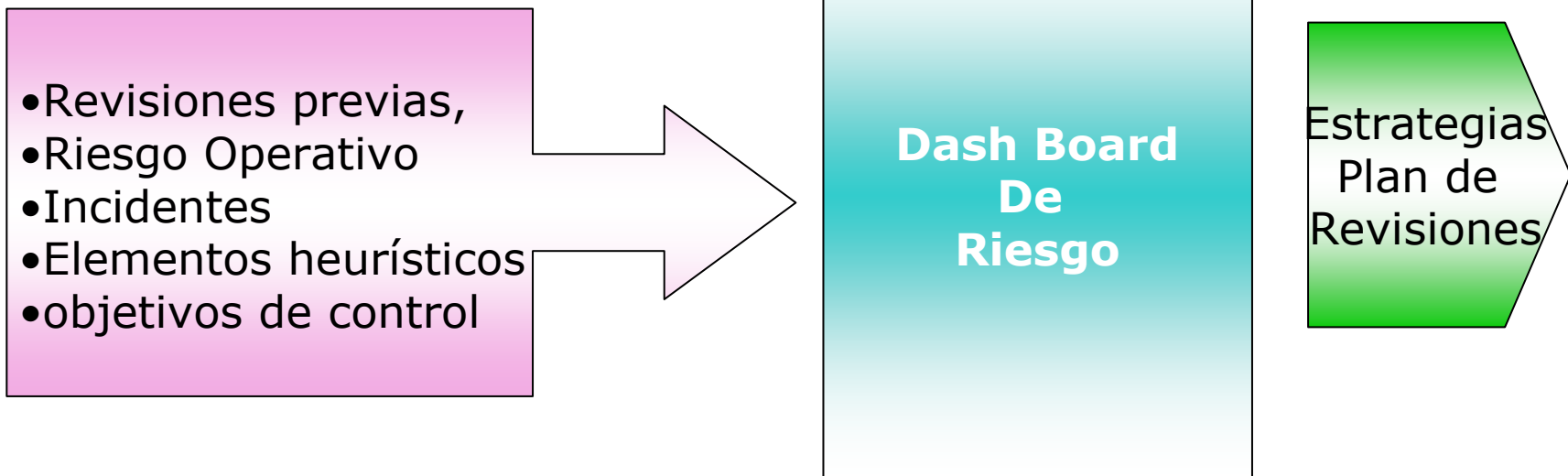


Punto a punto





El nivel de riesgo es elemento esencial para diseñar, desarrollar y ejecutar la Estrategia Auditoria de un área de la Organización

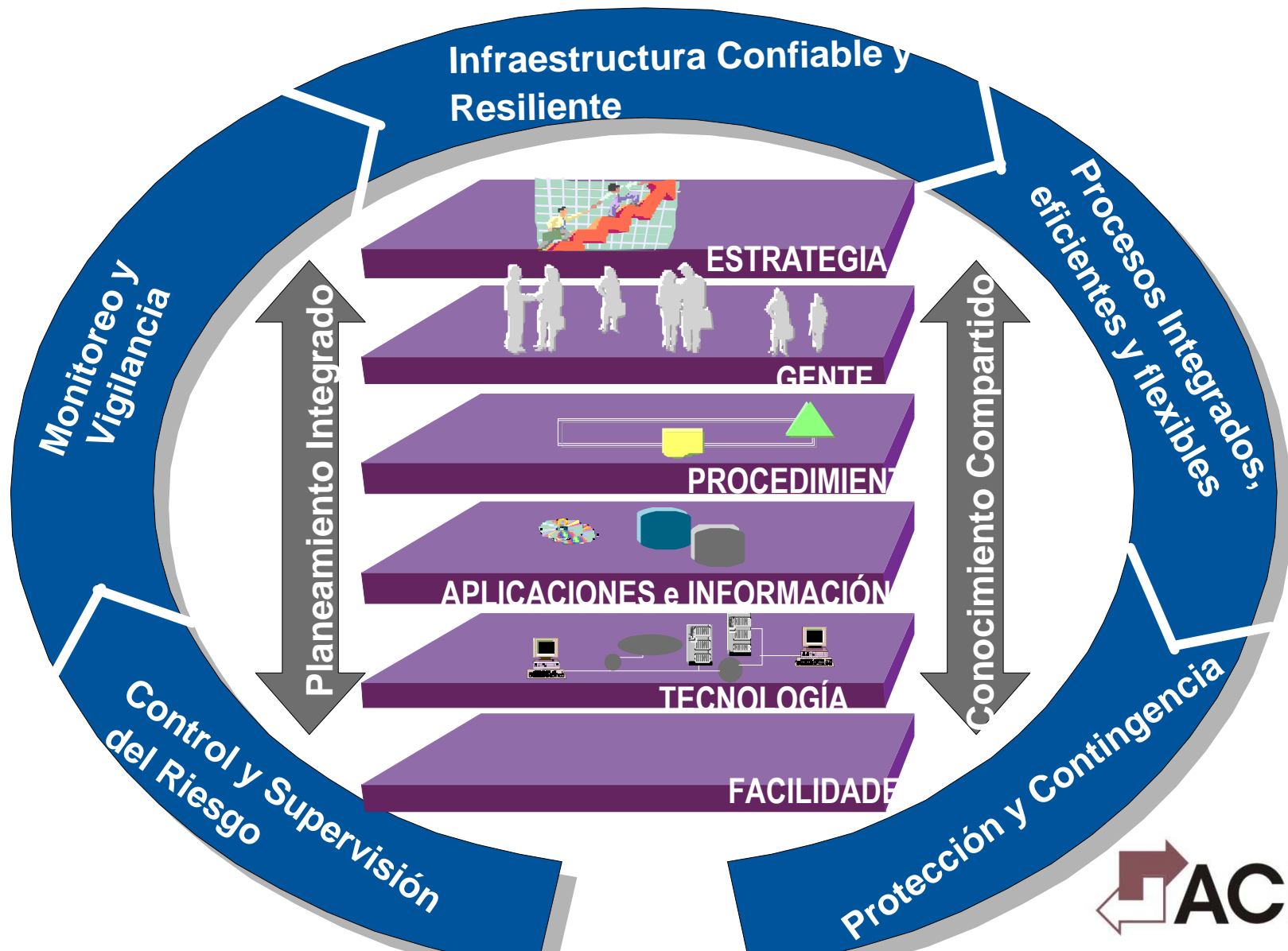




La misión de Auditoría y por ende los objetivos de control deben corresponder a un alineamiento a los del negocio


- Se deben propender la misión y los objetivos en las dimensiones de:
 - Valor a la organización.
 - Independencia.
 - Capacidad de ejecución e Integridad en sus actividades.
 - Pro actividad
 - Seguimiento.
 - Programa de Calidad.
 - Cumplimiento de normas, regulaciones y mejores prácticas.

Las revisiones deben ser integrales para que actúen de manera eficiente y efectiva, obteniendo sinergias Por ejemplo un proceso de negocio





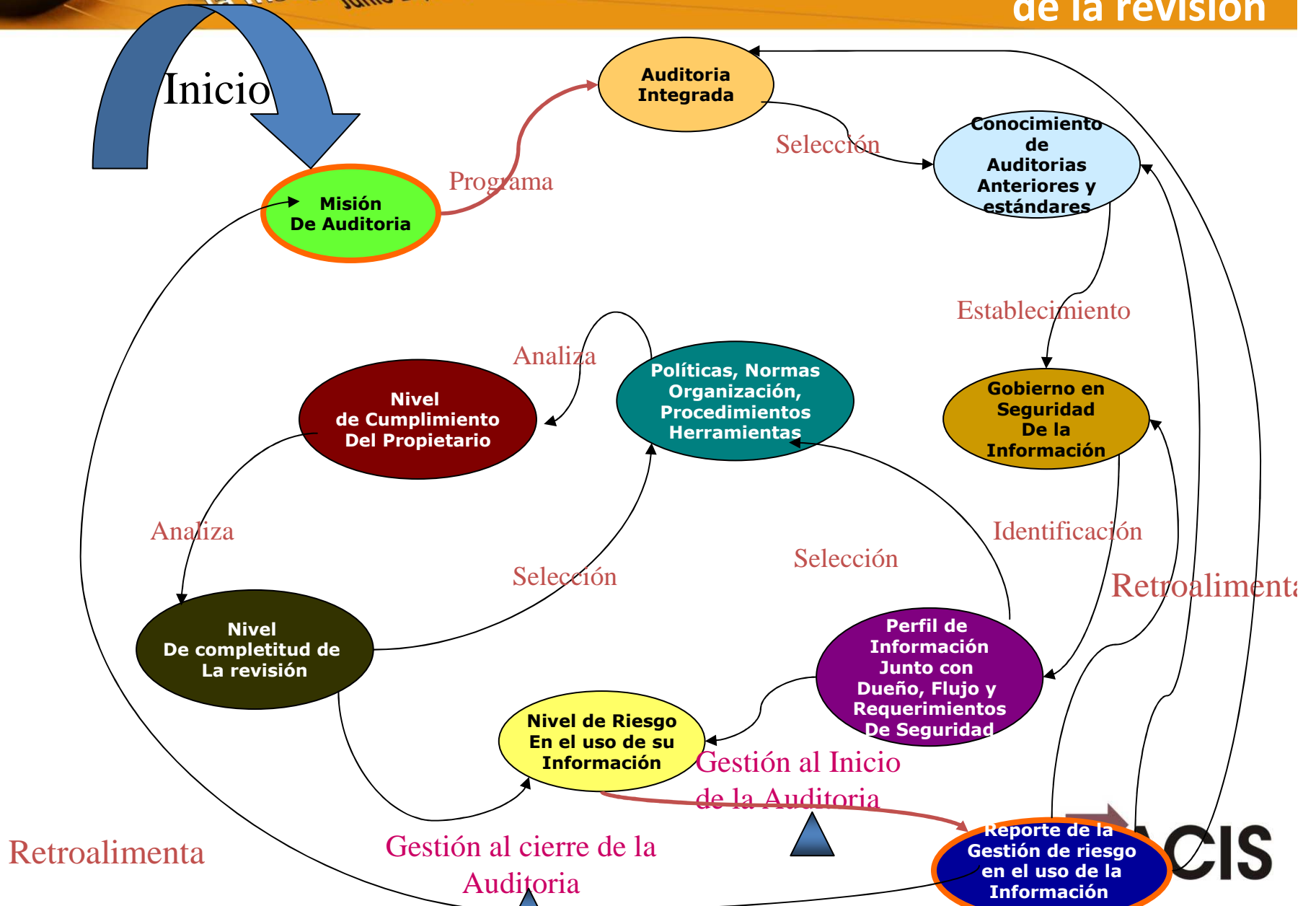
- Salida rápida a ejecutar servicios.
- Ejecución efectiva de Servicios.
- Aprender de las lecciones en proyectos ejecutados y evitar la futura repetición de errores.
- Mostrar la madurez del proceso de Auditoria.
- El crecimiento y riqueza del capital intelectual.
- La formación de unas categorías sólidas de conocimiento.



Con base en los puntos expuestos anteriormente se desarrolla la estrategia de revisión que debe responder a varias preguntas, como objetivo en el uso de la información

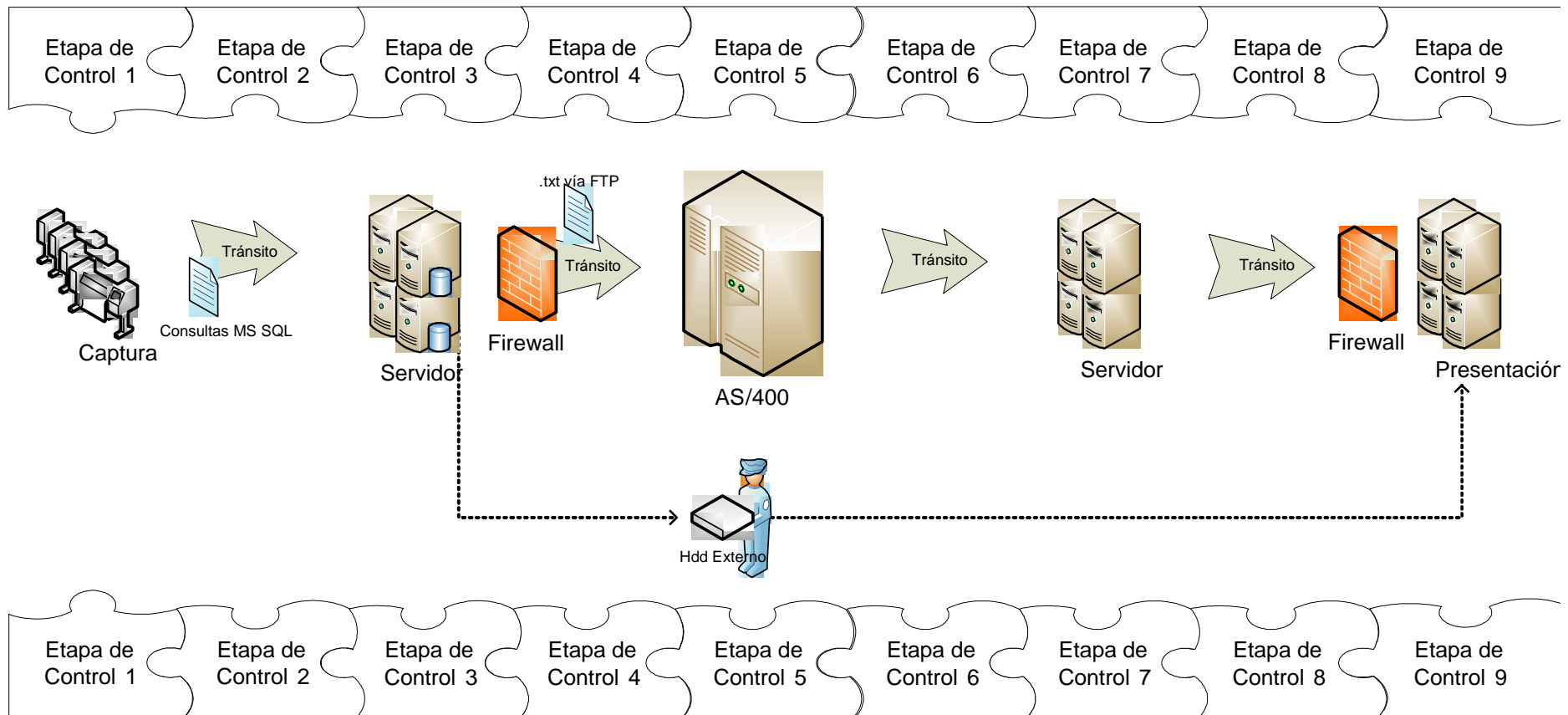
- La información es reconocida y tiene un propietario.
- El propietario sabe donde está su información y quienes son los usuarios con sus privilegios.
- Protege la información, en el lugar donde se encuentre independientemente del medio donde se encuentre y las manos que la esté utilizando para un objetivo de negocio.
- El uso de la información objeto de la revisión tiene un nivel de riesgo aceptado por la organización en cabeza de un propietario.
- El propietario con base en la criticidad de la información conoce y mitiga los riesgos, incluida la información que está en manos de proveedores.
- El nivel de riesgo en el uso de la información es conocido, aceptado y gestionado.
 - Se conocen los riesgos.
 - Se mitigan
 - Se actualizan
 - Hay foco en los críticos.

Con los objetivos en mente fundamentados en las 7 bases se desarrolla la estrategia de revisión que permita lograr el objetivo de la revisión





Flujo de Datos - Proceso de Negocio





Responsabilidad	Política	Norma	Meta a lograr dentro de la revisión	Comentario
Propietario de la información	3 numeral a)	3.1	<p>Establecer le protocolo de la revisión, el dueño del proceso/propietario de la información y lograr los compromisos que llevarán a la ejecución de la revisión.</p> <p>Crear cultura de Dueño de la Información</p>	<p>Se debe realizar una presentación que muestre al Propietario de la Información:</p> <ol style="list-style-type: none"> 1. El grupo participante, los roles y responsabilidades 2. El alcance de la revisión de parte de Auditoria y de parte del propietario de la información. 3. Definir el grupo que participará de parte del Propietario junto con rol dentro de la revisión. 4. Establecer un cronograma de común acuerdo, para que los permisos de acceso a la información se soliciten y tengan un soporte.

Ver anexo 2 uno como ejemplo.





**IX JORNADA
SEGURIDAD
INFORMÁTICA**
Monitoreo y Evolución de
la Inseguridad Informática
Junio 17, 18 y 19 de 2009

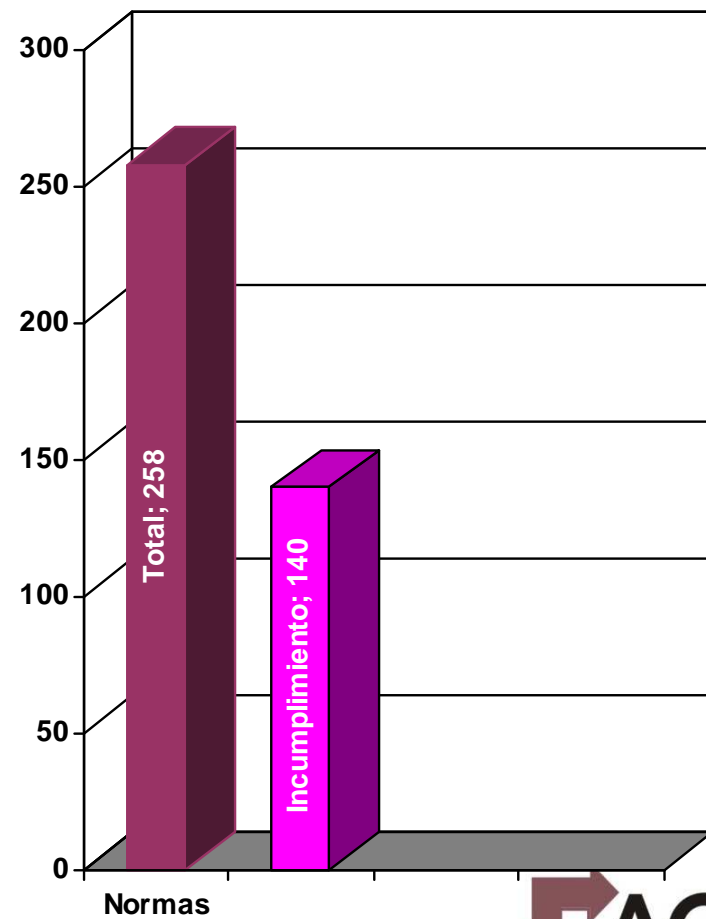
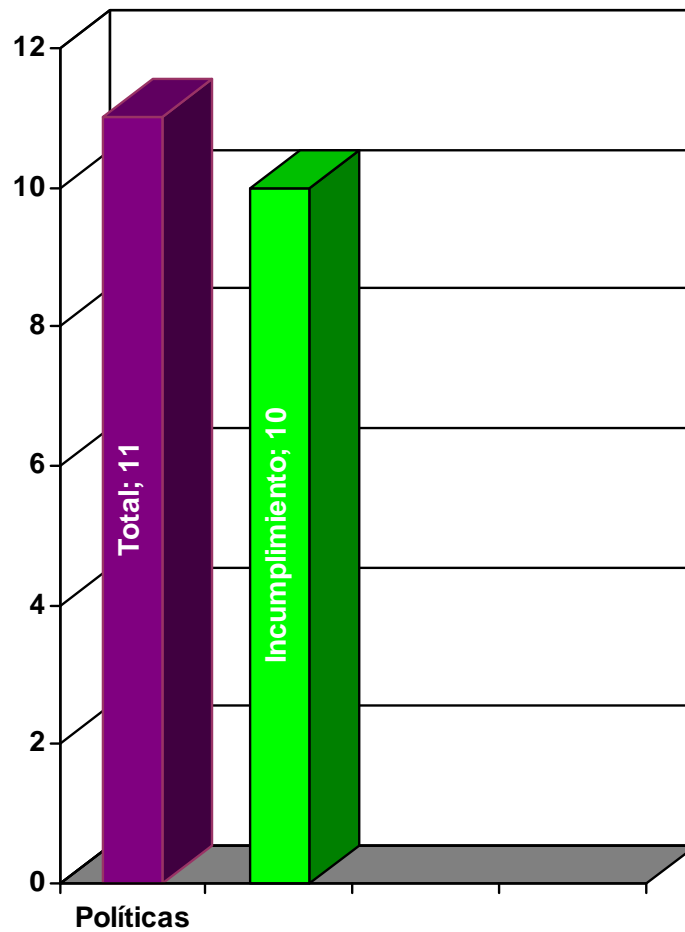
Se diseñó y desarrollo el plan de pruebas para la plataforma de Tecnología de la Información

N o.	Etapa de Control	Tipo de Dato	Pruebas Ejecutadas	Objetivo de la Prueba	Descripción de la Prueba
1	1	Almacenamiento / Proceso	Escaneo de Servicios (TCP, UDP)	Revisar servicios activos en los equipos conectados a la red	Consiste en detectar qué servicios comunes está ofreciendo la máquina y que posibles vulnerabilidades de seguridad existen según los puertos abiertos identificados. También es posible detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos.
2	1	Almacenamiento / Proceso	Evaluación de Vulnerabilidades (remoto)	Identificar posibles fallos de seguridad en los servicios activos, que dan la cara a Internet buscando cuales de estos podrían comprometer el proceso	Se utilizarán herramientas automáticas que buscan generar un comportamiento en el equipo a fin de identificar si este es vulnerable. Estas pruebas no explotan la vulnerabilidad en si, sólo identifican si el sistema es vulnerable. En caso de identificarse las vulnerabilidades se procederá a la coordinación con Auditoria para su corrección oportuna o en todo caso para continuar con las pruebas a un nivel intrusivo.



Su aplicación al proceso de negocio permitió conocer y reportar el nivel de cumplimiento de la Política de seguridad de la información

Proceso de Negocio





Nro.	Pruebas Ejecutadas	Etapas de Control	Tipo de Prueba	Dificultad de Prueba	Hallazgo	Políticas que se incumplen	Normas que se incumplen	Código de evidencia	Recomendación
1	Acta Visita Julio 18 y 19	1	Entrevista	N/A	Los parámetros generados en las estaciones son sensibles de las Cámaras, por lo que no se han cambiado.	3 y 6	3.15, 3.18, 6.11, 6.16, 6.19, 6.34	ActaVisitaI	Diseñar, Desarrollar, Implantar, mantener y gestionar Estándar de Seguridad en las plataformas con base en las normas de Seguridad de la Información



Igualmente se revisaron los servicios de Seguridad de la Información

Nro.	Hallazgo	Código de evidencia	Servicios de Seguridad Operativos afectados por el hallazgo										Servicios de Seguridad Administración afectados por el hallazgo		Servicios de Gerencia de la Seguridad afectados por el hallazgo		
			Identificación y Autenticación	Control de Acceso	Confidencialidad	Integridad	Disponibilidad	No repudio	Seguridad Física	Continuidad de negocio	Manejo de Alertas	Manejo de Auditoría	Administración de la Seguridad	Gerencia de Política	Organización de la Seguridad	Creación de Cultura	Gestión del Riesgo

54	Se identificó el uso de protocolos que no son cifrados. Estos facilitaron la captura de información confidencial en la red.	COIT - 01	X	X	X	X							X	X		
----	---	-----------	---	---	---	---	--	--	--	--	--	--	---	---	--	--

Totales de incumplimiento	27	32	30	22	32	24	26	13	25	19	26	25	28	4	23
% de incumplimiento	50,00%	59,26%	55,56%	40,74%	59,26%	44,44%	48,15%	24,07%	46,30%	35,19%	48,15%	46,30%	51,85%	7,41%	42,59%





Conclusiones

- Las revisiones de cumplimiento deben darse para poder retroalimentar el proceso de seguridad de la información.
- Cada Auditoria que involucre información debe revisar el cumplimiento del Gobierno en Seguridad de la Información acotado a unos objetivos.
- Auditoria debe desarrollar su programa de revisiones con base en el portafolio de servicios a ofrecer “Programa de Auditoria en seguridad de la información”
- El entrenamiento en el método y su práctica hará que los efectos de las revisiones sean
 - Valor para el negocio
 - Homogéneas
 - Reutilizable el capital intelectual
 - Agilidad en la salida a revisiones.
 - Facilita el Intercambio de funcionarios
 - Asimilables con facilidad por la Organización
 - Llegada a sitios no vistos anteriormente
 - Auditorias complejas se puedan direccionar con facilidad
 - Extrapoladas a otros tipos de revisiones.