Universidad Andrés Bello

Facultad de Ingeniería

Ingeniería en Computación e Informática

Tópico 1: Seguridad de la Información

Hito N°1:

Análisis GAP

Plan de director de seguridad

Integrantes : Rodrigo Bustos

Ricardo Césped

Cristopher Herrera

Fernando Olivares

Profesor : Eduardo Quiroga

Fecha : 06-04-2018

Introducción

La empresa que nos ayudará otorgando información con el fin de realizar un análisis GAP es Xemantics S.A.

Xemantics S.A. se describe como “Empresa de carácter innovador, enfocada en el almacenamiento, diseño, procesamiento y descubrimiento de los datos desde un punto de vista moderno”. Esta empresa otorga servicios como BI, Big Data, Development y Advanced Analytics.

Este proyecto tiene como fin identificar la distancia existente entre la organización actual de la seguridad de la información en la empresa y las buenas prácticas más reconocidas en la industria.

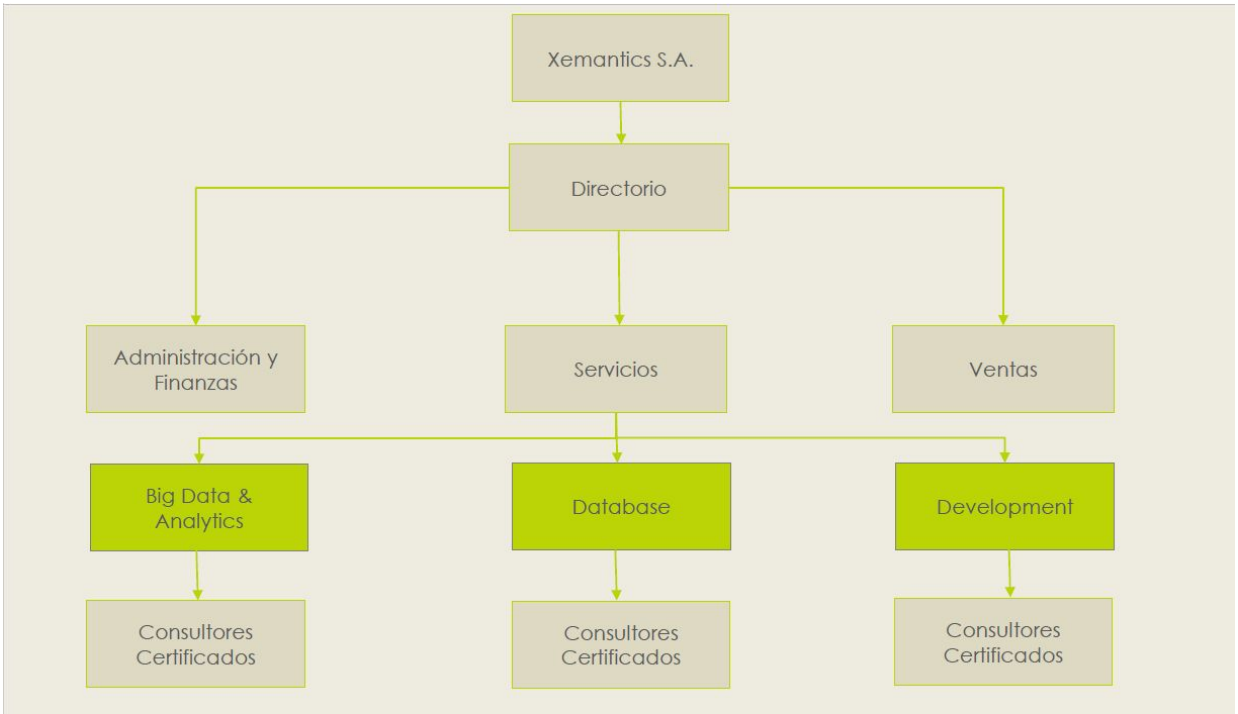
Gap Análisis

Contexto y rubro

Xemantics S.A. es una empresa dedicada a la prestación de servicios a clientes, especialmente a los del sector bancario. Prestan servicios relativos al área de TI tales como: migraciones de bases de datos, business intelligence, Big Data y advanced analytics. Todos asociados al manejo de información desde la base de datos.

Como parte de la empresa, han debido a desarrollar software como el “SQL Scripter” para la evaluación de sus proyectos y así ayudar con la toma de decisiones respecto a llevar a cabo un proyecto o no.

Organigrama de la empresa



Criterios utilizados en la evaluación del GAP

- Por una parte, se ha entrevistado a dos personas, Pedro Cesped, Gerente de Servicios, y Cristian Aguirre, Gerente Comercial. Las respuestas de ambos entrevistados tienen la misma importancia dentro de la encuesta.
- Dentro del proyecto se ha definido que se analizarán solamente las fallas de seguridad que están en gravedad alta para la compañía.

Gravedad	Porcentaje
Alto	Mayor 40%
Medio	20% - 39%
Bajo	0% - 19%

Identificación y descripción de los entrevistados

- El entrevistado de mayor importancia es Pedro Césped, debido a que es el gerente de servicios de la empresa.
- El segundo entrevistado es Cristian Silva, el gerente comercial de la empresa

Conclusiones en base a los resultados obtenidos de la entrevista

Checklist	Estándar	Dominio	Indicador del análisis	Porcentaje Cumplimiento	Porcentaje NO Cumplimiento
1	5	Política Seguridad	0%	0%	100%
2	6	Organización de la Seguridad Informatica	100%	100%	0%
3	7	Administración Activos	17%	17%	83%
4	8	Seguridad Recursos Humanos	36%	36%	64%
5	9	Seguridad Física y Ambiental	45%	45%	55%
6	10	Administración Comunicaciones y Operaciones	31%	31%	69%
7	11	Control de Accesos	20%	20%	80%
8	12	Adquisición, desarrollo y mantenimiento de Sistemas Informáticos	0%	0%	100%
9	13	Administración de Incidentes de Seguridad Informática	44%	44%	56%
10	14	Administración Continuidad de Negocios	0%	0%	100%
11	15	Cumplimiento	0%	0%	100%
Resultado de Evaluación			27%	27%	73%

Gracias al análisis GAP se logró identificar las diferencias existentes entre la situación actual y la deseable, se identificó un 73% de no cumplimiento con la situación deseable.

En consiguiente se plantean las siguientes recomendaciones en base a los dominios con una gravedad importante para la empresa:

Recomendaciones

Dominio	Subdominio	Recomendaciones
Política seguridad	Documento Política Seguridad Informática	Generar documento sobre las políticas de seguridad informática dentro de la empresa y que sea aprobada por la gerencia para luego ser publicada para los empleados de la empresa.
		Establecer por escrito el compromiso de la gerencia junto con el acercamiento organizacional a la administración de seguridad informática dentro de la política de seguridad de la empresa.
	Revisión de Política Seguridad Informática	Establecer periodos de tiempo para la revisión de las políticas de seguridad informática para actualizar los cambios significativos que se puedan generar a lo largo del tiempo de la empresa, asegurando la continuidad, adecuación y efectividad.
		Establecer un encargado que esté aprobado para el desarrollo, evaluación y revisión de la política de seguridad informática.
		Establecer un procedimiento para la revisión de la política de seguridad informática junto con los requisitos que debe especificar el gerente de la empresa.

		Considerar las revisiones gerenciales con una mayor ponderación dentro de la revisión.
		Al terminar la revisión de las políticas obtener la aprobación del gerente de la empresa para su validación.
Administración de activos	Dueños de Activos	Generar una clasificación de seguridad de los dueños de activos con sus respectivas restricciones de acceso y una revisión constante.
	Uso Aceptable de Activos	Documentar las regulaciones de los activos de manera constante para obtener un uso aceptable de ellos.
	Guía de Clasificación	Clasificar los activos en un documento considerando su importancia requisitos, sensibilidad y criticidad dentro de la empresa.
	Etiquetado y Manejo de la Información	Etiquetar los activos identificados para el manejo de su información de acuerdo a las clasificaciones generadas por cada activo dentro de la empresa.
Seguridad Recursos Humanos	Revisión Antecedentes	Realizar una revisión de los antecedentes de todos los candidatos, ya sean: empleados, contratistas o terceros, que están definidos en la documentación de los roles a través de RR.HH.
	Concientización, educación y entrenamiento sobre Seguridad Informática	Realizar capacitaciones o reuniones independientes o grupales (solo si es necesario) sobre la seguridad y actualizaciones de las políticas de seguridad establecidas por la empresa.
	Proceso disciplinario	Definir y documentar los procesos que se realizarán en caso de alguna falta en seguridad dentro de la empresa.
	Responsabilidades de término	Estipular las responsabilidades para realizar la terminación o cambio laboral dentro de un documento donde se definen claramente el cómo y cuándo se deben realizar estas acciones.
	Devolución de Activos	Estipular en un documento y definirlo en el contrato de trabajo las devoluciones de activos que fueron usados por los empleados, contratistas o terceros que son propias de la empresa.
	Eliminación de derechos de Acceso	Definir procedimientos y estipular en un documento donde los derechos de accesos dentro de la empresa sean eliminados cuando se realiza un término o cambio laboral de algún empleado.
Administración Comunicaciones y Operaciones	Procedimientos operativos documentados	● Documentar todos los procedimientos operacionales y dejarlos disponibles para los usuarios que lo necesiten. ● Establecer la autorización de la gerencia de la empresa para la actualización de los procesos operativos que existen.
	Control de Cambios Operacionales	● Establecer permisos en los cambios a los centros de procesamiento de la información para su respectivo control. ● Mantener los registros de auditoría dentro de la empresa para reflejar los cambios efectuados a los programas productivos

	Segregación de Funciones	Separar áreas de responsabilidades para reducir oportunidades de modificación o mal uso no autorizado.
	Separación de facilidades de desarrollo y operacionales	Separar facilidades de desarrollo de las facilidades operacionales.
	Administrando cambios a los Servicios de Terceros	Administrar los cambios de los servicios, mantenimiento y mejoras en las políticas relacionadas con la seguridad informática.
	Control contra código malicioso	Contratar empresas relacionadas con código malicioso para la prevención de ello.
	Control contra código móvil	● Definir los códigos móviles que se van a manejar dentro de la empresa y establecer la prohibición de algún otro. ● Establecer una configuración dentro de los equipos que permita asegurar el uso de código móvil autorizado. ● Prohibir el uso de algún código móvil dentro de la empresa que no esté establecido.
	Control de la Red	● Contratar un servicio de red confiable y que entreguen la validación de que está adecuadamente administrada y controlada. ● Realizar controles continuos dentro de la red para garantizar la seguridad de ella, prohibiendo el acceso de personal no autorizado.
	Seguridad de los Servicios de la Red	● Solicitar que todos los requisitos necesarios que fueron identificados estén estipulados en los acuerdos que se realizarán. ● Validar la capacidad del proveedor de red según los requisitos necesarios dentro de la empresa.
	Administración de Medios removibles	● Establecer procedimientos para la administración de medios removibles dentro de la empresa, tales como: discos duros, pendrives, tarjetas de memoria, etc. ● Documentar los procedimientos con sus respectivos permisos sobre la administración de medios removibles.
	Desechar Medios	Establecer permisos dentro de la empresa para el desecho de los medios, realizando una evaluación de ellos.
	Procedimiento Manejo Información	Establecer procedimientos para manejar el almacenaje de información, tales como: la protección de información, como la divulgación de ella.
	Seguridad de Documentación de Sistemas	Establecer claves de acceso para la documentación de sistemas y que sea entregada a los encargados correspondientes.

	Políticas y Procedimientos Intercambio Información	Establecer política o procedimiento que asegure la protección de información basada con las leyes existentes.
	Acuerdos de Intercambio	● Establecer acuerdos de intercambio de información y software que especifiquen los requisitos que son necesarios para su obtención por parte de los terceros. ● Reflejar la sensibilidad de la información que se le está entregando a un tercero en el acuerdo que se está estipulando.
	Medios Físicos en tránsito	Establecer claves de acceso en los medios de información evitando la corrupción de la información que contiene y entregar esas claves al encargado.
	Sistemas Informáticos de Negocios	Establecer en las políticas, acuerdos y procedimientos para la protección de información asociado con sistemas informáticos de los negocios.
	Comercio Electrónico	● Establecer redes seguras dentro de algún comercio electrónico. ● Considerar medidas de seguridad en los comercios electrónicos que se presenten, tales como la criptografía. ● Establecer documentación de los acuerdos realizados con los socios de comercio electrónico considerando los términos de ambas partes del acuerdo, como también los detalles de seguridad que se establecerán dentro del comercio.
	Transacciones en Línea Información	Establecer medidas de seguridad en las transacciones en línea en donde proteja la información de ellas evitando las transmisiones incompletas, mal rteo, divulgación no autorizada, etc.
	Disponible Públicamente	Definir los permisos pertinentes dentro de la información pública para que no puedan ser modificadas.
	Log de Auditoría	Generar registro de la actividad de los usuarios por un periodo de tiempo acordado para investigaciones y monitoreo de control de accesos.
	Protección de Información de los Registros/Logs	Aislar y controlar el acceso de los lugares de almacenamiento de los registros e informaciones.
	Registros/logs de Administradores y Operadores	● Registrar las actividades de los administradores y operadores dentro de la empresa y sus tiempos de trabajo. ● Establecer periodos continuos de revisión de los registros.
	Registros/logs de Fallas	● Registrar fallas y realizar un análisis para determinar las acciones correspondientes. ● Realizar evaluaciones de riesgos para determinar el nivel de registro necesario para el sistema considerando la degradación en performance.

	Sincronización de Reloj	Sincronizar los tiempos de los sistemas de procesamiento de información dentro de la empresa con una fuente acordada.
Control de accesos	Política de Control de Acceso	● documentar una política de control de acceso basada en los requisitos de negocio y seguridad ● Re-evaluar los controles de acceso y complementar, en caso de no estarlo, con un control de acceso físico y lógico ● Documentar los requisitos del negocio en relación al control de acceso y distribuirlo a los usuarios y proveedores
	Administración Privilegiada	Establecer privilegios de usuarios.
	Administración de Contraseñas del Usuario	Documentar, desarrollar e implementar un proceso de asignación y reasignación de contraseñas
	Revisión de los derechos de acceso del usuario	Establecer revisiones de privilegios con una frecuencia regular
	Uso de Contraseñas	Establecer un método de registro de contraseñas que restrinja la cantidad de caracteres mínimo a 8, y que este incluya números, letras y caracteres especiales.
	Equipos de Usuario desatendidos	Documentar y establecer procedimientos para la protección de los equipos, y disponibilizar esta información a los usuarios
	Política sobre el uso de Servicios de la Red	● Establecer privilegios de usuarios. ● Establecer política de configuración de redes y servicios a red
	Autenticación del Usuario para conexiones externas	Establecer privilegios de usuarios.
	Identificación de Equipos en la Red	Establecer identificación automática de equipos.
	Diagnóstico Remoto y configuración de Protección de Puertos	Proteger con un mecanismo de seguridad el acceso lógico y físico a puertos de diagnóstico
	Segregación en Redes	● Segregar en la red grupos de servicios informáticos, usuarios y sistemas informáticos ● Utilizar mecanismos de seguridad perimetral para segregar la red.

		• Establecer consideraciones para segregar redes inalámbricas de redes internas y privadas
	Protocolo de Conexión de Redes	Establecer una política de control de acceso que establezca el control de conexiones de redes para redes compartidas.
	Control ruteo de Redes	• Establecer una política de control de acceso que establezca la implementación de controles en el ruteo. • Establecer los controles de ruteo basados en las fuentes positivas y mecanismos de identificación del destinatario. Como por ejemplo Network Address Translation (NAT).
	Procedimiento Seguro de Log-on	Controlar el acceso a sistemas operativos a través de un procedimiento log-on seguro
	Sistema de Administración de Contraseña	Establecer un sistema de administración de contraseñas que establezca controles de contraseñas seguro.
	Utilización de Utilitarios de Sistemas	Controlar en forma rigurosa los utilitarios y aplicacione.
	Time-out de las Sesiones	Desactivar sesiones inactivas después de un periodo de inactividad definido.
	Limite de tiempo de Conexión	Establecer una restricción en el tiempo de conexión para aplicaciones de alto riesgo.
	Restricción Acceso a la Información	Establecer privilegios de usuarios.
	Aislamiento de Sistemas Sensitivos	Proveer de un ambiente computacional dedicado a los sistemas sensitivos.
Adquisición, desarrollo y mantenimiento de Sistemas Informáticos	Requisitos de Seguridad Análisis y Especificaciones	• Establecer en los requisitos de seguridad para nuevos sistemas informáticos y mejoras a sistemas informáticos especificaciones a los requisitos de controles de seguridad • Reflejarán los requisitos de seguridad y controles valores del negocio correspondiente a los activos informáticos involucrados y a las consecuencias en caso de fallas de seguridad. • Integrar en las etapas iniciales y los proyectos de sistemas informáticos los requisitos de sistemas para seguridad informática y procesos para la implementación de seguridad.
	Validación de Input de Datos	• Validar los datos que se ingresan a las aplicaciones. • Considerar controles de datos, respuestas a errores, definición de responsabilidades, etc.

	Control de Procesos Internos	● Incorporar controles de validación dentro de la aplicación. ● Establecer un diseño e implementación de aplicaciones que aseguren que el riesgo de fallas de proceso que conlleven a pérdidas de integridad son minimizados.
	Integridad de Mensajes	● Identificar los requisitos para asegurar y proteger la integridad de los mensajes en aplicaciones. ● Establecer una evaluación de riesgos de seguridad periódicamente.
	Validación de Datos de Salida	Validar los datos de salida de las aplicaciones.
	Política para el Uso de Controles Criptográficos	● Establecer una política relacionada al uso de controles criptográficos para la protección de la información ● Revisar y evaluar si la política ha sido implementada exitosamente, en caso contrario, re implementar. ● Considerar la administración hacia el uso de controles criptográficos, resultados de evaluación de riesgos en la política criptográfica
	Administración de Llaves	● Establecer una administración de llaves. ● Proteger las llaves criptográficas contra modificaciones pérdidas y destrucción ● proteger llaves secretas y privadas. ● proteger físicamente los equipos utilizados. ● Basar el sistema de administración de llaves en estándares acordados, procedimientos y métodos seguros.
	Control de Software Operacional	Establecer controles para la implementación de software en sistemas operativos
	Protección de Datos de Prueba	● Proteger y controlar los datos de prueba ● Enmascarar el uso de información personal o cualquier información sensitiva
	Control de Acceso a Librerías de Programas Fuentes	Establecer controles estrictos sobre acceso a la librería de programas fuentes.
	Procedimientos de Control de Cambios	● Establecer controles estrictos sobre la implementación de cambios a los sistemas informáticos ● Establecer procedimiento que considere la necesidad de evaluar riesgos, análisis de impacto sobre cambios.
	Revisión Técnica de aplicaciones después de	Establecer procedimiento para revisar y probar las aplicaciones críticas del negocio por impactos adversos en operaciones organizacionales o seguridad después de los cambios al sistema operativo.

	cambios a sistemas operacionales	
	Restricciones a cambios a paquetes de software	● Evitar modificaciones a paquetes de software. ● Controlar todos los cambios.
	Divulgación de Información	● Establecer controles para prevenir la divulgación de información. ● Considerar controles como el escaneo de medios saliendo, inspecciones regulares del personal y actividades de sistemas permitidas bajo legislaciones locales, uso de recursos de monitoreo
	Desarrollo de Sistemas Outsourced	● Supervisar y monitorear el desarrollo de software externalizado. ● Considerar puntos como acuerdos de licencia, requisitos contractuales sobre calidad, pruebas antes de instalación para la detección de troyanos etc.
	Control de vulnerabilidades Técnicas	● Obtener en forma regular información sobre vulnerabilidades técnicas relacionado con sistemas informáticos utilizados. ● Evaluar exposiciones de la organización a vulnerabilidades.
Administración de Incidentes de Seguridad Informática	Reportando eventos de Seguridad Informáticos	● Reportar información sobre eventos de seguridad informáticos tan rápido como sea posible. ● Desarrollar e implementar un procedimiento formal para reportar eventos de seguridad informática.
	Reportando debilidades en la Seguridad	Establecer un procedimiento que asegure que todos los empleados de informática y servicios son requeridos de notificar y reportar cualquier observación o debilidades de seguridad sospechosas en el sistema o servicios.
	Responsabilidades y procedimientos	● Establecer procedimientos y responsabilidades administrativas. ● Utilizar monitoreo de alertas y vulnerabilidades de sistemas. ● Acordar con la gerencia objetivos de la administración de los incidentes de seguridad informáticos.
	Colectar evidencia	● Establecer acciones legales acciones como seguimiento contra una persona u organización después de un incidente de seguridad informático ● Recolectar, retener y presentar la evidencia relacionada al incidente ● Desarrollar procedimientos internos para colectar y presentar evidencia.
Administración Continuidad de Negocios	Incluyendo Seguridad Informática en la Continuidad de Negocios	● Establecer un procedimiento administrativo que define los requisitos de seguridad informática para el desarrollo y mantenimiento de la continuidad de negocios a través de la organización. ● Establecer proceso que contempla los riesgos que la organización está enfrentando, identificación de activos del

		negocio críticos, identificación del impacto de incidentes, consideración de la implementación de controles adicionales de prevención y la documentación del plan de continuidad de negocios definiendo los requisitos de seguridad.
	Continuidad de Negocios y Evaluación de Riesgo	Identificar eventos que causan interrupciones a los procesos del negocio
	Desarrollando e implementando planes de continuidad incluyendo seguridad informática	● Desarrollar planes para mantener y restaurar las operaciones del negocio, asegurar la disponibilidad de la información dentro de los niveles requeridos en los tiempos requeridos seguidos a una interrupción o falla a los procesos de negocios. ● Considerar en el plan la identificación y acuerdos de responsabilidades, identificación de pérdidas aceptables, implementación de procedimientos de recuperación y restauración, documentación de procedimientos y pruebas regulares.
	Arquitectura de Planeación Continuidad de Negocios	● Establecer una arquitectura para el plan de continuidad de negocios ● Evaluar que la arquitectura garantice que todos los planes son consistentes e identifican prioridades para pruebas y mantenimiento. ● Definir en plan de continuidad de negocios los requisitos sobre seguridad informáticos identificados.
	Pruebas, Mantenimiento y re-evaluación de Planes de Continuidad de Negocios	● Probar regularmente para garantizar su actualización y efectividad los planes de continuidad de negocios ● Garantizar e las pruebas de los planes de continuidad que que todos los miembros del equipo de recuperación y otros grupos de empleados relevantes están concientes del plan y de sus responsabilidades por la continuidad del negocio y la seguridad informática y conocen su rol cuando el plan es activado.
Cumplimiento	Identificación de Legislación aplicable	● Definir explícitamente y documentar para cada sistema informático y organización todos los requisitos relevantes a regulaciones, contratos, etc. y el enfoque organizativo para cumplir los requisitos ● Definir y documentar controles específicos y responsabilidades individuales para cumplir con los requisitos
	Derechos de Propiedad Intelectual	● Establecer procedimientos que garanticen el cumplimiento con requisitos legislativos, regulaciones y contratos en el uso de material en el cual pueden existir derechos de propiedad intelectual y en el uso de productos de software propietarios. ● Re evaluar si los procedimientos están bien implementados, y re implementarlos. ● Considerar controles como políticas de cumplimiento sobre los derechos de publicación de propiedad intelectual, procedimientos para la adquisición de software, políticas de concientización, mantener prueba de propiedad, cumpliendo con los términos y

		condiciones
	Protección de Registros Organizacionales	● Proteger de pérdidas destrucción y falsificación de acuerdo con regulaciones, contratos y requisitos de negocios los registros importantes de la organización ● Considerar la posibilidad del deterioro de los medios de para el almacenaje de los registros. ● Escoger los sistemas de almacenamiento de datos para que datos requeridos puedan ser recuperados o restaurados en un tiempo y formato aceptable, dependiendo en los requisitos a cumplir.
	Protección de Datos y Privacidad de Datos Personales	Asegurar la protección y privacidad de los datos según legislación, regulación relevantes y si es aplicable según cláusulas contractuales.
	Prevención del mal uso de las facilidades de procesos informáticos	● Tratar como uso inapropiado de las facilidades el uso de las facilidades de procesos informáticos para efectos personales o no autorizados sin el consentimiento de la gerencia ● Presentar un mensaje de advertencia al momento de log-on ● Obtener asesoría legal antes de implementar cualquier procedimiento de monitoreo.
	Regulación de Controles Criptográfico	Utilizar en cumplimiento con acuerdo, leyes y regulaciones relevantes los controles criptográficos
	Cumplimiento con Políticas y Estándares de Seguridad	● Asegurar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad son efectuados correctamente para lograr cumplimiento con las políticas y estándares de seguridad. ● Revisar periódicamente el cumplimiento de las facilidades de procesamiento informáticos dentro de sus área de responsabilidad para el cumplimiento con procedimientos y políticas de seguridad apropiados.
	Revisión del Cumplimiento Técnico	● Revisar los sistemas informáticos con relación al cumplimiento con la implementación de estándares de seguridad. ● Efectuar por o bajo la supervisión de personal competente y autorizado la revisión del cumplimiento técnico.
	Controles de Auditoria de Sistemas Informáticos	● Plantear cuidadosamente los requisitos de auditoría y actividades que involucran revisiones de los sistemas operacionales ● Acordar con la gerencia apropiada los requisitos de auditoría y alcance
	Protección de las Herramientas de Auditorías de Sistemas Informáticos	● Proteger el acceso a las herramientas de auditoria de sistemas como ser software o archivos de datos ● Separar las herramientas de auditoria de sistemas informáticos de los sistemas de desarrollo y operacionales a menos que se les haya dado un nivel apropiado de protección adicional

Identificación de factores críticos