¿Cuáles son las ventajas y limitaciones de tener el área de seguridad dentro o fuera del área de informática de la organización?	
Autor	**Respuesta**
Gloria P. Arenas M. Martes 21 de Agosto de 2007	**AREA DE SEGURIDAD DENTRO DEL ÁREA DE INFORMÁTICA** <u>Ventajas</u> - Es más fácil de crear ya que no requiere un cambio organizacional drástico <u>Limitaciones</u> - El alcance queda automáticamente reducido a la información digital y otros sistemas netamente informáticos, de redes o infraestructura. - Los presupuestos deben ser divididos con otras áreas de IT. - Es más difícil crear y fomentar una cultura de seguridad de la información en todos los niveles, que considere aquella información almacenada en seres humanos. - Algunos gerentes o altos niveles suelen solicitar excepciones y dado que el área de sistemas usualmente no tiene el poder ni el apoyo, la posibilidad de "huecos" es mayor. - La alineación de la estrategia de seguridad de la información con la estrategia de la empresa se hace más difícil, pues el acceso a la última por parte del departamento de sistemas es reducido; además, el alcance del área sería de por sí menor. **AREA DE SEGURIDAD FUERA DEL ÁREA DE INFORMÁTICA** <u>Ventajas</u> - El ideal es que a largo plazo no sólo exista un área de seguridad, sino de manejo de la información que incluya en sus tareas la seguridad y el aprovechamiento de la información de la empresa. Iniciar el área de seguridad de manera independiente a la de informática hace más fácil el recorrido a esa meta. - El apoyo de gerencia suele ser mayor y por ende la cultura es más fácil de fomentar, los presupuestos relativamente más amplios y el provecho para la empresa puede ser mayor. - El cambio en la percepción de los empleados de la organización (en todos los niveles) con respecto a qué es seguridad es mejor recibido pues su emisor y su mensaje tienen de por sí más peso. - Facilidad de alineación con la estrategia de la organización. <u>Limitaciones</u> - Costos de creación y cambio organizacional - Demoras en su puesta en marcha real.
R. Fabian G2X GSEC Silver Jueves 16 de Agosto de 2007	**AREA DE SEGURIDAD DENTRO DEL ÁREA DE INFORMÁTICA** <u>Ventajas</u> - Ideal en compañías pequeñas para optimizar recursos - El proceso de integración es menos complejo, los procedimientos se adecuarían y administrarían por el mismo personal administrador de

	infraestructura y controles, lo cual llevaría menos tiempo. <u>Limitaciones</u> - Con habilidades y conocimiento técnico que superan y opacan las habilidades gerenciales en proyectos, negociación, motivación, etc necesarias para una buena gestión de seguridad de la información. - Estaría más enfocada o se percibiría como seguridad informática, cuando lo que se busca es seguridad de la información. - El área de seguridad no debería hacer parte de áreas de apoyo en la organización (como se considera IT en los mapas de procesos),ya que de ser así, es posible la creencia por los empleados de que el área y sus proyectos no son estratégicos. - La seguridad de la información no puede darse el lujo de percibirse como un proyecto solo de IT. **AREA DE SEGURIDAD FUERA DEL ÁREA DE INFORMÁTICA** <u>Ventajas</u> - Independencia, imparcialidad y objetividad - Si reporta directamente a la dirección, o hace parte de un área gerencial como Control interno, Auditoría, gestión de riesgos, se percibe como un área estratégica de la organización. <u>Limitaciones</u> - Resistencia por parte del área de IT, debido a por ejemplo el deseo del Director de Informática de no perder el control de la seguridad de IT, el temor a que se descubran controles existentes inadecuados.
Juan Carlos Cocunubo Cocunubo TSRS – Technology & Security Risk Services Ernst & Young	**AREA DE SEGURIDAD DENTRO DEL ÁREA DE INFORMÁTICA** <u>Ventajas</u> <u>Limitaciones</u> - Temas técnicos: se pierde de alguna manera el tema estratégico de la compañía para tocar temas netamente técnicos. - Escalamientos: dado que el tema no es corporativo, el escalamiento de temas de seguridad de la información a los directivos queda en un plano que quizá ellos no puedan comprender adecuadamente por su desinformación al respecto. **AREA DE SEGURIDAD FUERA DEL ÁREA DE INFORMÁTICA** <u>Ventajas</u> - Control a nivel corporativo de la seguridad de la información: lo cual significa que los directivos de la compañía hacen parte del modelo de seguridad de la información y están comprometidos con el mismo. - Creación de un comité de seguridad de la información: involucramiento de áreas funcionales y técnicas (TI) para aportar al beneficio de la seguridad de la información. - Participación del área de auditoría: mayor compenetración de ésta área en el tema de seguridad de la información, con aportes valiosos al respecto de acuerdo a sus metodologías de auditoría.
Mauricio Gómez B. ALAPSI COLOMBIA Miércoles 15 de Agosto de 2007	Dado que el área de Seguridad es un ente de Monitoreo y aplicación de controles no se sugiere que dependa de las áreas de Contraloria para que no haya problemas de competencias. Así mismo lo ideal dentro de las nuevas estructuras es que dependa de un área de Riesgo, en caso de que no se tenga se puede integrar en las áreas de Sistemas,

César Tarazona ETEK Agosto 16 de 2007	**AREA DE SEGURIDAD DENTRO DEL ÁREA DE INFORMÁTICA** Solo si se piensa en seguridad informática, sería un área de soporte para mejorar la seguridad en la gestión y operación de los recursos tecnológicos de la organización (no solo informática), por lo que inclusive podría depender de una dirección de tecnología que abarque sistemas (informática) y otras áreas como redes de datos-comunicaciones, etc. según los esquemas propios de cada organización. <u>Ventajas</u> - Enfoque directo en las necesidades del área (Tecnología) - Contar con el personal técnico necesario para que se pueda dedicar a las funciones designadas. - Aprovechar el conocimiento para la operación de la plataformas de seguridad (Firewall, IDS/IPS, Gestión de algunos Servidores de Log´s, etc) <u>Limitaciones</u> - Visión aislada del contexto general del negocio o de la organización - No es independiente. - No se tiene un ente de nivel superior que pueda tomar decisiones relacionada con niveles de riesgos aceptables y residuales, lo cual en la práctica significa establecer el balance adecuado entre seguridad y operatividad. - Generación de conflictos internos en el área, al realizar tareas de operación y gestión por parte de personas del mismo grupo. <u>Algunas funciones:</u> Funciones estratégicas (definición de planes, políticas, etc.) Definición, implementación y operación de aspectos tecnológicos de seguridad (estándares, plantillas, políticas) **AREA DE SEGURIDAD FUERA DEL ÁREA DE INFORMÁTICA** Tener como foco la seguridad de la información (no solo informática) en toda la organización. Una buena aproximación actual es que forme parte del área de riesgos. <u>Ventajas</u> - Permite ver la gestión de la seguridad de la información como un componente de la gestión del negocio - Deja de ser un aspecto relacionado con una problemática puramente técnica - Involucra y le llega a los niveles superiores (directivos) de la organización - Es un enfoque más adecuado para la realidad actual - Puede interactuar con otras áreas de la organización (seguridad física, Riesgos operativos, Aufitoría/contraloría/Control interno)para que los esfuerzos se sumen <u>Limitaciones</u> - Se requiere que sea liderada por una persona con un perfil más amplio e inclusive más gerencial que técnico: conocimientos técnicos y gerenciales, conocimiento de todos los aspectos y procesos del negocio, etc. - Puede ir en contra de esquemas organizacionales ya definidos o muy rígidos y por lo tanto generar roces internos a niveles directivos. (creación de más áreas o vicepresidencias en la organización). - Es difícil romper el esquema inicial que la relaciona siempre con el área de tecnología (cambios en la cultura de la organización) y se sigue viendo como un soporte técnico exclusivamente. - Falta de recursos que cumplan de los demás perfiles adecuados para los integrantes del área (conocimiento técnico, procesos, gerencia, operativos de plataformas de seguridad, etc.)
Gustavo Rodriguez Jueves 16 de Agosto	Doy por defecto por la temática del foro que cuando se dice " área de seguridad en la organización" se refiere a seguridad informática / Seguridad de la Información o

	Seguridad y Calidad (IT) o similar, ya que muchas organizaciones tienen en su organigrama: "Seguridad e Higiene" que apunta a otros temas en algunos muy vinculados con lo nuestro por ejemplo BCP/DRP y seguridad Física de la Información, donde este tipo de áreas tiene que participar por ejemplo con el tema de simulaciones y pruebas de los planes anteriormente nombrados mas la implementación, seguridad (Guardias, cámaras, etc) y soporte de los temas de seguridad física que son integrales para toda la empresa incluida todo lo se refiere a salas de comunicaciones y servidores. También está el tema del área "Auditoría / Auditoría de Sistemas / Auditoría y control / etc ." en muchas organizaciones existen estos sectores como otra área independiente de seguridad y también hay dudas de la dependencia y la relación con la dirección general y con seguridad informática. Sería ideal tratar también este tema. Muchas empresas tienen un solo sector que realiza tareas de Auditoría y seguridad informática en conjunto con los mismos RRHH. **AREA DE SEGURIDAD DENTRO DEL ÁREA DE INFORMÁTICA** <u>Ventajas</u> - Se tiene un contacto directo con sus pares (Personal IT) y con la realidad de la organización en relación a la tecnología y forma utilizada. - Se genera en algunos casos una mejor implementación (por ejemplo de los controles de la ISO 27001) por estar más en contacto con las primeras etapas de desarrollo de nuevos proyectos de producción de software y de actualización de infraestructura. - En algunos pocos casos en problemas o disputas generadas post auditorias o incidentes se puede lograr una especie de mediación entre los distintos sectores de IT involucrados con la participación del responsable máximo del área de informática. <u>Limitaciones</u> - Muchas observaciones de auditoría pierden objetividad - Puede faltar una definición clara de algunos temas por parte del responsable del área informática - Generalmente para casos particulares no se puede escalar problemáticas en la línea de mando de la estructura organizacional
Javier Estupiñan Universidad Libre Martes 14 de Agosto	Hoy en día con el nuevo concepto de oficiales de seguridad informática , cargo importantísimo dentro de la organización , dependería básicamente dentro del nivel de cargos directivos de la organización , esto de acuerdo a su ROL dentro de la compañía en cuanto a seguridad se refiere , documentos , locaciones, software , hardware , servidores , licenciamiento etc.....
Pedro María Buitrago Mantilla Martes 14 de Agosto	El área de seguridad de la información de una organización es un área estratégica en virtud que propende por la protección de la información. En general, la protección de la información es estratégica como discriminador de una organización en el mercado. De acuerdo a lo anterior, el área o dirección de seguridad de la información debería estar lo más cerca posible de la dirección general. En organizaciones a nivel internacional la intención de gestionar la seguridad de la información como factor estratégico ha tomado más fuerza a partir del 11S ya que un área o dirección en esta rama procura por temas como el análisis de riesgos, la continuidad del negocio, potencialización del valor de la información y, en general, apoyo directo a la concecusión de los objetivos de la organización.
Carlos Andrés Jiménez Rodríguez Administrador IT ISVI LTDA Martes 14 de Agosto de 2007	Depende del tamaño y objeto de la empresa: En una empresa pequeña o mediana, obviamente la Seguridad informática debe estar a cargo del área de IT, que a su vez dependerá de la Gerencia o Dirección Administrativa. Sin embargo en una empresa cuyo objeto principal tenga que ver con informática o cuyo tamaño sea considerable, la seguridad informática y todas las demás, (física, industrial, del personal, investigaciones, etc), según el nuevo modelo de Convergencia aplicado por ASIS Internacional, (que es el que manejamos en mi empresa y ayudamos a montar en otras

	afines) debe depender de un grupo interdisciplinario liderado por Seguridad, que a su vez depende de la Alta Dirección de la empresa.
Humberto Prieto Auditor de Sistemas	Es evidente que no puede depender del área de sistemas, por tanto existen dos modelamientos: - Depender del área de revisoría fiscal, aunque debo decir que un contador no es idóneo, para realizar ni evaluar auditorias de sistemas, - Depender del área de auditoría de sistemas de la empresa, (o en su defecto contratar un auditor externo).