Monitoreo y cumplimiento en la seguridad de la información

Sara Gallardo M.

La revista realizó por primera vez de manera virtual, el foro institucionalizado en esta sección. Considerando que las preguntas no fueron tratadas en su totalidad por los participantes en dicho encuentro, publicamos solamente las respuestas obtenidas en forma completa, por parte del coordinador del foro, Andrés Ricardo Almanza.

La Asociación Colombiana de Ingenieros de Sistemas (ACIS) se lanzó al mundo de la virtualidad y reunió en diálogo por chat a diferentes expertos en el tema de la seguridad informática y sus nuevos alcances.

Entre los invitados por la revista acudieron a la cita Hugo Sin, representante de Redes y Comunicaciones de Colombia Ltda., (Redcom); Gabriel Jaime Ríos y Álvaro Guzmán, directivos del área de Seguridad Informática de Avianca; y, el mayor Fredy Bautista, director de Delitos Informática de la Dijín, quienes estuvieron acompañados por el director de la revista Francisco Rueda y Andrés Ricardo Almanza.

Este último en su calidad de coordinador dio respuesta a todos los interrogantes. Andrés Ricardo Almanza es Ingeniero de Sistemas de la universidad Católica de Colombia, graduado de la Especialización de Seguridad en Redes en la misma entidad educativa; es master en Seguridad de la Información de la universidad Oberta de Cataluña. Se ha desempeñado como profesor de posgrados en la universidad Pontificia Bolivariana, en lo que a seguridad en redes y sistemas de detección de intrusiones se refiere.

Es docente de posgrado en la universidad Rosario de Colombia, en el área de seguridad en redes, y en la universidad Externado de Colombia en el área de Fraude Electrónico.

En otras latitudes, es miembro de la Red Iberoamericana de Cristología y Seguridad de la Información – CriptoRED (http: //www.criptored.upm.es). Y, en la actualidad, se desempeña como Jefe de Seguridad y Administración de la Información de la Cámara de Comercio de Bogotá.

¿Cuándo se debe plantear una infraestructura de monitoreo para las organizaciones?

Las infraestructuras de monitoreo se deben plantear en la medida que han evolucionado las tecnologías; el monitoreo es importante y debe estar presente desde el diseño de una infraestructura, pero como esto no es real, se sugiere que se planteen en la medida en que las plataformas tecnológicas posean madurez en el tema.

¿Cuáles deberían ser los elementos más importantes de la infraestructura? ¿Hasta qué nivel de integración y convergencia podemos llegar en las organizaciones, convergencia de tecnologías, convergencia de la gestión de riesgos?

Andrés Ricardo Almanza.

De la misma manera, pienso que debe evolucionar; en un primer lugar es posible observar que la integración se puede dar de lo físico a lo lógico, luego esa misma madurez llevará a la empresa a plantear la forma en cómo ver una gestión corporativa del riesgo, con el propósito de asimilarlo como un todo.

¿Es viable un modelo corporativo de gestión de riesgo donde se consideren todas las variables de este tipo, que afectan

a las diferentes unidades de negocio de la organización?

Sí es viable; la cuestión en este punto es pensar en los retos que esto enfrenta; en muchos de estos casos los retos culturales y organizacionales son grandes, en gran medida porque requiere del esfuerzo de alguien que condense, a través del apoyo mancomunado, una visual única de riesgo.

Adicionalmente, debe existir un apoyo de la alta dirección para que este tipo de situaciones se den.

¿Cuánto tiempo puede tomar una aproximación de esta naturaleza? ¿Debe existir algún tamaño límite de empresa para aplicar este modelo?

Pienso que no. Es posible que las empresas de mayor tamaño inclusive hoy, ya lo hayan contemplado como alternativa, puesto que con ello pueden existir ahorros significativos en temas de inversiones.

Disponer de un solo punto de seguridad donde se comparta una visión sobre la protección, puede permitirnos ver más como negocio dicho reto, con el ánimo de ser mucho más certeros a la hora de implementar soluciones de tal naturaleza.

En consecuencia, pienso que las mismas organizaciones, sin importar el tamaño, se volcarán a ese proceso, tal vez unas más rápido que otras.

¿Cómo podría ser la aproximación de las organizaciones a un modelo donde se implemente la convergencia entre lo físico, lo lógico y lo financiero?

En este caso, la situación que enfrenta en primera medida quien busca proteger los activos, es tener una visión global de la organiza-

ción y entender sistemáticamente tres cosas.

Por un lado, entender el negocio que está bajo su amparo, la tecnología que existe, y las necesidades de seguridad.

Con esto en mente creo que es viable que el panorama financiero esté claro y además posiblemente de acuerdo con las habilidades del director de seguridad y su sustento para invertir en algunas soluciones de protección, obviamente, las más adecuadas frente a los intereses de la organización.

¿Quién se debe encargar de gestionar este panorama? ¿Estaremos frente a un nuevo rol en la organización?

Yo creo que sí; se trata de alguien que debe tener necesariamente cualidades de gerencia muy desarrolladas.

El director de seguridad de la información, debe poseer una visión holística de la seguridad y de la tecnología, y se debe encargar por lo tanto de conciliar, a través de su trabajo, el esfuerzo de las diferentes participantes en procura de un objetivo común, la defensa.

¿Cómo convencer a las organizaciones de que ahora la seguridad no es un problema de TI, sino un problema que toca a todas las unidades de negocio?

En primer lugar pienso que este tema debe ser abordado desde la perspectiva del negocio; es decir, visualizar el servicio, producto que se tiene para la organización; ver cómo una falla de seguridad, en la secuencia por donde el servicio sucede, puede afectar el cumplimiento de un objetivo estratégico.

En ese mismo sentido se requiere tener una visión un poco más transversal para poder llegar a demostrar esta necesidad.

¿Cuál debe ser la aproximación en la definición de los eventos a monitorear que muestren la forma como se ven afectadas las unidades de negocio de la organización?

Cuando uno habla de monitorear eventos, lo importante es tener claro qué se debe monitorear, teniendo presente que todos los modelos no son iguales; por lo tanto, es donde entra en juego la pericia

del grupo de seguridad, para personalizar la seguridad, monitoreo y control.

Pueden existir algunas reglas generales, pero existirán patrones únicos de comportamiento anormal al interior de las organizaciones, que permitan definir estos eventos, y que, en últimas, con la visión transversal propuesta de poder ver al producto, y/o servicio como una secuencia de acciones ejecutada en procura de un objetivo, es donde podría verde la posibilidad de tal situación.

En un ambiente de monitoreo integral (físico, lógico) ¿cuál debe ser la estrategia para enfrentar los falsos positivos?

Los falsos positivos siempre los he considerado un problema de conocimiento de lo que se monitorea; por lo tanto, pienso que antes de abordar una propuesta de monitoreo es necesaria la claridad sobre lo que se debe monitorear, para que el número de falsos positivos disminuya.

De igual manera, una vez realizadas tales implementaciones, es necesario un estudio continuo sobre los eventos, para optimizar su monitoreo.

En otras palabras y como ya lo dije, la personalización de la seguridad es importante.

¿Cuánto tiempo puede durar implementar un proyecto de monitoreo de eventos de seguridad integral (SIEM)? ¿Qué tan costoso puede ser para la organización?

El tiempo no debería ser muy amplio, dado que eso como muchas de las tecnologías se requieren lo más pronto posible; según los datos de los proveedores, de 1 a 3 meses se puede demorar un proceso de estos, aunque su afinamiento debe ser continuo y constante para llevar a la organización a pensar en cómo debe mejorar sus tecnologías, los procesos y la seguridad en sí misma. El costo estará determinado en muchos casos por lo que se desea cubrir o monitorear.

Con las posibilidades existentes de comunicación, completamente abiertas ¿considera usted que hay seguridad? ¿Cómo protegerse frente a la posibilidad de que su informa-

ción se vuelva pública? ¿Cuáles ventajas y desventajas hay con las comunicaciones y dispositivos actuales, qué recomendaría?

Siempre he pensado que la seguridad es un estado de tranquilidad, por lo tanto en algunos ambientes se puede sentir seguro y en otros no. Por la trascendencia de la tecnología en la actualidad, que cada vez demanda de información para la prestación de los servicios, lo que pienso y ratifico es que es necesario conocer muy bien el negocio sobre el que se trabaja; con eso en mente se pueden definir estrategias de protección adecuadas.

Las ventajas que tenemos hoy con todos los sistemas de información y tecnología en general son muy importantes; pensaría que lo retador es conocer cada tecnología que la organización posee, con el objetivo de poder tener un control adecuado.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión Gerencial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Corresponsal de la revista Infochannel de México. Así mismo, ha sido corresponsal en Colombia de los diarios "La Prensa" de Panamá, "La Prensa Gráfica de El Salvador, y de la revista IN de Lanchile. Autora del libro "Lo que cuesta el abuso del poder" y colaboradora en varias publicaciones culturales. En la actualidad se desempeña como Ministra de La Palabra o Directora de Comunicaciones y Servicio al Comensal en Andrés Carne de Res.*