Seguridad híbrida

DOI: 10.29236/sistemas.n167a5

Un paradigma emergente

En este número 167 de la revista el tema para analizar en el marco de la sección Cara y Sello es la "seguridad híbrida, un paradigma emergente", encuentro al que fueron invitados varios especialistas.

"Es un privilegio contar con su presencia en esta reunión realizada en cada número de la revista para analizar los asuntos más relevantes del tema central, en este caso, sobre "seguridad híbrida, un paradigma emergente", señaló Jeimy J. Cano Martínez, director de la revista, acompañado en su bienvenida a los invitados por Andrés Almanza coeditor técnico en esta edición: Hamilton Moya, especialista en ciberseguridad; Wilson Prieto, consultor en ciberseguridad, Héctor Calderazzi, consultor independiente en desarrollo de políticas, normas y procedimientos y Arturo García, doctor en Defensa y Seguridad Nacional por la Universidad Naval de México, Gerente de Seguridad en Tecnologías de la Información en el Banco Central de México.

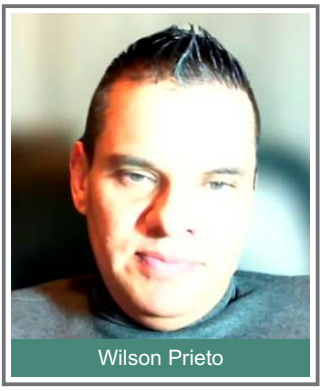
Después de la introducción los invitados procedieron a manifestar sus opiniones sobre las diferentes inquietudes planteadas.

Jeimy J. Cano M.
En un entorno cada vez más inestable, incierto, turbulento y ambiguo el concepto de seguridad debe evolucionar. En este sentido, ¿es necesario pensar ahora en una seguridad convergente? ¿Multidominio?

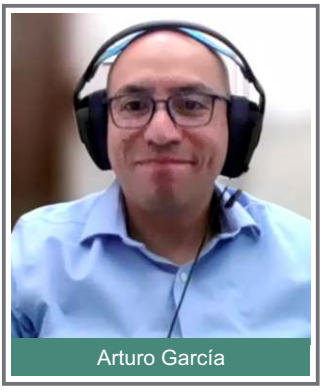
Arturo García
El término de seguridad nos refiere al concepto de paz. En ese sentido, sabemos que existen diferentes acepciones de paz. Las más comunes son la de "paz positiva", que refiere a la presencia de tranquilidad y armonía; y la "paz negativa" que implica la ausencia de conflictos. En mi opinión, lo que vivimos hoy en día en el ciberespacio es una "paz tolerada" que expresa la presencia continua de conflictos un punto tolerable pero que aún genera la sensación de tranquilidad.

De esta manera, existe realmente una evolución del concepto: estamos evolucionando hacia una paz que ya no es una ausencia de algo que nos ocasiona temor, pero tampoco estamos viviendo libres de preocupaciones. Yo creo que estamos tolerando esos conflictos, los cuales están escalando a diferentes dominios. Aquí es donde identifico claramente la connotación de


Hamilton Moya


Wilson Prieto


Héctor Calderazzi


Arturo García

"híbrido", que es lo que estamos revisando en este panel: se percibe tanto la parte de intangible, como el ciberespacio, como la parte tangible o física. Ambos dominios están convergiendo y ve claramente la tolerancia a esa inseguridad, un escenario gris de paz. Posiblemente estamos soportando más de lo que tal vez no deberíamos. Tenemos una gran tarea: repensar hacia donde queremos llegar.

Wilson Prieto

Entendiendo un poco la pregunta, pienso que la seguridad convergente o multidominio es un enfoque de seguridad que busca proteger múltiples dominios o sistemas informáticos utilizando una única solución de seguridad que proporcione la protección necesaria para minimizar el riesgo ante un posible ataque cibernético. Igualmente, este concepto se ha discutido durante los últimos años y puede verse como una estrategia enfocada a la protección de datos que unifique y coordine los esfuerzos del equipo de seguridad tanto en las entidades privadas como públicas creando un entorno seguro en diferentes contextos de la organización.

Por otra parte, la seguridad convergente puede aprovechar tecnologías emergentes que ayuden a prevenir posibles ciberataques y permite a las organizaciones enfrentar los desafíos de seguridad de manera más efectiva.

Hamilton Moya

Con respecto a la pregunta, desde mi punto de vista no es evolucionar hacia, porque los conceptos de una seguridad convergente y de seguridad multidominio ya se venían trabajando, por tal razón, creo que lo que se debe hacer es implementarla y arraigarla en las organizaciones, ya que muchos hablamos de que la seguridad debe ser aplicada en múltiples ámbitos de la organización, en los diferentes procesos, en las diferentes tecnologías que se utilizan, pero a veces se queda ahí, en aspectos aislados y no lo centralizamos, y esto, algunas veces, hace que se nos complique mucho más la tarea de asegurar o de disminuir ese factor de inseguridad que presentan nuestros activos. Como dije, para mí no es tanto evolucionar sino arraigar esos dos conceptos que ya se venían trabajando desde un tiempo hacia acá.

Héctor Calderazzi

Hay que tener una visión holística. Cuando me preguntan sobre seguridad convergente puedo afirmar que siempre he pensado con un enfoque integral de la seguridad de la información. Lo ideal es la convergencia, de tener el panorama del todo. Pero qué pasa, el costo de las herramientas para lograr esta convergencia y a veces aspectos estratégicos que no están bien definidos atentan contra dicha concentración. En este sentido me he encontrado con casos en los que, por ejemplo, adquirieron un "Qradar", con importantísimas inversiones en la herramienta y quedó "esperando en los cajones" un año o más, porque el personal no tenía la formación y no sabían cómo adecuar su implementación. Después me encontré con otro caso de migración de seguridad On-Premise a On-Cloud, en los que los responsables de sistemas decían "¿cuál es el sentido que nosotros controlemos a un proveedor On-Cloud de primer nivel internacional que lógicamente cumple con los estándares?". Es decir, tenemos una mezcla de situaciones estratégicas y culturales y observo que es más fácil una integración a nivel de lo que es el proceso de gestión de incidentes, antes que la integración de todo el ambiente. Coincido en comenzar por ahí, creo que lo dijo Wilson, integrar los conceptos más críticos, definirlos y establecerlos en forma uniforme a nivel de toda la organización. A su vez, varias organizaciones no tienen definiciones claras de todos los niveles de usuarios y sus permisos, no existen estándares de identificaciones de los usuarios, se utilizan usuarios genéricos y de servicio sin justificación, etc. Incluso no existen definiciones claras sobre control de cambios, muchas veces se implementa una metodología ágil y no se sabe dónde incluir el control de cambios. Dicho todo esto, estoy en un punto anterior todavía, me preocupa la estrategia integral de seguridad y después no tendría problemas que lo vayan implementando en forma multidominio, pero con un control centralizado.

Andrés Almanza

Quienes tenemos el privilegio de trabajar en el tema de seguridad llegamos a un momento en el que decimos la seguridad es de cobertura organizacional. Se trata de un pensamiento multidisciplinar para entender las múltiples vistas, las di-

mensiones de lo que empieza a suceder en la organización al hablar de protección y la generación de confianza de la información en sus diferentes formas.

Jeimy J. Cano M.

Las amenazas físicas se han transformado y evolucionado en diferentes contextos. En consecuencia, ¿cómo reconocer ahora estas amenazas en un entorno cada vez más incierto e inestable? ¿Cómo ayudar a las organizaciones en este nuevo ejercicio?

Héctor Calderazzi

Me parece que, respecto a metodologías y herramientas no hay una que sea la panacea. De hecho, si contamos con mucha información que puede servirnos como lecciones aprendidas y debemos ser autocríticos para repasar nuestro accionar hacia adelante. Pero, yendo a la pregunta concreta ¿cómo puedo reconocer las amenazas en un entorno cada vez más incierto? La respuesta sería por ejemplo mediante la realización de este tipo de reuniones, de la categoría de análisis de riesgo experto. En este momento no estamos leyendo ninguna matriz ni lista de amenazas específica, pero contamos con conocimientos de los riesgos en general, proponemos un escenario de riesgo, manteniendo los modelos a un costado que consultaremos en casos específicos. Proponemos el tema, abrimos el debate mediante lluvia de ideas, con una imaginación desde los zapatos del atacante, pensamos en el supuesto apetito que tiene el atacante, qué ven de interesante en nuestras organizaciones y en dónde estamos más débiles, en toda esa red que tenemos entre elementos lógicos, físicos (procesos, personas y tecnología). Por ejemplo, en una gran empresa de energía, hay una combinación entre lo que es la seguridad operacional y la seguridad lógica, que a veces no interactúa entre esos ambientes, no se comunican y esa desintegración juega en contra, cosas que sabe una parte de la organización y las desaprovecha la otra. Les cuento sobre esta organización que conocí, donde necesitaban tener una continuidad operativa durante los 365 días del año, con altos niveles de servicio y contaban con sensores automáticos (PLC – SCADA) que al llegar a utilizar un 80% a 90% de la capacidad instalada disparaban alertas. El punto es que todo ese control ope-

rativo no estaba integrado con la gestión de usuarios que llevaba seguridad lógica y tenía trabas para lograrlo. Creo que son aspectos propios de la naturaleza del negocio; en este caso el área operativa invirtió en tecnología avanzada y "desconoció" al área de TI, y por añadidura de pensamiento al área de Seguridad de la Información.

Finalmente, la incertidumbre de escenarios de riesgos que tenemos hoy en día surge sobre cuál es nuestro imaginario hacia adelante.

Hamilton Moya

Lo sintetizo en una expresión: vigilancia tecnológica. Considero que debemos estar haciendo vigilancia tecnológica permanente, pero, no únicamente de la tecnología que surge, esos cambios tecnológicos que nos ayudan a controlar, sino también en esos cambios tecnológicos que nos pueden llegar a generar más amenazas y que, por ende, nos pueden generar riesgos dentro de la organización. Por lo tanto, para mí es importante que quienes estamos gestionando la seguridad de la información, tengamos una actitud proactiva realizando actividades, como por ejemplo: análisis de riesgo, planificación, inteligencia de amenazas, estableciendo planes estratégicos, no haciendo trabajo individual sino colaborativo con el resto de las áreas de la organización, para evitar falta de comunicación y que los planes estratégicos vayan en una sola línea y cobijen al resto de la organización en procura de una seguridad multidominio.

Wilson Prieto

Es indudable que las amenazas físicas han experimentado una evolución y sofisticación considerable en los últimos años, lo cual ha generado un entorno de seguridad más incierto e inestable. En vista de ello, resulta crucial que las organizaciones adopten un enfoque holístico y proactivo en materia de seguridad física para poder identificar y hacer frente a estas amenazas en este nuevo contexto.

En consecuencia, resulta imperativo que las entidades dispongan de un plan de seguridad física sólido, el cual debe ser evaluado y actualizado de manera regular. Esto permitirá identificar posibles debilidades y vulnerabilidades que puedan comprometer la integridad de la entidad, y tomar las medidas necesa-

rias en línea con el plan de continuidad del negocio.

Otro aspecto de vital importancia radica en la inversión en tecnologías y herramientas de seguridad física avanzadas, que posibiliten la detección y monitorización de amenazas, así como el control de accesos no autorizados. Además, es esencial implementar medidas adicionales especialmente en un contexto en el que el trabajo remoto ha experimentado un incremento considerable, generando una brecha de seguridad en las organizaciones.

Por último, resulta fundamental proporcionar capacitación a los empleados en materia de seguridad física, dotándolos de conocimientos sobre técnicas de prevención y protección de datos para evitar el robo de información confidencial. Igualmente, fomentar la colaboración y cooperación con las autoridades locales y otras partes interesadas para mantenerse al tanto de las posibles amenazas cibernéticas y poder informar de manera eficaz cualquier incidente de ciberseguridad y seguridad física que pudiera surgir.

Arturo García

A pesar de que las amenazas y sus efectos están convergiendo, veo una constante en muchas organizaciones de todo tipo, públicas y privadas, en mantener una separación en las funciones de protección. Por ejemplo, en algunas corporaciones la seguridad muchas veces se focaliza en su vertiente física separada de las tecnologías de información, y viceversa, siendo que los efectos negativos implican afectaciones en ambos dominios, lo cual genera un problema mayor. Cuando ocurre un incidente, como en infraestructuras críticas del Estado, no importa si el origen es físico o del ciberespacio. Cuando el impacto escala se afecta en diferentes sentidos a la población, en diferentes campos: económico, político, diplomático, etc. Este escalamiento en las afectaciones no se está analizando como debía ser, siendo una causa intrínseca del escalamiento.

Me parece que es una parte de madurez en las empresas, en las organizaciones, en donde se debería dar un paso más fuerte, hacer una real integración de funciones. Como decía el doctor Cano: cuando tenemos un ambiente ciberfísico necesitamos gente que no solo deber saber de tecnología, también debe estar preparada en diferentes aristas y trabajar en equipo. Hay que tomar en cuenta el ambiente multidisciplinario de las consecuencias. Hoy debemos ver esas nuevas amenazas desde diferentes perspectivas y de manera integrada. En un mundo VICA esa es la única forma en afrontarlas de forma exitosa.

Jeimy J. Cano M.

El reto de la seguridad se ha transformado con el paso de los años.

En este sentido, la literatura advierte que el modelo de prevención se viene agotando. Así las cosas, si el reto es ir más allá de la prevención, ¿qué se debe actualizar, incorporar o deconstruir en las prácticas actuales para responder a la incertidumbre y la inevitabilidad de la falla propia de una sociedad cada vez más digital y tecnológicamente modificada?

Wilson Prieto

En la actualidad, el enfoque de prevención tradicional ha demostrado ser insuficiente ante el creciente número de ciberataques en un entorno digital y tecnológicamente cambiante. En este sentido, es crucial adoptar un enfoque integral de seguridad que incluya la detección temprana y una respuesta rápida frente a las amenazas cibernéticas. Esto implica la incorporación de tecnologías avanzadas de detección, análisis de amenazas y procesos ágiles y eficaces para gestionar los incidentes.

Es fundamental especializar a los profesionales en el tema de las amenazas cibernéticas y contar con expertos en caso de ataques, además de utilizar tecnologías y procesos especializados para la detección.

Debemos promover una cultura de ciberseguridad en toda la organización, no solo en el aspecto técnico, sino en todos los niveles, para que todos sepan cómo actuar en caso de un ataque cibernético.

La gestión de riesgos también desempeña un papel crucial y debe ser proactiva, basada en datos y estadísticas, para identificar posibles amenazas y evaluar su impacto potencial en la organización. El monitoreo continuo, respaldado por tecnologías y capas de seguridad especializadas, es esencial para identificar amenazas reales y garantizar la ciberseguridad de la compañía.

La integración de tecnologías avanzadas, como la inteligencia artificial y el aprendizaje automático, resulta imprescindible en la detección automática de amenazas. Asimismo, es importante contar con un plan de respuesta y recuperación efectivo que permita a la organización recuperarse y restaurar sus operaciones en caso de un ciberataque.

En resumen, es necesario abandonar el enfoque de prevención tradicional y adoptar un enfoque integral de seguridad cibernética que combine tecnología avanzada, capacitación especializada, gestión de riesgos proactiva y un sólido plan de respuesta y recuperación.

Hamilton Moya

Considero que prevenir no es la única forma de atacar la inseguridad a la que nos vemos enfrentados, pero entonces, que deberíamos hacer, pues adelantarnos a esta situación, entonces, si ya no puedo tener un modelo preventivo, tendría que tratar de pasarme a un mo-

delo predictivo, tratar de establecer a nivel de predicción que me puede llegar a pasar, a que riesgos puedo verme abocado pensando en esa tecnología tan prolifera que hay y tan avanzada y que sale constantemente, entonces, debemos ser predictivos y tratar de deconstruir ciertas ideas que tenemos. Un ejemplo muy pequeño, en cuantas empresas pequeñas, medianas, grandes, que invierten en seguridad o que ya tienen modelos de seguridad implementados, no hemos escuchado la expresión: "eso fue un problema de seguridad, se tiene que encargar el equipo de seguridad, el ciso, los analistas de seguridad". Debemos tratar de romper esa estructura mental de que la seguridad es solamente de un equipo, debemos interiorizar que la seguridad somos todos, volvernos convergentes, involucrar a todos los actores de la organización y decirles, ustedes hacen parte importante de esa protección, de esa seguridad de nuestra organización.

Adicionalmente, como parte de esa deconstrucción, es aplicar técnicas de resiliencia, participación activa de la alta dirección, esto último, es un concepto que hay que deconstruir, yo he visto y creo que muchos de quienes nos dedicamos a la seguridad, nos hemos encontrado en organizaciones donde la participación activa de la alta dirección es acá tienen el capital, acá tienen el presupuesto para algunas estrategias que se vienen trabajando y ya, y se considera que esta es la participación activa a través de la alta dirección, pero no, se deben involucrar en los procesos, impulsar y hacer esa divulgación de esa seguridad y decirle a todas las partes interesadas de la organización "hagámonos partícipes, somos uno solo protegiendo todos nuestros activos".

Arturo García

La pregunta me parece en extremo retadora: ¿cómo proceder ante la inevitabilidad? Esto es totalmente real; de hecho, esto es algo que he estado revisando en incidentes pasados de gran magnitud. A pesar de que existen países con fuertes estrategias de seguridad, mayor poder físico, legislación madura y múltiples organizaciones, te das cuenta que no necesariamente las hace invulnerables a brechas de ciberseguridad. Como dicen por ahí: "solamente existen dos tipos de empresas: las que ya hackearon y

las que van a hackear". Se podría añadir incluso unas terceras: las que no saben que las están hackeando. En ese sentido creo que hace mucho la labor de concientización sobre ese fenómeno.

También me parece que falta incorporar una figura diferente en las organizaciones que se conocería como "Chief Disruptive Officer", esto es, una figura de disrupción. Alguien que identifique escenarios cuando algo sale mal, que elabore escenarios donde algo no funciona como debería, y así pensar en cómo se podrían solucionar. Para muchos autores, esta es una gran diferencia entre la administración del riesgo, algo que piensas que puede ocurrir, y la ciberresiliencia, cómo adaptarse cuando algo que ni pensabas que podría ocurrir, sucede.

Recuperando las ideas del doctor Cano, debemos pensar en qué es lo que pasa después de un ciberincidente a más largo plazo, no inmediatamente, reflexionar sobre lo que ocurrió y cómo debes transformarte. Se debe tomar el tiempo necesario para meditar sobre las lecciones aprendidas, puede haber mucho conocimiento, mucha experiencia, mucha sabiduría, saber qué es lo que pudiste haber hecho diferente o que es lo que hay que transformar, conjugar el punto de vista académico y la experiencia práctica.

Actualmente no alcanzo a identificar con claridad qué es lo que cambiaron las organizaciones después de ser víctimas de un incidente de alto impacto, qué proceso cambió, qué personas o figuras se cambiaron para atender un nuevo escenario, qué fue lo nuevo que hicieron. Hoy en día, esto no se expresa y sería un excelente punto para mejorar.

Héctor Calderazzi

Pensar hoy en prevención es ser más resilientes. Esto significa contar con más información para poder actuar lo antes posible ni bien se detecta el incidente, toda vez que en varios escenarios no podemos prevenir su ocurrencia (generalmente porque no disponemos de las capacidades para hacerlo). Ser más resilientes es ajustar o tener la puntería de la detección lo más temprana posible, los pasos que hay que hacer para salir adelante y la recuperación si tuviera que recuperar la información en caso de un desastre. Ser resiliente es hacer una gestión del incidente de la forma más temprana posible y es parte de un análisis de riesgos preventivo, en donde ante la incapacidad de prevenir el incidente, se analiza qué se ejecutará o cómo se trabajará cuando el incidente ocurra. En otras palabras, es como ser lo más ágil para recuperarse lo más rápido posible, limpiar los falsos positivos, ajustar todas las situaciones y a su vez, definir que más se va a hacer ante el incierto o la ocurrencia de un incidente sobre el cual no tenemos experiencia, ni información de referencia.

En resiliencia podemos hacer un paralelismo con la prevención sobre lavado de activos, en donde se establece la política "conozca a su cliente". Aquí, se debe conocer cuál es la operatoria normal del cliente, pero este un día hace un depósito muy grande, entre otros controles, debemos averiguar sobre el origen genuino de esos fondos. Este análisis de comportamiento es trasladable al ambiente de Seguridad de la Información. Conocer si un usuario ingresa todos los días a nuestro sitio, en qué horarios y que acciones realiza. Este concepto que también se incluye dentro de la metodología "confianza cero". Asignar los mínimos privilegios necesarios, aplicar trazabilidad por todas las transacciones críticas que se realizan y análisis de comportamiento. A su vez, los análisis de comportamiento van a ligar a lo mejor con situaciones de "lecciones aprendidas" que ya conocemos, pero otras situaciones pueden ser nuevas, y algunas pueden ser operativas. En este sentido puedo agregar otro caso experimentado, relacionado con el sistema de información de prevención de lavado de activos (PLD). Cuando un cliente tomaba un préstamo por encima de los $50.000 se generaba un registro automático para PLD, pero el sistema fallaba y no controlaba el acumulado de varias operaciones que sumaban los $50.000 en su conjunto. Entonces el funcionario que conocía esa vulnerabilidad, y con mala intención confeccionó varios movimientos de cuyos valores individuales eran inferiores a $50.000, pero en su conjunto superaban ese parámetro. Esto determinó el análisis de la vulnerabilidad, el comportamiento de la persona, de las transacciones realizadas y permitió utilizar esa información para comprobar el adecuado funcionamiento de otras personas, procesos y tecnología, cruzando dicha información por vectores según diferentes criterios de análisis de comportamiento y proyección.

Jeimy J. Cano M.

Basados en sus respuestas se destacan algunas reflexiones. Prevención, no detección temprana; respuesta rápida y especializar personas. Así mismo, movilizar esfuerzos hacia los pronósticos basados en datos y en registros.

Hamilton Moya

Muchos de los CISO´S y de los encargados de la seguridad confundimos cumplimiento con aplicación de controles de seguridad, entonces asumimos que si cumplimos las normas, como la 27.001, cumplimos una lista de controles, ya estamos seguros, pero, esa implementación de controles solo la cumplimos para presentar una auditoría, mostramos en papel, si no tenemos algo implementado le damos manejo para poder responder lo que quiere oír el auditor, solo para pasar la auditoria, y al final, pasamos una auditoria, logramos la certificación, eso es lo importante, y ese tipo de cosas nos da una falsa sensación de seguridad.

Considero que todos debemos estar preparados para las fallas inevitables y para enfrentarlas, debemos ser proactivos, cambiar el esquema, pasar de un feedback a un feedforward, no llegar a mirar solo lo malo que sucedió, sino, mirar también que debo corregir para mejorar eso que hizo que se presentara una falla.

Resumiendo, aunque es importante contar con esas herramientas que nos dan confianza y nos dan tranquilidad, nos hace falta ir un poco más allá, ser proactivos, mejorar la cultura de ciberseguridad, nos falta mejorar muchos aspectos a nivel organizacional.

Jeimy J. Cano M.

¿Las buenas prácticas de seguridad y control vigentes en las organizaciones son suficientes para lograr concretar la confianza y tranquilidad que requieren las organizaciones en un escenario como el actual? Explique su respuesta.

Arturo García

Esta pregunta me fascinó pues la regulación es un problema complejo con soluciones inexactas y de difícil comprobación objetiva. Por ejemplo, ¿qué tanto es tantito?, ¿estás sobre regulando o subregulando? Existe literatura que indica que la sobrerregulación puede ocasionar exactamente el efecto contrario de querer fomentar la protección de la organización. Muchos CISOs están preocupados por el cumplimiento porque va a llegar una autoridad y los sancionará, o porque va a llegar una auditoria y les asignará observaciones, o porque no cumplieron un compromiso contractual que podría causar sanciones. Entonces tratan de cumplir lo mejor posible para obtener una palomita.

Lamentablemente, el fenómeno de "cansancio por cumplimiento" puede dejar sin atender algunos otros elementos básicos, muy necesarios para la protección informática. Coincido con lo que dice de la Ley de ciber-Pareto: el 80% de los ataques son generados por el 20% de las cosas que no hicieron bien, esto es, no se actualizó una aplicación o no se bloqueó un puerto de acceso.

A lo mejor esto sucede por causa de una sobre regulación y de la preocupación o estrés extremo que causa el cumplimiento. Por otro lado, también es un riesgo la subregulación; esto es, dejar de regular algún aspecto por el que podría generarse una brecha de seguridad. Eso también es observable. La sana medianía es muy complicada y es uno de los grandes retos a la hora de hacer políticas correctas, eficientes y efectivas. Ese punto aún no tiene una respuesta concreta y eso sería tal vez tema para otro panel.

Wilson Prieto

Es fundamental tener en cuenta que las buenas prácticas de seguridad y los marcos de referencia constituyen una base sólida en el

ámbito de la seguridad cibernética. Las organizaciones tienen a su disposición estándares y una abundante información que resulta valiosa. No obstante, es importante reconocer que los actores de amenaza actuales se encuentran en constante evolución y sofisticación, lo cual implica que estas prácticas pueden resultar insuficientes para responder de manera adecuada ante una amenaza o ciberataque.

En este sentido, es importante que las organizaciones adopten un enfoque proactivo y no reactivo en cuanto a la seguridad para que puedan responder rápidamente ante un incidente cibernético. Esto significa que deben implementar medidas de seguridad y control no solo para prevenir las amenazas conocidas, sino también para detectar y responder a las amenazas desconocidas y emergentes. Un plan de respuesta a incidentes robusto es de suma importancia y como mencionó Andrés, llevar a cabo simulacros o ejercicios de equipo rojo de forma regular resulta crucial para evaluar la capacidad de resiliencia de una organización frente a un posible ataque cibernético.

Es necesario que las organizaciones adopten un enfoque más proactivo y holístico de la seguridad, abordando todos los aspectos del ciclo de vida de la seguridad, que incluye la detección, respuesta y recuperación. Es fundamental identificar y evaluar tanto los riesgos actuales como los que puedan surgir a corto y largo plazo. Esto implica implementar sistemas de monitoreo continuo, adoptar tecnologías avanzadas de seguridad como la inteligencia artificial y el aprendizaje automático, y establecer planes de respuesta y recuperación en caso de emergencias. Además, el monitoreo continuo y la gestión de identidad son aspectos de vital importancia para prevenir accesos no autorizados en la empresa.

La realización de pruebas de penetración y simulaciones de amenazas, junto con la colaboración y comunicación con otras organizaciones, son medidas altamente efectivas para fortalecer las mejores prácticas de seguridad cibernética. Estas acciones contribuyen significativamente a mejorar las defensas y garantizar la protección de los sistemas y datos frente a posibles ataques.

Héctor Calderazzi

En este punto, lo primero que me pregunto es ¿qué requieren las organizaciones? Porqué lo tienen que bajar desde el directorio, involucrar al directorio. El dueño de la seguridad de la información de la empresa no es el CISO. De vuelta digamos que es un tema primario, el directorio es el que determina los lineamientos y aprueba las pérdidas anuales esperadas (ALE) que está dispuesto asumir por incidentes de Seguridad de la Información. Hay organizaciones que son más riesgosas, de por sí, que están acostumbradas a que juegan con

inversiones que son más volátiles y hay otras que son más conservadoras. Tienen distintas culturas de riesgos y eso mismo se baja hacia toda la organización. Existen directores que no quieren escuchar sobre temas de seguridad, cuando en realidad para darle más confianza y tranquilidad a las empresas, ellos primero tendrían que bajar como lineamiento y decir, por ejemplo, nosotros queremos en tema de seguridad compararnos con tal nivel del mercado, entonces el profesional vuelve con una propuesta, para que después no se generen falsas expectativas. Es fundamental determinar esos valores que tienen que venir desde la dirección, que justamente están relacionados con temas de la cultura de las organizaciones y que se necesitan para darle todo el apoyo a las estructuras, porque siempre se necesitarán inversiones en personas, procesos y tecnología, y este apoyo es todo lo que el directorio podrá dar en materia de seguridad de la información para seguir adelante.

Por otra parte, me ha pasado en otra organización donde el responsable de seguridad me pidió ayuda para implementar la norma ISO 27001. Comencé a interactuar con su colaborador quién me dijo que le gustaba el modelo “Cis Controls”, seguí con otros colaboradores y se veían muy apegados al modelo Mitre. Llevó un tiempo lograr un acuerdo sobre la metodología a adoptar. Entonces para dar la tranquilidad ¿qué se debe hacer? Involucrar a la dirección en la aprobación de la metodología. El hecho de preparar la metodología y simplificar su explicación para su aprobación logrará el acuerdo en las definiciones básicas de las buenas prácticas de seguridad y desde allí en más se podrá crecer permanentemente en los nuevos escenarios, que se necesitan para ofrecer mayor confianza y tener tranquilidad.

Asimismo, siguiendo con la buena práctica, en el hipotético caso que se defina apetito cero de riesgo para seguridad, nuestra propuesta sería detallar todas las inversiones que tendrían que hacerse en capacidades para lograr ese objetivo, que de hecho serían onerosas. Aunque la decisión será facultad de la dirección.

En otras palabras, tendremos que presupuestar fondos para procesos, personas y tecnología, y la dirección posiblemente nos diga “Uds. están locos”. Esto nos hace menos perfectos, es una negociación permanente.

Entonces, ¿qué hace el responsable de seguridad de la información?, mira si el presupuesto preparado hace a la empresa estar más expuestos, si podremos tener una brecha de seguridad o no; es decir este es el trabajo del CISO, alertar a la dirección, pero ellos son los que fijan la estrategia general de la organización y deciden cuál modelo adoptar, según la relación costo/beneficio.

Jeimy J. Cano M.
Interesantes aportes, particularmente la palabra "cumplimiento", que cuando se pronuncia en dos tiempos a veces se vuelve real: cumplo y después miento, en particular, frente a los estándares. De otra parte, está el tema de las pérdidas esperadas, un concepto que en seguridad nosotros debemos tener en mente, pues en algún momento nos sorprenderá la inevitabilidad de la falla. Lo anterior nos remite al apetito de riesgo para concretar una nueva conversación entre el CISO (*Chief Information Security Officer*) y el equipo ejecutivo. Aquí le doy paso a Andrés con la frase que generalmente usa donde la ciberseguridad ocurre en la conversación.

Andrés Almanza.

Así es. La frase completa es "la ciberseguridad no sucede en la implementación, sucede en la conversación". Yo creo que la pregunta si es pregunta, es decir, están listas las prácticas de hoy para el momento y coyuntura actual, mi respuesta es no. Eso no quiere decir que estas prácticas no sean buenas y su aplicación no genere beneficios importantes. De otra parte, hay una palabra clave que es confianza y si vamos a hablar de confianza, esto es un ejercicio de conversaciones, no de implementaciones. Por esto insisto en que la conversación de un CISO resulta de una habilidad esencial, y más en esta pregunta, en donde yo necesito establecer un vínculo de confianza. El reto es prepararse y anticiparse, más que prevenir, y creería que otra práctica muy de la pregunta es desarrollar adaptabilidad en el momento. La adaptación como dice un libro que me gusta "*The handbook of Anticipation*"[1], se da en los momentos desconocidos, y la anticipación dice el autor, se da para los momentos conocidos; por tanto, tenemos que trabajar una nueva práctica mucho más desarrollada en conversar y una muy buena en adaptarnos.

Jeimy J. Cano M.
¿Qué deben hacer en forma diferente los ejecutivos de seguridad (en sus diferentes especialidades) para acompañar a las organizaciones en su creciente apetito de

[1] Poli, R. (Ed.) (2019). *Handbook of anticipation. Theoretical and Applied Aspects of the Use of Future in Decision Making*. Cham, Switzerland: Springer Nature Switzerland AG

riesgo cibernético, una mayor demanda de negocios y oportunidades digitales?

Wilson Prieto

Considero que los ejecutivos de seguridad deben adoptar un enfoque proactivo y estratégico en su gestión de seguridad. Es fundamental que posean un sólido conocimiento del negocio para poder identificar los riesgos reales asociados a la organización. Esto implica participar en la planificación estratégica, implementar un enfoque de gestión de riesgos, colaborar y comunicarse efectivamente con otros líderes, invertir en capital humano especializado y tecnología, priorizar las medidas de seguridad en función del impacto potencial de negocio y promover una cultura de seguridad en toda la organización.

Es de vital importancia adoptar una postura proactiva en cuanto a seguridad se refiere. Esto implica comprender y anticiparse a las tendencias y amenazas emergentes. Los altos ejecutivos deben estar plenamente preparados para responder de manera ágil ante cualquier incidente que se presente, colaborando estrechamente con sus equipos de seguridad y otros ejecutivos involucrados. Asimismo, es fundamental evaluar el impacto económico, profesional y tecnológico que podría tener un ataque en la organización.

Además, es crucial comunicar la importancia de la seguridad de manera efectiva. Los altos ejecutivos deben tener un profundo entendimiento de la seguridad y ser capaces de transmitir este conocimiento desde la alta gerencia. También deben respaldar a los líderes internos para que promuevan las mejores prácticas de seguridad a través de su comunicación. La presencia de ejecutivos comprometidos con la seguridad desde la alta gerencia desempeña un papel fundamental en la educación de las personas en este ámbito.

En resumen, los ejecutivos de seguridad deben ser aliados de las organizaciones, comprendiendo tanto el negocio como la estrategia, alineando la seguridad con los objetivos empresariales, adoptando un enfoque basado en el riesgo y mostrándose proactivos en materia de seguridad. Además, es fundamental que puedan comunicar de manera efectiva la importancia de la seguridad y brindar apoyo a los líderes internos para promover la educación en las mejores prácticas. En mi opinión, eso sería lo que consideraría como la respuesta adecuada a la pregunta planteada.

Arturo García

Las preguntas que nos hacen son muy buenas pues son cuestionamientos que te hacen reflexionar. Por ejemplo, no sé si hay que hacer algo totalmente diferente, sino tal vez se requiere que lo ya se conoce se ejecute mejor, de forma efectiva, medible, auditable, concreta y objetiva. Por ejemplo, pensemos en al-

go básico que se hace en todo el mundo: la labor de concientización. Esas campañas y esfuerzos habría que fortalecerlas y mejorarlas. Me explico ¿qué tal si incorporamos profesionales de mercadología? Sí, de esos profesionales que saben vender productos comerciales; tal vez requerimos psicólogos que conocen la mente humana y cómo reaccionan ante elementos nuevos, sorpresivos o incluso del día a día. Hace poco estuve en unas sesiones de neurociencias aplicadas a la ciberseguridad, en donde revisaban por qué las personas hacen lo que hacen, ¿por qué caen en ligas de ransomware o de phishing? O en momentos de crisis ¿cómo reaccionan? Es muy probable que la solución es ver las situaciones con un enfoque más amplio que solo centrarse en el enfoque tecnológico. Desconozco el número de empresas que estén haciendo esto, pero definitivamente me parece la manera correcta de hacer algo que ya conocemos, pero de manera más efectiva.

Héctor Calderazzi
El tema de la comunicación, el involucramiento de toda la organización es fundamental y es necesario profundizar en este aspecto. Siempre digo que el profesional de seguridad en la información tiene que ser más estratega que un técnico. Ahora fíjense justamente cuando observamos y analizamos desde un lado, el ranking de riesgo de la organización, “no pega ni con cola” con un plan estratégico de seguridad. Y esto me paso más de una vez, yo espero que un plan estratégico en seguridad de la información esté relacionado de alguna forma con un orden de un ranking de riesgo de seguridad en información de la organización.

Y cómo son dos estamentos diferentes, por ejemplo, si a su vez cada uno trabaja con su criterio y falta la integración conceptual, los resultados no serán estratégicos o no conducirán a mitigar los principales riesgos de seguridad.

El tiempo del ejecutivo de trabajo de un ejecutivo de seguridad tiene que ser 50% con su gente, liderando el equipo, viendo que pasa, en lo que temas están procesos internos (personas, procesos y tecnologías afectadas) y el otro 50% haciendo “lobby sano” con toda la organización, trabajando con sus pares, con los gerentes de mandos medios y la comunicación con la dirección, además de tener en cuenta que cuando tiene reuniones con el comité directivo, tiene entre uno y cinco minutos para explicar la situación, y que después perderá la atención.

Jeimy J. Cano M.
Es decir Héctor, como dicen ustedes “nos dan pelota” solo cuando algo pasa.

Héctor Calderazzi
Desde la definición temprana de los riesgos de seguridad de la información, me surge la siguiente expe-

riencia para compartir. El gerente de seguridad en información de una empresa estaba molesto con el área de desarrollo. Decía que no le hacían caso en el desarrollo de los controles de seguridad en la información. Entonces mi pregunta fue ¿qué les pediste? Y decía simplemente que desarrollen controles. Y mi pregunta siguiente fue: ¿qué controles le pediste? Y la charla quedó allí, sin una respuesta concreta. Mi sugerencia fue, debería comenzar pidiendo tres controles y después su medición. Por ejemplo, controles básicos de restricción de acceso, control de cambios y limitaciones para la alteración de datos. Luego se ponen de acuerdo en desarrollar esos controles, en evaluar posibles dificultades, en consensuar su implementación y comienzan a hablar todo el mismo idioma.

Esta comunicación fundamental a veces no es bien manejada por personal de seguridad, que generalmente son muy fuertes en formación técnica, pero tienen más dificultades de manejo de relaciones humanas.

Creo que la persuasión sobre la necesidad de los controles es fundamental. Nosotros teníamos un gobernante, en los años ochenta, que decía “con la democracia se come, se vive, se respira…” y esta persona iba a todos lados con el mismo discurso. En este sentido podríamos decir, por ejemplo, que con la seguridad se come, se vive, se respira y a todos los lugares vamos con este léxico, y por supuesto obramos en consecuencia.

Hamilton Moya

Primero, más que cambiar considero que debe ser reforzar. Por ejemplo, dijimos dejar de ser tan reactivos y volvernos más proactivos, no es volvernos, porque ya somos proactivos, solo que nos falta un poco más, debemos reforzar y mejorar esta proactividad en todos los que tenemos un rol de seguridad y todas las partes interesadas de la organización.

Segundo, mejorar la comunicación entre las diferentes áreas de la organización, quienes cumplimos un rol de seguridad en la organización no somos un mundito aparte. Hablamos de que la seguridad es logística, pero casi siempre trabajamos solos, en ese orden de ideas, considero que debemos involucrar a todas las partes de la organización, a todos los directivos e incorporarlos en un plan de trabajo conjunto.

Tercero, tenemos que volvernos vendedores de la seguridad al interior de nuestras organizaciones, vender correctamente la seguridad, lograr ese patrocinio de los directivos o de la alta gerencia. Considero que debemos mejorar esta parte, mostrando como la seguridad se alinea con las estrategias y los objetivos de la organización, porque si no lo hacemos, sencillamente no nos ven, nos prestan atención únicamente cuando pasa

algo, y esto, porque no vendemos correctamente, porque nos falta ese marketing.

Jeimy J. Cano M.
Al revisar todas las intervenciones encuentro un hilo conductor que es el tema del lenguaje, construir un lenguaje común. Una manera distinta de comunicar, que nos lean. Connotaciones que hablan de un nuevo lenguaje que conecte y movilice la distinción de seguridad, lo que implica salir de esa zona cómoda de los estándares y de la estrategia del miedo, la incertidumbre y las dudas para encontrarnos con el negocio, y terminar (o minimizar) los desencuentros permanentes de la seguridad y el modelo de generación de valor de la empresa. Por tanto, el CISO tiene que ser un estratega, esto es, alguien con una agenda que mueve, conecta y moviliza, desde un discurso concreto y seductor, para ubicar una distinción en el imaginario de las personas.

Jeimy J. Cano M.
Surtidas todas las preguntas lo que quisiera ahora para ir cerrando nuestro panel es que cada uno de ustedes haga una reflexión final a la luz de lo que hemos conversado.

Arturo García
Como cierre me parece que el escenario que estamos viviendo requiere de una visión interdisciplinaria, en donde tenemos efectos claramente ciber físicos, por lo que así hay que prepararnos y responder ante lo inevitable. Hay que pensar fuera de la caja, pensar las cosas que no nos han pasado, pero que nos pueden pasar. Reflexionar qué más se necesita, qué recursos nos hacen falta. Atender el binomio de escasez e inevitabilidad: escasez de recursos, tiempo, dinero, esfuerzo. Le pueden preguntar a cualquier profesional en cualquier parte del mundo sobre los recursos y siempre le va a faltar gente, dinero y tiempo. Estamos a tiempo de reflexionar e instrumentar acciones fuera de la caja.

Hamilton Moya
Mi reflexión es que debemos crecer como proceso a la par que va creciendo la tecnología, también debemos crecer a nivel profesional y tratar de entender todos esos nuevos conceptos, como lo planteaban hace un rato, no solamente es la parte técnica, no solamente es la parte tecnológica, sino la parte humana, la parte de liderazgo la que nos puede hacer mejorar las situaciones o las circunstancias de seguridad a las que nos enfrentamos dentro de una organización, en resumidas cuentas, el crecimiento continuo, la visión constante de los diferentes cambios y la adaptación a esos cambios que vienen surgiendo.

Héctor Calderazzi
Mejorar el sentido de la comunicación con todas las líneas, con la dirección, con los mandos medios y con las líneas inferiores, con los procedimientos que ya se conocen, que se trabajan.

Wilson Prieto
En resumen, la alta gerencia tiene la responsabilidad de liderar el negocio y debe adoptar un enfoque proactivo y estratégico para respaldar a la organización en cuanto a riesgo cibernético, así como aprovechar las oportunidades digitales mediante la implementación de tecnología emergente para mitigar el riesgo cibernético. Esto implica la contratación de personal especializado, promover una cultura de seguridad, diseñar nuevos procesos y procedimientos que sean ágiles y adaptables. Un aspecto destacado, mencionado por algunos colegas, es la formación de un equipo interdisciplinario con el fin de identificar posibles amenazas desconocidas para la organización. El compromiso tanto de la alta gerencia como de todos los líderes y miembros de la organización contribuye significativamente a la ciberseguridad de la entidad.