Patricia Prandini

Es argentina y su tarjeta de presentación una valiosa hoja de vida, evidente durante su amplio recorrido profesional.

DOI: 10.29236/sistemas.n175a3

Sara Gallardo M.

Magister en Seguridad Informática de la Universidad de Buenos Aires (UBA), Máster in Accounting Sciences de Universidad de Illinois, EE-UU y Contadora Pública de la UBA. “Poseo certificaciones en auditoría de sistemas, riesgo y COBIT 2019, todas de ISACA y soy auditora Líder ISO 27001. Trabajo actualmente como asesora en la Dirección Nacional de Ciberseguridad de la Subsecretaría de Tecnologías de Información de la Secretaría de Innovación, Ciencia y Tecnología y soy docente en posgrados en seguridad y auditoría informática de la UBA y la Universidad Nacional de San Martín. Soy actualmente Presidenta de la Red de Universidades Latinoamericanas 'Ciberlac', creada con el objetivo de incrementar las capacidades académicas en materia de Ciberseguridad en las Instituciones de Enseñanza Superior de la Región e impulsada por el Banco Interamericano de Desarrollo (BID)”, así se define.

Así mismo ha sido presidente del Capítulo Buenos Aires de ISACA entre 2010 y 2012 y ha participado en eventos nacionales e internacionales vinculados a ciberseguridad y firma digital. Lleva más de 25 años trabajando en el Estado Nacional de Argentina, durante los cuales ha participado en la creación del primer Grupo de Respuesta a Incidentes de Ciberseguridad (ARCERT) de su país, en el desarrollo e implementación de la infraestructura de Firma Digital nacional y en la creación del primer portal del Estado argentino.

"Mi hobby es viajar, visitar lugares exóticos, conocer la cultura de cada lugar. Esa misma lógica la aplico a la hora de elegir un sitio para disfrutar de un buen plato; soy una fanática tomadora de café –aseguró, declarándose optimista frente al futuro a pesar de los momentos oscuros. Creo en la tecnología, sin desconocer que puede haber un uso malicioso. Y, sobre todo, creo en el ser humano". Después de esta definición personal, entramos de lleno a la entrevista.

Sara Gallardo: *¿Cómo ve la evolución de la seguridad de la información a la ciberseguridad empresarial?*

Patricia Prandini: Creo que refleja un cambio notorio en la forma en que las organizaciones protegen sus activos digitales y colaboran entre ellas. Quiero destacar aquí tres aspectos que me parecen relevantes. Mientras que en seguridad de la información el objetivo es proteger la confidencialidad, integridad y disponibilidad de la información de la entidad, con independencia de formato o soporte utilizado, la ciberseguridad empresarial busca alcanzar la resiliencia operativa. En otras palabras, ante la inevitabilidad del incidente, sea que se trate de una falla en la plataforma o en los servicios tecnológicos o de un ciberataque, la ciberseguridad empresarial se concentra en la capacidad de responder buscando contener el impacto negativo y restablecer el servicio lo antes posible.

Un segundo aspecto que me parece relevante es la atención de los activos críticos. La ciberseguridad se concentra fundamentalmente en los activos de información críticos, es decir, aquellos que conteniendo información o interviniendo en su gestión, tienen más valor para la organización. La seguridad de la información, en cambio, debe preservar la confidencialidad, integridad y disponibilidad de los recursos utilizados, con independencia del formato y soporte en el que se encuentren. Efectivamente, las complejidades de las plataformas actuales, la disrupción que acompaña la aparición de nuevas tecnologías y la notable transformación digital que han experimentado las entidades en estos últimos años, llevan a asegurar la visibilidad y la protección de los activos de información que son considerados esenciales

para la supervivencia y el buen funcionamiento de la entidad.

Finalmente, si bien siguen siendo relevantes el tipo de medida de seguridad a adoptar y la vulnerabilidad que debe ser enfrentada, hoy damos un paso más atrás y el foco está en la predicción del tipo de situación o afectación que podría producirse. Así cobra cada vez más relevancia el campo de la inteligencia de amenazas cibernética; es decir, tratar de visibilizar las situaciones anómalas que pueden producirse antes de que ocurran. Esta visión de nuestra disciplina ha llevado al surgimiento de nuevos marcos, estándares y normas internacionales de gobierno y de gestión, así como técnicos, que muestran que las empresas deben considerar a la ciberseguridad como un tema estratégico y no solo como un "problema técnico". Solo así podrán contribuir a asegurar la continuidad del negocio, la transparencia y la confianza del usuario.

SG: *¿Cuáles elementos de la ciberseguridad hoy son completamente diferentes de lo que se conocía previamente en seguridad de la información?*

PP: Nos encontramos frente a un panorama cambiante y creciente de amenazas. Cambiante porque se recrean riesgos que persisten en cuanto a sus objetivos, pero adquieren nuevas modalidades. Creciente, porque la aparición de nuevas tecnologías y la mayor dependencia que tienen las organizaciones de los datos y de sus plataformas tecnológicas, genera una mayor exposición para la organización. Además, la seguridad de la información buscó siempre proteger el perímetro y su énfasis estaba puesto en el uso de redes internas protegidas. No es que hoy estas problemáticas no existan, pero el panorama es diferente. Hoy las fronteras de la organización se han extendido y ya no es posible limitar las medidas de seguridad a la protección de un lugar físico ni durante un "marco horario" determinado. Se requiere en cambio, una verificación permanente, evitando confiar en los controles existentes. A manera de ejemplo, cada entidad debe autenticarse y autorizarse constantemente, sin importar si está dentro o fuera de la red corporativa.

En cuanto a las infraestructuras tecnológicas, antes eran únicamente "on-premise," con límites y controles físicos y lógicos integrales. Hoy la tecnología de nube, en todas sus modalidades, llegó para quedarse, lo que obliga a extremar el uso del cifrado, de la autenticación federada, etc. Por otra parte, los ciberataques mostraban anteriormente un nivel bajo de sofisticación y la actividad maliciosa estaba en manos de delincuentes aislados. Hoy existe un verdadero mercado de la actividad maliciosa en el que reina el ransomware como servicio, el uso de herramientas de inteligencia artificial para reali-

zar ciberataques, amenazas persistentes avanzadas (APT), bots automatizados o el uso de información falsa para la ingeniería social. También la cantidad de dispositivos se ha diversificado. Mientras antes la seguridad estaba centrada en las computadoras de escritorio y los servidores, hoy deben protegerse miles de dispositivos móviles, sensores de Internet de las cosas y los llamados “endpoints”, lo que trae aparejado nuevos desafíos de visibilidad, autenticación y control.

Para ir cerrando, ha aumentado considerablemente la normativa vinculada a esta temática, generando mayor presión sobre las organizaciones. Hoy existe un verdadero enjambre de regulaciones locales e internacionales que deben ser cumplidas y que las exponen a sanciones de todo tipo y que requieren atención. Las empresas deben pensar la ciberseguridad de manera integral, es decir, considerando no solo la tecnología sino también los procesos y las personas. Son estas últimas quienes configuran, utilizan, desarrollan, implementan y monitorean la información. Efectivamente, son el primer escudo. Por lo tanto, resulta fundamental la generación de una cultura organizacional en torno al riesgo cibernético, centrada en una responsabilidad compartida.

SG: *¿Habría que actualizar las prácticas de seguridad de la información frente a los retos que tienen la empresa en el contexto digital? ¿Cómo se debería hacer ese cambio?*

PP: Sí, es fundamental actualizar las prácticas en torno a la protección de los activos de información frente a los retos del contexto digital actual. Como ya se dijo, las ciberamenazas han cambiado, los entornos tecnológicos también, y los modelos de negocio se han digitalizado. Continuar con prácticas tradicionales deja a las empresas expuestas a riesgos significativos. La transformación digital acelerada de las organizaciones, la disrupción de las nuevas tecnologías, la aparición de ciber amenazas más sofisticadas, el surgimiento de regulaciones más estrictas y mayores expectativas de usuarios y clientes en cuanto a su privacidad, seguridad y transparencia, requiere de nuevas maneras de hacer las cosas. Como todo cambio, debe empezar por un buen diagnóstico y una evaluación del estado actual. En ese proceso, se reconocerán

los riesgos actuales y el nivel de madurez en ciberseguridad de la organización.

Para avanzar, las prácticas deberán tener un enfoque basado en los riesgos a los que se expone la organización y priorizar aquellos que pueden afectar activos críticos. La protección debe centrarse en aquello que más afecta al negocio. En ese camino, será necesario revisar y actualizar periódicamente las políticas de seguridad digital y de uso responsable de la información y de las herramientas tecnológicas, de gestión de contraseñas, de cifrado, de acceso remoto, etc. Como todo proceso de transformación deberá estar acompañado de un cambio cultural que incluya programas de concientización, simulacros de ciber incidentes, talleres de ciberejercicios y la generación de una cultura de ciberseguridad adaptada al negocio. En suma, las prácticas deberán facilitar el establecimiento de un plan de respuesta y resiliencia ante incidentes, que refleje el estado actual del proceso de adopción tecnológica de la organización y proteja en forma efectiva su plataforma tecnológica.

SG: *¿Cómo debería variar la formación de los profesionales de seguridad/ciberseguridad frente a los escenarios que tenemos hoy?*

PP: La formación de los profesionales de seguridad/ciberseguridad debe adaptarse a la realidad y estar a la altura de los desafíos actuales. Ya no basta con saber configurar firewalls o conocer normas nacionales. Hoy se necesita una combinación de habilidades técnicas, estratégicas, legales y personales.

El entorno cambia constantemente. Por lo tanto, se requiere que los programas de estudio reflejen esta gimnasia de adaptación continua y de permanente actitud de alerta y desconfianza. Además, las organizaciones deben comprender que es necesario generar programas formación continua que incluyan laboratorios prácticos, nuevas regulaciones y estándares y un entrenamiento en amenazas emergentes (usos maliciosos de la inteligencia artificial, ransomware como servicio, etc.). El enfoque ha dejado de ser exclusivamente técnico y hoy es multidisciplinario. Como consecuencia, los profesionales deberán formarse en tecnología, administración del negocio, regulación y psicología, entre otras áreas.

Además, ya no existe un único perfil. Se requiere formar especialistas en inteligencia de amenazas, gestión de riesgos cibernéticos, técnicas de ciberataque y defensa, forensia digital, ciberseguridad en la nube, desarrollo seguro, usos ofensivos y defensivos de la inteligencia artificial, ciberseguridad industrial, cumplimiento, auditoría técnica, comunicación efectiva con dirección y con áreas no técnicas, toma de decisiones bajo presión, gestión de crisis y liderazgo en incidentes, por nombrar algunas.

Resumiendo, la formación debe ser ágil, práctica, multidisciplinaria y con una actualización constante. Hoy más que nunca, la ciberseguridad es un campo en donde quien no se actualiza, corre el riesgo de quedar obsoleto rápidamente.

SG: *¿Qué competencias deben cambiar o actualizarse frente al reto de la ciberseguridad empresarial en la actualidad?*

PP: Frente a los retos actuales de la ciberseguridad empresarial, las competencias que se exigen a los profesionales del área deben actualizarse significativamente. Como ya se dijo, no basta con tener habilidades técnicas básicas. Se necesita un perfil integral, adaptable y orientado al negocio. Sea cual fuere el rol que le toque cumplir, debe comprender el negocio, es decir qué hace la organización. Las decisiones que se tomen repercutirán tarde o temprano en la función que debe desempeñar. Y a su vez, el resultado de su trabajo tendrá un efecto sobre el negocio. Además, estará en condiciones de evaluar las posibles repercusiones que un ciberincidente pueden tener a nivel operativo, financiero, reputacional y de toda otra índole. Hecho esto, podrá delinear en forma precisa las acciones que deben ejecutarse para cumplir con los objetivos estratégicos de la empresa.

Asimismo, el profesional debe pasar de un enfoque meramente normativo ("hay que cumplir") a una gestión continua del riesgo de ciberseguridad, en el que la seguridad sea proactiva y no solo reactiva. Debe contar con la capacidad para evaluar y priorizar amenazas, establecer cómo proteger los activos críticos a través de controles eficaces y sostenibles. Además de conocer los riesgos que acompañan toda nueva tecnología, deberá desarrollar también las llamadas "habilidades blandas", vinculadas a la comunicación a no especialistas sobre los riesgos, la redacción de informes y los procesos de toma de decisiones del negocio. Todo esto devendrá en una labor alineada con los objetivos de la organización, que además sea colaborativa, transversal y que favorezca la creación de una cultura de ciber seguridad.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A. En la actualidad es asesora en escritura y producción de libros y editora de esta revista.*