Año 1. Número 1.

Bridge

The bridge to possible

Ciberseguridad

Orquestación

Contrapunto entre el maestro Carlos Vieu y Juan Marino

Observatorio ALMA

FakeNews

Contenido audiovisual

Argentina
Av. Independencia 1330 – Piso 14 - Of. B – CABA
Teléfono: +54.11.5273.4470

Colombia: +57.1.580.1333
Chile: +56.2.2938.1332 - **USA:** +1.786.358.6100

Editorial

Si a la adversidad que nos trae el crecimiento despiadado de la industria del cibercrimen, le sumamos el desafío de la digitalización del negocio y la complejidad de seguir acumulando tecnologías para protegerlo en un mercado de ciberseguridad tan fragmentado, imagino que en los lectores tal vez resuene la letra de la canción popular que dice “que difícil se me hace” y que al final es “todo a pulmón”.

Cuando se trata de construir las capacidades de ciberseguridad que necesita una organización o negocio, optando entre un sin fin de alternativas tecnológicas, la toma de decisiones acertadas se vuelve fundamental. Estar cerca de los profesionales de la industria puede ayudar. Estos equipos colaboran desde un abordaje consultivo y con una mirada amplia, saben escuchar, comprender y luego proponer caminos a seguir de acuerdo a la estrategia de cada organización.

Está claro que la ciberseguridad no es un asunto meramente tecnológico. El elemento humano, tanto como eslabón (generalmente débil) de la seguridad como en la definición de la estrategia, las políticas, la gobernanza, la gestión, ocupa un lugar central de la mano de las tecnologías que ayudan a prevenir, detectar y responder ante amenazas. Los hombres y mujeres que ocupan los zapatos de CISO, especialmente quienes tienen un ADN técnico, están atravesando un proceso de metamorfosis que los transforma de guardianes y tecnólogos a estrategas y consultores del negocio (tal como lo señalara Delloite en sus estudios sobre el rol del CISO).

Para colaborar con los profesionales C-Level a poner en perspectiva los desafíos, estrategias y tecnologías de ciberseguridad con un nivel de abstracción que aporte claridad y simplicidad creamos BRIDGE, una plataforma de comunicación que reúne múltiples miradas en distintos soportes tecnológicos. En BRIDGE confluyen los puntos de vista de clientes, integradores, vendors, especialistas, funcionarios públicos y usuarios que aportan, conjuntamente, una visión integral sobre la seguridad informática.

Existen el cibercrimen y la ciberguerra porque hay ventaja ofensiva, de lo contrario sería inverosímil. Sin embargo, esta ventaja no es absoluta. La ventaja defensiva es posible a nivel de cada organización articulando de forma adecuada estrategia y gestión de control del riesgo cibernético. A nivel general de industria, de la protección de infraestructuras críticas, de los estados mismos, la ventaja defensiva solo va a ser posible construyendo un sentido de corresponsabilidad que habilite una verdadera cooperación entre sectores. Vemos con optimismo que los actores del sector público y privado están tomando conciencia de esta realidad y comenzando a organizarse para actuar en consecuencia.

Cada uno de los que hacemos parte de esta industria así como cada persona que lea este editorial podrá inclinar la balanza en favor de un futuro que nos encuentre más conectados pero no más expuestos.

BRIDGE es una ocasión de encuentro entre personas, con el saber, con la información y con nuevas opciones. Ser puente es la elección y la misión de Cisco y sus socios de negocio, gracias a quienes este proyecto de comunicación es posible.

Juan Marino

Staff

Producción Integral
Basanta Contenidos

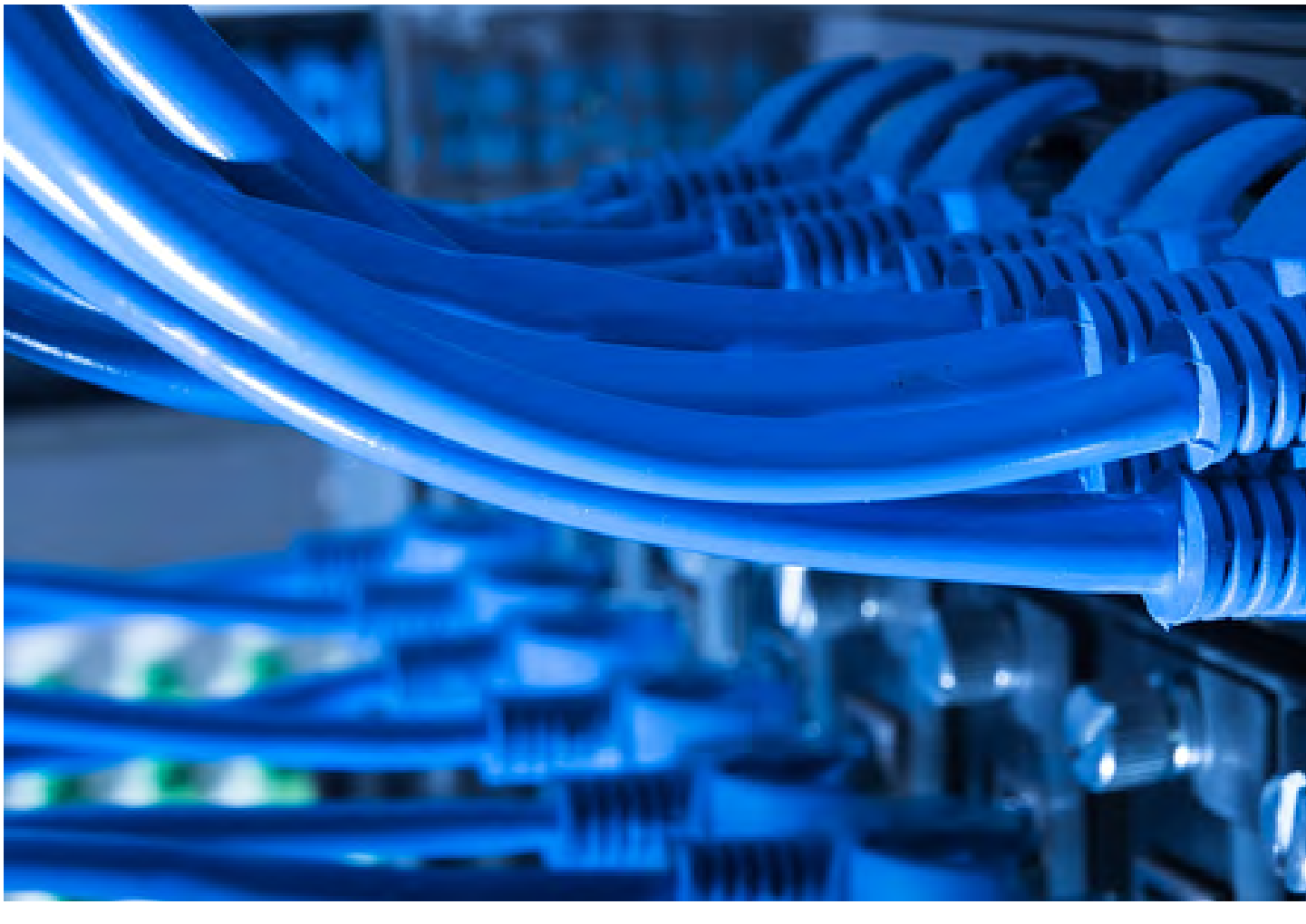
Directora Editorial
Karina Basanta
Director de Arte
Nicolás Cuadros
Coordinadora
Andrea Lecler
Colaboran en este número
Alicia Giorgetti, Irina Sternik,
Nano Pereyra, Jorge Prinzo
Producción audiovisual
Salpufilms

Directora Editorial
Karina Basanta

Director de Arte
Nicolás Cuadros

Agradecimientos:
Orquesta Sinfónica Nacional.
CCK (Centro Cultural Kirchner)
Nota y contenido audiovisual
Observatorio ALMA, gentileza Cisco.
Foto de Tapa:
Orquesta Sinfónica Nacional
durante un concierto en el CCK,
por Karina Basanta.

basantacontenidos.com
@basantacontenidos
+54 911 5014-4510 / 5260-8723



Cisco

Juan Marino
Gerente Regional de Ciberseguridad

Juan Ruiz
Especialista en Ciberseguridad

Antonio Hurtado
Arquitecto de Ciberseguridad

Marcelo Bezerra
Gerente de Ingeniería en Ciberseguridad

Arquitectos en Ciberseguridad
Cristian Venegas
Bruno Canales
Olga Cárdenas

Especialistas en Ciberseguridad
Walter Montenegro
John Ricardo León
Martín Vides
Patricio Esquivel

Editor General
Juan Marino

Marketing

Taiane Belotti
Gerente de Marketing para Seguridad Latin America
Renata Marcicano
Security Marketing Content Latin America

Bridge Nº 1

Sumario

Lo nuevo

Lanzamiento

SecureX, la plataforma más amplia e integrada para una experiencia simplificada

En el contexto del evento RSA Conference 2020, Cisco lanzó SecureX, la plataforma más amplia e integrada de seguridad que promete una experiencia de plataforma simplificada.
Conectada a la cartera de seguridad integrada de Cisco, la infraestructura existente de cualquier organización logrará ejecutar una experiencia consistente que unifique la visibilidad, permita la automatización y fortalezca la seguridad de la red, los endpoints, cloud y las aplicaciones.

Video
SecureX

Manual de Riesgos Cibernéticos para juntas corporativas

OEA (Organización de los Estados Americanos) e ISA (Internet Security Alliance) redactaron conjuntamente el manual de supervisión de riesgos cibernéticos para juntas corporativas. En él invitan a las juntas corporativas a asumir un papel de liderazgo en la supervisión de la seguridad de los sistemas cibernéticos de sus empresas. A través de la pauta de cinco Principios y diez Apéndices, las recomendaciones elaboradas buscan alentar la discusión y reflexión de las juntas directivas a fin de que cada una las aplique o adapte según sus características propias y únicas.
Texto completo del manual

Plan federal de prevención contra delitos tecnológicos y ciberdelitos 2019-2023

El Gobierno aprobó un Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos, que prevé la formulación de leyes específicas para la materia, además de acciones de formación y cooperación internacional. La resolución 977/2019, publicada en el Boletín Oficial, lleva la firma de Patricia Bullrich.

El plan, que queda bajo la órbita del Ministerio de Seguridad de la Nación, contempla un plazo de cuatro años y viene a complementar la creación del Comité de Ciberseguridad (2017) así como la Estrategia Nacional de Ciberseguridad (2019).
Texto completo publicado en Boletín Oficial

Lanzamiento Cisco Centros de Tecnología Avanzada

Cisco inaugura sus Centros de Tecnología Avanzada (ATC, por sus siglas en inglés) en Chile y Colombia, un espacio de innovación habilitado para mostrar, simular, entrenar y probar las nuevas soluciones tecnológicas.

Video ATC

Cisco expande sus ofertas de seguridad gratuitas

Ghassan Dreibi - 12 Marzo 2020

A medida que aumenta el número de trabajadores remotos, Cisco apoya a los clientes con la expansión de sus ofertas de seguridad gratuitas.

Más información

Ayudar a los empleados, clientes y socios en un momento de necesidad es uno de los valores fundamentales de Cisco. En este momento, COVID-19 está obligando a muchas personas en todo el mundo a trabajar de forma remota. Esto está poniendo una tensión repentina tanto en los equipos de TI como de seguridad que se encargan de proporcionar soporte para un número sin precedentes de trabajadores externos y sus dispositivos.

Recientemente, Cisco Webex expandió sus ofertas gratuitas para permitir que los empleados permanezcan conectados con sus equipos y continúen sus operaciones comerciales. En respuesta a los clientes que hoy nos piden orientación, Cisco está ampliando esta oferta para incluir la seguridad para los empleados remotos proporcionando licencias gratuitas extendidas y expansión en la cantidad de usuarios sin cargo adicional para tres de nuestras tecnologías de seguridad clave diseñadas para proteger a los trabajadores remotos en cualquier lugar, en cualquier momento y en cualquier dispositivo.

Cisco Umbrella protege a los usuarios de sitios malintencionados de Internet, ya sea que estén dentro o fuera de la red. Debido a que se entrega desde la nube, Umbrella facilita la protección de los usuarios en todas partes en cuestión de minutos.

Duo Security permite a las organizaciones verificar las identidades de los usuarios y establecer la confianza del dispositivo antes de conceder acceso a las aplicaciones.

Cisco AnyConnect Secure Mobility Client permite a los empleados trabajar desde cualquier lugar en los portátiles de la empresa o los dispositivos móviles personales. Estas ofertas estarán disponibles desde ahora hasta el 1 de julio de 2020. Es nuestra prioridad apoyar a nuestros clientes y socios, y esperamos que estos pasos proactivos ayuden a las empresas a administrar el impacto del negocio y a mantener a los empleados seguros durante esta situación en evolución.

Ciberseguridad que mejora la experiencia de usuario

Resguardamos la identidad digital de tus clientes para que tu negocio crezca.

- Prevención de Fraude
- Protección de la Identidad
- Biometría
- Gestión de Riesgo

vusecurity.com | @vusecurity | corporate@vusecurity.com

El Desafío de las fake news

por **Alicia Giorgetti**

La distribución de noticias falsas no es novedosa. Pero la tecnología amplificó y aceleró la propagación de esta práctica que no solo genera desinformación, también puede crear problemas de seguridad informática. ¿Qué riesgos plantean las *fake news* y cómo prevenirlos?

"Toda información fabricada y publicada deliberadamente para engañar e inducir a terceros a creer falsedades o poner en duda hechos verificables" es la definición de *fake news* que provee la Red de Periodismo Ético (EJN), perteneciente a la Fundación Gabo, creada por el Nobel de Literatura colombiano Gabriel García Márquez.

Esta expresión ganó popularidad en los últimos años, especialmente en 2016, durante las elecciones presidenciales de Estados Unidos. Pero las *fake news* también estuvieron presentes en el Brexit -apoyando un Reino Unido sin Europa-, en las últimas elecciones presidenciales francesas, en el referéndum independentista de Cataluña en 2018 y en las elecciones catalanas de fines del año pasado, entre muchas otras ocasiones.

Según el informe *The spread of true and false news online* publicado por el Instituto Tecnológico de Massachusetts (MIT), las noticias falsas tienen hasta 70% más probabilidad de ser compartidas que las verídicas. Y esto genera mayor velocidad de difusión y mayor audiencia.

De acuerdo con una investigación realizada por Buzzfeed, las *fake news* publicadas durante el último proceso eleccionario estadounidense tuvieron más interacciones en Facebook que las de medios como New York Times, NBC News o Washington Post. Y en abril de 2018, Mark Zuckerberg admitió ante el Senado de Estados Unidos que 80.000 publicaciones falsas llegaron a 126 millones de estadounidenses a través de Facebook.

No hay voces que indiquen que este fenómeno se detendrá. Todo lo contrario: la consultora Gartner

prevé que en 2022 la mayoría de los ciudadanos de países con economías maduras consumirá más información falsa que verdadera.

Los riesgos

La viralidad que la tecnología le dio a las noticias falsas sumada a su capacidad de atracción mediante títulos llamativos o fotos y videos desconcertantes, las convierte en una excelente vía de propagación de amenazas informáticas.

Además, la información personal que los usuarios comparten en sus redes sociales permite que los ciber atacantes generen *fake news* "personalizadas", que tienen más posibilidad de ser compartidas. Y como muchas personas acceden a sus redes sociales desde el trabajo, este tipo de ciberataque puede extenderse a la red de la compañía. "Existe una industria del cibercrimen bien organizada. Dentro de ella podría haber quienes se dedican a la ingeniería social y a la elaboración de *fake news* para ejecutar un ataque cibernético. Cada vez más los ataques persiguen un fin económico que puede ser espionaje industrial, transferencia de fondos o acceso a sitios para robar activos", dice Gabriel Sakata, Country Manager de Cisco para Argentina, Paraguay y Uruguay.

Según la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), las personas no están preparadas ni tienen herramientas y/o conocimientos para enfrentar campañas de *fake news*. Y Sakata agrega que "uno de los desafíos de la ciberseguridad es el comportamiento de las personas. Algo fundamental para que un ataque cibernético tenga éxito es que el usuario que recibe una *fake news* o un falso pedido de un anónimo que simula ser alguien de confianza, haga click en un link o abra un archivo. No obstante, la concientización y educación de los usuarios y las tecnologías de ciberseguridad están dificultando el éxito de este tipo de ataque de phishing tradicional. Pero una

noticia falsa puede persuadir a un usuario a tomar una acción. Por ejemplo, una *fake news* difunde el supuesto robo de passwords de una red social e invita a que sus usuarios renueven sus contraseñas, dirigiéndolos a un sitio web falso que simula ser la red social atacada. También, una *fake news* podría ser parte de un ataque generalizado de phishing que termine generando pérdidas por los pagos de rescate de datos –en caso de ransomware– o por los costos propios del incidente".

El ejecutivo explica que hay ataques más dirigidos y de mayor grado de sofisticación, que se conocen como Business E-Mail Compromise (BEC): "Se valen de un *deep fake* para emular la voz de un ejecutivo y lograr que un funcionario ejecute una operación, típicamente una transferencia de dinero, porque supuestamente lo está solicitando la voz de su jefe. Estos son los ataques más costosos porque generan un desvío de dinero. Inclusive se detectaron casos de desvío de mercaderías a falsos intermediarios o falsos clientes finales".

La protección

La mayoría de los usuarios sabe que no todo lo que se publica en Internet es verdadero, pero comparte compulsivamente los contenidos sin chequearlos. Por lo tanto, "hay que impulsar un cambio de postura: pasar de la confianza irrestricta en la información recibida o encontrada en Internet a un pensamiento crítico que cuestione su veracidad e indague. Dado que en una *fake news* suele haber alguien que se hace pasar por otro, hay acciones prácticas a realizar. Por ejemplo, verificar si el dominio del que proviene o hacia donde lleva el mensaje se ve genuino, si el remitente es conocido y tiene un dominio coherente con la entidad que dice ser. Si se trata de publicaciones en Internet hay que averiguar la reputación del medio, la vinculación con otros medios y si esa información fue publicada por otras fuentes confiables", advierte Sakata.

Además de la de concientización y educación de los usuarios, hay tecnologías para minimizar las consecuencias de estos ataques. "Cisco tiene varias soluciones que integran su arquitectura de seguridad y reducen el riesgo de las *fake news*", dice el ejecutivo, y destaca las siguientes:

* **Eliminación de correo no deseado**. Permite eliminar el volumen masivo de emails no deseados junto con los correos de phishing que pueden ser automáticamente identificados por la tecnología por sus características (hipervínculos, contenidos del mensaje, procedencia, etc.).

* **Sitios maliciosos o falsos identificados**. Si un ataque de phishing avanzado o un BEC superan estas barreras tecnológicas hay otras tecnologías para prevenir la infección. Por ejemplo, el uso de un servicio de DNS Seguro como Cisco Umbrella permite el bloqueo de las conexiones a sitios identificados como maliciosos. Cuando un usuario invoca un link que apunta a un sitio identificado como malicioso, automáticamente se ejecuta un proceso por el cual el dispositivo del usuario consulta la dirección IP del sitio invocado. En ese proceso -llamado Resolución de Nombre de Dominio- el Servidor de Dominio de Nombres (DNS) de Cisco Umbrella bloquea la respuesta y así el usuario queda protegido aún cuando haga click.

* **Validación de Identidad Multifactor (MFA)**. Si se comprometieron credenciales de usuarios como consecuencia del ataque, la tecnología Cisco Duo, de validación de identidad de multifactor (MFA), previene que el atacante pueda loguearse en la red, sistema o aplicación comprometidos usando las credenciales obtenidas. Con esta tecnología, el usuario que necesita acceder a un servicio y tiene usuario y clave, recibe en su aplicación Cisco Duo -que puede tener en su celular- un pedido de validación de acceso que debe autorizar. Si alguien roba credenciales de acceso de un usuario y quiere acceder al servicio no podrá hacerlo porque no tendrá la autorización.

El poder del usuario

El 54% de los usuarios de Internet usa las redes sociales como fuente de noticias, según una investigación realizada por la Universidad de Oxford en 36 países. Y para saber si esa información es verdadera o falsa, usan Google. Por lo tanto, desde esta empresa ofrecen las siguientes sugerencias para intentar detectar *fake news*:

* Leer la noticia entera, no solo el titular.

* Averiguar la fuente de la noticia. Si es de un medio de comunicación, es conveniente entrar a su sitio web y verificar si la noticia está allí.

* Buscar el titular en Google. Si es verdadera, es probable que otros medios la hayan reproducido. Si es falsa, tal vez algunos sitios de verificación de datos -como Chequeado- la hayan detectado.

* Buscar los datos citados. Si hay un textual de alguna persona, ¿fue reproducido por otros medios?

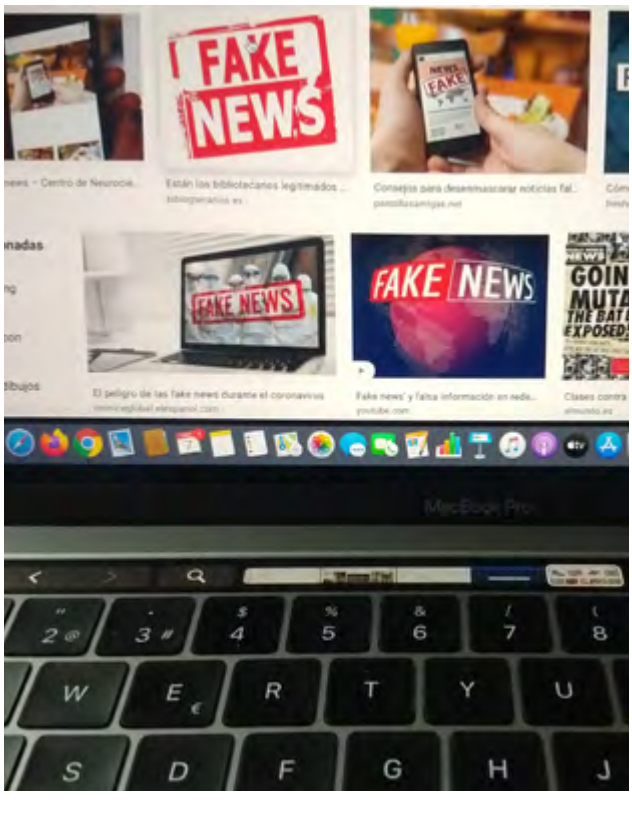
* Verificar la fecha de publicación. Divulgar una noticia en una fecha diferente también es una forma de desinformación.

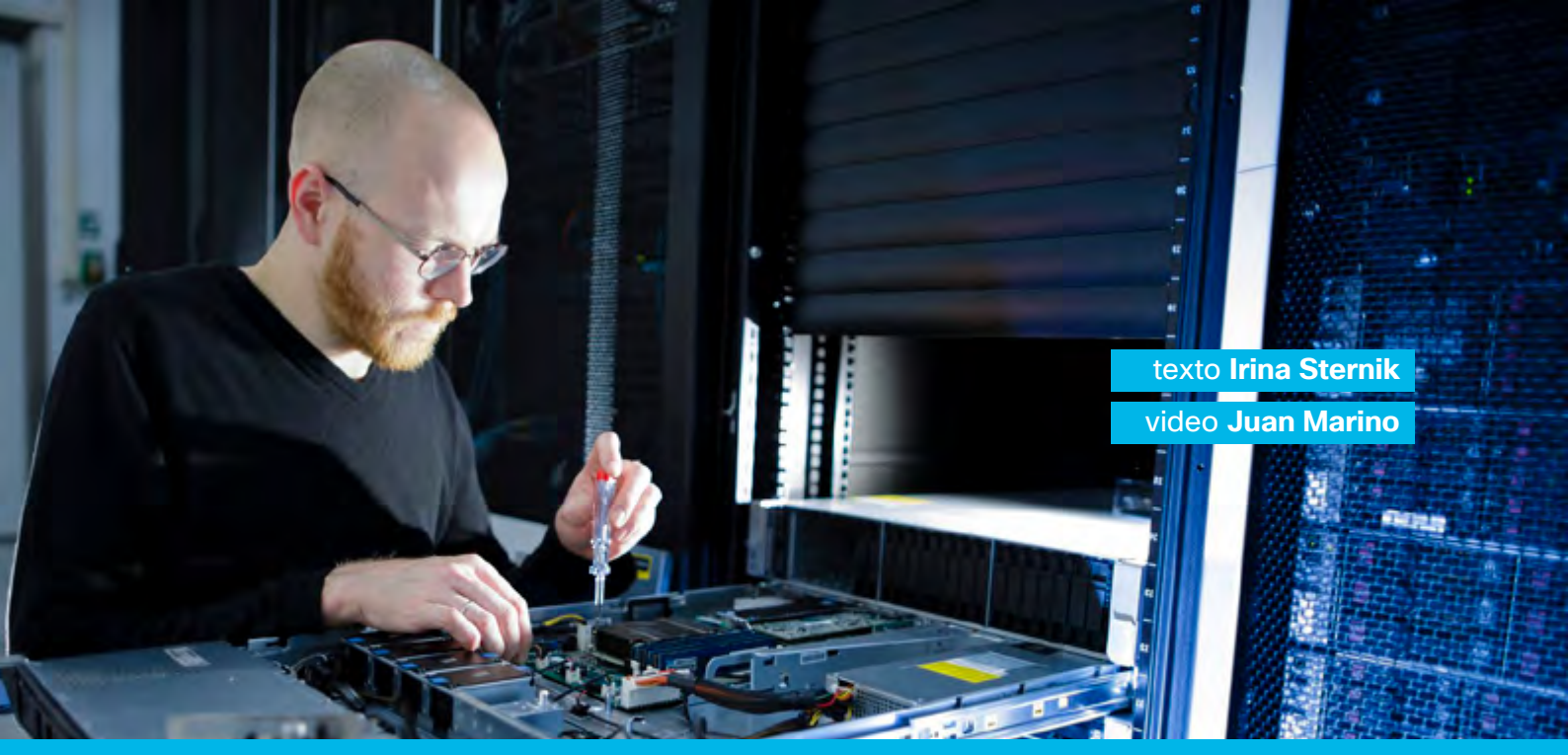
* Si es una imagen, buscarla en Google Imágenes para comprobar si otros sitios la reprodujeron.

Según Google, en general las *fake news* suelen ser historias poco creíbles, o empezar con alguien que publica algo humorístico para crear un hilo de diálogo que termine con dichos falsos. Luego de viralizarse, la información suele convertirse en un meme porque es algo que las personas tienden a compartir.

Los títulos son llamativos e incluyen palabras gancho que tal vez no se relacionan con la información contenida, y apelan a la empatía. Por ejemplo, piden ayuda para encontrar a una persona perdida, informan sobre determinada recompensa si se comparte una información, etc.

La empresa asegura que hay varios sitios web que emiten noticias irónicas que, luego, son compartidas como verdaderas, es por ello que es necesario que los usuarios de Internet desarrollen capacidades y habilidades para identificar si las fuentes son fidedignas





texto **Irina Sternik**
video **Juan Marino**

Contrapunto

¿Qué tienen en común un director de orquesta y un experto en ciberseguridad? Para descubrir las similitudes y diferencias recurrimos a dos apasionados de su materia: el maestro Carlos Vieu, Director de Orquesta y Juan Marino, Gerente Regional de Ventas para Ciberseguridad. La locación elegida para la charla fue ni más ni menos que la Plaza Lavalle, frente al Teatro Colón, lugar emblemático para los argentinos, para el mundo y también, para nuestro entrevistado.

El currículum de Vieu es fructífero. Para resumir diremos, que además de ser Personalidad Destacada de la Cultura por la Legislatura de la Ciudad de Buenos Aires, lleva dirigidos más de treinta títulos operísticos entre el Teatro Colón, Teatro Argentino de La Plata, Buenos Aires Lírica, Ópera de Rosario, Teatro Solís de Montevideo, Teatro Municipal de Río de Janeiro (Brasil), Ópera de Lausanne (Suiza), Asociación Romanza (Perú) y Ópera Nacional de Armenia.

Por su parte, Marino es Gerente Regional de Ventas para Ciberseguridad de Cisco Security. En la actualidad lidera un equipo de profesionales que asesoran a las organizaciones públicas y privadas para protegerse del cibercrimen.

El factor humano

El puntapié inicial de la charla es, justamente, la vinculación entre la tecnología, los procesos y las personas. Desde el punto de vista de la dirección musical ¿Qué deberían aprender quienes trabajan con la orquestación de tecnología en cuanto al manejo de personas?

“A revalorizar el factor humano. La toma de decisiones, el control, ese toque personal que tiene que ver con la sensibilidad y con la inteligencia humana no puede faltar. En el caso de mi profesión uno trabaja con un nivel de disociación hemisférica enorme porque hay que estar atentos a muchas cosas a la vez” indica Vieu, haciendo una analogía con los eventos tecnológicos: “Esas cosas que están muchas veces en manos de aparatos, de consolas y de coordinaciones eléctricas, requieren de un cerebro humano que tenga ese toque de sensibilidad que la máquina todavía no tiene”.

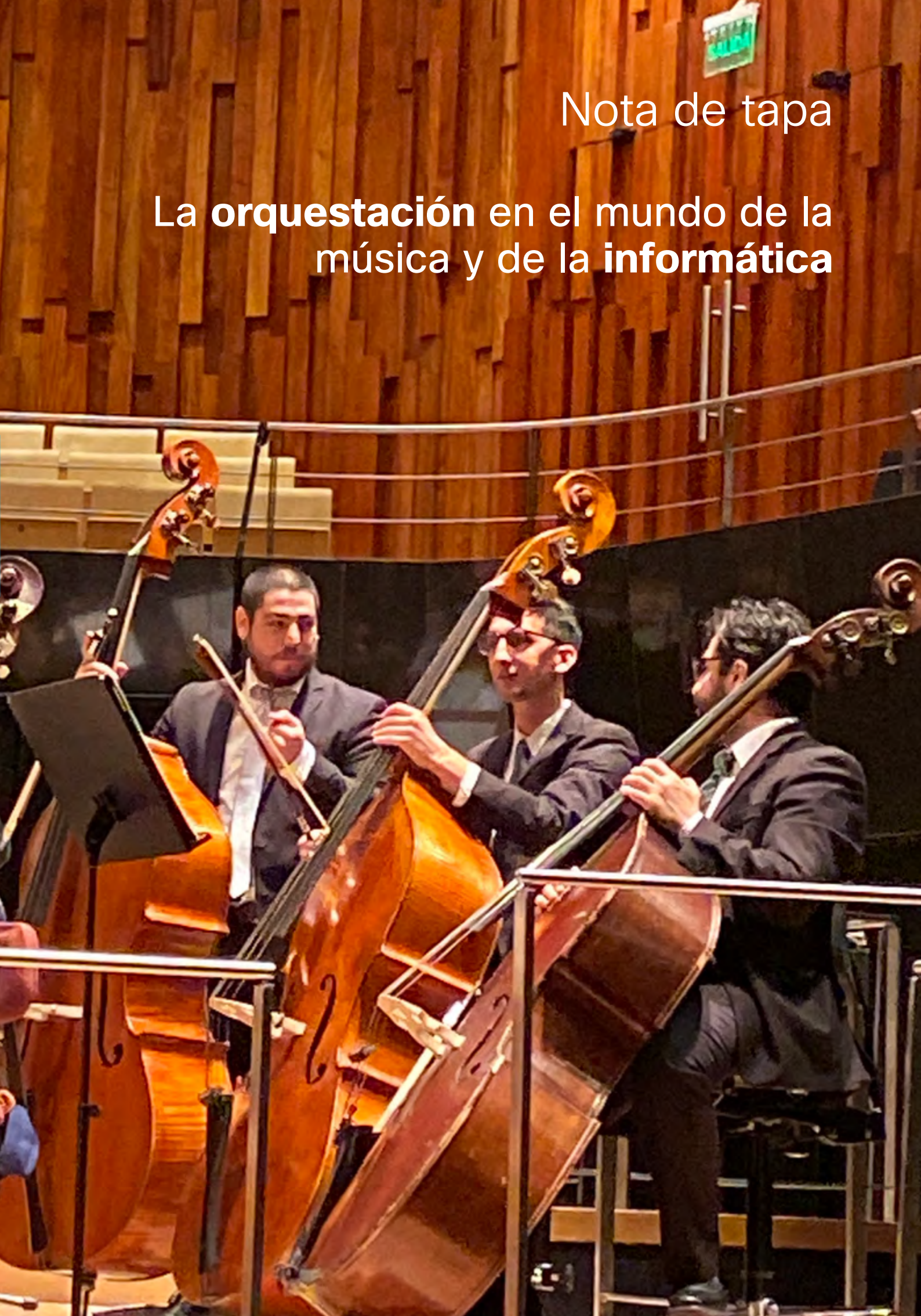
En este sentido, Marino coincide con el elemento humano y la visión de Vieu: “Nuestro mundo se está empoderando demasiado con la tecnología pero la tecnología sola no resuelve el problema de la ciberseguridad en la escala y nivel de madurez actuales”.

La propuesta de comparación, en este caso, es el proceso de gobernanza. ¿Cómo se gestionan tantos elementos para ejecutar?

En el caso de su profesión, dice Vieu, el factor humano es preponderante porque el director de orquesta no provoca el sonido, provoca el estímulo a las personas que hacen el sonido. “No solamente

Nota de tapa

La **orquestación** en el mundo de la música y de la **informática**



Sorpresivo y cálido encuentro de Carlos Vieu con compañeros del Teatro Colón.

están el factor técnico de la comunicación, de la gestualidad y de todo aquello que tiene que ver con el aprendizaje de la profesión, sino que tiene que ver con el estímulo directo a las almas de las personas para que no sólo lo hagan con la precisión matemática y técnica sino también para que le pongan el sentimiento, el color y todo aquello que a la vez trianguló con el compositor que es el que tiene la idea primigenia. La tecnología, por más compleja que sea, la inventó el hombre como una necesidad de ampliar sus horizontes comunicativos pero basados en algo primigenio que es el ser social del hombre. Sin el otro, no existe: lo necesita como espejo y como reflejo. Entonces tal vez este factor humano del que hablamos es el que vuelva al origen del por qué de la tecnología, que es para mejorar la vida del hombre en definitiva", concluye.

En el caso de la ciberseguridad -indica Marino- ese origen tiene que ver con una necesidad de controlar el riesgo del negocio, que es algo dinámico y diferente en cada empresa o actividad: "Muchas veces parece no haber una buena conexión con ese origen o propósito y la seguridad se implementa como algo independiente y muy centrado en tecnología en base a protegerse de las amenazas, como un sustrato abstracto que "rogamos no ocurra". Pero la esperanza no es una buena estrategia. En nuestro ámbito las organizaciones más maduras son aquellas que cuentan con profesionales capaces de articular una estrategia bien vinculada al negocio y gobernar los recursos para que se ejecute exitosamente".

La partitura

El manual de instrucciones de una canción es una partitura, un documento que indica cómo debe interpretarse una composición musical, mediante claves, tonalidades, *tempi* y notas musicales, entre otros signos del sistema musical.

"En el mundo de la tecnología suele no haber partitura. Tenemos el elemento tecnológico pero falta un plan rector" dice Marino.

Sí, pero ahí está la cabeza humana, retruca Vieu. Para el músico, la analogía con la tecnología tiene que ver con tener en claro cuál es el propósito. "A partir de allí, hay que poner todos los elementos tecnológicos al servicio del producto que uno quiere lograr. En el caso nuestro, si no hubiera una idea de por dónde organizar todo el plan de trabajo y cuál es el objetivo final, sería inabarcable porque desde el momento en que vos recibís estas "hormiguitas trepando un alambrado" lo tenés que volver a decodificar en términos de lo que era el sonido en la mente del compositor en esa época y trasladarlo a los medios técnicos con los cuales vos te comunicás con la orquesta". Otros factores que influyen en dicha decodificación son una sala adecuada, los músicos contratados con el nivel de su instrumento óptimo y la partitura individual leída, la coordinación del ensayo y también, el factor nervioso de salir al escenario e interpretar en vivo. "El público sufre otra decodificación del sonido

Juan Marino y Carlos Vieu posan para la cámara luego de la filmación.

donde están el juego la sensibilidad, la emoción, el impacto visual, etc. Todo esto lo hacemos sin más elementos tecnológicos que una lamparita que refuerza la iluminación del atril".

En el caso de la tecnología, indica Vieu, tienen todos los botones posibles para ir a la Luna, pero si esos botones no los maneja un controlador aéreo, los aviones chocan.

"Así es. En nuestro ámbito se está volcando la atención cada vez más a la capacidad de interpretar lo que sucede en tiempo real para poder apretar los botones necesarios a tiempo, pero para eso es fundamental que las tecnologías estén bien integradas para ofrecer información humanamente discernible y accionable", agrega Marino y dice que si desde un comienzo no se definió "la partitura" a seguir, las organizaciones tienen que lidiar con la complejidad de múltiples herramientas y recursos sin orden suficiente.

El estilo y el talento

¿Hay relación entre el talento y el estilo de conducción y dirección?, se pregunta Marino, pensando en lo que ocurre justamente en una sala repleta de ingenieros informáticos que, en conjunto, tienen que lograr un complejo fin sin esta hoja de ruta que es la partitura. ¿Hay un estilo que hace la diferencia?

Para Vieu, la persona que conduce fundamentalmente tiene varias responsabilidades. Una es tomar decisiones, otra es hacerse cargo de esas decisiones porque no siempre son las acertadas, o si lo son, a veces son muy juzgadas y hasta combatidas por aquellos dirigidos. En el caso de la orquesta, todo sucede en vivo y tiene que ver con el tiempo. Entonces, el nivel de resolución es casi reflejo y casi inmediato. "Uno no se puede detener a pensar porque cuando estás pensando está sucediendo y llegás tarde. Tal vez nuestro cerebro funciona como una computadora y hacemos que una computadora se parezca a un cerebro".

"Hablando del tempo, en nuestro mundo pasa esto. Los que gestionan la tecnología y la seguridad están en una carrera contra el tiempo, en un *allegro prestissimo*, corriendo, esperando que nada falle", compara Marino.

Vieu coincide y hace hincapié en que el hombre es el creador de la tecnología. Una que ocurre en microsegundos y se refleja en todos los hechos de la vida. "De alguna forma ese reflejo de necesidades primigenias que no se podían solucionar o que se solucionaban con otros tiempos y hoy en día esto es tan vertiginoso que no sabemos si es vertiginoso porque la tecnología le da más velocidad o porque nosotros necesitamos más velocidad y por eso creamos tecnología que nos facilita las cosas pero necesitamos del contralor del cerebro humano y sobre todo de la sensibilidad humana para que esa tecnología no nos supere y esté siempre a nuestro servicio y no nosotros al servicio de ella".

La falla

Tanto en la música como en la tecnología, está la posibilidad de que algo falle. ¿Se puede preparar la orquesta para cuando todo falla?, reflexiona Marino, quizás pensando en los ataques que puede recibir una empresa de parte del cibercrimen y la necesidad de seguir operando a pesar de eso. Y pregunta: ¿cómo se transita en un espectáculo el concepto de resiliencia?

"Nosotros, a diferencia de un escultor o de un pintor, nos enfrentamos a factores accidentales que tienen que ver con el vivo y tenemos que estar preparados al 150% para que podamos rendir el 100%. Por ejemplo, si se trata de un espectáculo complejo como una ópera -que es como si fuera un recinto lleno de computadoras porque tenés el técnico, el escenógrafo, todos los que están detrás de escena, el apuntador, el cantante, etc.- enfrentamos un terreno apabullante si uno lo analiza desde la descripción. Un cantante puede tener una "laguna" en la memoria o un asistente de escenario le puede haber dado el acceso a escenario tarde a un actor o a un cantante y eso provoca algo así como la caída de fichas de dominó. Es el director en quien convergen todas las miradas para poder solucionar lo que accidentalmente no funciona".

En el mundo de la tecnología, el foso es una gran analogía. "Es ahí detrás, a veces no se ve, pero cuando falla algo en las bambalinas el impacto está en el escenario", dice Marino y agrega: "sin embargo, el éxito no está en la ausencia de fallas sino en lograr resiliencia para superarlas con un impacto mínimo en la operación".

"Una cantante amiga decía: no hacemos neurocirugía; si cortamos un milímetro para allá no dejamos cuadripléjico a nadie, pero desde la vocación y desde la responsabilidad profesional nos lo tomamos como si hiciéramos neurocirugía. La música es matemática también, es ciencia y la perfección estructural y el ajuste es algo básico antes de ir a lo que llamamos expresión. Tenemos que tener un factor de control de coordinación casi tecnológico a pesar de que somos humanos y por ser humanos tenemos un margen de error enorme", indica Vieu.

Control

El director, en teoría, siempre tiene control de todo, analiza Marino y pregunta: ¿Cuál es el temor que tiene un director, de qué depende su éxito y cuál es la enseñanza que se podría transpolar al campo de la tecnología?

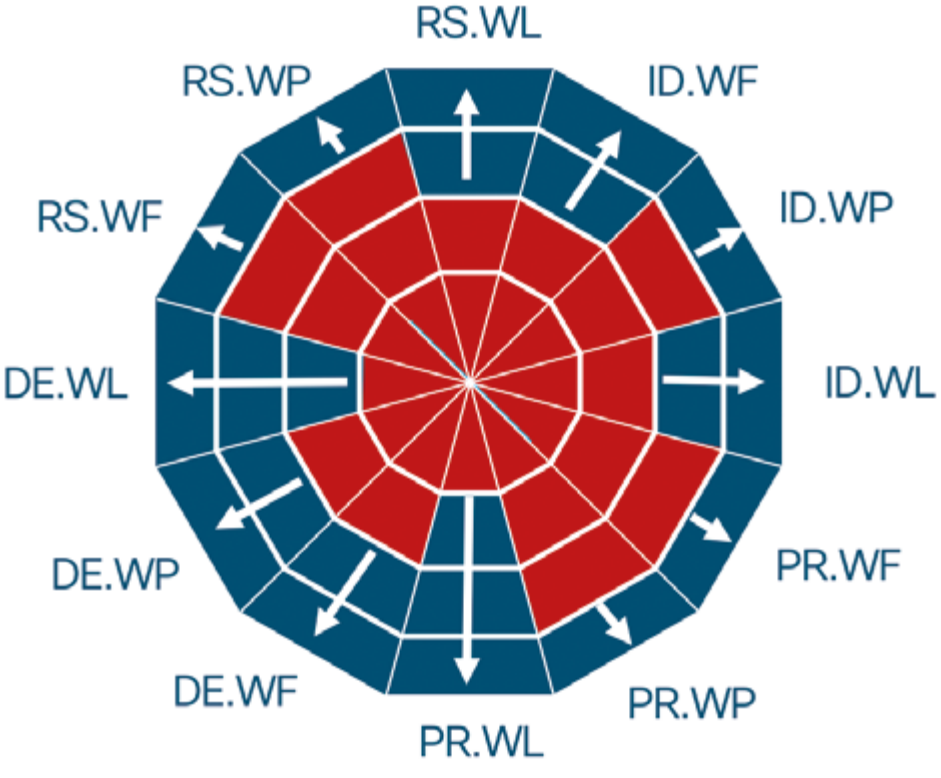
Instalaciones Cisco.

Orquesta Sinfónica Nacional.

La preparación y la excelencia, sintetiza Vieu. La enseñanza que puede servir para ambas áreas, indica el director de orquesta, es el tratar de anticiparse a los eventos: “Tratar de conocer muy bien cada elemento con el que se trabaja para poder optimizar el rendimiento de sus elementos, su coordinación y su puesta en marcha, incluido el estímulo. Tal vez una máquina no tiene un estímulo humano desde el punto de vista de la sensibilidad, pero si hay un mal manejo puede provocar una catástrofe”.

En el caso de la música es parecido. Si uno no conoce a todos los elementos con los que trabaja no puede vislumbrar cuál puede ser la vara de medida del producto final. “Yo siempre le digo a mis alumnos que uno tiene un criterio de realización que sale del análisis y de una preparación muy sólida pero la realización de ese criterio varía según las circunstancias. La capacidad de resolver tiene que ver con esta preparación, con estar atento, con utilizar la inteligencia al servicio de un buen producto, con la concentración y el compromiso” concluye Vieu

Los beneficios del assessment



Resultados individuales (cliente anónimo)

En la vista de una empresa individual, se pueden identificar con claridad las áreas de mejora prioritarias

Referencia siglas:
ID: Identificar / **PR:** Proteger /
DE: Detectar / **RS:** Responder /
WP: Workplace / **WF:** Workforce /
WL: Workload

Industrias, gobiernos y empresas usan las entrevistas de evaluación situacional con un fin concreto: predecir cómo se comportaría un empleado o ciudadano en una determinada situación. Pero no solo personas de carne y hueso son beneficiadas con este proceso, también la infraestructura y la situación de sus componentes críticos en casos cruciales como la ciberseguridad. Los beneficios del assessment son poder revisar, en profundidad, la capacidad de una empresa para proteger los activos de información contra amenazas relevantes.

En esta nota veremos, a modo de ejemplo, en qué consiste una evaluación tipo en Cisco orientada a auto-evaluar el nivel de madurez de la estrategia, procesos, indicadores de desempeño (KPIs), tecnologías y amenazas según la percepción del responsable de tecnología informática de la compañía con respecto a su organización en materia de Ciberseguridad.

Esta encuesta digital demora solo 10 minutos y tiene muchos beneficios: es gratuito, permite predecir la madurez de las implementaciones y tecnologías de ciberseguridad y sus potenciales riesgos y ahorra valiosos tiempos al identificar tempranamente los problemas.

Al escanear el código QR ubicado al final de esta nota se inicia el proceso de preguntas relativas a *Workforce*, *Workplace* y *Workload*. La evaluación está dividida en:

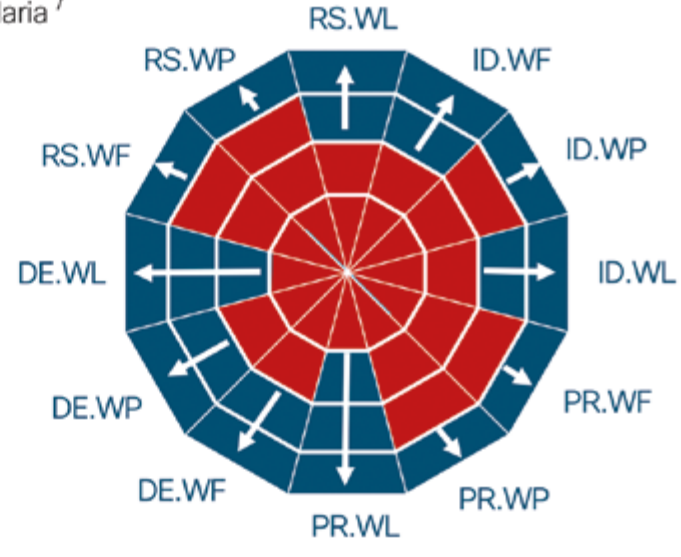
- **Identificación** del estado de situación (incluyendo usuarios, dispositivos, aplicaciones y su interacción),
- Capacidades de **protección** de usuarios ante

Vive tu propia aventura

1. DUO
2. ISE
3. STEALTHWATCH
4. TETRATION
5. UMBRELLA
6. FIREPOWER
7. E-MAIL SECURITY
8. CLOUDLOCK
9. AMP
10. THREATGRID
11. SD-ACCESS / ACI

	WORKFORCE	WORKPLACE	WORKLOAD
IDENTIFICAR	1, 2, 3, 4, 5	2, 3, 6	4, 3
PROTEGER	1, 2, 5, 6, 7, 8, 9	2, 5, 6, 9, 10, 11	4, 3, 5, 6, 8, 11
DETECTAR	1, 2, 8	2, 3, 6	4, 3, 8
RESPONDER	1, 2, 6, 8	2, 6, 11	4, 3, 8, 11

Solución Primaria
Solución Secundaria



Ej. Definición de prioridades "Cliente x"

1- PR.WL ..... ↦ **Tetration**, Stealthwatch
2- DE.WL ..... ↦ **Tetration**
3- ID.WF, ID.WL ..... ↦ **Duo, Tetration**
4- DE.WF, DE.WP ..... ↦ **Duo, ISE**
5- RS.WL ..... ↦ **Tetration**

amenazas dentro y fuera de la red, de perímetros y de aplicaciones y servicios.
- Recursos para **detectar** actividad sospechosa de usuarios, de comportamientos maliciosos de la red o la actividad de las aplicaciones y servicios.
- Capacidades de **responder** ante amenazas que comprometan a los usuarios, amenacen a la red o a las aplicaciones y servicios.

Por último, se realiza una evaluación de madurez en estrategia y procesos de ciberseguridad con respecto a tendencias o iniciativas que esté llevando a cabo su organización, se analiza también la integración segura de IT con OT y el nivel de madurez en diferentes aspectos que tenga implementado -o planeado hacerlo- su organización.

En función de las respuestas a la encuesta, la evaluación arrojará una serie de resultados que presentamos en este artículo en una de sus posibles formas. El resumen gráfico de la información se acompañará, además, con una explicación detallada para cada cliente.

El *assessment* se convierte entonces en un excelente punto de partida que permite contar con una visión general del estado de ciberseguridad de los sistemas, sin llegar a profundizar en una consultoría personalizada. Comencemos juntos el recorrido desde aquí:

Iniciar evaluación

El integrador **Braycom** utiliza su creatividad y las soluciones de **Cisco** para detectar amenazas de seguridad en el ciber espacio y solucionar los problemas que éstas puedan causar. ¿Cómo lo hace? Lo cuenta **Martín Marino,** su director.

Martín Marino

Braycom + Cisco

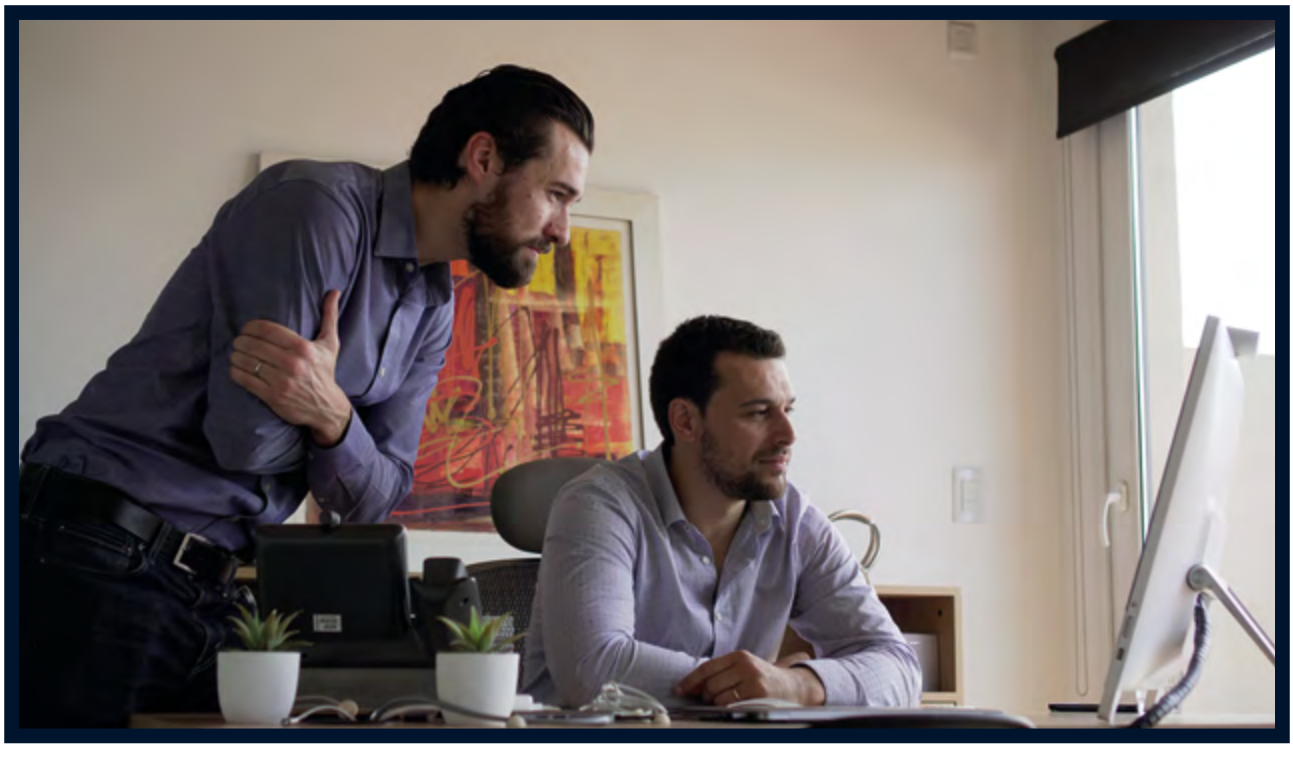
Un refuerzo a la ciberseguridad

Ingeniería + servicios profesionales para proyectos de TI: éste es el compromiso que Braycom asume con sus clientes. A partir de un equipo de ingenieros y consultores, el integrador ofrece soluciones de ciberseguridad, networking, data center y colaboración.

Martín Marino, socio fundador y director de Braycom, acompaña el desarrollo del mercado de las TIC y de la ciberseguridad desde los tiempos del dial up. “Tenemos 17 años de actividad y estamos convencidos de que la única forma de trabajar es de la mejor manera. Eso nos obliga a comprometernos a que nuestros servicios sean los mejores del mercado. Para lograrlo nos asociamos con las marcas número 1 en cada tecnología, y Cisco es una de ellas”.

El ejecutivo destaca que el valor diferencial de Braycom es sumar los mejores servicios, el mejor hardware y la mejor tecnología, y conjugar todo en una solución. “Los servicios deben abarcar el ciclo de vida completo de un proyecto: venta, implementación y, principalmente, preventa y diseño. Ahí tenemos el diferencial porque nuestros consultores están siempre actualizados con la última tecnología. Muchas veces somos los primeros partners en implementar tecnologías nuevas. Somos *early adopters* incluso en nuestra propia infraestructura”, afirma Marino.

Contenido audiovisual



Juan Marino y Martín Marino en Braycom durante la previa de la entrevista.

Ingeniería + Servicios

En cuanto al estado actual de la ciberseguridad en las empresas argentinas, el ejecutivo asegura que “hay una gran inmadurez”. Pero quizás no se deba a fallas o errores de los clientes sino a la aceleración en la digitalización, que derivó en que años atrás era suficiente tener un firewall y un antivirus, y hoy esto no alcanza porque las amenazas son mucho más complejas.

En este sentido, Marino describe que encuentran redes LAN donde los servidores comparten el mismo segmento que los usuarios o excelentes firewalls que están configurados de manera muy laxa, entre otros ejemplos. “Lo notable es que esto sucede en empresas de todo tamaño y de todos los segmentos”, dice.

Según Marino, la respuesta a esta situación está en “construir una solución que no sea solo la suma de muchos componentes excelentes en lo suyo, sino que se integren como en una orquesta.

Y ahí Cisco ayuda muchísimo porque tiene una cartera de productos de seguridad lo suficientemente abarcativa y, a la vez, integrada”.

Por otro lado, el consultor explica que hay una tecnología de Cisco que ofrece gran rapidez de implementación y amplia protección: “Umbrella es poco conocida y ofrece un gran valor agregado porque brinda una capa más de protección que engloba al antivirus, el firewall y todo lo que ya esté instalado. Así, complementa lo que no hacen estas soluciones de nicho y brinda una visión global”. Y agrega que es la elección de Braycom ante casos de emergencia: “Un domingo llamó un gran cliente porque se había infectado de ramsonware y su problema era cómo operar el lunes estando infectado y sin tiempo para resolverlo. La solución fue Umbrella por la rapidez de implementación y porque permitió evitar que el ramsonware encriptara el resto de los equipos”.

Pero, además de profesionales capacitados y una excelente tecnología, se requiere velocidad en la oferta de servicios profesionales.

Y Marino asegura que en Braycom son muy creativos para hacer el delivery del *know how*, especialmente cuando es necesario investigar y hacer un *trouble-shooting* de una red. Para eso desarrollaron Virtual Expert, una solución que muestra en el video de la entrevista

Argentina
Av. Independencia 1330 - Piso 14 - Of B - CABA
Teléfono: +54.11.5273.4470

Colombia: +57.1.580.1333
Chile: +56.2.2938.1332 - **USA:** +1.786.358.6100

Observatorio ALMA

Nota producida por **Cisco**

Imagen: ESO/C. Malin

Caso de negocio

Operación de **red segura** y de **alta disponibilidad**, al servicio de la **comunidad**.

La Entidad

En el desierto de Atacama, en Chile, se ubica el Atacama Large Millimeter/submillimeter Array (ALMA), el radiotelescopio más grande del mundo; cuya operación se basa en un esfuerzo de cooperación internacional encabezado por cuatro entidades principales: el Observatorio Europeo Austral (ESO), la Fundación Nacional de Ciencia de Estados unidos (NSF), los Institutos Nacionales de Ciencias Naturales de Japón (NINS) y la República de Chile.

Ubicada a 5 mil metros de altura sobre el nivel del mar, en cercanías de la ciudad de San Pedro de Atacama, II región, y en medio del desierto de Atacama, este radiotelescopio está integrado por 66 antenas, la mayoría de ellas de 12 metros de diámetro (en el rango de un edificio de 3 a 4 pisos) y con un peso de más de 100 toneladas cada una. Su conjunto principal de 50 antenas actúa coordinadamente como si fuera un solo telescopio gigante; además, estos sistemas de observación se pueden configurar (distribuirse) de distintas maneras y las distancias máximas entre antenas pueden oscilar entre los 150 metros y los 16 kilómetros.

Como ejemplo de la gran potencia de este gran radiotelescopio, en abril de 2019, ALMA fue parte de la alianza astronómica mundial "Event Horizon Telescope", desempeñó un rol clave en un logro científico histórico: la primera fotografía de un agujero negro. "ALMA era imprescindible en dicho proyecto. Podía fallar otro elemento de la iniciativa, pero no nuestro observatorio. Sin ALMA no conseguíamos esa foto", señala Christian Saldias, IT Manager de ALMA.

Un reto de origen

Desde su origen, este observatorio astronómico representó un desafío enorme. En primer término, ALMA se localizaría a 5 mil metros de altura sobre el nivel del mar, una escala sin precedentes en el contexto chileno (otros observatorios en la zona se ubican en el rango de los 3 mil metros de altitud) y con impactos claros en el funcionamiento de la tecnología. En dicha área, pleno desierto de Atacama, ALMA despliega sus 66 antenas, todas conectadas a un edificio técnico donde se ubica el supercomputador que digitaliza y unifica las señales captadas.

A una altitud de 5 mil metros, con una densidad de aire muy baja, muchos componentes tecnológicos (diseñados para trabajar al nivel del mar) tienen dificultades para operar correctamente. Por ejemplo, los ventiladores de las fuentes de poder de los equipos presentan fallas, causando calentamiento excesivo que daña los sistemas. "En nuestra historia, cada metro cuenta", apunta Cristóbal Achermann, IT Project Manager de ALMA.

La relación con Cisco y su partner Dimension Data se inicia en tales circunstancias. Hacia 2008, ALMA, Cisco y Dimension Data prueban y adaptan equipos con el fin de construir una infraestructura de red que pueda operar eficientemente en semejantes condiciones ambientales. ALMA optó por basar su plataforma -switching, routing, Wifi, videoconferencia, telefonía IP, etc.- en soluciones de Cisco. La decisión de optar por Cisco, no fue solo tecnológica, sino que se basa en dos hechos fundamentales.

Por un lado, la dupla Cisco-Dimension Data garantizaba disponibilidad local de soporte, repuestos y expertise en ingeniería. En instalaciones como ALMA, ubicadas en zonas remotas y con actividades 7x24, es indispensable el acceso -rápido y sencillo- a equipos de reemplazo y al conocimiento experto que ayuda a obtener el máximo provecho de las soluciones. "Necesitábamos tecnología robusta, pero también un soporte igual de robusto", comenta Achermann.

Al mismo tiempo, al elegir a Cisco podría aprovechar un ecosistema de productos y soluciones

Imagen: ALMA (ESO/NAOJ/NRAO)

integradas, con capacidades de administración centralizada, compatibilidad entre equipos, inteligencia, automatización, etc., esto evitaría el tener que lidiar con múltiples proveedores y equipos, lo que siempre causa dificultades -operativas y técnicas- a la hora de gestionar una plataforma tecnológica.

En ese sentido, vale la pena señalar que la infraestructura de conectividad de ALMA tiene características excepcionales. La información del Universo captada por las antenas (que operan en una red aislada) es digitalizada y enviada -vía fibra óptica- a un correlacionador (supercomputadora), el cual combina las señales de todas las antenas y genera datos científicos. Esta información se envía a un centro de operaciones (Data Center) en Santiago de Chile, y tras ser procesada (calibrada y optimizada), se distribuye a las organizaciones científicas afiliadas en Europa, Norteamérica y Asia.

Esta plataforma tecnológica con más de 3 mil dispositivos de red, es atendida por un equipo de IT que está integrado por solo cuatro especialistas. Considerando el personal que trabaja en la base de operación en las cercanías de San Pedro de Atacama así como los que laboran en las oficinas centrales de Santiago, ALMA cuenta con alrededor de 300 colaboradores. En tal contexto, los valores de integración, inteligencia y proactividad de las soluciones de Cisco resultaron sumamente convenientes.

El reto de seguridad: no puede fallar

Aunque su vocación sea observar el Universo, ALMA no podía ignorar el entorno donde opera. En materia de ciberseguridad, esto planteaba varios riesgos importantes.

A diferencia de lo que ocurre en un banco o comercio, en donde un ciberataque busca una recompensa evidente (dinero, datos personales, secuestro de equipos, fraude, etc.), la información científica recopilada por ALMA parecería de poco interés para los cibercriminales. Sin embargo, el observatorio astronómico pronto entendió que su mayor amenaza radicaba en otro aspecto: la potencia de su infraestructura tecnológica.

Además, en el caso del Observatorio ALMA en pleno desierto chileno, la seguridad es un aspecto íntimamente ligado a la operación. Si un ciberataque logra afectar la disponibilidad de la infraestructura, el daño sería verdaderamente grave. Como lo resaltan Achermann y Saldias, el activo principal de ALMA es la observación; si no tiene la capacidad para realizar observaciones astronómicas, pierde la capacidad-habilidad de generar los datos que necesita la comunidad científica mundial.

Peor aún, la falla en la disponibilidad puede resultar desastrosa para el avance de la ciencia: hay fenómenos astronómicos que sólo pueden observarse en un momento específico (un minuto u hora particular) y quizá no se repitan sino hasta dentro de 100 o 200 años -o nunca. Hay otros eventos que implican coordinación de investigadores y observatorios a nivel mundial en un momento preciso, por lo que un atraso podría afectar la realización de dichos proyectos. “Por tanto, la disponibilidad de nuestra plataforma es crítica, no puede ser amenazada por un ciberataque”, señala Achermann.

Asimismo, el intercambio de información en el contexto interno y con los asociados en otras partes del planeta tiene que estar protegido contra los ataques conocidos -virus, ransomware, hackeos a servidores o páginas web, spam, etc.- que podrían frenar la operación de la red.

“Tenemos compromisos de tiempo muy estrictos, desde que se realiza la operación hasta la entrega del dato al científico, hay lapsos bien acotados. Si alguien entra a la red de ALMA, aunque no dañe algo, el retraso en la entrega de información ya nos significa un problema mayor”, afirma Saldias.

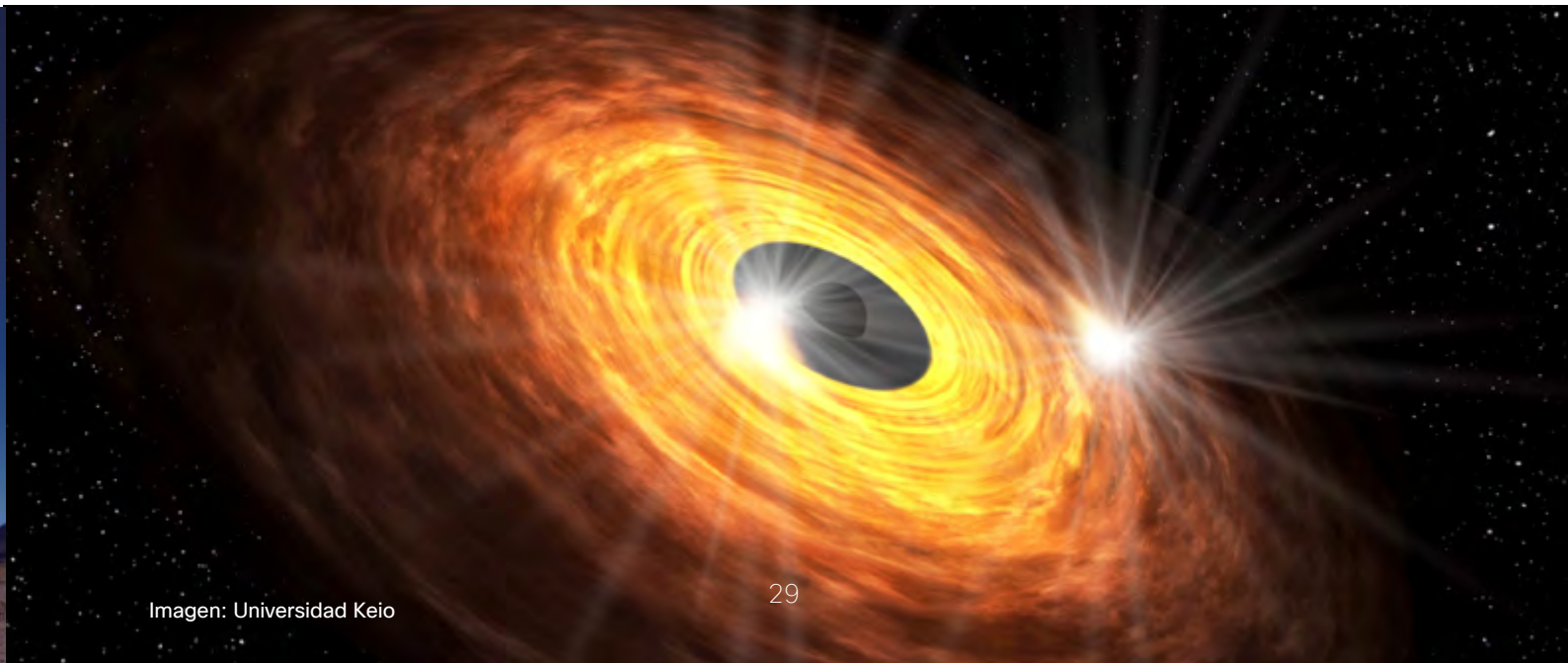


Imagen: Universidad Keio

Imagen: ESO/C. Malin

La estrategia

Consciente de las amenazas potenciales en su entorno, el equipo de IT, en primer término, decidió olvidarse de los planteamientos reactivos y optó por definir una visión estratégica de su ciberseguridad. Una postura que se benefició de dos factores: el hecho de que la red de ALMA estaba basada en soluciones de Cisco; y sobre todo, que las tecnologías de ciberseguridad de la empresa se sustentan en un modelo de arquitectura -y no de productos independientes- en el que la integración, la visibilidad y la centralización son los pilares. Esto terminaría por facilitar la integración, centralización e implementación, sin afectar la productividad de un equipo de IT pequeño.

Los beneficios

Con el respaldo de Cisco y su partner Dimension Data, ALMA está consolidando una operación de red más segura y de mayor disponibilidad; no sólo mejorando su nivel de servicio a la comunidad científica nacional e internacional, sino que contribuyendo a materializar proyectos que marcarán un hito en la historia del conocimiento -y para confirmarlo, ahí está la primera imagen de un agujero negro (2019) y la imagen de la formación de planetas (Disco de Acreción 2018).

Las implementaciones de seguridad -beneficiadas por operar en una infraestructura de red basada en tecnologías de Cisco- no sólo resultaron más fáciles de aplicar, sino que con el tiempo también revelaron varias ventajas operativas, las cuales han sido muy valiosas para un equipo de TI pequeño, que debe atender un gran reto de conectividad y ser un habilitador de servicios.

Las soluciones se integraron fácil y rápidamente entre sí, permitiendo una visión centralizada de toda la plataforma y un control estricto de cambios a las configuraciones de equipos -ambos factores, esenciales para prever amenazas y tomar medidas preventivas con agilidad.

“Además, como nuestra red está sustentada en soluciones de Cisco, si aprendes a configurar un firewall, ya aprendiste a configurar todos los demás, y eso incluye tareas como la puesta a punto, los temas de licenciamiento, los procesos para levantamiento de casos de seguridad, el soporte, etc. Esta capacidad de integración ha resultado clave, de lo contrario, tendríamos que inventar la rueda con cada implementación”, asegura Cristóbal Achermann, IT Project Manager de ALMA.

Adicionalmente, las ventajas de visibilidad y centralización, potenciadas por las capacidades proactivas de las soluciones de Cisco, están impulsando la productividad del personal de TI de ALMA, podrá dedicar menos tiempo a actividades como búsqueda de virus o descarte de falsos positivos.

De hecho, ALMA y la dupla Dimension Data – Cisco ya trabajan en ampliar la automatización inteligente. A la fecha, si un científico llega a las instalaciones del observatorio ubicadas en el desierto de Atacama y desea conectar su laptop a la red, aún es necesaria la intervención de un especialista de TI, quien deberá confirmar que el equipo no tiene virus y cuenta con los parches de seguridad necesarios.

La meta en corto plazo es que dicho proceso manual deje de ser necesario: que la red, por sí misma, realice esa revisión de seguridad y determine si el laptop cumple con los requisitos para conectarse a la plataforma; mejor todavía: si no satisface los criterios, que ayude al usuario a obtener el software y los parches necesarios para habilitar su conexión

Así, desde hace tres años, de la mano de Cisco y su partner Dimension Data, ALMA ha implementado las siguientes soluciones:

- **Firewalls, Firepower** para visibilidad completa de la red, y detección y protección avanzada contra amenazas, así como prevención de intrusiones.
- **Umbrella (DNS):** primera línea de defensa de la red contra amenazas a través de manejo del tráfico DNS, permitiendo visibilidad de las actvidades en la web para detener amenazas antes de que lleguen a la red o sus endpoints. Por su forma de trabajar, es capaz de proteger desde la red de antenas, hasta los usuarios dentro y, eventualmente, fuera de la red de ALMA.
- **Cisco ISE:** para controlar el acceso a la red y, colaborando con las otras soluciones, con capacidad de contención automática de amenezas.
- **Email Security:** para proteger los correos electrónicos de los colaboradores.
- **Swiches**
- **Routers**
- **Border Firewalls & VPN (ASA)**
- **Firewalls virtuales** para aplicaciones internas (protección de redes OT).

Imagen: Sergio Otárola – ALMA (ESO / NAOJ / NRAO)

Prevenir el fraude: misión posible

por **Sebastián Stranieri**, CEO de VU Security

En el último año, según la Online Trust Alliance (OTA), se produjeron más de 2 millones de ataques informáticos. Mientras tanto, según el Banco Interamericano de Desarrollo (BID), el cibercrimen le cuesta a Latinoamérica y el Caribe unos 90 mil millones de dólares al año.

Muchos de estos ataques masivos no capturan datos bancarios, sino que son utilizados por *hackers* o cibercriminales para adueñarse de las credenciales individuales de las personas. ¿Cuántos nos hemos anotado en MyFitnessPal para rastrear las calorías de nuestros alimentos, o en Canva, para mejorar el look and feel de nuestros posteos de redes para luego olvidarnos por completo? Aún si dejamos de utilizar las aplicaciones, nuestros datos personales siguen allí, y ahora están disponibles para todos aquellos dispuestos a pagar por ellos, y que sean capaces de crackear el contenido. Una vez que logran acceder a las credenciales, pueden robarse nuestras identidades digitales y hacerse pasar por nosotros, pero también acceder a otros sitios o plataformas donde usemos la misma contraseña.

Hay algunos sitios donde podemos rastrear si nuestra dirección de correo electrónico ha sido vinculada a alguna cuenta robada, como por ejemplo Have I Been Pwned. Sin embargo, una vez que la información ha sido vulnerada, la única acción que podemos tomar como usuarios es el cambio de contraseña, y verificar que esa contraseña no se repita como código de acceso en otras cuentas.

Si bien este tipo de ataques son frecuentes y suelen ser cada vez más sofisticados, muchas organizaciones ignoran o subestiman medidas de seguridad esenciales que pueden ahorrar tanto dolores de cabeza como pérdidas económicas y de reputación.

Una forma de prevención es la utilización de un segundo factor de autenticación adicional al simple usuario y contraseña como, por ejemplo, los One Time Passwords (OTP) que podemos configurar para recibir vía SMS o correo electrónico. En todos los casos donde nos sea posible, es recomendable habilitar un segundo o tercer factor de autenti-

cación biométrico con nuestro rostro, voz o huella dactilar como soporte a la contraseña tradicional, puesto que siempre se podrán modificar las claves o contraseñas, pero nunca podremos cambiar quienes somos.

Es fundamental tener en cuenta que el principal factor de riesgo es la vulnerabilidad humana. Por eso, es necesario llevar a cabo políticas de capacitación para todos los empleados y dejar claras medidas de seguridad individuales como el uso de contraseñas robustas y múltiples factores de autenticación.

Del mismo modo, es imprescindible para cualquier organización tener un plan de crisis en el que se consideren los aspectos anteriores y un protocolo detallado de cómo se actuará ante un posible ataque. De esta manera, se evitan las pérdidas de tiempo y se solucionan imprevistos de forma rápida y eficiente. Esto es lo que hacemos en *VU Security*, donde trabajamos con más de 130 clientes en Latinoamérica y Europa para ayudarlos a implementar soluciones de prevención de fraude y protección de la identidad

VU Security

Ciber ¿realidad o representación?

por **Pablo Lutenberg**
Especialista en ciberseguridad

Nano Pereyra, artista plástico, concibió esta pintura especialmente para esta columna.
La obra está realizada en acrílico sobre cartón y mide 8,5 cm x 19 cm.

Cuando escuché sobre el ataque con drones a refinerías de petróleo en Arabia Saudita, me pregunté: ¿Es ataque o ciberataque? ¿Cuándo un ciberataque deja de tener el significado de "ciber"? Para que el ataque se pueda llamar "ciber": ¿debe realizarse desde una "ciberfuente"?, ¿se debe dirigir hacia un "ciberdestino"?, ¿debe realizarse a través de un "cibercanal"?
En general el prefijo "ciber" se utiliza cuando se quiere significar "que está relacionado a la cibernética o informática". Es decir, cuando estamos hablando de algo representado en digital y no en físico.
Por otro lado, consideremos cuántas veces por día nos basamos en la credibilidad o en la confianza: dejamos el auto dentro de un estacionamiento a cambio de un papel que guardamos. Y confiamos. El papel ¿lo representa?, ¿qué representa?, representa el acuerdo de que nos devolverán nuestro vehículo a cambio de un pago por el tiempo de guardado. Lo mismo ocurre en los guardarropa, y hasta en los bancos con nuestro dinero. Solemos tomar como realidad a sus representaciones.
Para esto también es imprescindible que tengamos algún grado de confianza.
Por ejemplo, si nos muestran un video de Obama hablando de economía, lo aceptamos como posible y lo incorporamos automáticamente como algo real, algo que ocurrió o está ocurriendo. Damos por sentado que a quien vemos es Obama y que estamos escuchando su voz.
El libro "Ser Digital" (Being Digital) de Nicholas Negroponte marcó para siempre mi forma de pensar la tecnología, así que recurro a él siempre, por diferentes motivos. Para describir algunos conceptos, Negroponte nos invita a pensar en sus partes indivisibles. Acordemos con él entonces que "lo físico (analógico)" y "lo digital", tienen respectivamente al ÁTOMO y al BIT como expresiones mínimas.
Digitalizar algo significa en cierta manera "representar" átomos con bits.
El problema que enfrentamos a partir de esto (y será cada vez más frecuente) es preguntarnos cuándo vamos a confiar en esa representación como fiel y cuándo no. Es decir, ¿cuándo confundiremos representación con recreación?
Los *deepfakes* son el ejemplo más acabado de esto y pueden dejarnos boquiabiertos con unas pocas imágenes animadas y audio. ¿Era Obama con su voz hablando de economía en el video?
Los bits se manipulan (se crean y recrean) mucho más rápido y más fácilmente que los átomos: hace falta software, no laboratorios ni quirófanos.
Espero persuadirlos y acudir a la interpelación modelo siglo XXI:
¿Qué es lo que compone nuestra conciencia?¿Lo representado por los bits o los bits en sí mismos?
¿Tenemos siempre presente que el diseño digital puede tener errores de formación y representación (intencionales o no)?
Los drones estrellan átomos contra átomos "piloteados" por bits: ¿escapa eso a la condición de "ciber" del ataque, por más que las consecuencias sean físicas?
¿Sabemos que la realidad está hecha de átomos más que de bits?
Tal vez las generaciones nativas digitales, puedan plantearse las diferencias mucho mejor que las anteriores

Pablo Pereyra

CISO Dirección General de Gestión Informática Ministerio del Interior, Obras Públicas y Vivienda

texto: **Karina Basanta**
video: **Juan Marino**

Contenido audiovisual

La locación elegida para esta nota fue el Parque “Mujeres Argentinas”, ubicado en el barrio porteño de Puerto Madero.

Gobierno

Tres minutos antes de la hora pautada del encuentro, recibí un mensaje de Pablo avisándome que llegaría en tres minutos. Esa atención, su dedicación y el mismo respeto se sostuvieron durante toda la entrevista, mientras conversábamos y luego en la filmación de la versión audiovisual junto a Juan Marino. Pablo tiene una escucha atenta y la atención dirigida. “Es un orgullo trabajar para mi país”, me dice. Y le creo.

¿Qué significa ser CISO del Ministerio del Interior, Obras Públicas y Vivienda?

Ser el CISO es una gran responsabilidad, tanto con los actores internos del ministerio, como con los servicios de uso público que soportamos. Es un orgullo poder trabajar para mi país. Algunas personas se ponen la camiseta cuando juega la selección de fútbol, nosotros nos ponemos la camiseta todos los días cuando abocamos nuestro tiempo a proteger los sistemas de la Nación.

¿Qué activo se protege?

Desde el ministerio protegemos los activos de uso público y los sistemas internos de gestión pues deben estar resguardados ante filtraciones, modificaciones u otras amenazas que puedan afectar el desempeño de las tecnología. La prestación de servicios ágiles permite tanto a la ciudadanía como a la administración pública nacional la reducción de tiempos de gestión y costos, ese es el fin de los sistemas, por ese motivo deben estar disponibles los 365 días del año, las 24 horas.

¿Cuál es el principal foco de atención actual?

Actualmente nuestro foco está puesto en mantener la continuidad operativa de los sistemas de información a cargo el ministerio. Desde el punto de vista de seguridad se está llevando a cabo un plan estratégico en materia de ciberseguridad que cubre los aspectos de confidencialidad, integridad y disponibilidad. Para cumplir este objetivo, se evalúan constantemente tecnologías y procesos y se forman equipos altamente capacitados en la materia, asimismo, dentro de la administración pública nacional existen lineamientos dirigidos por la Secretaría de Modernización. En los últimos 10 años se ha puesto foco en la protección de los sistemas de la administración pública tanto por los datos contenidos como así también por la criticidad que tienen en la población. El contexto internacional de ataques hace que los estados tengan la necesidad y la obligación de trabajar en conjunto con los demás actores, fortaleciendo la estrategia de ciberseguridad.

Juan Marino y Pablo Pereyra ultiman detalles antes de la filmación.

“Nosotros nos ponemos la **camiseta** todos los días cuando abocamos nuestro tiempo a proteger los sistemas de la **Nación**”

¿Cuáles son las principales acciones que se realizan en términos de ciberseguridad?

Como comenté anteriormente, nuestro foco está puesto en mantener los servicios que presta el organismo respetando los parámetros de confidencialidad, integridad y disponibilidad. Para conservar dichos parámetros en un nivel aceptable realizamos distintos controles. Los parámetros de referencia están basados en las normativas y resoluciones vigentes en materia de ciberseguridad.

Dentro de nuestros planes estratégicos consideramos la entronización de los empleados del ministerio como un pilar fundamental para la prevención. Trabajamos en el fortalecimiento de nuestros centros de datos, aplicaciones, procesos de calidad y recursos humanos, contemplando como plan estratégico las tecnologías, los procesos y las personas.

¿Argentina adhiere a algún lineamiento internacional de ciberseguridad?

Desde la Secretaría de Modernización se dirigen las políticas de filiación a los distintos convenios multilaterales en materia de ciberseguridad, de todos modos hay algunos lineamientos como los estándares tomados por la ONTI en materia de estandarización de normas, que son referencia, por ejemplo las normas ISO, mediante ellas se estandarizan las tecnologías solicitadas y adoptadas por la administración pública nacional.

¿Cómo se trabaja la concientización de los ciudadanos en relación a la ciberseguridad?

Nuestra esfera de trabajo comprende la seguridad del ministerio, respecto de la ciudadanía se encarga la Secretaría de Modernización. Desde mi punto de vista considero importante que se defina una estrategia de concientización ciudadana que incluya campañas referidas a la seguridad de la información, la exposición en redes sociales y el uso seguro de los recursos tecnológicos.

¿Hay proyectos para trabajar conjuntamente con el Ministerio de Educación de la Nación?

Al momento en el Ministerio del Interior no tenemos una directiva de trabajo directo con el Ministerio de Educación, pero entiendo que la potestad de este tema la tiene la Secretaría de Modernización, ellos se encargan de llevar adelante la adopción de políticas públicas relacionadas a las nuevas tecnologías y la ciudadanía, desde el Ministerio del Interior, Obras Públicas y Vivienda el nexo es a nivel de las obras públicas.

¿Se evaluó incorporar este tema en la currícula escolar formal?

Este tema es potestad del Ministerio de Educación. Desde mi punto de vista creo que sería una buena acción generar un espacio donde a temprana edad se hable de los aspectos relacionados con la seguridad de la información, las formas de prevención e incluso los delitos que se cometen en este espacio.

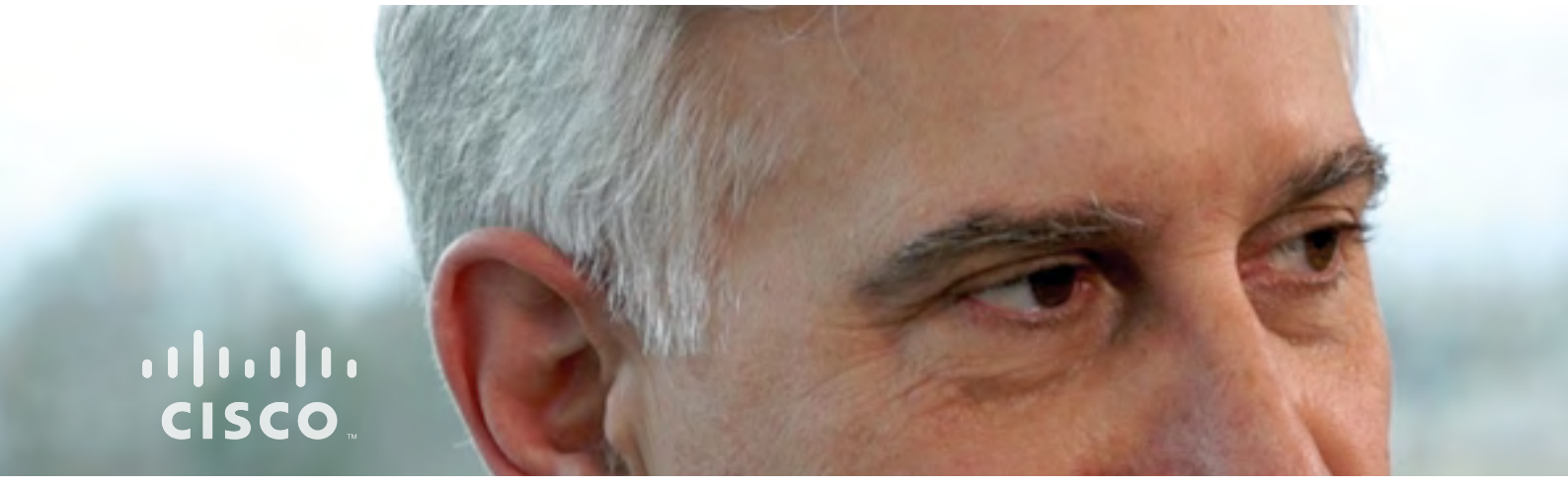
Pablo Pereyra.

Las tecnologías son utilizadas de forma masiva, el ciberespacio está plagado de amenazas, pishing, ransonware, contenidos ilícitos que configuran delitos, malware, operación delictiva de organizaciones, sextorsión, porno venganza. Así como fuera del ciberespacio contamos con fuerzas de seguridad, dentro del ciberespacio existen divisiones especiales que se encargan de procesar y formalizar este tipo de acciones, dándole curso judicial. Es importante que los derechos y leyes que involucran este espacio sean difundidos como así los espacios de acción, en mi opinión esto fortalece la estrategia y conocimiento de la población respecto a sus derechos.

¿Cómo se retiene talento en los equipos técnicos desde el Ministerio?

El sentir pertenencia es uno de los motivos para la retención de talento. Como comenté en la primera pregunta creo que nos ponemos la camiseta de Argentina sabiendo que atendemos las necesidades tecnológicas para la prestación de servicios a la ciudadanía y la administración pública. Sin duda el valor agregado está en hacer más eficiente la gestión del estado mediante las nuevas tecnologías. El ser parte de estos proyectos de gran escala es otro de los factores que creo importante a la hora de considerar el espacio de trabajo en la administración pública nacional

por **Juan Marino y Maximiliano Scheinkman**



Imaginemos ser el CISO de una organización líder en tecnología, a cargo de proteger información confidencial de clientes, patentes, desarrollos y activos; una organización con más de 100.000 empleados, con operación en más de 100 países y decenas de miles de empleados conectados cada día desde sus casas o viajando por el mundo, todos accediendo a una única red corporativa. Esta es la tarea de Steve Martino, el CISO de Cisco quien desde hace casi una década define su trabajo como "habilitar el negocio en forma segura".

Toda estrategia de ciberseguridad requiere de tecnologías, procesos y personas que operan en equilibrio. En ocasión del RSA Conference tuvimos la oportunidad de conversar con Steve y conocer su filosofía y estrategia en cada uno de estos pilares.

- ¿Por dónde comenzar para armar una estrategia de ciberseguridad?

Con gran claridad, Steve nos reveló la importancia de comenzar por entender lo que necesita el negocio y construir la estrategia de ciberseguridad verdaderamente centrada en ese contexto, que es único en cada empresa, y evoluciona de forma continua. Mantener reuniones C-Level periódicas para comprender cómo evoluciona el negocio y cómo adaptar la estrategia a estos cambios es para él un tema prioritario.

- ¿Qué debemos evitar durante la gestión?
- La ciberfatiga, responde.

Hoy en día, la mayoría de las organizaciones sufre este cansancio debido a la gran complejidad que implica llevar adelante la propia operación de seguridad. Es demasiado el tiempo destinado en mantener las cosas funcionando y cuando ocurre un imprevisto negativo, los tiempos de detección y respuesta resultan inaceptables. En este sentido, Steve mencionó los alarmantes 100 días promedio de industria en detectar una brecha y que con la correcta combinación de tecnologías, procesos y personas se puede bajar a cuestión de pocas horas.

Cisco en números

Cada día en **Cisco** se procesan **4.400.000 correos electrónicos**, se analizan **28.000.000.000** de flujos de comunicación, **7.600.000.000** de consultas DNS, y se detectan **13.400.000** intentos de intrusión. Se bloquean **6.000.000** de esas consultas DNS, **2.500.000** millones de los correos son bloqueados y **17.000** archivos son enviados al sandbox para análisis dinámico en profundidad.

Cliente cero

Todas las tecnologías de detección, protección y respuesta implementadas en Cisco funcionan como una arquitectura de seguridad unificada que permite por medio de la automatización, resolver la gran mayoría de las amenazas sin intervención humana, dejando por día, solo un puñado de casos para ser analizados por los especialistas del CSIRT (Computer Security Incident Response Team).

Formar una arquitectura de seguridad unificada es imprescindible para lograr esto y es por eso que muchas de las integraciones en la arquitectura de seguridad que se desarrollan con el portafolio de Cisco han surgido de las necesidades de Steve y su equipo en la búsqueda de eficiencia y efectividad.

Esta es una de las razones por las que Cisco es considerado internamente como el "cliente cero" del cual las áreas de desarrollo de producto aprenden y desarrollan capacidades de ciberseguridad en base a las demandas de la propia empresa como cliente interno.

La visión de nuestro CISO

Steve Martino

En términos de tecnologías, no hay soluciones mágicas, pero Martino dejó bien claro que es fundamental buscar aquellas que brindan visibilidad en lo que está ocurriendo en todos los entornos de red. Al fin, “sabemos que las amenazas se comunican a través de la red”, dijo.

¿Qué piensa Steve acerca de los usuarios como eslabón de la cadena de ciberseguridad? Como parte de su filosofía, no cree que haya que provocar alarmismo generalizado en los empleados sino, en cambio, acciones de concientización y educación personalizadas, basadas en cada rol. Luego, asumir que los incidentes van a ocurrir de todos modos, basando su plan en un “95/5”: proteger el 95% de las amenazas y lidiar con el 5% restante. En ambos casos, la clave está en la construcción de una arquitectura tecnológica adecuada con sus políticas y procesos de ciberseguridad.

– ¿Cuál es la mejor inversión que ha hecho? – preguntamos. Las personas, respondió. Y nos habló con orgullo del equipo que lo acompaña hace años, que son el talento necesario para que funcione su estrategia.

A modo de cierre

Como responsable de seguridad de una organización, sea o no de la magnitud de Cisco, ¿qué podemos tomar del mensaje de Steve? Es indudable que hay que comenzar por entender el negocio, las regulaciones y riesgos que lo atraviesan y a partir de allí trazar un camino. Las personas son un pilar fundamental, es imprescindible educar y concientizar. Respecto a la tecnología, es necesario construir una arquitectura de seguridad unificada que permita automatizar la detección y protección de amenazas, ya que es la única manera de poder hacer frente a las amenazas a las que estamos expuestos en un tiempo razonable. Como se ve en RSA, hay cientos de fabricantes de ciberseguridad, todos ofreciendo algo bonito, brillante, que prometen más o menos las mismas cosas. Ninguno tiene las soluciones para cubrir todos los gaps, pero tal vez hay solo una compañía con una arquitectura de red segura que es efectiva, abierta y automatizada y los profesionales de seguridad que trabajan junto a los clientes para ayudarlos a atravesar el desafío

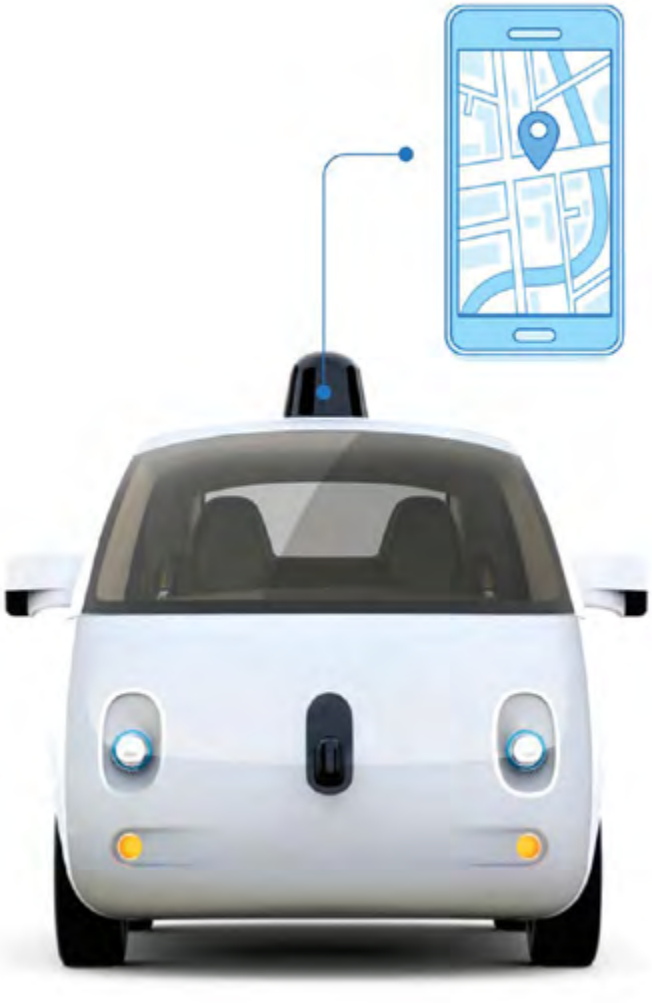
Las cinco claves de Steve Martino

1. **Habilitar el negocio en forma segura.**
2. **Evitar la “ciber-fatiga”**
3. **Proteger el 95% de las amenazas y lidiar con el 5% restante.**
4. **La mejor inversión son las personas.**
5. **Personalizar las acciones de concientización y educación.**

Columna

Ciberseguridad en vehículos autónomos

por **Gonzalo Zabala**
Centro de Altos Estudios en Tecnología Informática
Universidad Abierta Interamericana



Google Koala

Imaginemos cómo sería si cada vez que subimos a un ascensor temiéramos que se descontrole y nos deje caer al vacío. O para ser menos dramático, ¿cómo sería la sensación de quedarnos parados frente al lavarropas durante todo el lavado verificando si la tarea que realiza es la correcta?

Una de las condiciones que debe cumplir un sistema automático para que nos entreguemos en sus manos, es que nos brinde confianza. En el caso del lavarropas, seguramente no nos preocupa (demasiado) el efecto de sus fallos. Pero en el piso 24, si nos detenemos a pensar que el ascensor puede ser hackeado, las cosas se ponen más complicadas.

Mientras avanza el desarrollo de vehículos autónomos, el tema de la seguridad se convierte en un factor fundamental. Si esa máquina fuera un compartimiento estanco, sin ningún tipo de conectividad, los parámetros a controlar serían más acotados. Pero es imposible pensar en un vehículo que no necesite información de la red, como estado del tránsito, comunicación con otros vehículos autónomos, conexión con sistemas de señalización y hasta ciertos tipos de procesamiento que utilicen bases de datos en la nube.

De esta manera nos enfrentamos a dos riesgos de diferente magnitud: por un lado, la posibilidad de que puedan acceder a datos personales del dueño del vehículo, como trayectos habituales, viajes futuros y otros. En este caso, nada muy diferente a lo que pueden encontrar en nuestros smartphones. El problema grave es el otro riesgo: que en forma externa puedan tomar control del vehículo. Allí pueden ocasionar consecuencias muy graves no sólo para sus ocupantes sino para todo el ambiente que lo rodea.

Es por este motivo que los desarrolladores han comenzado a aislar los sistemas críticos para reducir los efectos posibles de un hackeo. El desarrollo de nuevos protocolos *ad-hoc* permiten asegurar este aislamiento. El paso que faltaría es definir un estándar que haga más robusto el sistema de seguridad, que no necesite de interfaces posteriores de adaptación que abra nuevas puertas de entrada a los ataques, y esencialmente, que ponga más cerebros a pensar en la misma dirección. Lamentablemente, no todos están actuando de esta manera. No sería la primera vez en la industria que la ambición de estar primero en la fila arrastre al colapso a muchos fabricantes, y por qué no, a vehículos con sus ocupantes dentro. Esperemos que no sea así en este caso

Ciberseguridad presente en Cisco Live

Emanuel Almeida,

Cisco Talos, sede de San Pablo, Brasil.

Talos se divide en cinco áreas clave:
Detection Research (análisis de malware y vulnerabilidades para diseñar el código capaz de detener las amenazas en todos los dispositivos de seguridad de Cisco).
Threat Intelligence (correlación y seguimiento de amenazas).
Engine Development (mantenimiento y actualización de los motores de inspección para que puedan detectar amenazas emergentes).
Vulnerability Research & Development (diseño de las herramientas y metodología para identificar ataques de 'día cero' y brechas de seguridad en plataformas y sistemas operativos que utilizan los clientes de Cisco).
Outreach (investigación, identificación y divulgación de nuevas tendencias y técnicas de los ciberdelincuentes).
En nuestra conversación, Emanuel invitó a quienes se ocupan de seguridad cibernética en instituciones públicas y privadas a conocer la investigación en desarrollo de Cisco Talos destinada a sistemas de seguridad, enfocada específicamente en la protección de infraestructuras críticas, por ejemplo, servicios públicos que requieren mantenerse sin interrupciones, y también a sus aplicaciones para las industrias.

Maximiliano Scheinkman

Ciberseguridad y juegos.

Vann Walters

Micro entrevista, Vicepresidente de Ciberseguridad América, Cisco.

Cristopher Leach,

Senior CISO/CSO Advisor, Cisco.

-La seguridad está cambiando muy rápidamente. En mis comienzos no había tantas oportunidades de crecer, ni de mantener un alto nivel de seguridad como ahora. Nosotros queremos avanzar con nuestros programas, pues Cisco tiene muchas opciones diferentes para ayudar en este aspecto.
Cuando yo empecé como ejecutivo de seguridad informática, hace casi veinte años atrás, no había tantas herramientas para combatir los virus informáticos que circulaban entonces. Los ataques informáticos cambian, evolucionan, y nosotros como responsables todavía pensamos como pensábamos entonces. Precisamos cambiar nuestra mentalidad, y evolucionar también. Tenemos que avanzar con nuestros mensajes, con nuestros programas, con nuestra arquitectura, y conectarnos de equipo a equipo para evitar los virus que estamos enfrentando hoy en día.

Ghassan Dreibi,

Security Director, Cisco para América Latina.

-Nuestro equipo para América Latina está creciendo mucho. Estamos organizados y dedicados, comprometidos con nuestros clientes para brindarle seguridad informática, poniendo a su disposición recursos y personal especializado. Incorporamos a nuestra región a responsables de seguridad con experiencia en el mercado de Estados Unidos, para que compartan sus conocimientos, tanto en ciberseguridad como en inteligencia cibernética. Más conocimiento permite tomar mejores decisiones, y elegir los equipos óptimos que necesita cada empresa. Vamos juntos a hacer posible la ciberseguridad en América Latina.

Ghassan Dreibi y Christopher Leach

Micro entrevista

The bridge to possible