WORLD COMPLIANCE

MAGAZINE

Nº 1 CIBERSEGURIDAD- World Compliance Magazine - Octubre 2022

World Compliance Magazine es un proyecto de la World Compliance Association y Women in a Legal World, que tiene por objetivo conocer y comparar la visión de diversos profesionales de diferentes países sobre materias que giran en torno al compliance.

Nº1 CIBERSEGURIDAD

WLW
WOMEN IN A LEGAL WORLD

WORLD® COMPLIANCE ASSOCIATION

PRÓLOGO

Me complace presentar el primer número de este nuevo Proyecto de la World Compliance Association. Han sido y son muchas las iniciativas y los trabajos de nuestros Comités Técnicos y de nuestros Capítulos, que buscan concienciar en temáticas nuevas y de actualidad inernacional, apoyados en grandes expertos.

Así, hace unas semanas, hacíamos público Paideia, un proyecto educativo y, a los pocos días, presentábamos la puesta al día de la Guía de Derecho Comparado sobre responsabilidad penal de las personas jurídicas.

Hoy tengo el honor de presentar este primer número de la revista bimensual World Compliance Magazine, un compendio de visiones sobre un tema de absoluta actualidad y en estado de cambio permanente, que estará ya siempre entre nosotros, la ciberseguridad.

La ciberseguridad, es ya un fenómeno común, en el que, desde la escuela, tenemos que formar a nuestras futuras generaciones. Las organizaciones empresariales son conscientes de lo que está en juego a la hora de aplicar y perfeccionar sus protocolos y las medidas de seguridad frente a los ataques informáticos Qué decir de las grandes corporaciones, de las infraestructuras críticas, de la enorme transcendencia de la protección de datos, y de la de neutralizar los, cada vez más comunes, robos de identidad.

Leyendo a estos grandes expertos internacionales, sacamos conclusiones transcendentales para nuestra educación, nuestras inversiones y para la coordinación entre Compliance y CIFOS. Pero sobre todo, para la educación, desde la escuela hasta la empresa y en todos los órdenes de la vida.

Espero que estas entrevistas de expertos nos sirvan a todos para avanzar en este tema esencial.

Estamos ya preparando, con muchas ganas, el próximo número, que versará sobre protección de datos.

Desde la World Compliance Association estamos abiertos a recibir sus propuestas y a trabajar a su lado para ofrecerles todo lo que sea útil, en este mundo cambiante. Esperemos que sea también un mundo cada vez más transparente y humano.

Diego Cabezuela Sancho.
Presidente World Compliance Association.

G A _ P
Gómez-Acebo & Pombo
Moody's ANALYTICS
EQS GROUP
SGR COMPLIANCE

Patrocinadores WCA

Nº1
CIBERSEGURIDAD

WORLD COMPLIANCE
MAGAZINE

CONTENIDO

5 **ALEMANIA**
MICHAL VICAN

7 **ANDORRA**
NÚRIA VILADRICH GENÍS

9 **ARGENTINA**
MARTÍN FRANCISCO ELIZALDE

11 **CHILE**
FACUNDO JAMARDO

13 **COSTA RICA**
FABIÁN SOLÍS

15 **ECUADOR**
GABRIEL EDUARDO CUESTAS FLORES

17 **ESPAÑA**
MARÍA JESÚS HERNÁNDEZ-ELVIRA

20 **GUATEMALA**
CARLOS GIOVANNI GUZMÁN DE LEÓN

22 **ITALIA**
JANICE CARLING

24 **MÉXICO**
JOSE DÍAZ CUADRA

26 **PANAMÁ**
FELIX NEGRON

28 **PERÚ**
MANUEL ALEXANDER GARCÍA RIVAS

30 **PORTUGAL**
MARIA CANO HERNÁNDEZ

33 **REPÚBLICA DOMINICANA**
DANIEL PUJOLS

35 **SUECIA**
ANDREW TABONA

37 **VENEZUELA**
LISANDRO BAUTISTA

ALEMANIA

MICHAL VICAN

1. Has the management of cybersecurity changed after the pandemic?

Even before the pandemic, cyber-attacks had been increasing across many industries. We can say the pandemic accelerated this somewhat, but even without it the risks would have been there. Even without the pandemic, cybersecurity would still be assessed as one of the top risks the companies currently face.

Of course, because many employees moved their workplaces from offices to their homes, cybersecurity at home got more into focus. Home workplace are probably here to stay, so if some companies were relying on quick solutions, going forward they will need to think about a long-term concept and build a reliable and of course cyber-secure infrastructure.

2. What are the main cybersecurity risks in compliance models?

The main risks are:

- Financial risk: If a company gets hacked and all its data encrypted, a request to pay ransomware will be made by the hackers. In case the company does not find any other option but to pay without a recourse from the insurance policy, this will have a material impact on company's bottom line.

- Business continuation: Between the company's data getting compromised by hackers and restoring the data from backups or by receiving the encryption key, a lot of time can pass during which the company will not be able to operate and lose revenue and customers' and suppliers' goodwill. In the worst-case scenario, when the backups were compromised as well and the company cannot afford to pay the ransomware, this could be a threat to the company as a going concern.

3. What basic cybersecurity measures should companies implement to prevent cyberattacks?

There are several measures companies need to implement to prevent cyberattacks as well as possible. We can think of them as the low hanging fruits. By implementing them, companies already get a good level of protection. These measures are:

-Dedicated person for security, firewall and intrusion prevention and detection rule.

It starts in HR with hiring. IT professionals with enough expertise and experience, who know what they are doing, but also know the company, the industry and its risk, are really the corner stone of any security efforts. These colleagues then take care of such measures as setting up a firewall, intrusion prevention and detection rules and maintain them.

- Strong password, Multi factor authentication.

Everyone has heard of using strong passwords, with appropriate length, special characters, which need to be changed regularly etc. This is still considered best-practice. At the same time, companies need to make sure their employees are able to manage their passwords.

As an addition, it is standard now to use multi-factor authentication. At least, if the login attempt is coming from unexpected destination or source. This prevents malicious logins if the password has been compromised in one way or another.

- Awareness

Training of all employees is a very basic measure, which should never be underestimated. Employees can still be a weak link in any security model. This is because for attackers, the employees are the easiest to

> Financial risk: If a company gets hacked and all its data encrypted, a request to pay ransomware will be made by the hackers. In case the company does not find any other option but to pay without a recourse from the insurance policy, this will have a material impact on company's bottom line"

target. A lot of it are not only complicated IT tricks, but use of psychology, human weaknesses, inattentiveness, pressure and similar things.

-Patching

New vulnerabilities in software are constantly getting discovered, some before an exploit has been developed, but often the exploit is quicker. If such a vulnerability remains open for longer time, after an exploit has been made public, the risk can become too high. Here again, an experienced IT security expert can make the call if a patch can be installed instantly, or more analysis is needed so that business processes can continue smoothly.

-Business Continuity Management

Business continuity plays an important if something indeed goes wrong. Companies must have plans to react in such situations. Typically, in cyber-security, this would mean scenarios such as, e.g., malicious software was sneaked in and data got encrypted or power supply was cut off. Ideally, these plans are kept up-to-date and tested regularly.

4. What can be done from the department of compliance to reduce the number of security breaches?

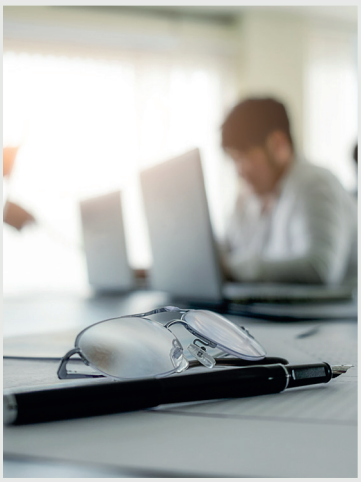
I can see a role for compliance department to play especially in supporting the security awareness efforts. This means helping in organizing the trainings, e-learnings or releasing materials which teach and remind the employees of the necessary controls to adhere to.

Another important role is to liaise in releasing security policies, which are appropriate to manage the risks, and are also calibrated well for the maturity of companies' security program and thus can be easily implemented.

5. What are the next challenges in cybersecurity?

When the conflict in Ukraine started approximately three months ago, there was a lot of fear that cyber-attacks will increase and become a part of the new warfare. So far, the most massive attacks have not occurred or are at least have not been made known to broader public, but of course this can easily and quickly change.

Otherwise, one can say that the problems we have experienced over past few years, will become worse. Number of ransomware attacks will increase, higher sums for ransom will be demanded and cyber insurances policies can become too expensive. Supply chain attacks have also shown that companies need to be mindful of how to react when their suppliers are not able to provide the IT services for some time due to cyber-attacks. This is connected to vulnerabilities management, will also keep playing an important role. Last year, there was a high threat scenario with the Log4J zero-day vulnerability. It showed that many systems used by top companies had been affected. Huge efforts were made to prevent any exploits, but a feeling has remained that similar scenarios can easily be repeated in future.



MICHAL VICAN

Michal Vican is the information security officer at Primagas Energie GmbH, a Germany-based supplier of off-grid energy in form of LPG. Besides information security, he is also responsible for data protection and compliance management. He joined his current employer in 2018. Previously, he spent over 7 years at a Big 4 company and was based in offices in Germany and Czech Republic. He also participated on international projects abroad. His professional focus there was consulting clients from various industries, e.g., life sciences, automotive, banking sector, on compliance projects and investigations. He has a law degree from Charles University in Prague. He is a member of German Association of Compliance Managers.

ANDORRA

NÚRIA VILADRICH GENÍS

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

Efectivamente, la pandemia supuso un cambio de criterio en la forma de trabajar, en el sentido que obligó a las empresas al uso de nuevas tecnologías y aplicar el método de teletrabajo, que tuvo efectos significativos en las infraestructuras IT, aumentando así la posibilidad de sufrir ataques informáticos.

El hecho de realizar conexiones a distancia a los sistemas de la información de la empresa, se hicieron patentes nuevas vulnerabilidades que comportaron que las empresas se replanteasen la gestión de la ciberseguridad para gestionar los riesgos.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

Para un modelo de compliance es muy importante conocer cuáles son los principales riesgos y amenazas para poder aplicar medidas de seguridad que permitan afrontarlos y reducirlos. En este sentido, podríamos decir que los principales riesgos, a día de hoy son:

1. Robo de credenciales: sustraer credenciales puede implicar un abanico de acciones tales como acceso a cuentas bancarias, robo de secretos de empresa y bases de datos…

2. Estafas y suplantaciones de identidad: tanto de delincuentes que suplantan la identidad de directivos para engañar a empleados y obtener así claves y códigos para realizar transferencias bancarias; como delincuentes que suplantan la identidad o se hacen pasar por empresas y solicitan datos personales tales como números de cuenta, seguridad social…

3. Ataques botnet: a través de Botnets los ciberdelincuentes convierten los equipos y servidores en "zombies" para evitar ser rastreados y de esta manera pueden llevar a cabo otras acciones ilícitas como el envío de correos masivos o ataques de denegación de servicio (DDos).

4. Ramsomware: que significa el secuestro de información mediante un malware que encripta el contenido de unidades, discos duros y servidores. Los ciberdelincuentes han mejorado algoritmos de encriptación y utilizan sistemas de pago –por ejemplo, la criptomoneda- que evita el rastreo posterior. Por lo que los delincuentes ven una cierta impunidad en sus acciones.

5. Ataques a servidores: acceden a los servidores aprovechando brechas de seguridad en los mismos y de esta manera sustraen datos allí contenidos.

6. Deepfakes: es un sistema de suplantación de identidad a través del cual el ciberdelincuente crean un vídeo sustituyendo la cara de una persona por otra.

7. Amenazas asociadas al teletrabajo.

8. Amenazas internas dentro de la empresa.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

Cualquier empresa debería contar una buena gestión del riesgo, siendo que 1) deberían conocer los activos de información y servicio, así como datos personales que tratan; 2) identificar los riesgos y amenazas y; 3) aplicar las medidas técnicas y organizativas para evitar o mitigar los efectos negativos de la materialización de un riesgo. En este sentido, las empresas deberían aplicar como mínimo, las siguientes medidas:

1. Disponer de contraseñas seguras y actualizarlas periódicamente. Además, para sistemas más críticos, y atendiendo a los robos de contraseñas, disponer del doble factor de autenticación.

2. Realizar copias de seguridad para poderse recuperar de cualquier

NÚRIA VILADRICH GENÍS

Núria Viladrich Genís es socia de la empresa familiar española Tarinas Law & Economy y CEO de empresa andorrana Andorra Tarinas. Se formó como experta en Derecho Digital cursando el Máster en Auditoria de Entornos Tecnológicos y el Máster de Propiedad Intelectual e Industrial (ICAB). La defensa de derechos en el ámbito de la tecnología es su pasión, motivo por el cual, es reconocida por su labor práctica en Protección de Datos y Ciberseguridad.
Actualmente, Núria Viladrich y su equipo de Andorra Tarinas, emprenden con mucha ilusión el camino como miembros del comité de la WCA Andorra, aportando al país todo su conocimiento en cumplimiento normativo en el ámbito de la tecnología e innovación.

incidente que afecte a la disponibilidad de la información.

3. Que los sistemas estén actualizados en todo momento, aplicando continuamente los parches y mejoras de seguridad de los fabricantes.

4. No exponer servicios a internet, por cuanto pueden suponer un agujero de seguridad abierto.

5. Cifrar los dispositivos (ordenadores, tabletas, móviles, discos duros, copias de seguridad…) para asegurar la confidencialidad de la información.

4. ¿Qué se puede hacer desde el departamento de Compliance para reducir el número de brechas de seguridad?

Para reducir el número de brechas de seguridad se deben seguir los siguientes pasos:

1er paso: establecer una Política de Seguridad de la Información en la que se describan los elementos clave, tanto humanos como organizativos, tecnológicos y documentales, que las entidades deben aplicar con la finalidad de proteger la información, información durante todo su ciclo de vida –es decir, desde la creación/recepción, procesamiento, comunicación, transporte, almacenamiento, difusión y hasta la eventual supresión o destrucción.

2do paso: gestionar el riesgo. Las empresas deben seleccionar las medidas para gestionar el riesgo con el fin de salvaguardar la disponibilidad, confidencialidad, integridad. Para ello pueden utilizarse estándares de seguridad ya existentes en el mercado como la norma ISO 2700, y en el caso de entidades públicas destacamos el Esquema Nacional de Seguridad (ENS).

3er paso: realización de protocolos y procesos internos, a través de los cuales se establezcan las medidas técnicas que debe y aplica la empresa, entre las que destacamos el uso de contraseñas seguras y segundo factor de autenticación, copias de seguridad, actualización de sistemas, cifrado de dispositivos, gestión de incidencias, adquisición de componentes, entre otros.

4to paso: concienciación y formación a los trabajadores. Las personas con responsabilidad en el uso, desarrollo de operaciones o administración de sistemas TIC deben recibir formación para la utilización segura de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación la debería recibir el trabajador antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o responsabilidad en el mismo. Asimismo, todo el personal debe ser formado e informado sobre sus deberes y obligaciones en materia de seguridad, esencialmente mediante los procedimientos de seguridad que en cada caso sean procedentes y mediante la normativa de uso de los activos.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

Según las informaciones extraídas de Incibe o BeyonTrust, entre otras entidades especialistas en ciberseguridad, los ciberataques en las redes corporativas, según estadísticas, en 2021 han aumentado un 50% frente al 2020, y parece que no tiene fin.

Estas entidades destacan las siguientes tendencias:

- Debido al aumento del teletrabajo, las vulnerabilidades de conexiones externas aumentaran y se deberá aplicar medidas de seguridad como la integración de VPNs o de firewalls, entre otras estrategias adecuadas al riesgo.

- Cada vez más vamos a encontrarnos con accesos basados en Biometría conductual a través de la inteligencia artificial.

- Disponer de un equipo interno o externo dedicado al Compliance Digital, encargado de la seguridad de la información corporativa.

- Se está creando, a nivel europeo, una solución para proteger a las empresas del volumen creciente de sofisticadas amenazas y riesgos para los datos en la nube, como por ejemplo Next Generation Secure Web Gateway (NG SWG).

- Antes de contratar a un proveedor externo, la entidad deberá asegurarse que éstos cumplen con las medidas técnicas y organizativas exigidas por la normativa vigente.

ARGENTINA

MARTÍN FRANCISCO ELIZALDE

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

Es difícil hacer una generalización. La pandemia tuvo efectos "democráticos"para casi todos los usuarios: trabajo remoto, descentralización súbita de las arquitecturas centrales de seguridad, aumento exponencial de las vulnerabilidades y de los ataques.

Pero con el tiempo, en la práctica la respuesta no fue uniforme. Los sectores más regulados, como finanzas, salud y seguros a partir de la pandemia quizás aumentaron su inversión en herramientas de seguridad. No me queda tan claro si lo hicieron en capacitación. El resto, pasada la crisis, no tanto - ni en herramientas ni en capacitación. Me viene a la cabeza en este sentido el sector de las instituciones educativas, tan liberales a la hora de compartir información, con una rotación muy rápida de usuarios, mucha diversidad en los equipos y un legendario nivel de descuido en algunas de las áreas que las componen. Y con un botín de datos comerciales, de salud y financieros muy valioso, por cierto.

En el área de infraestructuras críticas, a raíz de la notoriedad de algunos ataques y más de cerca, por las amenazas percibidas tras la invasión rusa perpetrada en Ucrania, un sentido de urgencia parece haberse instalado. Cuánto durará y cuál será su real impacto, está por verse. Tras cada "pico" de aprehensión, parecerían volver los viejos hábitos de descuido en este sector, es decir el desorden en las políticas de inversión en seguridad, un déficit estructural en capacitación y la "herencia" obsoleta en materia de sistemas y programas.

Párrafo aparte merece el cuidado (o no) del descomunal volumen de datos personales que recolectaron y trataron los Estados soberanos y sus agencias durante la pandemia. No he escuchado mucho acerca de la limitación de su tiempo de almacenaje, sus condiciones de seguridad y las políticas de eliminación que se proponen al respecto; con la excepción de las normas europeas al respecto, como de costumbre.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

Es conveniente que los modelos pongan énfasis en la seguridad de la información recolectada en cada denuncia y luego, en cada investigación. Con protocolos para garantizar la legalidad del acceso por parte del empleador a la información contenida en servidores, celulares y equipos informáticos de los integrantes de la organización y su posterior preservación forense. Mi experiencia me sugiere que no siempre se atiende este aspecto, poniendo en riesgo la integridad probatoria de los documentos electrónicos sobre los que se asienta una investigación interna, cuando luego se los presentan en un tribunal.

El área de compliance también debería involucrarse junto con IT y con el CISO en la formulación del documento de uso de herramientas digitales, que es la matriz donde se establecen las condiciones y límites del acceso y el control por parte del empleador sobre los miembros de la organización.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

La receta no es sorprendente: (posiblemente será por eso que raramente se sigue) buenas prácticas, herramientas de

> El área de compliance también debería involucrarse junto con IT y con el CISO en la formulación del documento de uso de herramientas digitales, que es la matriz donde se establecen las condiciones y límites del acceso y el control por parte del empleador sobre los miembros de la organización"

seguridad integradas en una arquitectura central y capacitar para alcanzar una cultura de seguridad que permita seguir esas buenas prácticas y usar bien esas herramientas.

Otra cosa, los incidentes y las violaciones de seguridad (son dos conceptos bien distintos) no se" evitan", solo se limitan, en el mejor de los casos, sus daños. Entonces, ¿para qué seguir las buenas prácticas y haber hecho lo que corresponde, si al final del día no consige evitarse el incidente o la violación de seguridad? La respuesta es para limitar en esos casos la responsabilidad del Directorio y de la Alta Gerencia. Y para defender con éxito a la empresa en una ola de acciones civiles y penales de los damnificados, evitar pago de multas astronómicas y librarse de un daño reputacional severo. No es poco.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

Mucho: trabajar con el CISO para crear una cultura de seguridad informática. Eso sí que es novedoso: el área de compliance siempre trabaja con la de RRHH: es hora de ampliar el espectro.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

Creo que la amenaza más fuerte viene por el lado de las infraestructuras críticas. Pero, en general, no veo ataques extremadamente sofisticados, veo organizaciones descuidadas. Un ejemplo: el ataque a la pipeline en la costa Este de USA fue super promocionado. El estado de descuido de la empresa, que ameritó sanciones hace unos días, fue menos publicitado. Y en eso me hace acordar a uno de los primeros ataques: el de Target. Poco cambió desde entonces...

Otra vez, el reto más importante es formar más cultura de seguridad y ejercitar más auditoría del cumplimiento de esa cultura. Y lograr más interacción de compliance con el CISO (a quien, por una vez, sería bueno que Directorio le haga caso...)

MARTÍN FRANCISCO ELIZALDE

Martín es abogado, egresado de la Universidad de Buenos Aires, Argentina, y tiene un Master en Leyes (LLM) con major in Finance & Banking, de la American University, Washington DC. Fue certificado en EDiscovery por Kroll Ontrack, Minneapolis, Minnesota.

Es Founding Partner en Foresenics Prueba Digital, firma de investigaciones internas y preservación de evidencia electrónica. Es Senior Consultant en Cingitel Argentina y fue Senior Consultant y contractor en The Berkeley Research Group LLC, Alvarez & Marsal LLC y Kroll Ontrack, actualmente lo es de JS Held LLC. Dirige procedimientos de investigaciones informáticas en litigios, cuidado de la privacidad y seguridad informática en Latam, EU y USA.

Es profesor de la Universidad de las Américas en Quito, Ecuador (Facultad de Ingeniería) en su postgrado de Seguridad Informática.

CHILE

FACUNDO JAMARDO

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

La pandemia nos trajo la urgencia transformar, de la noche a la mañana, las capacidades tecnológicas, las formas de operar y hasta los modelos de negocio para permitir el acceso de nuestros clientes, empleados, colaboradores y proveedores desde cualquier parte del mundo para asegurar la continuidad de negocio. Todo esto, ejecutado de la noche a la mañana.

Sin embargo, muchos de estos cambios llegaron para quedarse, y lo que fue temporal se debió transformar en una capacidad (negocio/proceso/tecnología) permanente. Por esta razón, las áreas de ciberseguridad debieron acelerar el desarrollo de sus capacidades para acompañar adecuadamente al negocio/operación.

Esta transición no fue fácil para los CISOs y, en muchos casos, no ha terminado aún y requiere incrementar los niveles de madurez de sus procesos internos para asegurar una adecuada protección de los activos de la organización.

A esto se suma la escasez global de profesionales del área de ciberseguridad, que obliga a las organizaciones a buscar alternativas más creativas para resolver los problemas (a través de la automatización o tercerización de procesos).

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

Existen múltiples marcos regulatorios que impactan de manera significativa en la ciberseguridad en la mayoría de las organizaciones actuales:

- Privacidad y protección de datos personales:
  - o Riesgo de robo o fuga de datos personales que afecten la privacidad de las personas.

- Ciberseguridad en la industria financiera
  - o Riesgos de fraudes a raíz del rápido avance en el proceso de digitalización y transformación de las operaciones financieras.

- Ciberseguridad en infraestructuras críticas
  - o Riesgo de afectación en la disponibilidad de activos que soportan la operación de infraestructuras críticas.

Los ataques de ransomware, que crecieron significativamente durante los últimos 2 años, tienen la capacidad de incrementar estos riesgos y fuerzan a las organizaciones a estar preparadas para poder mitigar el impacto.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

En el contexto actual, es muy importante conocer la superficie de ataque a proteger, es decir, la totalidad de recursos que soportan la operación de la organización. Los cambios transformación digital de los últimos años hizo crecer significativamente estos recursos, al punto tal que lo convierten en una tarea casi imposible en todas las industrias (y la complejidad va en aumento).

A raíz de esto, las organizaciones y regulaciones incorporan el concepto de "secure by design" que implica el análisis de riesgos, definición y aplicación de controles, desde el momento mismo de la concepción de cada nuevo proyecto, lo que simplifica y reduce el esfuerzo de aplicación de controles.

Adicionalmente, creemos que es imprescindible contar con capacidades de identificación, correlación y respuesta ante eventos e incidentes de seguridad sobre todos los activos tecnológicos de la organización, inclusive aquellos activos que residen fuera de las redes propias de la organización (ej: recursos cloud).

Finalmente, es de vital importancia tener capacidades definidas, implementadas y probados para asegurar la continuidad de la operación tecnológica ante eventos de ataques o desastre. En este mismo sentido, vimos que las simulaciones de ataque cibernético proporcionan una base excelente tanto a las áreas operativas como ejecutivas para agilizar la ejecución de estas capacidades.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

Como vimos, la transformación tecnológica en muchos casos sobrepasó las capacidades de gestión y supervisión de ciberseguridad, por esto creemos que las áreas de compliance pueden ser un aliado en la gestión de ciberseguridad ya que pueden participar activamente en la evaluación de la correcta ejecución de los procesos de seguridad en cada nuevo proyecto o iniciativa de negocio, así como también verificar que los activos críticos de tecnología cumplan con las medidas de seguridad establecidas por las áreas de seguridad.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

Durante el COVID-19, los negocios tuvieron que adaptarse a la disrupción.

Las organizaciones implementaron nuevas tecnologías orientadas al cliente, buscando apoyar el trabajo remoto y mantener abierto el canal al mercado.

Pero la velocidad del cambio tuvo un precio: muchas empresas no involucraron al equipo de ciberseguridad en el proceso de toma de decisiones, esto dio paso a nuevas vulnerabilidades dentro de un entorno muy dinámico y vital para el negocio

Según nuestro último estudio global de seguridad (GISS) (https://www.ey.com/en_gl/giss) realizado durante 2021, se identificaron 3 grandes desafíos a los que se enfrentan los CISOs:

I. El área de ciberseguridad está seriamente desfinanciada, pero la financiación es más necesaria que nunca ya que:

- 77% de las compañías vio un incremento en el número de ataques disruptivos en el último año.
- 43% está más preocupado que nunca por la habilidad de la organización de gestionar una ciber-amenaza.
- 56% no está seguro si las defensas de su organización son adecuadas para contener las nuevas técnicas de ataque.
- 67% de las compañías no tiene certezas acerca de la capacidad de defenderse y recuperarse ante un ciberataque a su cadena de suministros.
- 58% manifiesta que los cronogramas no permitieron evaluaciones de ciberseguridad adecuadas en los nuevos proyectos.

II. La fragmentación regulatoria es un dolor de cabeza, creando trabajo adicional y problemas de recursos

- 49% manifestó que el cumplimiento de regulaciones puede ser la parte más estresante de su trabajo, y se espera más fragmentación.
- Las organizaciones multinacionales tienen el desafío de gestionar múltiples regulaciones superpuestas con sistemas integrados donde la información fluye por toda la organización y por todo el mundo.
- El entorno de cumplimiento es cada vez más complejo, con regulaciones a nivel nacional, regional y sectorial por industrias. Esto incrementa significativamente el esfuerzo de cumplimiento de los CISOs.

III. La relación de los CISOs con el resto de la organización es débil, lo que dificulta implementar la seguridad por diseño.

- El 76% manifestó que sus pares de las áreas de negocio no los incluyen en las iniciativas hasta después de finalizada la planificación.
- Para aportar el mayor valor posible, los CISOs necesitan analizar y aconsejar desde el inicio de los nuevos proyectos, pero la falta de solidez en la relación con las áreas de negocio dificulta este proceso.
- 56% dijo que los equipos de ciberseguridad no siempre son consultados a tiempo.
- 54% manifestó que las áreas de negocio evadieron controles para facilitar el trabajo remoto.
- A su vez, el 44% sugiere que a sus equipos les cuesta aconsejar sobre ciberseguridad en términos comerciales. Sólo el 29% dijo que puede cuantificar en términos financieros la efectividad de las inversiones en ciberseguridad.
- De manera general, los CISOs manifestaron que el negocio los identifica con fortalezas tradicionales como controlar riesgos, sin embargo, no los percibe como un socio estratégico.

FACUNDO JAMARDO

Cyber Security Services leader at EY Chile (Líder en servicios de Ciberseguridad en EY Chile). Facundo cuenta con más de 22 años de experiencia ayudando clientes en Latino América, a mejorar sus capacidades de ciberseguridad, actualización de estrategias, control de vulnerabilidades, protección de información, implementación de nuevos controles y herramientas de mitigación de ciber-riesgos, así como también asistencia en la evolución de procesos de gestión y en el cumplimiento a múltiples regulaciones.

Es ingeniero en computación de la Universidad Nacional de Tucumán y cuenta con una especialización en redes de datos del Instituto Tecnológico de Buenos Aires.

COSTA RICA

FABIÁN SOLÍS

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

Asunto de perspectiva. La existencia o no del cambio en la gestión podría depender del giro de negocio y su alta dirección. Intereses diferentes dependiendo del posicionamiento en el ecosistema o cadena de valor específicos. Esquemas de aseguramiento de la información más o menos sofisticados.

Por ejemplo, algunos han mantenido sus altos estándares y controles de seguridad que tenían desde antes de la pandemia, implementando proyectos con esencia de mejora continua; otros han invertido por primera vez en asuntos de seguridad, en atención al entorno (enfoque preventivo); hay quienes han tenido que invertir a la fuerza luego recibir impactos negativos no planeados (enfoque reactivo), y hay quienes a la fecha no han invertido de forma consciente en recursos relacionados, por dar énfasis a otras prioridades, por falta de interés o por tener todavía desconocimiento absoluto del alcance del tema, entre otros motivos.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

Los riesgos podrían ser muy variados. Podrían tener diferente naturaleza dependiendo de factores como el giro de negocio de la organización, industria donde opera, jurisdicciones donde opera, enfoque(s) del modelo de compliance (por ejemplo, qué áreas del Derecho cubre y cuáles son los objetivos y metas del modelo diseñado e implementado).

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

Paso 1. Identificar los activos de la empresa y clasificarlos según su relevancia y criticidad. Activos tangibles e intangibles. Ejemplos de activos tangibles: colaboradores con puestos de confianza quienes poseen información confidencial y sensible de la empresa, instalaciones físicas (oficinas, bodegas) y soportes de información (servidores físicos, computadoras, teléfonos móviles, tabletas, dispositivos USB). Ejemplos de activos intangibles: bases de datos de clientes y colaboradores, contratos comerciales suscritos con clientes, proveedores y aliados comerciales, información técnica de productos y servicios, planes y estrategias de negocio, usuarios y contraseñas.

Paso 2. Identificar las amenazas a las que están expuestos cada uno de los activos identificados. Inicialmente se podría dar prioridad a los activos más relevantes y se podrían considerar amenazas como las siguientes: amenazas provenientes a la naturaleza, de origen industrial, amenazas por defectos o deficiencias técnicas de soluciones de tecnología, amenazas por soporte técnico deficiente, amenazas causadas por personas físicas, de forma accidental o intencional (factor humano).

Paso 3. Identificar las vulnerabilidades actuales de la empresa. Debilidades propias de los activos identificados y de sus medidas de protección (en caso de que existan medidas o controles ya asignados).

Paso 4. Identificar posibles impactos negativos en los activos, tales como: impacto en la imagen o reputación corporativa, impacto en las relaciones con clientes actuales o potenciales, impacto en relaciones con sus propios colaboradores, con sus accionistas, proveedores o aliados; impacto en el diseño o implementación de iniciativas comerciales o impacto por sanciones administrativas o judiciales.

Paso 5. Estimar o calcular el riesgo: Cuál es la probabilidad de que la amenaza aproveche la vulnerabilidad y se materialice, causando un impacto negativo en la empresa.

Para realizar esta estimación es posible acudir a estándares, soluciones, metodologías o marcos disponibles a nivel internacional y emitidos por organizaciones públicas y privadas.

> Un reto de peso es la ciberguerra. Problema que ya es una realidad y podría aumentar. Sumamente preocupante y delicado. La desigualdad e intereses económicos y políticos de los países hacen de este tema algo complejo, con un alcance difícil de medir"

Este ejercicio ayudará a la empresa a identificar efectivamente cuáles son sus riesgos y qué nivel de importancia o peso tiene cada uno de esos riesgos.

La herramienta a elegir dependerá mucho de los gustos e intereses de la empresa.

Sugerencia 2. Tratar o gestionar los riesgos identificados. Iniciando por los riesgos de nivel alto, la empresa podría elegir diversos caminos, entre ellos: asumir o aceptar (y no hacer nada), mitigar, compartir, delegar o intentar eliminar del todo cada riesgo. La empresa podría asignar a cada riesgo un camino diferente (o podrían haber coincidencias).

Para esta gestión de los riesgos también existen herramientas a nivel internacional, emitidas por entidades como la Organización Internacional de Normalización, ISACA, el Instituto SANS y el Instituto de Estándares y Tecnología del Departamento de Comercio de los Estados Unidos de América.

Sugerencia 3. Actualizar el marco de gobierno corporativo y la gestión del conocimiento dentro de la empresa. Esta tarea incluiría una actualización de las políticas, procesos y procedimientos internos de la organización para reflejar el ejercicio previo realizado, a lo interno, de forma integral.

Sugerencia 4. Dar seguimiento periódico a los ajustes e iniciativas implementadas. Esto incluye validar si los resultados obtenidos concuerdan o no con lo planeado y deseado. Sin duda los cambios constantes en el entorno (comportamientos de consumo, nuevas tecnologías, aspectos regulatorios, aspectos de salud, aspectos bélicos) podrían ser motivos de cambio y actualizaciones respecto al funcionamiento de la organización.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

En caso de que la compañía cuente con un departamento de cumplimiento independiente, sería recomendable que este departamento trabaje de forma integral, coordinada y en equipo con todos los otros departamentos y secciones de la organización. Con todos los niveles jerárquicos.

Un departamento aliado importante sería el departamento de comunicación de la empresa que ayude en el diseño del mensaje y en cómo se comparte este mensaje a lo interno y externo de la compañía. Mensaje de cómo debemos protegernos, cómo nos estamos protegiendo, cómo usted, al estar ligado a nuestra empresa, debe protegerse.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

Un reto de peso es la ciberguerra. Problema que ya es una realidad y podría aumentar. Sumamente preocupante y delicado. La desigualdad e intereses económicos y políticos de los países hacen de este tema algo complejo, con un alcance difícil de medir.

El impacto de un movimiento bélico en contra de un Estado puede llegar a afectar diferentes industrias, modelos de negocio e individuos (independientemente de su clase social), a diferentes niveles.

FABIÁN SOLÍS

Fabián Solís ha asistido a compañías en asuntos de tecnología por más de 15 años. Tanto a proveedores de tecnología como a sus clientes y aliados comerciales que a menudo aparecen en el ranking Fortune Global 500, incluyendo 26 compañías de la edición 2021. Corporaciones globales y empresas emergentes basadas principalmente en Norteamérica, Europa y Asia Pacífico, con iniciativas comerciales en Latinoamérica y el Caribe. Trabajo desarrollado a partir de relaciones de confianza con sus departamentos legales, abogados internos y alta gerencia. Fabián también asiste regularmente a firmas legales internacionales para atender los requerimientos de sus clientes.

Diferentes industrias, culturas, jurisdicciones y proyectos generalmente relacionados con fusiones y adquisiciones, transacciones y contratos relacionados con tecnología, ciberseguridad, comunicaciones, tecnologías blockchain, privacidad, GRC y ESG. Fabián se unió a Aguilar Castillo Love en el año 2021 proveniente de Deloitte, donde fue Consultor Senior promotor

ECUADOR

GABRIEL EDUARDO CUESTAS FLORES

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

Por su puesto, la pandemia de Covid-19 causó que todas las organizaciones tuvieran que adaptarse a la disrupción de una forma u otra; se tuvieron que ajustar arquitecturas y prácticas para admitir cambios no planificados al trabajo remoto y mantener abierto el canal de comercialización. Pero la rápida transformación tuvo un precio alto y trajo nuevos riesgos que continúan amenazando al negocio en la actualidad, de acuerdo con la Encuesta Global de Seguridad de la Información de EY 2021, el 81% de los ejecutivos indicaron que el COVID-19 obligó a las organizaciones a eludir los procesos de seguridad.

Tras la pandemia las organizaciones necesitan una gestión diseñada a medida de la ciberseguridad para garantizar su resiliencia, pero aún tienen que abordar y gestionar los riesgos diferidos y las vulnerabilidades potenciales que se introdujeron durante sus esfuerzos de transformación durante la pandemia; esto es comprender las implicaciones de las amenazas existentes y desconocidas.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

De acuerdo con la Encuesta Global de Seguridad de la Información de EY 2021, más de tres de cada cuatro 77% representantes de organizaciones advierten que han visto un aumento en la cantidad de ataques perjudiciales, como ransomware, en los últimos 12 meses, aquí se vuelve de vital importancia la seguridad por diseño donde las organizaciones comprendan cuáles son los riesgos que los pueden afectar si se materializan y cuáles son los tipos de controles adecuados (conocer el riesgo y gestionarlo).

La industria de la ciberseguridad es en gran medida impulsada por el cumplimento o la crisis, durante el último año se ha evidenciado el aumento de ciberataques comunes, avanzados y emergentes que van desde: ransomware, métodos de ingeniería social, robo de credenciales, filtración de datos personales, phishing, estafa de CEO, APT (amenaza persistente avanzada), aprovechamiento de vulnerabilidades presentes en sistemas desactualizados y trabajo remoto, entre otros.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

Las medidas a adoptar deberán estar ceñidas a la seguridad por diseño para cada organización, donde exista un vínculo directo entre la inversión en ciberseguridad, el valor comercial y la reducción de riesgos. Como parte de las medidas básicas que las organizaciones pueden adoptar para tener la capacidad prevención, detención, respuesta y recuperación; es fortalecer su estrategia y programa de ciberseguridad pasando de un enfoque reactivo a uno proactivo que considere a la ciberseguridad desde el diseño dentro del negocio. (Política de seguridad cibernética)

Las organizaciones deberán en la medida de sus posibilidades cerrar la puerta a ciberataques, pero también deben ser consientes y aceptar que un atacante podrá ingresar en algún momento y es donde se deberá considerar una primera línea de defensa como parte de la estrategia:

- Implementar software de antivirus y firewall,
- Encriptación de comunicaciones a través de correo electrónico,
- Copias de seguridad de información en sitio alternos seguros o nube y
- Capacitación constante al personal (eslabón más débil)

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

Las brechas de seguridad no son solamente responsabilidad del personal de TI o del CISO (Chief Information Security Officer); la capacidad de trabajar juntos y mejorar el intercambio de inteligencia sobre amenazas constituye una de las armas más poderosas disponibles actualmente, pero esto implica el uso eficiente del tiempo dedicado a la ciberseguridad.

De acuerdo con la Encuesta Global de Seguridad de la Información de EY 2021, la regulación exige tiempo que los CISO no tienen que dar, uno de cada dos (49 %) advierte que garantizar el cumplimiento puede ser la parte más estresante de su trabajo. Seis de cada 10 (57%) predicen que la regulación se volverá más heterogénea, lenta y, algunos podrían decir, caótica en los próximos años. El cumplimiento se ha vuelto tan fragmentado y complejo que ahora es una distracción y carga de trabajo, los CISO tienen menos confianza en que la regulación apoye la mejora de los estándares de ciberseguridad en las organizaciones.

El área de cumplimiento deberá trabajar en volver a ser apoyo y soporte para el área tecnológica que impulse a pensar estratégicamente en la seguridad, a mantener comportamientos correctos de los usuarios en la organización, cambiar la tendencia de considerar la seguridad como una función de cumplimiento y no sobrecargar de tecnologías, políticas, etc., desde la perspectiva de controles de seguridad.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

Los próximos retos respecto a ciberseguridad tienen que vislumbrarse a nivel de procesos, personas y tecnología involucrada, donde las organizaciones se encuentren preparadas para el nuevo panorama de riesgos y conocer qué funciona, qué no y dónde se deben ahondar los esfuerzos de colaboración.

De acuerdo con la Encuesta Global de Seguridad de la Información de EY 2021, se destacan tres desafíos:

- La organización actual de ciberseguridad no cuenta con fondos suficientes: donde los procesos de asignación presupuestaria son en gran medida inflexibles, a pesar de la necesidad de respuestas ágiles frente a la volatilidad de la era la pandemia y la perspectiva de interrupción futuras, además que los presupuestos no están sincronizados con las necesidades y el talento humano es cada vez más difícil de encontrar.

- La complejidad regulatoria es un dolor de cabeza para los CISO: lo que conlleva a sólo "superar" el obstáculo de la auditoría de cumplimiento sin una perspectiva de seguridad por diseño.

- Relación de ciberseguridad con líderes se están deteriorando: los líderes empresariales están eliminando la ciberseguridad de las conversaciones vitales; Alrededor de seis de cada 10 (58%) dicen que su organización a veces implementa nueva tecnología con escalas de tiempo que no permiten una evaluación o supervisión adecuada de la seguridad cibernética.

Los actores de amenazas han alcanzado un nuevo nivel de madurez, han adoptado cada vez más nuevas estrategias, ya sea dirigiéndose a las empresas con campañas de phishing o incorporando un código de puerta trasera que les permite explotar el software comercial después de que los clientes lo hayan adquirido. Menos de la mitad (47%) de los CISO indica que entiende y puede anticipar las estrategias que usan los atacantes.

Las organizaciones deben considerar la seguridad por diseño en los proyectos antes de ponerlos en marcha, soportarse en el talento adecuado y ver a la seguridad como un facilitador.

GABRIEL EDUARDO CUESTAS FLORES

Gabriel es Ingeniero en Sistemas Informáticos de la Escuela Politécnica Nacional, en la actualidad cuenta con las certificaciones: EnCase Examiner EnCe, Implementador/Auditor Líder Antisoborno ISO 37001 y perito informático acreditado ante el Consejo de la Judicatura de Ecuador.

Gabriel es Gerente en la práctica de Forensics en el Ernst & Young Ecuador, especialista en tecnología forense de la práctica de Integridad en los Negocios e Investigación de Fraude, a cargo del Laboratorio de evidencia Forense de EY Forensics; cuenta con más de 11 años de experiencia profesional en el sector privado y público relacionada a revisiones de tecnología forense, análisis de datos, eDiscovery y ciberseguridad.

Ha liderado investigaciones de delitos informáticos, utilizando protocolos y metodología forense para la preservación, procesamiento y presentación de evidencia.

ESPAÑA

MARÍA JESÚS HERNÁNDEZ-ELVIRA

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

La pandemia ha cambiado drásticamente muchos aspectos de nuestra vida y desde luego uno de ellos es el exponencial aumento de los riesgos de seguridad en la red. Hemos pasado a teletrabajar de forma mucho más usual de lo que venía haciéndose no solo en España sino a nivel global.

De tal manera que, con la pandemia, hemos aprendido a estar mucho más visibles en la red, ha relacionarnos mucho más con nuestros amigos, familiares y compañeros, a realizar de forma más habitual compras de todo tipo a través de internet, a hacer deporte utilizando distintas plataformas en lugar del gimnasio, a buscar el ocio en las redes, a realizar inversiones digitales, e incluso a transportarnos virtualmente a los lugares más insospechados.

Todo ello conlleva un tráfico de datos que se ha disparado en un 50% durante el confinamiento en España. Si antes de la crisis el tráfico de datos venia experimentando un crecimiento anual de entre un 10 y un 50%, durante la crisis ese aumento ha sido diario.

Si bien, la pandemia ya va quedando atrás, lo cierto es que el estado del bienestar de la sociedad actual ya no puede representarse sin una dependencia relevante de las TICs.

Y aquí radica el problema, que, además, está en clara fase creciente. La avalancha de daños se empieza a evidenciar y afecta no solo al consumidor y a las empresas sino a los gobiernos, a los gobernantes, a los políticos, alcanzando a la seguridad nacional.

Sin embargo, la gestión de la ciberseguridad no ha cambiado al ritmo que sería esperable. Es cierto, que la sensibilidad a la necesidad de protección va calando, pero de forma muy superficial a nivel general siendo que la concienciación de protección solo se palpa en grandes corporaciones, entidades financieras y algunas administraciones, pero desde mi punto de vista, a todas luces insuficiente por el momento.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

Es conveniente que los los programas de compliance penal se construyen sobre la necesidad de transmitir una cultura de ética y responsabilidad por parte de las empresas a sus miembros, desde los empleados hasta la alta dirección. Y con ese objetivo unido al catálogo de delitos que son susceptibles de ser cometidos por una persona jurídica se identifican todo un elenco de riesgos, principalmente penales, pero cada vez más, habida cuenta de esa cultura que se va tratando de transmitir en la empresa, en riesgos operaciones relacionados con la seguridad.

Como riesgos concretos que se valoran en un programa de compliance están todos aquellos relacionados con el descubrimiento y revelación de secretos, con los daños informáticos, con el blanqueo de capitales, con la publicidad engañosa, propiedad industrial e intelectual, entre otras.

No obstante, aspectos que se analizan de forma transversal, son los accesos a contenido en las redes autorizados por parte de la empresa a su personal, sistemas de control de medios de pago, sistemas de verificación de la identidad de clientes y proveedores, sistemas de descarga de archivos por parte del personal, sistemas de protección antivirus y de control del adecuado estado de los mismos, seguimiento de los niveles de acceso del personal a las redes, etc.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

Hay varias básicas que deben estar presentes e identificadas en toda empresa porque debemos tener presente que los ataques pueden venir tanto del exterior como del seno de la misma empresa, de ahí la importancia de no compartir contraseñas ni reutilizarlas, de implementar estrictos protocolos de actuación para verificación de datos y transmisión de información, controlar el uso de dispositivos de USB, controlar el acceso a las instalaciones así como el acceso a las redes de nuevos empleados, revisiones periódicas de permisos y privilegios de los usuarios o utilizar sistemas de encriptación de datos sensibles.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

María Jesús Hernández Elvira, Licenciada en Derecho en la Universidad Complutense de Madrid.
Posee un Master Triple en Derecho Público Internacional, Master en Criminología y Master en Derecho Procesal, de la Universidad Complutense de Madrid

Desde mi punto de vista, el escollo a superar es dar con una estrategia válida que no impida la productividad ni sea un obstáculo a la innovación, no obstante, ello no debe impedir plantearse objetivos ambiciosos, de ahí la importancia de realizar estrategias serias en materia de seguridad digital. Es importante evaluar la madurez de la seguridad de la organización en el que se tengan en cuenta tanto los aspectos relativos a las técnicas de seguridad como los procesos de respuesta a incidentes. Es necesario contar con protocolos claros y bien arbitrados para evitar que una brecha de seguridad se convierta en un serio problema para la empresa. Los primeros momentos son de vital importancia para la satisfactoria resolución de la incidencia.

Ello justifica que las empresas deban plantearse empezar a contar con abogados externos a modo de "consejeros independientes" que presten asesoramiento recurrente dentro de los comités u órganos de cumplimiento para lograr un extra de imparcialidad y control, que redunde en un eficiente sistema de seguridad.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

Tan sencillo como difícil, concienciación del empresario, inversión, planificación y educación.

MARÍA JESÚS HERNÁNDEZ-ELVIRA

María Jesús Hernández Elvira es actualmente Socia en el área Procesal de Andersen en la oficina de Madrid y Responsable del área penal y de compliance a nivel nacional.

Previamente, fue socia co-fundadora y directora del área penal de CHR LEGAL hasta la integración de la firma en Andersen en 2022. Ha sido juez durante más de 13 años y ha trabajado en diversos despachos internacionales como Ontier o Rousaud Costas Duran. Cuenta con más de 20 años de experiencia, en los que se ha especializado en derecho penal económico y programas de Corporate Compliance para empresas.

Junto con su especialidad en Compliance, por la que ha sido reconocida por directorios internacionales como Chambers & Partners, es especialista en Derecho Penal Económico.
Académicamente, ha impartido clases en la Universidad Pontificia de Madrid dentro del Master de Derecho de la Empresa, así como en la Escuela de Practica Jurídica de ICAL, habiendo sido ponente en varias ocasiones en el Colegio de Economistas de Cataluña.
Es, además, autora de diversos artículos y publicaciones legales para revistas especializadas, y colaboradora en la publicación "Memento Concursal Francis Lefebvre 2015". (Facultad de Ingeniería) en su postgrado de Seguridad Informática.

NUESTROS PRÓXIMOS EVENTOS

GUATEMALA

CARLOS GIOVANNI GUZMAN DE LEON

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

En cuanto a esto considero que si ha cambiado, pero también depende mucho del giro del negocio y de la cantidad de usuarios o computadores que se tienen dentro de la organización, hay que recordar que hace un par de años nos conformábamos con tener un firewall y posiblemente unas cuantas políticas y procedimientos dentro de la organización, ya que según nosotros, esto era más que suficiente para tener seguridad, sin embargo, hoy en día por el tipo de conexiones que se tienen y por la cantidad de usuarios que tenemos dentro de la organización con VPN´s desde casa, nos vemos en la necesidad de tener más herramientas como por ejemplo: Monitoreo 7x24x365 y el cual nos proporciona continuamente alertas, IPS que también nos alertan del tráfico malicioso dentro de la red los cuales llegan a un SIEM en donde correlacionamos, los logs que nos llegan de la mayor parte o si no es que toda la red y sus dispositivos. Debiendo incluso crear unidades dentro de la organización que se encargan específicamente de realizar las revisiones y evaluaciones correspondientes a los sistemas de la organización, para tratar de evitar un incidente o hacer un poco más difícil el ingreso de personas NO autorizadas a nuestra red.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

En lo referente a los modelos de compliance, considero que uno de los principales riesgos que existe, es el factor humano ya que muchas veces se concientiza y se trata de hacerlo de una manera bastante esforzadas, pero ese recurso humano, muchas veces se le olvida y omite las políticas, procedimientos y normas que se han generado para cubrir las brechas o vulnerabilidades que se dan en los Sistemas tanto Hardware como Software que se han venido implementando tratando de proporcionar un tratamiento a los riesgos para que no se materialicen dentro de la organización.

Otro de los grandes riesgos es la falsa sensación de seguridad que se contempla muchas veces en las áreas de Tecnología, debido a que se aferran a herramientas automatizadas lo que les da una falsa sensación de seguridad, ya que en un momento determinado dejan el control descuidado y también se aferran a prácticas que han venido realizando sin actualizarse con los avances tecnológicos que están día a día renovándose. Considerando que ya nada ni nadie les puede hacer ningún daño.

Otros de los grandes desafíos y que generan riesgos es que La Alta Dirección, no le da el valor correspondiente a la Ciberseguridad, ya que se conforman con hacer lo mínimo en cuanto al cumplimiento, puesto que en ocasiones es difícil convencerlos en cuanto a una inversión en este tema, lo que conlleva a riesgos colaterales que pueden causar un grave impacto en la infraestructura de la organización. Los cuales adoptan únicamente la práctica que emite el ente regulador, cuando el mismo indica que son requerimientos mínimos los que se emiten en los documentos en mención.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

Dentro de las medidas básicas que se deben considerar para implementar para evitar ataques es primordial, proporcionar constantemente concientización al recurso humano, debido a que hay que recordar que éste es el eslabón más débil en la cadena

> Otros de los grandes desafíos y que generan riesgos es que La Alta Dirección, no le da el valor correspondiente a la Ciberseguridad, ya que se conforman con hacer lo mínimo en cuanto al cumplimiento, puesto que en ocasiones es difícil convencerlos en cuanto a una inversión en este tema, lo que conlleva a riesgos colaterales que pueden causar un grave impacto en la infraestructura de la organización"

de la seguridad, y por lo tanto es donde atacan primero, ya sea por situaciones de desconocimiento que es lo más frecuente y hasta las situaciones económicas como ha venido suscitándose últimamente en donde los grupos de Hackers reclutan a personas estudiando su situación económica y les ofrecen un incentivo económico para que ingresen un dispositivo de almacenamiento USB, descargando un attachment en un correo electrónico u otra situación que se pueda dar dentro de la organización.

Adoptar un enfoque de confianza cero es decir NO confiar de manera predeterminada en nada que este dentro o fuera de su red o perímetro, como, por ejemplo: en donde se deben parchar todas las vulnerabilidades, fortalecer los equipos o computadoras que se encuentran en uso dentro de la organización, asumir que haya atacantes dentro o fuera de la red por lo que no se debe confiar predeterminadamente en ningún usuarios o dispositivo.

El Monitoreo constante de todas las actividades, transacciones, dispositivos, alertas, reportes actividades sospechosas, reportes de que no existen alertas, debido a que cuando no suceda nada. Es aún más sospechoso.

Adoptar marcos de referencias, metodologías o mejores prácticas de la industria para poder tener una base en cuanto a la adopción de controles, políticas, procedimientos, guías y otros.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

Establecer una línea base, para determinar la efectividad de los controles adoptados y el conocimiento de los mismos por parte de los usuarios y en realidad toda la organización, además que se corrijan las faltas a la Línea Base establecida dentro de la Organización.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

Hoy en día, con el avance tecnológico, que se ha suscitado en los últimos años, ya tenemos demasiados artefactos maliciosos al alcance de cualquier persona tanto de pago como gratuito como por ejemplo el arrendamiento de los siguientes servicios: Ransomware, Ataques de Denegación de Servicios, Crímenes Digitales, Amenazas Persistentes Avanzadas, los Troyanos Remotos y herramientas de explotación de vulnerabilidades, los cuales con el tiempo se van haciendo más comunes en nuestro medio.

Por lo que el convenio de BUDAPEST y otros convenios similares alrededor del mundo tienen un gran papel que jugar en cuanto al control de estos cibercriminales y la persecución de estos delitos alrededor del mundo. Mientras tanto en nuestros países debe existir alguna Norma, Política o Ley que pueda regular esta clase de actividades.

CARLOS GIOVANNI GUZMAN DE LEON

Especialista en Ciberseguridad, Estándares y Mejores Prácticas, con más de 20 años de experiencia en Instituciones Financieras y Educación Universitaria, en temas relacionados con Auditoria de Tecnología de Información, Seguridad Informática y Ciberseguridad. Fundador y Subdirector de Ciberseguridad del Equipo de Respuesta a Incidentes Cibernéticos del Ministerio de Gobernación.
Ingeniero en Sistemas de Información y Ciencias de la computación y Licenciado en Administración de Empresas, cuenta con maestría en Finanzas, Proyectos, Postgrado en Dirección de Negocios, candidato Doctoral en el doctorado de Investigación e Informática Aplicada, fue doctorando en INSTEC (Instituto Superior de Tecnología y Ciencia Aplicada en la Habana, Cuba en Administración de Proyectos), cuenta con certificaciones: CISM, ITIL, COBIT, PFD "Perito Forense Digital", ISO/IEC 9001/27001, LCSPC, FCSPC realizando cursos y seminarios en áreas relacionadas al ámbito tecnológico en México, Panamá, Costa Rica, Colombia, Chile, USA, Israel, España, Corea del Sur, Brasil y Guatemala.

ITALIA

JANICE CARLING

1. Has the management of cybersecurity changed after the pandemic?

Following the pandemic, there has been a clear increased risk and attention on cybersecurity including in the media and by businesses. The immediate and sudden need for remote working and discovering new digital ways of working has forced the topic to come to the forefront of business discussions like never before, for many reasons including the of protection of assets, business continuity, and company reputation.

At the same time, legislators are also enhancing regulatory obligations with respect to cybersecurity events, such as new reporting and audit requirements and increased penalties if organisations are found to not have adequately protected their data, both from a technical as well as an organizational perspective. And all of this has been accompanied by an increase in follow on litigation in the wake of a cyber crisis. As a result, cybersecurity is, and should no longer be, only a topic for IT teams, but rather it is now a concern of every part of the business, and especially management.

2. What are the main cybersecurity risks in compliance models?

Two of the main risks related to cybersecurity from a non-IT perspective are (i) communication channels and (ii) roles and responsibilities. IT teams must now promptly share information about cyber events in order to ensure regulatory obligations are met, and business and supply chains can continue. The message from the company should be consistent and aligned both internally and externally, not only to manage regulatory risks but also the due to the increased risk of follow on litigation.

Related to this is the real need during cyber crises for employees to understand who are making the decisions who needs to be involved –and this should be clear before any event occurs, because once a cyberattack does hit, reaction and action must be immediate. Clear and known policies, logical and rehearsed procedures, and agreed-on roles and responsibilities must be prepared and rehearsed in advance.

3. What basic cybersecurity measures should companies implement to prevent cyberattacks?

In addition to solid incident response and cyber crisis management procedures, another important basic measure that companies should take is training for employees on recognizing phishing and other cyber techniques used by cyber criminals. Successful phishing attempts are still the number one cause of cyberattacks; recognizing possible threats is the first step to effective detection.

4. What can be done from the department of compliance to reduce the number of security breaches?

In addition to what has already been mentioned, compliance can help reduce the risks by preparing in advance together with other departments such as IT, procurement and internal audit departments. IT will of course remain responsible for technical measures, but compliance can assist to ensure cyber events are dealt with in an appropriate way, such as implementing appropriate communication models so those who need to know about the event (both internal and external) will receive that knowledge (from IT) in a timely and organized manner. Additionally any required notifications to relevant authorities such as under GDPR in the EU or state authorities in the US will require coordination and monitoring.

Procurement also play an important role in reducing the risks related to third parties – security due diligence procedures should be implemented to check their procedures and systems prior to engagement, and effective work instructions with third parties also assist to reduce the risk of cyber incidents.

Last, as with other areas, internal audit play an important role in mitigating the risks associated with security breaches as they can detect weaknesses or

vulnerabilities in your own or in third party systems. Compliance can work with audit to present strong multiple lines of defense against these real risks.

5. What are the next challenges in cybersecurity?

In the current political climate, there is much suspicion of the use of cyberattacks for political reasons and as an additional method of warfare. If and when deployed, cyber warfare has proven to cause significant amounts of disruption; for example American oil, Colonial Pipeline, was hit in May 2021 with a ransomware attack which led to an emergency declaration being called in 17 states plus Washington DC in order to keep necessary fuel lines open in states across the nation. In 2015, a cyberattack on Ukraine's electricity grid caused blackouts for 80,000 customers and a year later, an attack in Kyiv took out power to one-fifth of the city for at least an hour. From these experiences and more, the US, UK, EU and other NATO states are on heightened alert for cyberattacks to hit critical infrastructure in particular, which if successful, could cause extreme disruption to basic services to citizens, severe economic loss, and mass political and social chaos. In response is a wave of increased regulation with the US, EU, Australia, India, China and many other nations proposing or implementing strict procedures, including regulatory audits/ inspections and notifications in cases of threats to critical infrastructure.

JANICE CARLING

Janice Carling is the data protection and cybersecurity specialist of Teva Pharmaceuticals' Global Legal team, providing advice to all areas of Teva's business. She is the strategic legal partner to Teva's privacy compliance, risk management, and IT teams, all of whom she works closely with to ensure Teva's compliance with global privacy and cybersecurity laws and regulations. Janice is a member of the EFPIA Data Governance Working Group, participates in other European and international forums for data protection specialists, and is a regular speaker at various conferences on the topics of data protection and cybersecurity.

Although born and raised in Canada, following graduation from McGill University Law and qualification as a lawyer in the province of Ontario, Janice moved to Europe where she has so far lived, studied and worked in Sweden, Switzerland and now Italy where she currently lives with her husband, two teenage daughters and cairn terrier dog(Facultad de Ingeniería) en su postgrado de Seguridad Informática.

MÉXICO

JOSÉ DÍAZ CUADRA

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

Definitivamente, la forma en cómo se detonó la operación de forma remota de compañías de muchos sectores fue exponencial. Simplemente y solo por citar al sector financiero, las transacciones de e-commerce tan solo en México crecieron casi 2 veces con un valor en cifras cerradas del 11 mil millones de dólares.

El reto ante ello es la mezcla de conocimiento de cliente, programas anti fraudes con algoritmos diseñados para el entendimiento del comportamiento transaccional de usuarios de medios de disposición electrónicos y desde luego, regulación que fue desarrollándose como mandatoria como es el caso de geolocalización en equipos electrónicos.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

La convivencia entre sistemas es un reto. Tienen que alinearse los parámetros en los sistemas "core" con los periféricos de PLD&CFT, que a su vez fueron programados con base en los modelos de evaluación de riesgos, que no son más que metodologías por las que las entidades financieras llevan a cabo los procesos de identificación, medición y clasificación de clientes por su nivel de riesgo. Ahora es indispensable conjuntar como un factor adicional el uso específico de medios de disposición electrónicos y la operativa, forma, costumbre y reiteración para protección en la transacción, información en tiempo real y desde luego, todo al tiempo de la experiencia de usuario.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

El conocimiento de los productos y a quien van dirigidos es básico para la Concepción de los esquemas de protección de fraude y ataques, sin embargo desde controles de accesos, contraseñas seguras (longitud y caracteres), trabajo en la nube y monitoreo contínuo es lo mínimo indispensable.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

Lo primero es establecer controles de seguridad conjuntamente entre quienes determinan los procedimientos normativos y los elementos técnicos de seguridad, con eso se puede construir una infraestructura tecnológica que pueda evaluar y gestionar el riesgo tecnológico desde varios puntos de vista, que hacer el cumplimiento normativo mandatorio que regula una entidad, los procesos de cumplimiento interno de la organización, mismos que en cumplir el ciclo de vida del servicio, es decir desde el diseño y construcción del proceso y la infraestructura tecnológica hasta el mantenimiento y operación contínua.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

Desafortunadamente todo comienza con una falta de cultura financiera, entender la comunicación que las entidades dirigen a sus usuarios es vital porque de esa manera se evitan filtraciones. Al interior de las empresas hacer ejercicios de hackeo ético así como una intensa comunicación entre los usuarios internos respecto requerimientos mínimos de revisión actualización de contraseñas son básicos.

JOSÉ DÍAZ CUADRA

Licenciado en Derecho con especialidades en Derecho Financiero y Derecho Mercantil, Instructor Habilitado por el ITESM, Consejero Independiente en Grupo Bolsa Mexicana de Valores y diversas entidades Financieras y Fintech, conferencista y profesor (Ley Fintech a CNBV, Blockchain for Lawyers y el Programa de Alta Dirección LATAM de FintechU).

Su trabajo ha sido en el sector financiero durante casi 20 años como Director Jurídico y Head Compliance en diversas entidades como HSBC México, Bx+, Prudential Bank, Actinver y PagaTodo; fundando desde hace 6 años Legal & Compliance Advisors (L&CA) una firma de abogados rankeada en categoría diamante en diversas prácticas (Fintech, Bancario, Compliance y Corporativo) la cuál cuenta con oficinas en CDMX, Guadalajara y Austin, TX en la que colaboran más de 100 asociados.

PANAMÁ

FELIX NEGRON

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

Tras la pandemia, las empresas tomaron un rol activo en adaptarse rápidamente, y adecuar sus políticas, procesos, procedimientos, etc. para fortalecer las capacidades de su estructura de red y así proteger sus activos, tratar de detener los eventos de seguridad y poder recuperarse adecuadamente de incidentes de ciberseguridad. Muchas empresas tomaron la iniciativa de proponer medidas mínimas de ciberseguridad para sus operaciones internas. Estas medidas, les proporcionarían confidencialidad, disponibilidad, e integridad de la data, además de reducir el impacto en caso de la empresa fuera víctima de algún incidente. Además, hemos visto que se designan equipos de trabajo exclusivos para el manejo y prevención de las amenazas, los cuales son encargados de implementar las medidas propuestas.

Sin embargo, aunque las empresas han experimentado una gran evolución en este ámbito, así también las ciber-amenazas y los ciber-atacantes. El panorama mundial nos muestra que todas estas estrategias de ciberseguridad propuestas por las empresas no van proporcional a su madurez, por lo tanto, no están a la vanguardia de las amenazas modernas.

Así mismo, las restricciones impuestas por la pandemia provocaron un aumento en la cantidad de trabajadores remotos. Esto ha comprobado ser una pesadilla para las compañías, pues los dispositivos entran y salen de las redes de las empresas y no existe un control responsable de credenciales que podrían caer en manos equivocadas. Sin duda, esto jugado un papel importante en la cantidad de incidentes de ciberseguridad registrados desde finales de 2022.

*Igualmente, ante la ausencia de madurez en ciberseguridad, vemos estructuras y políticas muy frágiles en lo siguiente:

Plan de contingencia - sin haber alcanzado madurez en ciberseguridad, no es efectivo

Plan de desastre - sin haber alcanzado madurez en ciberseguridad, está destinado a crear caos, perdidas y no soluciones.

Plan de mecanismos de ciberseguridad tradicionales - dentro de un nivel de madurez en ciberseguridad bajo, este no es eficiente en el momento de evaluar el retorno de la inversión. Es por ende que se invertirá capital en soluciones que dejan claro su inefectividad.

Plan de evaluación de riesgo - sin tomar en cuenta la madurez del equipo responsable de TI en la empresa, trae confusión y no soluciones viables.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

Para diseñar un programa de "Compliance" o cumplimiento, es importante identificar los riesgos específicos y particulares de la empresa donde se pretende implementar. Es importante estudiar cuales son los riesgos más relevantes; basados en esto, diseñar diversos controles asociados a los mismos. Algunos de estos podrían ser:

a. usuarios - múltiples procesos de autenticación y capacitación en mejores practicas

b. tecnología – proactiva como primera línea de defensa

c. ciberseguridad – nivel de madurez

e. cumplimiento – políticas obsoletas o que, aun siendo innovadoras, se quedan plasmadas en papel y no son puestas por obra

También es importante, monitorear los sistemas para evaluar la eficacia de los controles existentes. Así se podrán resolver las dificultades que se vayan presentando.

Incluir a un tercero en el proceso de certificación del modelo de cumplimiento o programa de "Compliance" es una buena alternativa para que, una persona con vasta experiencia, lo evalúe y determine las brechas y mejoras que pueda sugerir en su análisis. A pesar de que un programa de Compliance o modelo de prevención de delitos no es un remedio milagroso contra los eventos de alto riesgo, bien implementado, puede ser de gran ayuda para detectar y alertar al departamento de TI sobre situaciones de peligro.

> En momentos donde los atacantes de ciberseguridad más sofisticados de la historia son nuestros principales contrincantes, debemos acudir a expertos de ciberseguridad capacitados para comprender y mitigar tan gran amenaza"

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

Dentro de las medidas básicas de seguridad que deben implementar las empresas para tratar de evitar ciberataques están las siguientes: las empresas necesariamente deben adoptar un modelo y arquitectura de mecanismos proactivos en la deteccion de eventos de alto riesgo y a la vez deben alejarse de las alternativas tradicionales de deteccion, las cuales comprenden mecanismos reactivos. Al implementar el tipo de mecanismos sugeridos, las empresas alcanzarán el avance en madurez y podrán implementar medidas efectivas que sean de beneficio para la estabilidad y futuro de la organización.

Uno de los ejemplos más claros y el cual ha sido de conocimiento mundial respecto de la importancia en al ámbito de la madurez han sido los ataques sofisticados por el grupo de atacantes CONTI al país de Costa Rica. Esta desafortunada situación nos ofrece una aclaración del nivel de madurez de la estructura de seguridad en las redes de las agencias gubernamentales del país. En este caso en particular, se confió en los mecanismos tradicionales de deteccion como lo son los firewalls y antivirus; que como ya mencioné antes, son mecanismos reactivos. La situación tan alarmante y comprometida en la que estos ataques han dejado al país es suficiente prueba de que la estrategia de seguridad implementada fue una de baja efectividad y de extremo riesgo operacional.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

Desde mi punto de vista, es práctico y efectivo que el departamento de riesgo o "Compliance", contemple modificar la manera en que trabaja y que evalúe la inclusión de expertos en ciberseguridad, y no exclusivamente del personal de TI. Hay que destacar que, en la mayoría de los casos, el personal de TI no cuenta con el conocimiento necesario para asistir en la implementación o modificación de las políticas creadas en cuanto a ciberseguridad. Consultando con expertos en el campo, les hará ver desde un foco mas amplio cual es el verdadero riesgo. Cuando esto se cumple, el departamento de riesgo podrá ofrecer medidas y políticas que verdaderamente mitiguen el riesgo, eleven el retorno de inversión y prevengan un desastre

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

Después de haber ejecutado sobre 5,000 ingenieras inversas en ataques sofisticados años recientes, y ser parte de las negociones mas grandes en ciberseguridad son; he llegado a la conclusión de que los retos actuales más grandes en la industria son:

a. Los ejecutivos empresariales no comprenden el riesgo al que está expuesto su empresa.

b. Se descansa sobre el personal de TI para tomar decisiones en cuanto a la implementación de medidas de ciberseguridad y para lo cual no tienen el conocimiento requerido.

c. Implementar controles proactivos, fáciles de cuantificar y de monitorear

d. Contar con un personal íntegro, humilde que verdaderamente se preocupe por el bienestar y el futuro de la empresa.

FELIX NEGRON

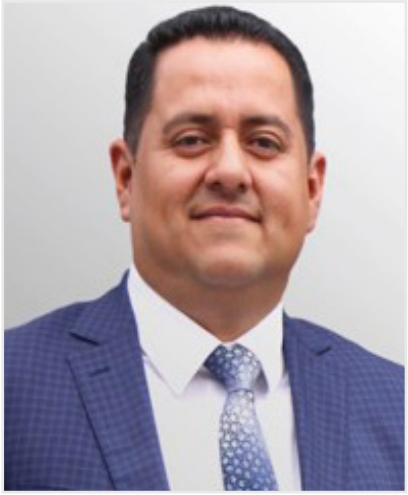
Félix Negrón se graduó con un B.S. en Tecnologías de la Información y una Maestría en Ciencias de la Computación. Tiene más de 20 certificaciones en una variedad de campos y es un experto en serialización. El Sr. Negron es un miembro activo de la Alianza del Sector Privado del FBI y posee un Certificado CJIS de Nivel 4.

El Sr. Negron es actualmente el director ejecutivo de ThreatSHIELD Security and Intelitechnologies, una empresa dedicada exclusivamente a los servicios de vCIO. En su cargo, ha podido trabajar en colaboración con el FBI/Mandiant/FireEye, controlando y remediando ataques cibernéticos a PYMES y Grandes Empresas de EE. UU. Jugó un papel decisivo en la construcción de la red negra para las industrias de Coca-Cola y protegió la receta de Coca-Cola durante 8 años.

Entre sus muchos logros, Félix ha desarrollado y construido un dispositivo patentado para detectar comportamientos anormales dentro de las redes informáticas en TIEMPO REAL. La ciencia alimentada a este producto patentado ha permitido que ThreatSHIELD Security logre un récord de "5 AÑOS" sin una sola violación de seguridad cibernética para ninguno de sus clientes. Este dispositivo de seguridad ha sido aprobado por el Departamento de Cumplimiento de la Ley de Florida. El Sr. Negron también ha desarrollado un producto para detectar y restaurar datos en minutos en caso de un ataque de Ransomware.

PERÚ

MANUEL ALEXANDER GARCÍA RIVAS



1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

La gestión de la ciberseguridad ha cambiado sustancialmente en pocos años, debido a que las ciberamenazas que uno enfrentaba antes de la pandemia se han incrementado significativamente, lo cual ha forzado un rediseño en la estrategia de ciberseguridad en las organizaciones. Por otro lado, los proyectos de transformación digital se adelantaron de 5 a 2 años en muchas organizaciones y el trabajo remoto que no era una modalidad muy utilizada a explosionado convirtiéndose en la nueva normalidad. Estos cambios han originado no solo nuevas amenazas cibernéticas, sino que han obligado a incrementar los presupuestos de ciberseguridad, incorporar especialistas de ciberseguridad en las organizaciones y que los colaboradores seamos parte activa de las medidas de seguridad en sus equipos de trabajo.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

Los principales de riesgos en los modelos de Compliance bajo el contexto post pandemia son los siguientes:

a) Robo de información personal (clientes, proveedores, socios estratégicos) que puede exponer a la organización a penalidades y/o sanciones por parte de reguladores y terceros.

b) Adopción de tecnologías emergentes cuyas medidas de seguridad no estén alienadas a las políticas de seguridad existentes y que generen nuevos riesgos.

c) Proveedores de servicios con contratos que no incorporan cláusulas de seguridad de información y privacidad; que proteja a la organización ante ataques informáticos y cuyas políticas de seguridad no estén alineadas a los requerimientos de la organización.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

Las medidas básicas de ciberseguridad que se deben implementar en toda empresa son las siguientes:

a) Identificar y proteger los activos de información que son críticos para nuestro negocio. Cada organización es distinta y dependiendo de su industria, los activos críticos pueden variar. La regla que nunca falla es identificar aquellos activos de información que pueden interrumpir mi operación. Cuando hablamos de activos de información puede ser hardware, software, servicios en la nube, canal digital, entre otros. Una vez identificados, lo importante es que medidas de seguridad se han implementado para protegerlos y asegurar su operación de acuerdo con las necesidades del negocio.

b) Realizar (al menos) una evaluación de ciberseguridad anual incluyendo pruebas de ethical hacking: esto es como nuestro examen médico anual que nos ayudará a identificar condiciones de salud que deben ser tratadas (brechas de seguridad) con apoyo de medicamentos, alimentación u procedimientos médicos (nuevas medidas de seguridad).

c) Sensibilizar y concientizar a la Alta Gerencia sobre las amenazas cibernéticas que pueden impactar a su organización y brindarles información oportuna para tomar las decisiones de negocio que permitan reducir el riesgo empresarial. Esto permitirá que se entienda que la ciberseguridad no es un gasto sino una inversión necesaria que acompaña los procesos de transformación digital e innovación tecnológica.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

Las áreas de Compliance, dependiendo de cómo ha sido diseñado su rol dentro de la

> El primer reto que las organizaciones están enfrentando es la cultura de ciberseguridad en sus colaboradores, debido a que el 30% del origen de los ataques informáticos son las personas que son engañadas a través de diversas modalidades de ingeniería social (como phishing, vishing, smishing, otras)"

empresa, puede aportar mucho valor en fortalecer la ciberseguridad. En primer lugar, velar por el cumplimiento de las regulaciones sectoriales que involucran aspectos de ciberseguridad, privacidad o digital. En segundo lugar, hacer sinergias con las áreas de TI, Seguridad de Información, Control Interno y Auditoría Interna; para poder maximizar el uso de recursos para monitorear el cumplimiento de las medidas de seguridad. Finalmente, retroalimentar los hallazgos y desviaciones observadas en las revisiones de cumplimiento de ciberseguridad a las áreas de negocio, TI y Seguridad de Información. En tercer lugar, velar por el cumplimiento de las políticas y procedimientos de seguridad de la organización. En diversas investigaciones forenses después de un ciberataque, se ha podido evidenciar que los atacantes han podido infiltrarse en las redes de la empresa debido a brechas de seguridad cuya causa-raíz es el incumplimiento de las políticas de seguridad de la empresa. Por ejemplo: utilizar contraseñas fáciles de adivinar, no cambiar las contraseñas de usuarios de red, crear cuentas genéricas con altos privilegios y no verificar la calidad de las copias de seguridad.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

El primer reto que las organizaciones están enfrentando es la cultura de ciberseguridad en sus colaboradores, debido a que el 30% del origen de los ataques informáticos son las personas que son engañadas a través de diversas modalidades de ingeniería social (como phishing, vishing, smishing, otras). Esta demostrado que no solo basta con implementar tecnología, procesos robustos y servicios gestionados de ciberseguridad; si el colaborador no tiene un adecuado comportamiento en el ciberespacio utilizado los activos digitales que pone la organización a su disposición, los ataques van a seguir llegando. Es por ello que toda estrategia de ciberseguridad debe considerar mejorar la cultura de ciberseguridad de sus colaboradores, que no es otra cosa que los hábitos, comportamientos, costumbres y conductas que deben tener los usuarios cuando acceden a recursos tecnológicos o información sensible de la organización, clientes, proveedores y socios estratégicos.

El segundo reto que tienen las organizaciones es articular un programa de respuesta a incidentes de ciberseguridad y la gestión de crisis. Hoy en día, un ataque informático puede poner en jaque la supervivencia de una compañía, y dependiendo de la magnitud del evento, puede inclusive originar el cierre de empresas. En ese sentido, es importante que la Alta Gerencia y los colaboradores entiendan que en la eventualidad de un ataque informático, la respuesta y contención al evento es una labor de toda la organización y no solo del área de TI o del oficial de seguridad.

MANUEL ALEXANDER GARCÍA RIVAS

Alexander es Socio de Consultoría de Negocios y dirige la práctica de Ciberseguridad y Privacidad en PwC Perú. Actualmente, lidera la implementación de metodologías ágiles e innovación bajo el enfoque "BxT" (Business, eXperience and Technology) orientadas a mejorar la experiencia de los clientes.

Posee una amplia experiencia y ha asesorado empresas de diversos sectores económicos en USA, Canadá, Israel y Latinoamérica. Asimismo, es expositor en diversos foros profesionales y es docente en los programas de posgrado de Pacifico Business School y Universidad Peruana de Ciencias Aplicadas.

Ha dirigido diversos proyectos entre los cuales podemos mencionar:

- Gobierno y estrategia de ciberseguridad
- Programa de cultura de ciberseguridad
- Respuesta a incidentes y diseño de playbooks
- Diagnóstico e implementación del marco NIST CSF
- Seguridad en la nube
- Implementación de sistema de gestión de seguridad de información
- Riesgos de seguridad en terceros
- Auditoría de ciberseguridad
- Diseño e implementación de programas de privacidad

PORTUGAL

MARÍA CANO HERNÁNDEZ

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

En cuanto a esto considero que la pandemia nos ha puesto a prueba a nivel tecnológico, tanto a las organizaciones que partían de cero y han tenido que dar un giro radical para continuar su actividad, como aquellas que, aun teniendo riesgos identificados, controles y procedimientos, han detectado puntos críticos y han tenido que potenciar su inversión en tecnología y apuesta en ciberseguridad para continuar con su plan estratégico.

A medida que la sociedad sigue migrando al mundo digital, la amenaza de la ciberdelincuencia crece exponencialmente, sectores vitales como la energía, salud, transporte, telecomunicaciones, finanzas, seguridad, dependen mucho más de los sistemas de información. Nos hemos dado cuenta de su papel relevante y significativo en la sociedad.

Como consecuencia, han aumentado las actividades ilegales en línea, tanto por el confinamiento social y la adopción de tecnología acelerada, como por el mayor uso y necesidad de la tecnología. Estas amenazas asociadas al trabajo en remoto y a la mayor exposición a la filtración de información confidencial han puesto de manifiesto la importancia de proteger la información valiosa de los clientes y la reputación de la organización.

Por ejemplo, al digitalizar las cadenas de suministro físicas han dado lugar a nuevas vulnerabilidades porque esas cadenas de suministro dependen de proveedores de tecnología y otras terceras partes, que también están expuestos a unas amenazas similares, potencialmente contagiosas.

En este sentido, Portugal ha sufrido una oleada de ciberataques a organizaciones estratégicas que han hecho que, según el Centro Nacional de Ciberseguridad (CNCS), el 77% de las organizaciones de Portugal hayan invertido en proyectos de seguridad por dos motivos, para poder dar respuesta ante un incidente y por riesgo a sufrir una sanción.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

La ciberseguridad y el cumplimiento normativo resultan clave para identificar y asegurar la protección de datos, están interrelacionados. Requieren del principio de responsabilidad proactiva, establecimiento de controles y seguimiento de planes de acción para mitigar estos riesgos.

Cuando hablamos de riesgos en modelos de compliance, es muy amplio. Si nos referimos a un modelo de compliance penal del 31bis, en primer lugar, analizaríamos las conductas del grupo de delitos de daños informáticos, revelación de secretos y contra la propiedad intelectual, mercado y consumidores. Ahora bien, no podemos olvidar delitos relacionados con la información confidencial, secreto empresarial, información privilegiada, así como los reputacionales.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

En primer lugar, identificaremos las amenazas que podemos recibir, tanto amenazas externas, a través de un fraude o un malware que intentará robar datos para venderlos, como internos, (spoofing-snooping) cuando se trata de filtraciones de datos que provienen de empleados o venta de secretos a un competidor.

Para ello, las organizaciones en función de su tipología deberán, una vez identificados los riesgos aplicar controles y medidas para mitigarlos. Entre las básicas: contraseñas, sistemas nemotécnicos, control de accesos, restricciones de usuarios, formaciones, aplicación de políticas de buen uso de dispositivos, serían comunes a todo tipo de organización

con independencia de su exposición al riesgo.

Para la difusión y sensibilización de estas medidas básicas es muy importante la coordinación entre los departamentos responsables del riesgo y un correcto establecimiento de medidas. Con una comunicación abierta, trasparente y eficaz, ya tenemos mucho camino recorrido.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

Desde Compliance, podemos implicarnos de múltiples maneras. Entre ellas, monitorizar, supervisar, hacer auditorías internas y, muy importante, la concienciación. Desde la incorporación del trabajador, se debe trasladar la cultura empresarial. Por ejemplo, incluyendo en su welcome pack, el código ético, la política de buenas prácticas informáticas, de dispositivos o unas instrucciones básicas en materia de ciberseguridad.

No se trata de hacer muchas políticas ni procedimientos restrictivos que frustren a los usuarios al no ser aplicadas. Se trata de hacer pocos procedimientos, claros y, lo más importante, que se pongan en práctica en la organización.

Aquí es donde el departamento de compliance juega un papel fundamental para continuar esa monitorización y seguimiento, así como para mantener informado al Órgano de Administración que es el que debe de manifestar la voluntad cumplir y predicar con el ejemplo.

Así mismo, el habilitar un canal que abra una vía para reportar esos incumplimientos o brechas también resulta esencial, tanto por la normativa vigente en España, como la que entrará en vigor próximamente. Cada vez se da mas fuerza a la obligatoriedad de contar con un canal y un modelo de compliance.

En este sentido, nuestros vecinos de Portugal han dado un paso adelante, ya que a partir de junio de este 2022, las filiales y sucursales españolas con 50 o más empleados y con presencia en Portugal también son entidades obligadas a contar con un modelo de compliance en el marco del novedoso Decreto Ley 109-E/2021.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

Si hablamos de amenazas, seguirán estando presentes este 2022, una de las más conocidas, Business Email Compromise (BEC) " fraude del CEO"; Ransomware, de mayor ocurrencia en lo que llevamos de 2022; Deepfakes, Virus y otras amenazas internas: mal uso de los dispositivos, desconocimiento o malintencionado, lo que se conoce como "chatarreros de datos", se trata de la venta de datos robados mediante un malware y Phishing, entre otros.

Tanto en España como en Portugal la tendencia es alcista, se espera un crecimiento del sector y un aumento de la demanda sobre todo en compañías bancarias, relacionadas con el sector energético y sanitario que manejan datos sensibles que pueden ser objeto de actividades relacionadas con el cibercrimen.

Para las pymes se están dotando herramientas de autodiagnóstico y guías para acompañarlos en los procesos internos de renovación de sistemas y tecnologías obsoletas que todavía persisten en muchas organizaciones y dificultan este avance tecnológico.

Se han creados centros de competencia y de investigación en ciberseguridad, como referente nacional y europeo, con la finalidad guiar el crecimiento en el sector y orientar a las organizaciones.

A nivel empresarial, considero que el reto es anticiparnos con rapidez a estas amenazas, lograr una estructura de control robusta, así como potenciar la seguridad informática, proteger los datos y difundir la cultura preventiva y concienciación en la organización.

MARÍA CANO HERNÁNDEZ

Abogada y máster en Business Law, por la Universidad Pontifica de Comillas, ICADE. Certificada en COMPLIANCE CESCOM® por ASCOM (Asociación Española de Compliance); IFCA International Federation of Compliance Association; Certificada en Blanqueo de Capitales por INBLAC; Certificada como Perito de Compliance por el IOC (Instituto Oficiales Cumplimiento).

Con amplia experiencia en delitos socioeconómicos y, desde 2016, dedicación exclusiva en BROSETA donde, en la actualidad, es Jefa de Equipo en el desarrollo de proyectos de cumplimiento normativo y penales, gestión de riesgos corporativos y control interno. Experiencia que le ha permitido asesorar y acompañar a los Compliance Officer o Comité de Compliance en el análisis, desarrollo y establecimiento de sus modelos en más de 20 organizaciones distintas.

A su vez, es miembro de la Comisión Ejecutiva de la Sección de Cumplimiento Normativo y Empresa del Colegio de Abogados de Valencia (ICAV), miembro de Grupos de Trabajo y Comisiones en materia de Compliance. Así mismo, también colabora como docente de Compliance y Gobierno Corporativo. Cuenta también con expertise en la elaboración y verificación de estados de información no financiera (EINF), así como en materia prevención de blanqueo de capitales.

NUESTROS PRÓXIMOS EVENTOS

G A _ P
Gómez-Acebo & Pombo
MOODY'S
ANALYTICS
eqs GROUP
SGR
COMPLIANCE

Patrocinadores WCA

REPÚBLICA DOMINICANA

JUAN DANIEL PUJOLS

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

La ciberseguridad es un tema que ha cobrado la más alta importancia en la última década en la que las empresas han aumentado su consciencia respecto de la protección de los datos que generan. Sin embargo, aunque los pasos de avance en esta materia habían sido significativos, es durante la pandemia por COVID-19 que la ciberseguridad tiene un repunte ante la necesidad de implementar el trabajo remoto de modo obligarorio en todos los sectores e industrias del quehacer económico de los países.

Es una realidad que el COVID-19, sin dudas, transformó la forma en la que trabajamos, incluso desde dónde lo hacemos, motivo por el que las entidades se vieron en la obligación de robustecer sus esquemas de ciberseguridad considerando que ante el teletrabajo impuesto por la pandemia era necesario blindar las informaciones partiendo de la realidad de que sus empleados estarían dispersos y expuestos a conexiones que no contarían con las medidas de seguridad establecidas en la organización.

Esto, por ende, transformó la visión en esta materia. Había que proteger más dispositivos como superficie de ataques para ser gestionados desde la óptica de la ciberseguridad para evitar que estos se convirtieran en un punto de entrada a los datos de la organización.

Este proceso significó también un enorme avance en materia de transformación digital, la mayoría de las empresas debieron buscar alternativas para ofrecer su servicio de manera virtual y sin requerir presencia de las personas a través de plataformas que también debian de ser protegidas.

Los ciber-atacantes no dejaron pasar esta oportunidad y aprovecharon para lucrarse de la situación. Los ataques de "phishing" (engaño vía email o mensajes falsos) crecieron al menos un 50% durante la pandemia. Asimismo, el ransomware, entendido como un ataque cibernético mediante el cual "secuestran" nuestros datos importantes haciéndolos inaccesibles a menos que paguemos una suma de dinero determinada, tuvo un crecimiento de 72% y ha costado al menos US$ 590 millones de dólares en 2021 y con miras a continuar creciendo cada año.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

El manejo de ciber-riesgo debe ser parte fundamental de cualquier organización en la era de la digitalización. Partiendo de la responsabilidad moral de las empresas, es necesario regirse por las normativas establecidas para cada sector. Esto nos dá un parámetro del nivel de compromiso que estas deben tener con el tratamiento responsable y seguro de las informaciones disponibles en la red, para prevenir cualquier exposición que atente contra la integridad de las mismas y de sus usuarios.

Es importante tomar en cuenta que uno de los objetivos principales de los ciber-delincuentes es obtener informaciones sensibles de las organizaciones, razón por la que los ataques cibernéticos más trascendentales son dirigidos a los usuarios, siendo el "phishing" el vector de entrada más común. En este sentido, la información y educación en esta materia es relevante para el capital humano.

Así mismo, la ciber exposición de los activos que están colocados en internet y su nivel de parchado o actualizaciones de seguridad establecidas regularmente son tan imprescindibles, como la correcta segmentación de la red, el monitoreo constante de eventos de seguridad y el establecimiento de un programa corresponden a los mayores agujeros de ciberseguridad que vemos hoy en día. Esta protección de los datos va de la mano con el nivel de cumplimiento de las normativas que rigen a cada empresa.

También, existen marcos de ciberseguridad que pueden ayudar a manejar y prevenir los riesgos de manera priorizada y mediante guías preestablecidas y probadas por la industria que contribuyen con el establecimiento de un programa de seguridad de información que permita establecer una base consolidada de cumplimiento en este sentido. Tal es el caso del framework de ciberseguridad de NIST, Los 18 controles críticos de CIS y la base de datos de observaciones de ataques reales de Mitre Att&ck.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

Todos los sistemas requieren una forma de validación de usuario, por lo cual el manejo de las identidades es fundamental gestionarlo y monitorearlo correctamente. Las relaciones digitales con terceros se han vuelto un punto recurrente en

los atacantes debido a que pueden "pivotear" o saltar a nuestra red desde otra que esté conectada a nosotros y conocer los activos vinculados a nuestra red y garantizar las protecciones básicas en los mismos.

En resumen, una buena estrategia de ciberseguridad debe considera, al menos, los siguientes factores:

- Definir un marco adecuado para el manejo y prevención del ciber-riesgo según el tipo de industria.

- Desarrollar un programa de ciberseguridad basado en las mejores practicas universales.

- Establecer un proceso robusto de gestión de identidades y accesos.

- Identificar los activos tecnológicos formales e informales de la institución (servidores, redes, computadoras, datos, etc.).

- Gestionar la ciber-exposición y vulnerabilidades en los activos a través de los mecanismos pertinentes.

- Mantener una estrategia de entrenamiento continuo sobre ciberseguridad al capital humano y los usuarios.

- Gestionar los incidentes de ciberseguridad y mantener un monitoreo constante de manera que se pueda responder adecuadamente ante una amenaza o posible impacto.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

Compliance y Ciberseguridad deben crear una sinergia de trabajo que garantice una correcta gestión del ciber riesgo de una organización. El riesgo cibernético es dinámico y cambiante según el entorno o industria y debe adaptarse según nuestro apetito de riesgo y estrategia de cumplimiento. Algunas consideraciones serian:

- Crear un programa de ciberseguridad con una visión global, alineado y acorde con los riesgos del sector en el que se desempeña y a los objetivos de la organización.

- Establecer un canal recurrente de comunicación con las áreas a cargo de la ciberseguridad para validar el cumplimiento del programa establecido y poder tomar decisiones a tiempo.

- Adoptar un marco de referencia para establecer un lenguaje común entre "compliance", ciberseguridad y el alto mando en la dirección.

- Establecer objetivos a corto y mediano plazo y dar seguimiento mediante indicadores (KPI) que contribuyan a la comprensión y análisis permanente del estatus y por ende a la consecución de los objetivos establecidos.

- Diseñar y ejecutar un plan de comunicación interna constante que garantice la sensibilización y educación del capital humano en esta materia.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

El mayor reto en materia de ciberseguridad es conocer y anticiparse a los nuevos métodos y ataques que cada día surgen en el entorno. Crear una organización ciber resiliente mediante el establecimiento de un programa de seguridad de información que responda a las necesidades y los riesgos del entorno de la organización.

Es imprescindible que la alta dirección establezca una postura sobre la ciberseguridad y comprenda la importancia del manejo del riesgo y la protección de información en general.

JUAN DANIEL PUJOLS

Es sub director de Ciberseguridad de la Superintendencia de Bancos de la República Dominicana. Es experto en ciberseguridad y tecnologías de la información, SOC y Open Source, entre otras.

Cuenta con más de 15 años de experiencia en la industria de servicios financieros, en la que ha desempeñado funciones gerenciales en las principales entidades bancarias del país.

Es ingeniero en sistemas y computación con una maestría en Dirección de Sistemas de Información por el Stevens Institute of Technology International -SITI-.

Actualmente cursa el programa Desarrollo Ejecutivo en la escuela de alta dirección BARNA Management School. Es docente de tecnología de la Universidad Dominico Americana.

SUECIA

ANDREW TABONA

1. Has the management of cybersecurity changed after the pandemic?

In short – yes. The shift to a fully remote or hybrid working model has forced some companies to adopt technologies at a faster pace than they were ready for – opening up more opportunities for attackers to exploit the essential tools and technologies that the remote workforce is using.

And now that employees have embraced this "new normal", there is little sign that we will go back to the way things were.

2. What are the main cybersecurity risks in compliance models?

At a fundamental level, a regulated entity – especially in the Financial Services industry –

should be thinking of cyber resilience not just as a cyber issue, but also a regulatory one. Organizations must consider integrating the relevant regulatory compliance requirements (e.g. NIST, PCI DSS, FedRAMP) into business operations. Non-compliance could mean increased liability and reputational damage should a security breach occur.

3. What basic cybersecurity measures should companies implement to prevent cyberattacks?

I always like to recommend that companies operate under the assumption that it is not a matter of if you will be attacked, but when you will be attacked.

Adopting this mindset, and focusing resources on detecting, preventing, and responding to a cyber-attack at the earliest opportunity will help to limit the impact to the business and the associated reputational and financial damage.

Good cyber hygiene goes a long way in helping to thwart most cyber-attacks. At a minimum, organizations should:

- Understand what their digital footprint looks like by maintaining an inventory of assets and software within the environment.

- Reduce their attack surface by removing systems or services that they don't need, and hardening their security devices and endpoints (e.g. by following the CIS Benchmarks).

- Establish a robust vulnerability and patch management program.

- Educate their user population to remain vigilant to cyber threats and know how to report anything suspicious.

- Implement Multi-Factor Authentication (MFA) on all public-facing and critical assets.

- Implement a defence-in-depth approach across their technology stack that includes multiple layers of preventative controls.

- Monitor for malicious or anomalous activity across their environment and have an incident response plan in place to reduce the likelihood of a damaging cyber intrusion and subsequently maximize the organization's resilience to a destructive cyber incident.

As a medium to long term goal, organizations would benefit from modelling their cybersecurity programs around industry recognized standards and frameworks such the NIST Cybersecurity Framework or CIS Controls.

4. What can be done from the department of compliance to reduce the number of security breaches?

The compliance department can play an essential role in ensuring the organization meets various requirements to protect the confidentiality, integrity, and

> The shift to a fully remote or hybrid working model has forced some companies to adopt technologies at a faster pace than they were ready for – opening up more opportunities for attackers to exploit the essential tools and technologies that the remote workforce is using."

availability of data.

By partnering with various stakeholders – including Legal, HR, and Cybersecurity –Compliance departments can design and implement policies, procedures and controls that meet these requirements.

As an example, think of the IT Use Policy that most organizations ask their employees to abide by. Compliance with this policy will help to reduce the number of security breaches by dictating what an employee should and shouldn't do with their organization's digital assets (e.g. not downloading or installing software unless it comes from an approved internal software catalogue).

5. What are the next challenges in cybersecurity?

An ongoing challenge organizations face today is staffing their cybersecurity teams. There is generally more demand for cyber talent than there is supply. Retaining staff and creating a pipeline for new talent will no doubt be on the mind of cybersecurity leaders.

The prevalence of cyber-attacks will increase. We only have to look at recent history to see that there is an upward trajectory year-on-year. This is in part driven by more attackers entering the market because of the "as-a-service" model (e.g. ransomware-as-a-service). So long as cybercrime continues to be profitable, attacks will continue.

With the almost overnight transition to remote work brought about by the pandemic came a rapid adoption of Infrastructure-as-a-service (IaaS) and Software-as-a-Service (SaaS) cloud solutions. Cyber threat actors will continue to work overtime to outpace cyber defenders and take advantage of the security gaps created by this accelerated IT transformation.

Ransomware attacks will continue to be a leading cyber threat for organizations for so long as they remain effective and profitable for attackers.

Recent high-profile supply chain attacks have highlighted this attack vector as viable and profitable for cyber threat actors. This 'one-to-many' model has allowed threat actors to amplify the reach and impact of their attacks. We can expect to see more of the same in 2022 and beyond.

ANDREW TABONA

Andrew Tabona (MSc, CISSP, GISP, GCFA, GCIH, GCFE) serves as Senior Vice President of Cybersecurity for a Fortune 500 company. He heads a global team of Digital Forensics and Incident Response Analysts, Threat Intelligence Analysts and Red Team Operators – collectively responsible for reducing an organization's exposure to cyber risk.

VENEZUELA

LISANDO BAUTISTA

1. ¿Ha cambiado la gestión de la ciberseguridad tras la pandemia?

En palabras de Fernando Miró Linares, la pandemia del Covid-19 supuso un gran experimento social que forzó a los ciudadanos a volcarse en el ciberespacio, bien para el entretenimiento, el trabajo, los estudios y la continuidad de los negocios en las empresas, en tanto, ese incremento inusual en la actividad digital trajo una ola sin precedentes de ciberdelincuencia que desnudó las vulnerabilidades en ciberseguridad de los usuarios como de las empresas. En retrospectiva, ya en el 2017 un estudio de la Universidad de los Andes sobre actividades rutinarias y cibervictimización en Venezuela, alertaba que las actividades ilícitas asociadas al ciberespacio que ocurrían en el país presentaban un patrón similar a los de otros países de América Latina y, con el transcurrir de la pandemia, en efecto pudimos observar un marcado incremento de las tipologías de hechos disvaliosos en el ciberespacio, lo que ameritó la actualización y ajustes en la gestión de la ciberseguridad en Venezuela.

Este nuevo enfoque post pandemia se ha desarrollado primero, desde lo más básico, como asumir la necesidad de mejorar el estándar de las claves de usuarios; segundo, entender que una de las brechas en ciberseguridad que más daño ocasiona, está formada por los denominados insiders, es decir, aquellos empleados o personas que tienen acceso privilegiado a la información de la empresa y que por motivos económicos, sociales, laborales, de forma intencional o por negligencia, violentan o permiten que se violente la ciberseguridad empresarial para dar paso a la comisión de delitos informáticos de mayor envergadura; y, tercero, entender la sinergia necesaria entre el compliance y la ciberseguridad como herramientas vitales para el resguardo de los activos digitales de las empresas.

2. ¿Cuáles son los principales riesgos de ciberseguridad en los modelos de compliance?

Es necesario destacar que los ciberriesgos, la mayoría de ellos, están previstos como delitos en Venezuela, específicamente en la Ley Especial contra los Delitos Informáticos y en la Ley de Instituciones del Sector Bancario, entre otras, partiendo de la idea básica de que los ciberriesgos son aquellas amenazas que pueden convertirse en vulnerabilidades, bien porque se ejecutan con herramientas de tecnología informática o en contra de ellas, que pueden causar graves daños patrimoniales, personales y reputacionales; siempre teniendo presente que el artículo 5 de la referida Ley Especial contra los Delitos Informáticos prevé la responsabilidad penal de las personas jurídicas por la comisión de este tipo de delitos.

Los modelos de compliance IT en Venezuela, construyen las matrices de riesgos a partir de los tipos penales previstos contra los accesos no autorizados, los sistemas que utilizan medios informáticos, contra la propiedad de activos digitales, contra la privacidad de las personas y las comunicaciones digitales, contra indemnidad de niños y adolescentes, contra la propiedad intelectual y contra el orden económico, por mencionar algunos de los riesgos de ciberseguridad que se consideran en los modelos de compliance.

Así las cosas, el compliance IT, es de necesaria implementación en todas las empresas para la protección y regulación del uso de la tecnología de la información y comunicación y demás activos digitales. En derivación, se trata de un modelo de gestión eficaz que permite mitigar el riesgo de la comisión de delitos informáticos y de daños económicos y reputacionales a la empresa. En ese sentido, la ciberseguridad es un eje fundamental de cualquier programa de Compliance como expresión de exhaustividad y coordinación de todos los riesgos de una empresa para el logro de los fines corporativos; realmente, no es posible imponer un criterio netamente técnico al cumplimiento normativo, así como tampoco a la inversa, es decir, de la supremacía de la integridad normativa sobre el uso las medidas de ciberseguridad.

3. ¿Qué medidas básicas de ciberseguridad deberían implementar las empresas para evitar ciberataques?

Soy de la opinión que las medidas de ciberseguridad empiezan con el compromiso de la alta dirección de la empresa y de todo el componente humano de erradicar el analfabetismo sobre ciberseguridad; de aquí parten las medidas objetivas para evitar ciberataques, es decir, adoptar medios efectivos de control de acceso con contraseñas robustas, no escribir en el hardware las claves para no dar posibilidades a los

> El primer reto que las organizaciones están enfrentando es la cultura de ciberseguridad en sus colaboradores, debido a que el 30% del origen de los ataques informáticos son las personas que son engañadas a través de diversas modalidades de ingeniería social (como phishing, vishing, smishing, otras)"

insiders, no permitir instalaciones de aplicaciones, ni alteraciones a los equipos, bloquear los equipos una vez concluido el trabajo y de aquellos empleados o directivos que se ausenten por vacaciones u otros motivos, mantener actualizados los sistemas operativos y herramientas antimalware, usar hostings privados, establecer las políticas de uso de internet, redes sociales, correos electrónicos con la advertencia de la ausencia de expectativas de privacidad en los recursos tecnológicos de la empresaria.

4. ¿Qué se puede hacer desde el departamento de compliance para reducir el número de brechas de seguridad?

El trabajo del departamento de compliance debe estar estrechamente coordinado con el departamento de seguridad informática o, el que haga sus veces, para el desarrollo del módulo de Compliance IT; de esta forma se puede disponer de una matriz de ciberriesgos, con las medidas y controles necesarios para estar preparados en casos eventuales de vulnerabilidad y poder reducir las brechas, daños y pérdidas de activos digitales. No es posible hacer frente a las brechas de ciberseguridad con una herramienta netamente tecnológica como un firewall o antivirus, o con una herramienta netamente de cumplimiento normativo; recalco, es necesario la sinergia entre Compliance IT y la Ciberseguridad.

5. ¿Cuáles son los próximos retos y amenazas en materia de ciberseguridad?

En Venezuela, los principales retos en materia de ciberseguridad estriban en los riesgos asociados a los criptoactivos, a pesar de que es un sector altamente regulado por el Estado, los expertos auguran la aparición de nuevas tipologías delictuales y, el otro reto, corresponde a la contención de la ciberdelincuencia organizada, dado que al estar altamente motivada con recursos tecnológicos de vanguardia, aunado ello a la identificación de cibervíctimas con significativas vulnerabilidades, ha permitido que las organizaciones delincuenciales irrumpan progresivamente con nuevas tipologías específicas para ejecutarlas en el ciberespacio con incidencia en el país.

LISANDRO BAUTISTA

Lisandro Bautista L. Abogado, graduado en la Universidad Santa María, Caracas, Venezuela. Magister en Ciencias Jurídicas Militares, Instituto Universitario Politécnico de las Fuerzas Armadas Nacionales, Caracas, Vzla. Especialista en Derecho Penal Económico, Universidad Castilla-La Mancha, Toledo, España. Especialista en Derecho Constitucional, Universidad Castilla-La Mancha, Toledo, España. Experto Universitario en Corporate Compliance, Universidad Internacional de La Rioja, España. Experto Universitario en Informática Forense, Universidad Internacional de La Rioja, España. Programa de Ciberseguridad para Managers Instituto de Estudios Superiores de Administración, Caracas, Vzla. Experto en Tecnologías aplicadas a la Investigación Universidad Austral, Buenos Aires, Argentina / Universitat Abat Oliba, Barcelona, España. Magister en Ciberdelincuencia Universidad Internacional de La Rioja, España. Socio del gabinete Bautista & Perche Abogados.

¡ASÓCIATE A LA WORLD COMPLIANCE ASSOCIATION!

G A _ P Gómez-Acebo & Pombo

Moody's Analytics

EQS Group

SGR Compliance

Patrocinadores