CONGRESO DE
PREVENCIÓN
DEL
FRAUDE Y
SEGURIDAD

Construyendo **experiencias** desde un **entorno seguro.**

FECHA 15 - 16 DE NOVIEMBRE /2018
HOTEL GRAND HYATT BOGOTÁ

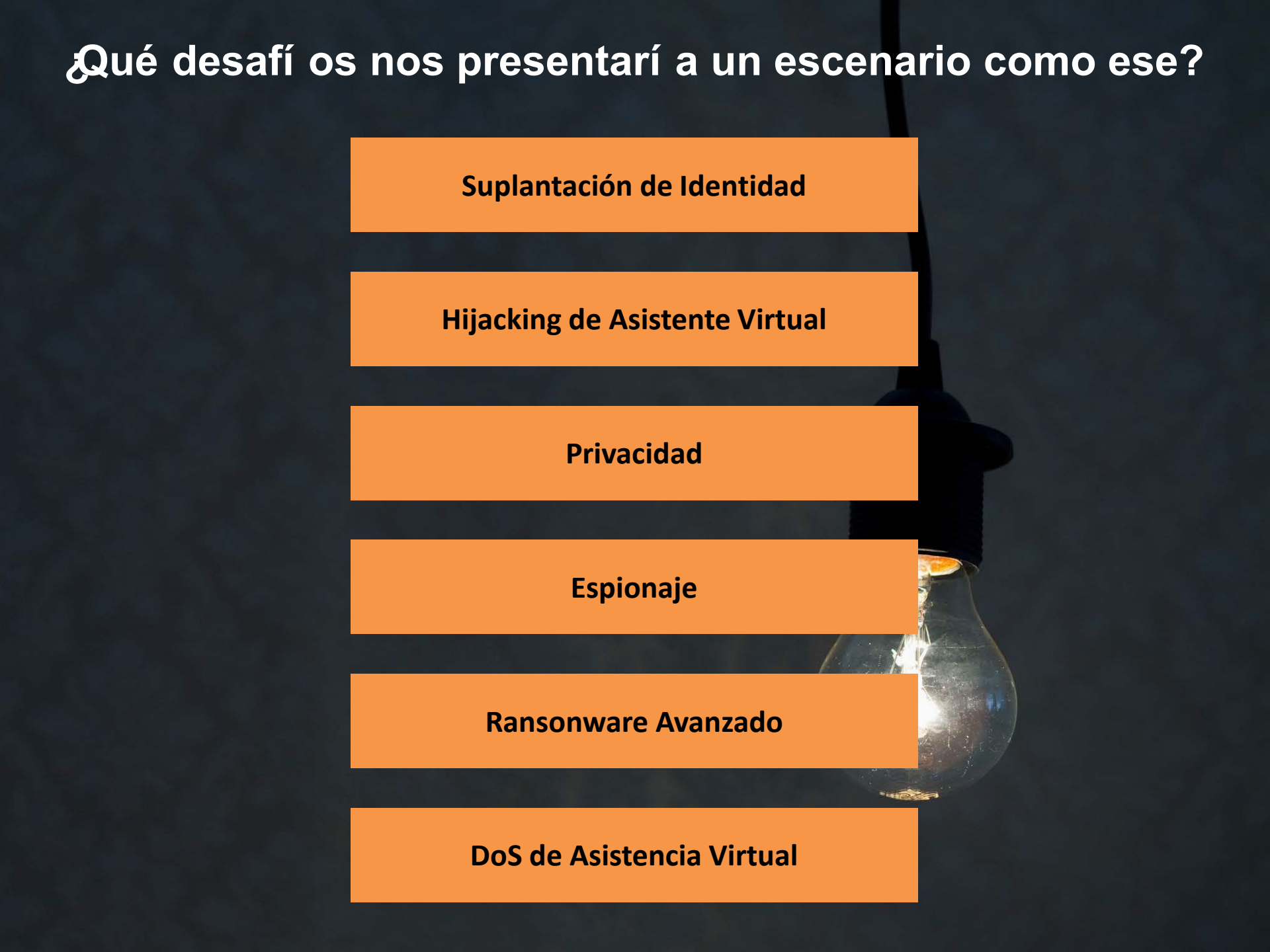
Transformando el Rol de Ciberseguridad para la Era de las Finanzas Digitales

Walter Ariel Risi

Socio, Tecnología y Ciberseguridad
KPMG Argentina

¿Cómo serán las finanzas del … 2025?

¿Qué desafí os nos presentarí a un escenario como ese?



- Suplantación de Identidad
- Hijacking de Asistente Virtual
- Privacidad
- Espionaje
- Ransonware Avanzado
- DoS de Asistencia Virtual

Pero … ¿debemos esperar al 2025 para renovar nuestra enfoque de ciberseguridad?

Algunas realidades de hoy mismo …

¿Hay algún elemento subyacente a estas transformaciones?

¿Casos de Negocio de 2 meses?

¿Fases de Análisis de 3 meses?

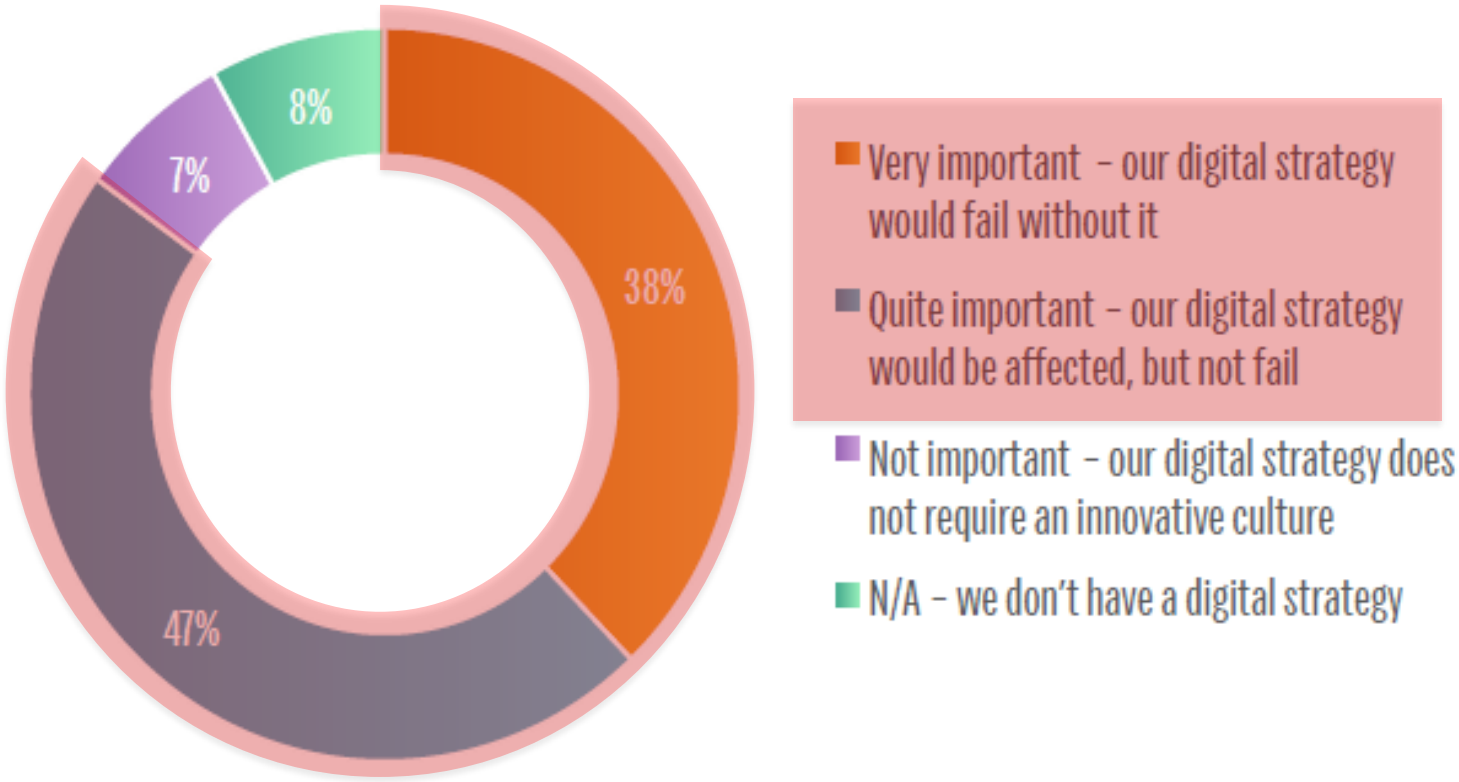
¿Implementaciones de 6 meses?

¿Certificaciones de 1 Mes?

ESTA FORMA DE TRABAJO ESTÁ QUEDANDO OBSOLETA MUY RÁPIDAMENTE

La capacidad de experimentación rápida es la CLAVE COMPETITIVA de la era en que vivimos.

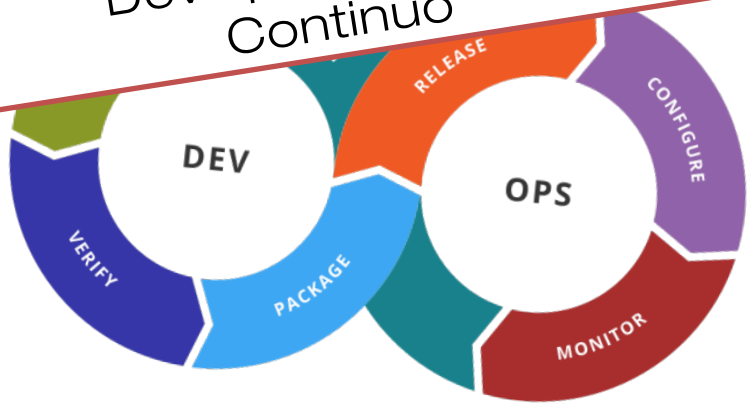
¿Qué tan importante es contar con una cultura innovadora y experimental en su organización a fin de que la estrategia digital tenga éxito?

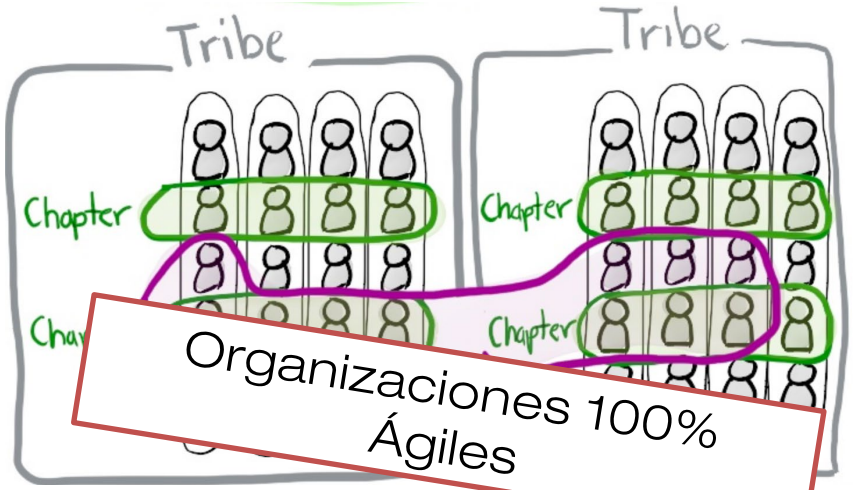


https://home.kpmg.com/xx/en/home/insights/2018/06/harvey-nash-kpmg-cio-survey-2018.html

Lo que ya vemos y veremos cada vez más …

DevOps y Delivery Continuo





Organizaciones 100% Ágiles

DISTRITO

Innovación con Ecosistemas

Integración Multicompañía por medio de APIs

¿Cómo se lleva nuestra área de ciberseguridad con esta dinámica?

Pensemos honestamente unos segundos sobre la percepción que puede haber sobre nuestras áreas de ciberseguridad …

Transformándonos
de perro guardián
a guardaespaldas

¿Cómo?

7

Recomendaciones Para Transformarnos

1

Ciberseguridad Continua en la Construcción

En el ciclo tradicional, los puntos de control de seguridad (si los hay) normalmente se planifican al principio y al final del proyecto.

En un ciclo continuo, las interacciones estarán distribuidas a lo largo de múltiples iteraciones. **Interacciones más cortas y más frecuentes**.

¿Cómo lograrlo?

Ser integrante constante del equipo ágil es el ideal, aunque no sea en forma full-time. Complementariamente, proveer a desarrollo de herramientas adecuadas desde el principio.

Incorporación del representante de Ciberseguridad en Proyectos. El Cyber Partner, embebido dentro de los equipos ágiles.

Incorporar Cyber (User) Stories y participar en Sprints Cyber Intensive a lo largo de la construcción.

Proveer a Desarrollo con Estándares, Activos y Herramientas Self-Service de Antemano

2

Mentalidad de Delivery en el Área de Ciberseguridad

Los profesionales de ciberseguridad típicos normalmente tienen perfiles muy diferentes a los de desarrollo de software.

En un ciclo de interacciones breves y frecuentes, el área de ciberseguridad debe **comprender mejor la realidad de desarrollo** para mejorar su interacción.

¿Cómo lograrlo?

Un mayor entendimiento de la dinámica y necesidades de desarrollo ayudará significativamente a crear más empatía y diseñar mejores interacciones.

Formar a nuestro equipo de soporte a proyectos con entrenamientos y certificaciones en software seguro (cuidado con cuales).

Entrenar a nuestro equipo en Agile y DevOps (ej. Scrum, SAFe), idealmente JUNTO al equipo de Desarrollo.

Idealmente, realizar un "intercambio" (pasantía, *internship*) de tiempo limitado dentro del equipo de Desarrollo.

3

Mentalidad de Seguridad en el Área de Desarrollo

De manera inversa al caso anterior, durante años las áreas de desarrollo fueron adversas a los controles de seguridad.

A fin de que las soluciones nazcan seguras, las mismas áreas deben considerar la **seguridad como un elemento clave y prioritario**.

¿Cómo lograrlo?

La forma más natural, fácil y segura de que la ciberseguridad forme parte de la solución es que sea priorizada como elemento clave por Product Owners y equipos de desarrollo.

Formar al equipo de desarrollo de software con entrenamientos y certificaciones en software seguro (cuidado con cuales).

Realizar concientización en seguridad especialmente a Product Owners y Arquitectos dentro de los equipos ágiles.

Nuevamente "intercambio" de desarrolladores en seguridad (ej. ¡automatizando controles para ellos mismos!).

4

Balance (Trade Off) y Deuda Técnica de Ciberseguridad

En un contexto de rápido movimiento, la necesidad de time-to-market más agresiva puede requerir decisiones de tradeoffs más frecuentes.

Pero un **tradeoff viene de la mano de una mitigación** y el concepto de Deuda Técnica debe incorporarse también a la ciberseguridad.

¿Cómo lograrlo?

En ciclos más dinámicos y con time-to-market más agresivos, la deuda técnica es una metáfora (tomada de desarrollo) que nos permite "tomar riesgo" siempre que se pague a la brevedad.

Incorporar **Modelado de Amenazas** y determinar **Trade Offs** en base a análisis de riesgos (probabilidad e impacto del caso).

Todo Tradeoff es un **Generador de Deuda Técnica** que debe tener un "plan de pago (remediación" asociado.

Incorporar el **Seguimiento de Cierre de Deuda Técnica** tanto dentro de Desarrollo como en el Seguimiento de Observaciones.

5

Co-Diseño de Telemetría de Seguridad en las Soluciones

En un contexto de desarrollo de soluciones cada vez más dinámico y distribuido se hace cada vez más difícil prevenir todo posible suceso.

En esta situación, es clave embeber elementos que nos permitan darnos cuenta – y accionar – **lo antes y más rápido posible.**

¿Cómo lograrlo?

El área de ciberseguridad es un "stakeholder" más de la solución y es fundamental que sus necesidades de monitoreo, logging y "palancas de corte" estén bien representados en el software.

En base a los escenarios analizados, determinar qué información podría requerir nuestro SIEM para monitorear la solución.

Asimismo, trabajar en diseñar logs adicionales (activables bajo demanda) que pudieran requerirse en una investigación.

Dependiendo de la criticidad de los escenarios, diseñar "palancas de corte" de funcionalidades específica.

6

Seguridad Como Código y Automatización Despiadada

Los buenos equipos de desarrollo tratan de automatizar pruebas y chequeos para evitar que los errores vuelvan a suceder.

Automatizar chequeos de seguridad **dentro de las aplicaciones y ciclo de vida** puede hacer la vida más fácil para todas las partes.

¿Cómo lograrlo?

Embeber controles en la batería de pruebas de desarrollo y revisiones automatizadas del "build" del software, tanto para estándares como para evitar errores pasados.

Escaneos de código automáticos ante cada check-in ayudarán a prevenir las cuestiones más básicas.

La ejecución automática de un escaneador de vulnerabilidades en el ambiente de integración continua nos dará otro chequeo.

Ante un problema de seguridad, analizar conjuntamente con desarrollo si puede escribirse una prueba que lo prevenga.

7

Ciberseguridad en el Ecosistema de Aliados y Proveedores

Con soluciones que combinan proveedores SaaS, interconexión mediante APIs e integración de soluciones de FinTech, la situación es compleja.

En este contexto, el área de ciberseguridad debe estar preparada no sólo para proteger a su organización, sino **también a aliados y proveedores**.

¿Cómo lograrlo?

¡En este nuevo contexto, extremar las barreras de aceptación de proveedores y aliados nos puede dejar solos! Debemos prepararnos para ayudar a nuestro ecosistema a ser más seguro.

Diseñar niveles de aceptación y "planes de pago de deuda técnica" de soluciones de terceros (vs. Go / No Go).

Anclar la seguridad en el proceso de adquisición (compras, fusiones, etc.) para lograr nuestro involucramiento temprano.

Incorporar un servicio de asistencia a terceros (proveedores, aliados, etc.) que pudieran no tener áreas propias de ciberseguridad.

¿Cómo empezar?

3

Conversaciones Honestas Necesarias

LÍDERES SENIOR NEGOCIO

- Apetito Digital
- Ciber Conciencia
- Nivel de Compromiso

LÍDERES SENIOR TECNOLOGÍA

- Aptitud Ágil
- Ciber Conciencia
- Actitud Colaborativa

NUESTRO PROPIO EQUIPO

- Actitud Ágil
- Conciencia Digital
- Actitud Constructiva

Una función de ciberseguridad ágil y constructiva no es una opción … ¡es el único camino!

CONGRESO DE
PREVENCIÓN DEL FRAUDE Y SEGURIDAD

Construyendo **experiencias** desde un **entorno seguro.**

FECHA 15 - 16 DE NOVIEMBRE /2018
HOTEL GRAND HYATT BOGOTÁ

¡MUCHAS GRACIAS!