COVID-19

Security Operations Center

Julio 2020

Expositores

Marcos Giménez
Senior Manager
PwC Uruguay

Diego Taich
Managing Director
PwC Argentina

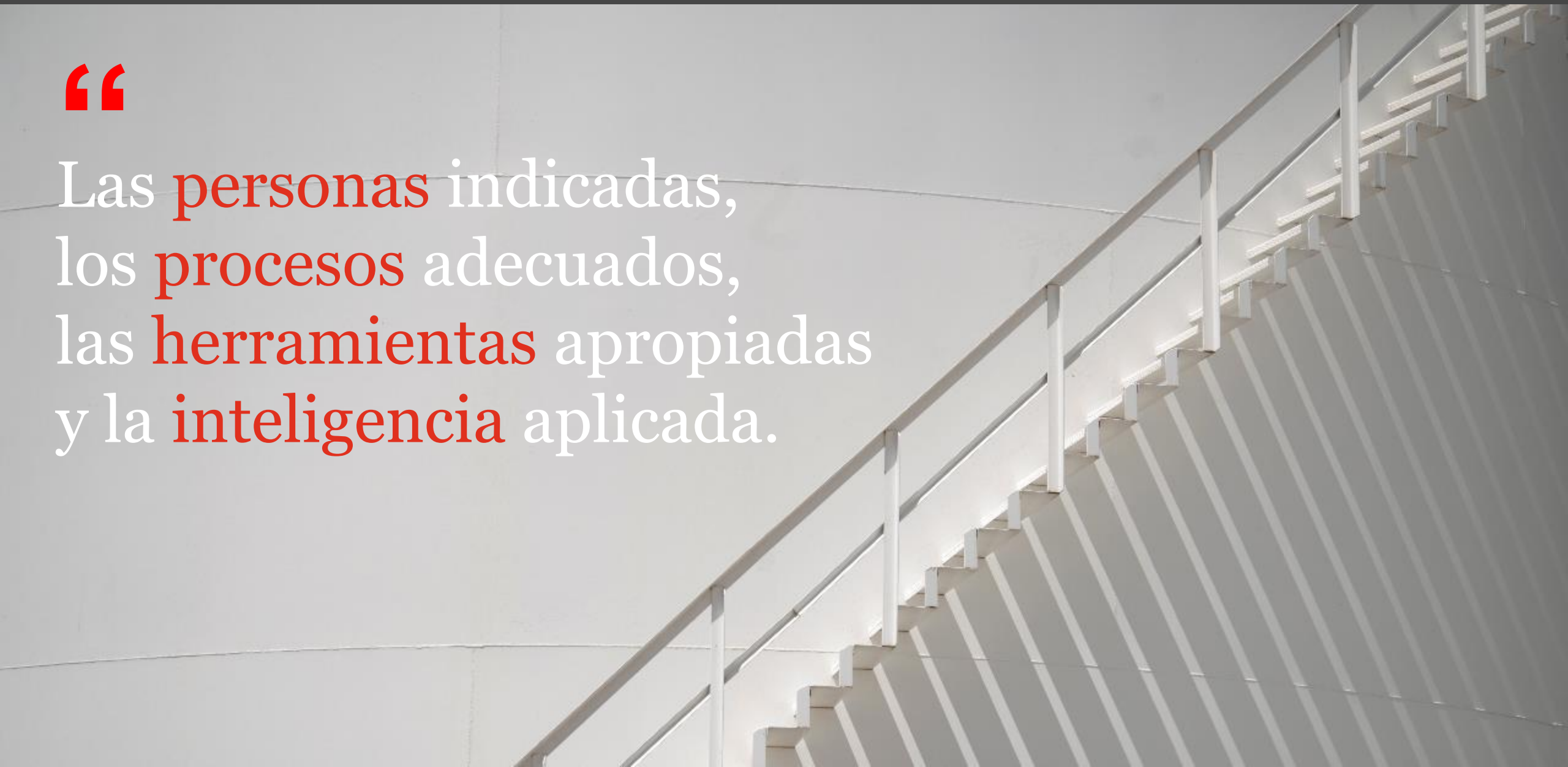
Viviana Basso
Manager
PwC Argentina

Introducción

Definimos el concepto de **cerebro único** a la característica de centralizar en una solución “WorldClass” todas las alertas de eventos de los diversos componentes de la infraestructura crítica del negocio.

Esto permite una rápida categorización y priorización de aquellos que son más críticos, pudiendo correlacionarlos de manera optima y ante un posible ataque, minimizar el efecto del posible impacto.

SOC: pilares



“

Las personas indicadas,
los procesos adecuados,
las herramientas apropiadas
y la inteligencia aplicada.

SOC: procesos

Todos los procesos, tanto para la gestión integral del SOC como los reportes de incidentes de seguridad y de las métricas del servicio, han sido diseñados en cumplimiento de normativas y estándares ISO 27001, PCI-DSS, BCRA, HIPAA, NIST, IRMs, y GDPR.

SOC: procesos

Lista de tareas claves

Esencial para que el equipo de SOC sepa qué debe hacer y cómo hacerlo correctamente.

Clasificación de eventos

Se clasifican según la criticidad predefinida acorde a cada tipo de origen del evento.

Priorización y análisis

Revisar cualquier actividad sospechosa que indique un posible ataque.

Remediación y recuperación

Se sugieren las posibles tareas a realizar: System Upgrades, Patching, Reconfig. reglas FWs, recuperación desde un Backup, etc.

Evaluación y auditoría

Tanto el Análisis de vulnerabilidades como las revisiones periódicas de Audit & Compliance son parte del proceso de mejora continua del SOC.

SOC: escalabilidad

SOC acompaña la evolución de la organización, agregando componentes para monitorear de acuerdo a sus necesidades.

Esta escalabilidad del servicio evita incurrir en grandes inversiones en servicios y herramientas de monitoreo de seguridad, lo que le permite optimizar sus esfuerzos enfocándolos al negocio.

SOC: profesionales

Los profesionales que dan respuesta a incidentes son:

- Analistas Forenses (especialistas en Triage)
- Gestión de Crisis(Treat Hunting)
- Ethical Hackers

SOC: herramientas

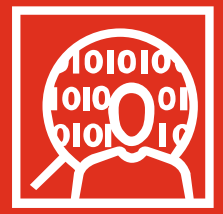
La metodología y herramientas de monitoreo permiten asegurar que los *logs* de eventos de seguridad siempre estarán almacenados en la organización.

De esta manera, se asegura la privacidad de la información de los clientes en cumplimento de la Ley de Datos Personales, regulaciones vigentes y las buenas prácticas de Data Privacy.

SOC: herramientas

Descubrimiento

Un inventario de activos confiable y automatizado es fundamental.



Evaluación de vulnerabilidades

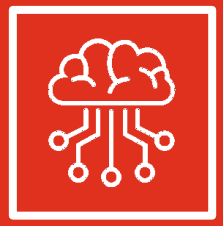
Determinar la “superficie de ataque” y el cumplimiento de estándares.

Monitoreo de comportamiento

Crear una línea base del comportamiento permite detectar posibles Ciberatacantes.

Detección de intrusos

Conocer es la clave. Tener sus reglas de correlación actualizadas permite detectar nuevas amenazas.



Threat Intelligence

Detectar y vincula patrones de comportamiento, indicando cuáles son las amenazas más importantes que enfrenta su red en un momento.

Security Information Event Management (SIEM)

Buscar patrones de actividad y secuencias de eventos de posible ciberataque. Generan reportes de cumplimiento.

SOC: enfoque

En caso de que la organización necesite no solo asesoramiento sino también apoyo en la ejecución de la respuesta al ciberataque, la sinergia PwC & SkyOnline puede proporcionarle servicios específicos para la respuesta a incidentes y la investigación forense, entre otras soluciones del portfolio.

SOC: principales beneficios

1. **No incurrir en altos costos de inversión en actividades que no son el *core* de la organización.**
2. **Servicio escalable y adaptable según sus necesidades.**
3. **Mejora en los niveles de protección de los activos.**
4. **Mejora la capacidad de respuesta a incidentes.**
5. **Posibilidad de tener gestión y monitoreo de su Infraestructura de manera centralizada.**

SOC: Caso de negocio

- La identificación temprana y la respuesta inmediata ante un incidente típicamente reduce en forma muy significativa su daño y costo para la organización.
- En términos de gestión de riesgos, la gran mayoría de los controles usados en ciberseguridad (aún en organizaciones que implementan conceptos modernos como *“defense in depth”)* atacan la dimensión de probabilidad, mientras que un SOC (unido a un buen procedimiento de gestión de incidentes) se centra en la mitigación del impacto.
- Los costos vinculados a seguridad son usualmente de los más difíciles de introducir en una organización, por lo cual pensar en personal interno con disponibilidad 24/7 suele ser inviable.
- Tanto las tecnologías aplicadas como la dedicación del personal de un SOC se prestan para la obtención de economías de escala al centralizar el servicio para múltiples organizaciones.
- En el escenario actual creado por la pandemia, muchas organizaciones han incrementado sensiblemente sus riesgos vinculados a ciberseguridad.

Servicios adicionales

Servicios de valor agregado que, gracias a esta sinergia, podremos brindarle generando una solución integral.

1. **Análisis Forense, Ciberinteligencia, Test de Penetración, Respuesta a Incidentes.**
2. **Modelado de riesgos y amenazas, Evaluación de riesgos tecnológicos.**
3. **Privacidad y protección de datos.**
4. **Administración de Infraestructura Tecnológica.**
5. **Servicios Cloud, Procesos de Backup y Restore, etc.**

SOC: Conclusiones

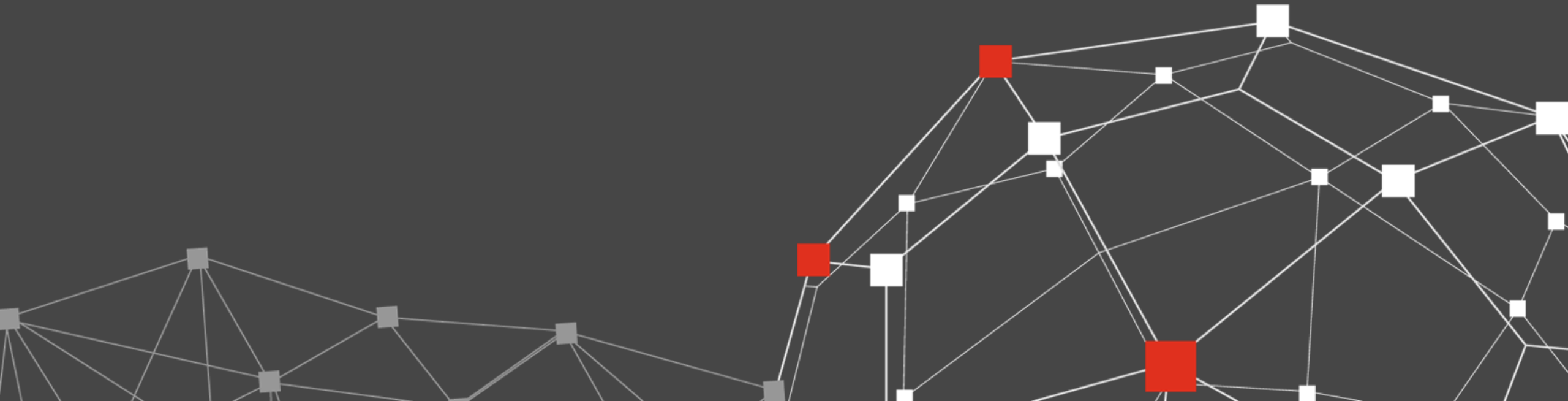
Un **cerebro único** monitoreando los activos críticos del negocio.
Servicio escalable a las necesidades.

Procesos diseñados de acuerdo a los **estándares de seguridad** de la industria y cumpliendo con las regulaciones SOX, BCRA, PCI-DSS, NIST, IRMs, ISO 27001.

Detección centralizada de **amenazas** en la infraestructura.
Ej: AWS, Azure , On-Premise & Cloud Apps como G Suite.

Los **datos siempre almacenados** dentro de la organización.

¡Gracias!



Contactos

Marcos Giménez
marcos.g.gimenez@pwc.com

Diego Taich
diego.taich@pwc.com

Viviana Basso
viviana.basso@pwc.com