KPMG

BOARD Leadership Center COLOMBIA

¡Bienvenidos(as)!

COMITÉ ACADÉMICO

Auditoría y Riesgos

Mike Tyson

KPMG

TENDENCIAS CIBERSEGURIDAD

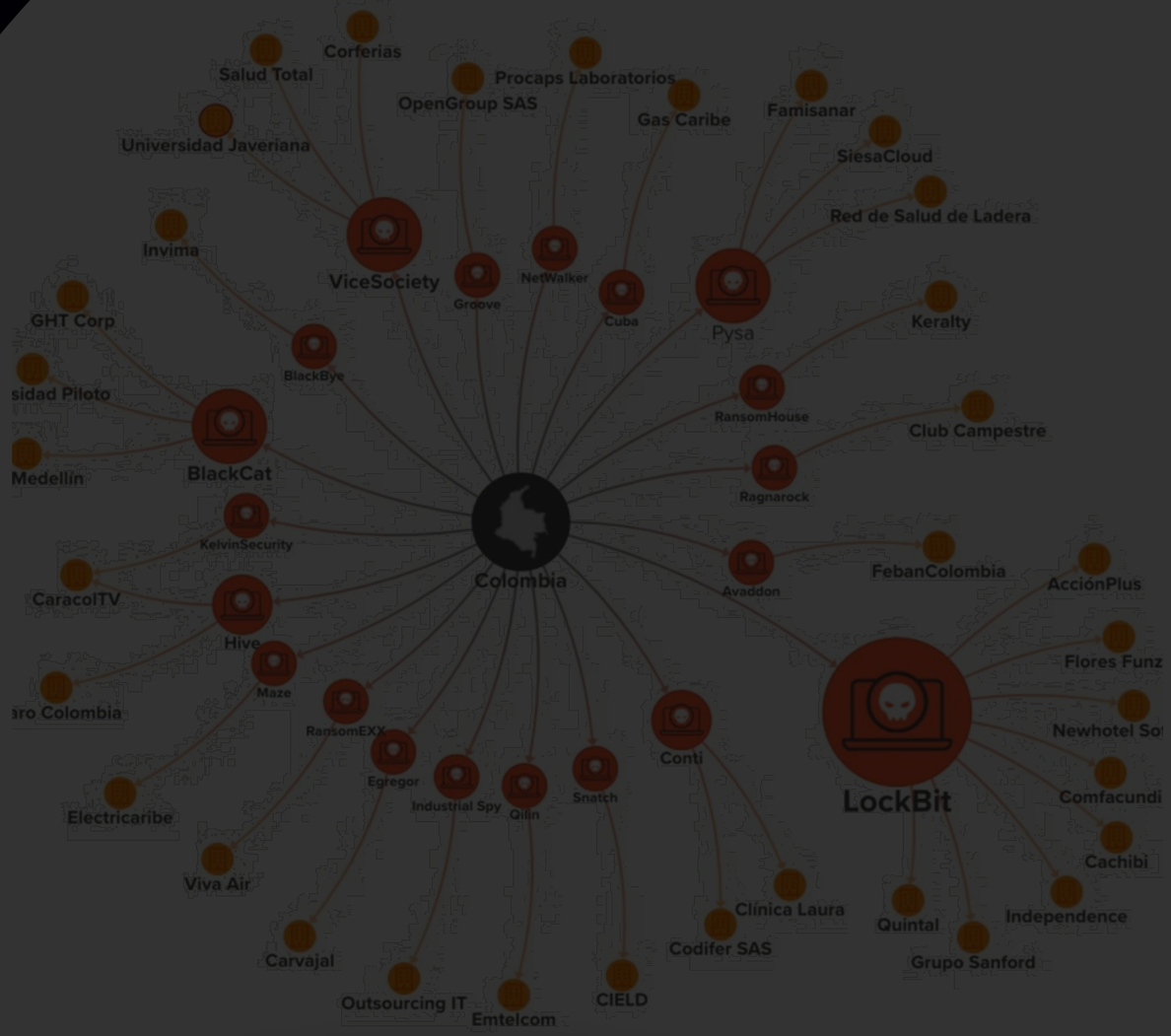
La pregunta correcta no es si van a atacar a mi organización, sino:

¿Cuándo?

- Salud Total
- Procaps La
- Invima
- Universidad Javeriana
- GHT
- EPM
- VIVA

- Famisanar
- Corferias Bogotá
- Famisanar
- Red de Salud de Ladera

21% of ransomware attacks are via remote Access.



*** Over 51% companies said they had ransowar incident in the last year**

KPMG

KPMG CYBER TRUST INSIGHTS 2022

KPMG CEO OUTLOOK 2022

77% Ven la seguridad de la información como una **función estratégica y una ventaja competitiva** potencial.

73% La incertidumbre geopolítica aumenta la preocupación de muchos CEOs por los ciberataques corporativos.

Cada vez más CEO´s reconocen estar **POCO preparados** **ante un ciberataque**, con un **24%** que lo admite en 2022, frente al **13%** en 2021.

KPMG

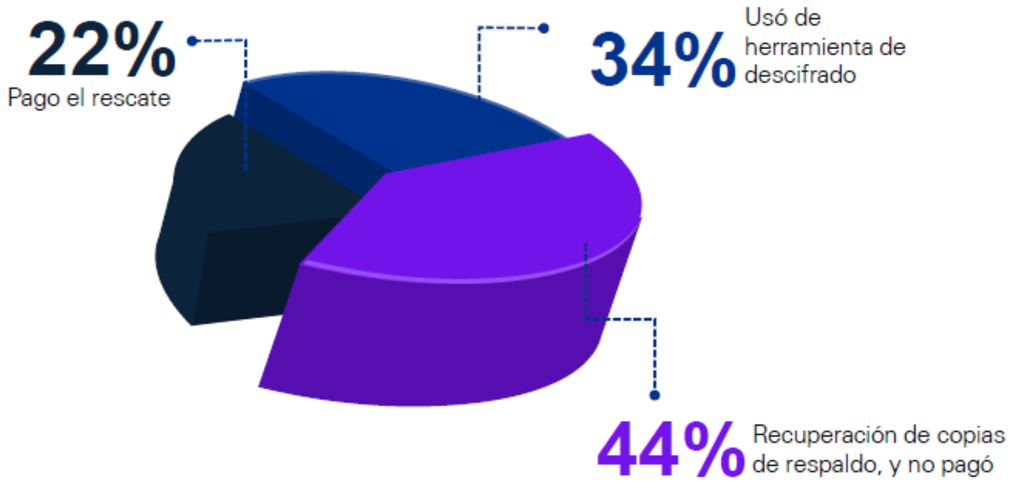
Ponte a prueba

Reto Ciberseguridad

START

¿Pagarías un rescate ransomware?

¿Cómo respondieron al ataque?



¿Tiene su empresa una política para pagar en caso de ataque?

32% Ninguna Política

21% No pagar rescate es nuestra Política

14% No lo sabe

65%

de los datos son recuperados después de que una organización paga por un rescate extorsivo de ransomware.

MICROSOFT.

¿POR QUÉ NO PAGAR?

14%

Pagamos si el rescate es menor que el costo de recuperar el sistema

13%

Pagamos si el rescate está cubierto por un seguro cibernético

6%

Pagamos solo como último recurso si no hay otra forma de recuperar los datos

Fuente: Data Health Check 2022 (databarracks.com)

TENDENCIAS EN VECTORES DE ATAQUE A LA SEGURIDAD DE LA IA

Ataque de intoxicación

Se refiere a un ataque en el que un adversario busca interferir en el proceso de entrenamiento de un modelo, normalmente entrenando el modelo con datos envenenados para incrustar una vulnerabilidad.

Ataque de inferencia

Una técnica similar a la vista en la extracción de modelos, donde un adversario busca observar los comportamientos de un modelo de aprendizaje automático a través de consultas repetidas.

Modelo de evasión

Se refiere a ataques adversarios que buscan evitar ser descubiertos por los sistemas de detección.

Extracción de datos

Busca duplicar un modelo privado a través de consultas repetidas al modelo para recoger las inferencias del modelo.

Riesgo en la operación

- Continuidad de la operación
- Impacto en el día a día
- Pérdidas de ingresos

Riesgo Operacional

▲

Riesgo de Ciber Seguridad

Riesgo a la reputación

- Posiblemente el más difícil de reparar
- Es probable que impacte tanto en la organización como al individuo (directivo)

Riesgo Reputacional

Riesgo de litigios costosos

- Impacto Organizacional
- Impacto a los Directivos
- En algunos casos litigios a los miembros responsables de la organizaciones si se alega descuido, negligencia o falta de gestión

Riesgo Legal

Participación y supervisión de la Junta Directiva

LIDERAZGO Y GOBIERNO

- Reexaminar el resultado de la evaluación de la capacidad de protección de la organización.
- Revisar y aprobar la estrategia y las solicitudes de financiación.
- Métricas: presupuesto ejecutado de iniciativas de protección de la estrategia aprobada vs. Total del presupuesto.

LEGAL Y CUMPLIMIENTO

- Comprender el panorama regulatorio que afecta a la organización.
- Revisar y aprobar la financiación del seguro cibernético (si procede).
- Métricas: revisar las tendencias de litigios.

FACTORES HUMANOS

- Establece el tono de la cultura.
- Comprender los protocolos de capacitación y concientización en ciberseguridad.
- Métricas: revisar patrones / tendencias de incidentes de personal por falta de sensibilización vs. Total de personal sensibilizado.

OPERACIONES Y TECNOLOGÍA

- Comprender la madurez actual de la estructura de control.
- Revisar las métricas de tendencias de incidentes relevantes.
- Métricas:
  – Nivel de madurez actual vs. El objetivo.
  – Incidentes de impacto alto vs. Total de incidentes.

GESTIÓN DE RIESGO DE LA INFORMACIÓN

- Revisar y aprobar la tolerancia al riesgo de ciberseguridad.
- Comprender el programa de proveedores externos.
- Métricas:
  – Riesgos mitigados dentro del nivel de tolerancia vs. Total de riesgos.
  – Proveedores externos que cumplen las disposiciones de seguridad de la organización vs. Total de proveedores.

CONTINUIDAD EMPRESARIAL Y GESTIÓN DE CRISIS

- Comprender la capacidad de respuesta actual.
- Revisar el estado de madurez general del plan.
- Participar en ejercicios de mesa (table top).
- Métricas: cantidad de pruebas realizadas satisfactoriamente vs. Cantidad de pruebas planeadas.

El marco de seguridad para la IA

Evaluar

- Gestión de canalizaciones AI
- Evaluación de riesgos para la seguridad de la IA
- Gestión de riesgos de seguridad de la IA
- Gobernanza de canalizaciones de IA
- Concienciación sobre IA adversaria

Asegurar

- Seguridad del ciclo de vida de la IA
- Solidez de la IA
- Detección de anomalías y eventos
- Seguridad de la cadena de suministro
- Supervisión continua de la IA

Responder

- Planificación de la respuesta
- Análisis
- Mitigación
- Mejoras
- Remediación

Cybersecurity considerations 2023

Nuestro informe identifica ocho (8) consideraciones a las que los CISOs deben dar prioridad en 2023, conoce más información escaneando el código QR.

Alain Almeida
Servicios de Tecnología
KPMG Colombia
abalmeida@kpmg.com

Felipe Silgado
Director Cyber
KPMG Colombia
fsilgado@kpmg.com

KPMG Colombia

KPMG_CO

Inspire Confidence. Empower Change.
Inspire Confidence. Empower Change.

#PromovemosLaTransformación

BOARD
Leadership Center
COLOMBIA