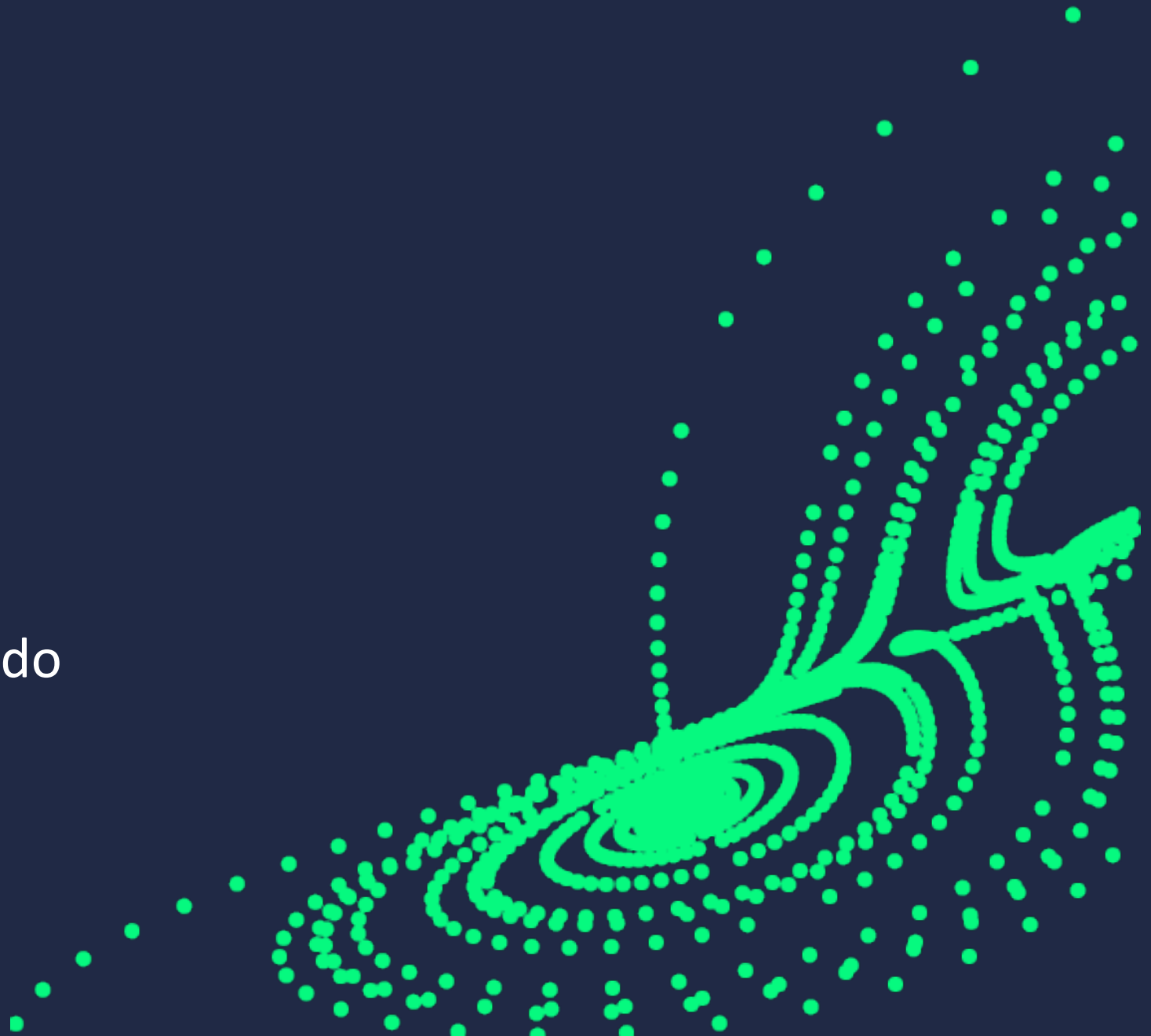
Ciberseguridad

// Sobreviviendo en el cibermundo

METABASE Q



¿Quiénes somos?

En Metabase Q, protegemos a las organizaciones de pérdidas financieras y de reputación con una ciberseguridad más inteligente.

Pensar “eso no nos va a pasar” es de los errores más grandes que puede cometer en la ciberseguridad.

Gracias a los análisis sistémicos del mercado y a las revisiones constantes, calibramos sus defensas para lograr que tenga una seguridad efectiva, que le permita crecer e innovar sin preocuparse por las ciberamenazas.

- Conglomerados y Corporativos
- Servicios Financieros
- *Retail*
- Sector Industrial

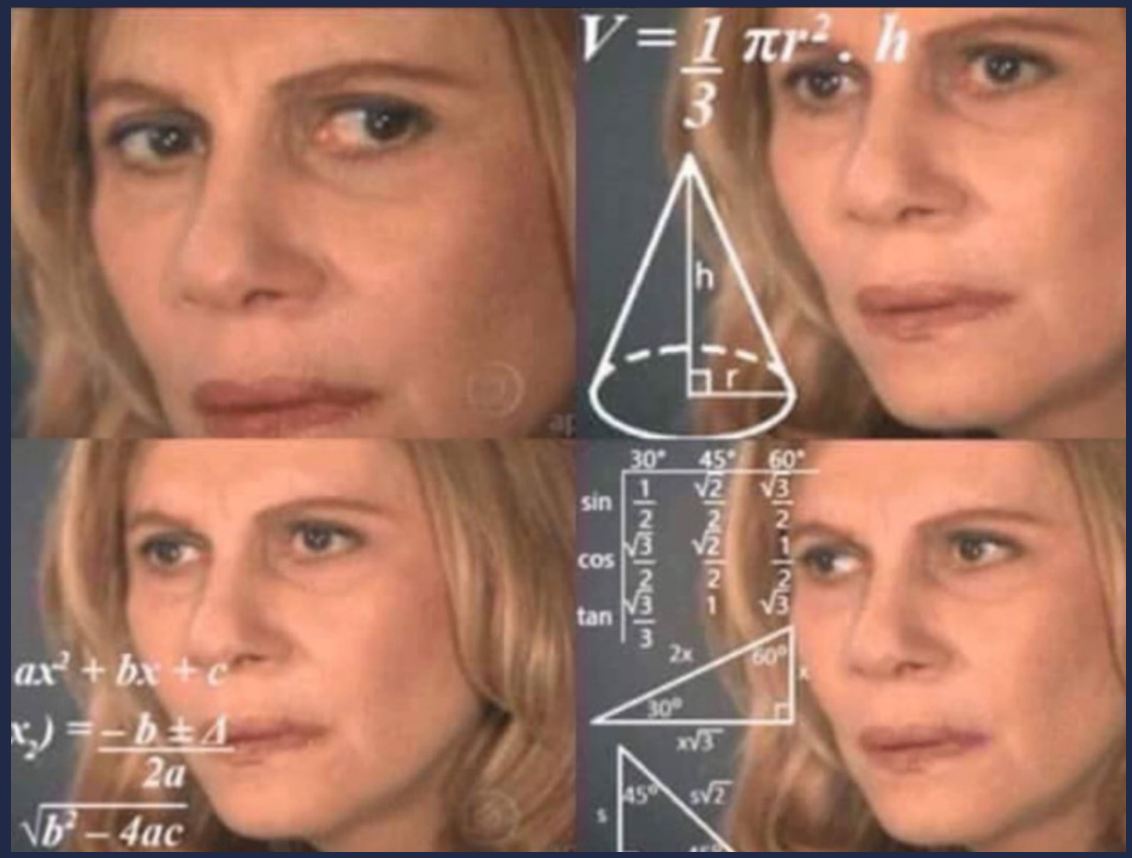
10 de las compañías más grandes de América Latina, agencias gubernamentales y más del 80% de las transacciones financieras en México dependen de Metabase Q para proteger sus sistemas e información contra ciberataques.

Contenido

// Better Base, Better Future

METABASE Q

¿Qué es eso de “Ciberseguridad”?

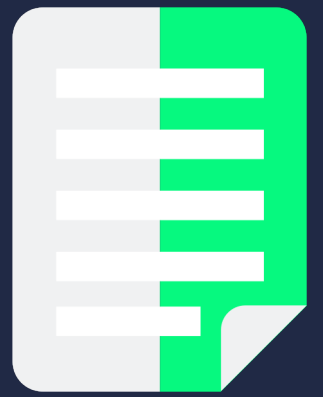


// Better Base, Better Future

METABASE Q

Ciberseguridad = ?

También tiene su historia, su idioma,
sus reglas, sus héroes y sus criminales.



// Better Base, Better Future

METABASE Q

Había una vez...

2013

SNOWDEN Y LA NSA

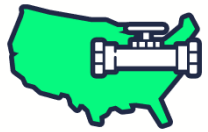
En 2013, **Edward Snowden, exempleado de la Agencia Central de Inteligencia de Estados Unidos (CIA), filtró información clasificada de la Agencia de Seguridad Nacional.** Si bien no es la mayor amenaza interna de la historia (que aún recae en Boeing), fue la más controvertida y con gran impacto social.

2020-2021

SOLARWINDS

El 13 de diciembre de 2020, SolarWinds, una empresa estadounidense que provee la red SolarWinds Orion a 300.000 clientes en todo el mundo, fue objeto de un ciberataque que se extendió a su clientela y pasó desapercibido durante meses. Empresas de la lista Fortune 500 y varias agencias del gobierno de Estados Unidos, fueron afectadas por este incidente.

2021



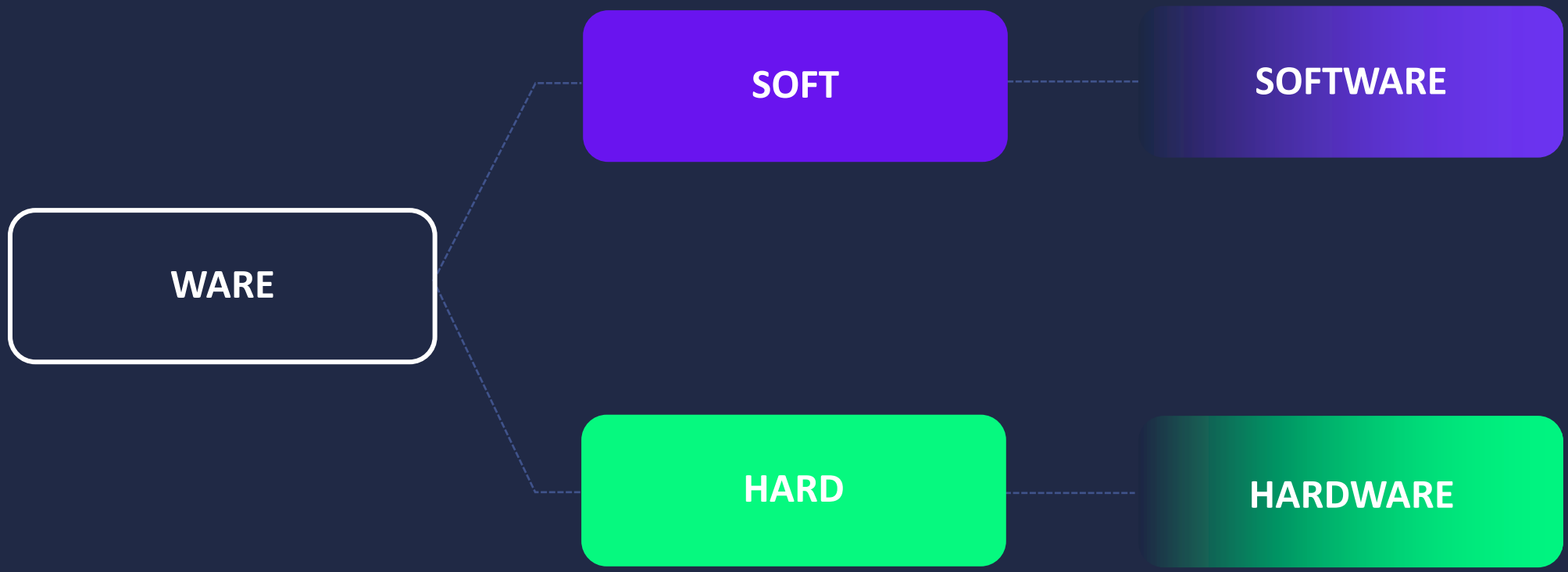
COLONIAL PIPELINE

El 7 de mayo de 2021, Colonial Pipeline, operador de un oleoducto que va desde Texas a Nueva Jersey, reportó que su infraestructura había sido comprometida por un ataque de tipo ransomware. El ciberataque se le atribuye al grupo DarkSide, bajo el modus operandi Ransomware as a Service. El incidente comprometió los sistemas que apoyan y gestionan el funcionamiento de los oleoductos y la distribución de combustible, generando escasez de gasolina e incremento en su precio. Es uno de los mayores y más exitosos ciberataques a un componente crítico de la infraestructura de un país hasta la fecha.

// Better Base, Better Future

METABASE Q

ABC de la Ciberseguridad



// Better Base, Better Future

METABASE Q

Adivina adivinador...

// Better Base, Better Future

METABASE Q

ABC de la Ciberseguridad

VIRUS

Tipo: Malware

Atributo: Infección

Nivel de daño: ★★★★★☆☆☆☆☆

Ataque: 5000

Defensa: 500

Forma de ataque: Este virus se activa al adherirse a otro programa, al momento de ejecutarse se replica modificando a otros programas e infectándolos con sus propios bits de código.

MALICIOUS CRYPTOMINING

Tipo: Malware

Atributo: ?

Nivel de daño: ★★★★★☆☆☆☆☆

Ataque: 7000

Defensa: 2000

Forma de ataque: Es una aplicación maliciosa que utiliza los recursos de los equipos (celular, computadora, entre otros) para minar cryptomonedas.

// Better Base, Better Future

METABASE Q

Estadísticas

Cada 39 segundos
ocurre un ciberataque.

(Universidad de Maryland EEUU, 2018).

100% de las organizaciones
con más de 500 teléfonos móviles sufrieron ciberataques en estos dispositivos.

(*Mobile Cyberattacks Impact Every Business. Check Point Software*).

3 de cada 5 empresas
que han instalado tecnologías IoT han sufrido ciberataques en estos dispositivos.

(*Internet of Things Cybersecurity Readiness - Osterman research for Trustwave*).

1 de cada 2 directivos de TI
de Agencias Federales consideran su mayor ciberamenaza la baja o nula formación en ciberseguridad en proveedores.
(*Federal Cybersecurity Survey, SolarWinds*).

// Better Base, Better Future

METABASE Q

Estadísticas

1 de cada 2 víctimas de ciberataque

vuelve a ser atacada con éxito en menos de un año.

(FireEye, 2018).

1 de cada 2 directivos de tecnología

identifican el *Phishing* como su principal ciberamenaza

(*Global Advanced Threat Landscape Report 2018 (Vanson Bourne for CyberArk*).

Las variantes de *Ransomware*

aumentaron un 45% en 2017

(Symantec, 2018).

Las variantes de *Malware*

en dispositivos móviles aumentaron un 54% en 2017

(Symantec, 2018).

El costo del *Ransomware*

para las organizaciones aumentó un 400%, llegando a $5,000 millones.

(Stroz Friedbere, 2018).

// Better Base, Better Future

METABASE Q

Vectores de ataque más comunes

Clic en un enlace:
E-mails, archivos, *webs* o redes sociales.

Clic en una imagen:
E-mails, *pendrives*, webs, etc.

Descarga/apertura de archivos:
Pop-ups, *banners* publicitarios, *e-mails* o archivos.

Actualizaciones:
No tenerlas al día o disponer de programas o sistemas operativos sin el debido mantenimiento y actualización.

Ausencia de controles:
Personas capacitadas, programas robustos, sistemas operativos bien configurados, redes, dispositivos o infraestructura vulnerable, etc

Ingeniería social:
Engañando o manipulando a las víctimas para que les faciliten información a través de una *web*, llamada, sms, etc.

// Better Base, Better Future

METABASE Q

Motivaciones principales

01

Espionaje industrial o inteligencia competitiva

02

Denegación de servicio

03

Instalación de programas no deseados (*malware* del tipo *spyware, keyloggers*, virus, *adware, bundleware, junkware, etc…*)

04

Monitorización de la conexión y control del dispositivo, obtención de nuestra huella digital, etc.

// Better Base, Better Future

METABASE Q

Repercusiones personales y profesionales

Perjuicio económico

Pérdida de tiempo

Pérdida de información

Pérdida de confianza en la información

Reducción en la productividad

Crisis reputacional personal y/o empresarial

Disminución de la confianza de clientes y personas usuarias

Posibles repercusiones legales

// Better Base, Better Future

METABASE Q

Las personas usuarias: el eslabón mas débil

39% de filtraciones de información es debida a la pérdida del dispositivo móvil en el área de trabajo y 34% en un vehículo.

(*Verizon Data Breach Report*).

191 días (aprox.) son los que las empresas necesitan para detectar una filtración de datos y 66 días para contenerla.

(*Cost of Data Breach Study - Ponemon Institute for IBM Security*).

1 de cada 3 personas abren *e-mails* de *phishing*, mientras que 1 de cada 5 abre archivos adjuntos maliciosos

(*Verizon Data Breach Report*).

4 de cada 5 ciberataques se produjeron por el uso de contraseñas débiles o robadas

(Stroz Friedberg).

La ingeniería social se está sofisticando mediante la personalización avanzada, el uso de datos reales y la omnicanalidad (*email*, SMS, publicidad web, etc.).

// Better Base, Better Future

METABASE Q

Las personas usuarias: el eslabón mas débil

El 39% de filtracio… de información

es debida a la pérdida del dispositivo móvil en el área de trabajo y el 34% en un vehículo. El 47% de filtraciones son causadas por *Malware*, el 28% por errores humanos y el 25% por un fallo de procesos o configuración.

(*Cost of Data Breach Study - Ponemon Institute for IBM Security*).

Hubo un aumento de 45%

en filtraciones de datos e información respecto al año anterior.

(*Annual DataBreach Year-end Review - Identity Theft Resource Center*).

4 de cada 5

empresas reconocen haber sufrido, al menos, una filtración de datos.

(*Global Threat Report - 451 Group for Thales*).

1 de cada 5 filtraciones

fue por error de un empleado interno.

(*Data Breach Investigations Report - Verizon*).

3.6 millones de dólares

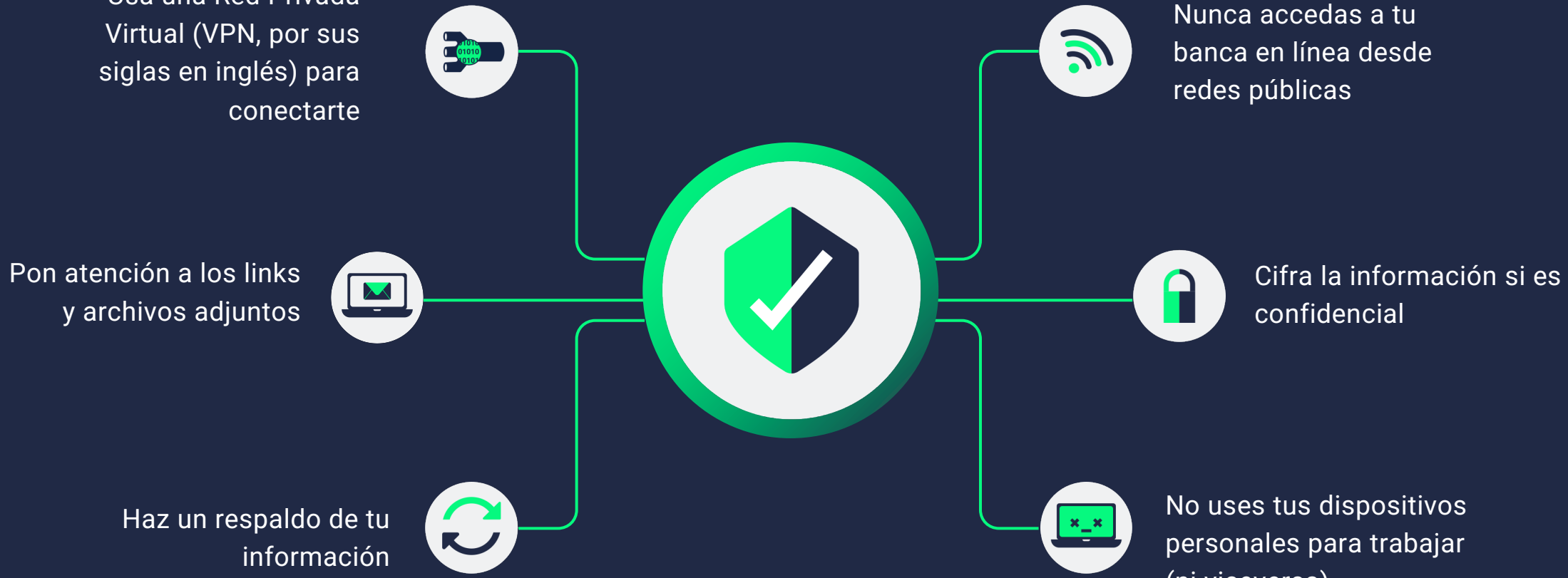
es el costo promedio de una filtración de datos.

(*Cost of Data Breach Study - Ponemon Institute*).

// Better Base, Better Future

METABASE Q

Recomendaciones



// Better Base, Better Future

METABASE Q

Recomendaciones

Al realizar tus pagos en línea utiliza una tarjeta digital

Cambia el nombre de tu contraseña y el nombre de tu red

Usa un gestor de contraseña y no repitas contraseñas

Mantén actualizados tus equipos

Refuerza la autentificación multifactor (MFA, por sus siglas en inglés)

Siempre presta atención a tus cuentas (Y ¡NO LAS COMPARTAS!)

// Better Base, Better Future

METABASE Q

¡Síganme los buenos!

// Creemos en el libre acceso a la educación

en ciberseguridad.

Cómo funciona:

- Gratuita
- La mejor educación
- Posibilidades de empleabilidad
- Compañías, instituciones, universidades y estudiantes colaboran para cerrar la brecha de talento en ciberseguridad.

// Better Base, Better Future

METABASE Q

Digital Cyber Academy

//¿Cómo funciona?

On-Demand

Nuestros laboratorios incluyen sistemas operativos virtuales, aplicaciones y muestra de *malware*, todo accesible desde el navegador.

Lúdico

Ataques simulados o ejercicios de “caja negra” que requieren pensamiento lateral y resolución de problemas creativa.

Alineado con el panorama de ataques

Nuestro equipo experto en el desarrollo de contenido de amenazas rápidamente crea nuevos laboratorios interactivos que sirvan como capacitación ante ellas.

// Better Base, Better Future

METABASE Q

DCA e Immersive Labs

//¿Qué logra la plataforma?

Equipar

Acceso a contenido interactivo que proporciona habilidades directamente relacionadas a los riesgos que actualmente enfrentan las empresas

Ejercitar

Aplicación de las habilidades ante los desafíos que se presentan en el mundo real, encontrando soluciones reales

Evidenciar

El progreso de quienes estudian en Immersive Labs se traza en función de marcos como NIST-NICE para garantizar que se desarrollen las habilidades adecuadas y MITRE ATT&CK para que los equipos practiquen las técnicas de amenaza

// Better Base, Better Future

METABASE Q

Cuando su seguridad funciona, su futuro funciona

Construya un mejor futuro con Metabase Q

contact@metabaseq.com
+52 55 2211 0920

// Better Base, Better Future