Medidas preventivas y recomendaciones

Por METABASE Q

//Medidas preventivas y recomendaciones

Conexión a red WIFI segura

¡Di no a las redes públicas! Evita ataques como *Man-in-the-Middle* (MITM). Si es posible, cambia el nombre de la red y la contraseña. Si tienes que conectarte a redes públicas, evita hacer transacciones sensibles (bancarias o de trabajo) y hazlo a través de una VPN

Administrador de contraseñas

Utilizar una aplicación o servicio de administración de contraseñas. No permitas que tu navegador las memorice. Selecciona una contraseña maestra difícil pero fácil a la vez de recordar para ti. Se recomienda que sean tres palabras no relacionadas pero significativas para ti.

Características de una buena contraseña

Crea contraseñas de uso único de al menos 12 caracteres e incluya letras, números y caracteres especiales.
Evita contraseñas débiles y comúnmente usadas.
No uses información personal como respuesta a tus preguntas de seguridad. Cambia tus contraseñas después de incidentes y no las compartas por medio de mensajes.

Actualizaciones al día

Instala todas las actualizaciones de los programas y sistemas que utilizas en todos tus dispositivos. No hacerlo representa un riesgo que puede ser aprovechado por ciberdelincuentes de todo el mundo. Regularmente, las actualizaciones solucionan fallas de seguridad encontradas en versiones previas.

Aplicaciones de mensajería

Si vas a enviar información confidencial o delicada, evita hacerlo a través de los servicios de mensajería instantánea de redes sociales. Si vas a utiliza algún servicio de mensajería instantánea asegúrate que sea una que cifre tu información como Telegram, Wire o Signal.

Navegador web seguro

Asegúrate que las páginas que visitas cuenten el certificado de seguridad HTTPS. Utiliza navegadores que bloqueen automáticamente cookies intrusivas y *ad trackers* cuyo fin sea recopilar información de tus búsquedas con fines comerciales (*privacy badger*).

Autenticación multifactor

Refuerza la autenticación multifactor (MFA) en donde sea posible:

- Correo electrónico
- Redes sociales
- Plataformas de *e-commerce*
- Software para almacenamiento en la nube (DropBox, Google Drive, etc.)

Una capa adicional de protección: 2FA

metabaseq.com
contact@metabaseq.com

METABASE Q

//Medidas preventivas y recomendaciones

Red Privada Virtual (VPN)

Utiliza una Red Privada Virtual (VPN) en tus dispositivos. Esto permite que te conectes a Internet a través de esta red en lugar de hacerlo de manera directa con tu módem o *router*. En la sección de configuración de tu celular o tus dispositivos encontrarás la opción de activar la VPN.
También puedes descargar algún *software* comercial.

Computadora "Dedicada"

Mantén la información de tu trabajo en la computadora del trabajo. Evita usar tu computadora o dispositivos personales para cuestiones laborales. Asegúrate de que sólo tú la uses, para tu protección y la de tu empresa.

Ciberconciencia: *phishing*

Date cuenta que eres un blanco. Los ataques ya no van dirigidos a personas o empresas específicas, se hacen a todos los niveles porque así es más probable que tengan éxito. Mantén un estado de alerta constante al abrir enlaces electrónicos o archivos descargables. En cualquier momento puedes ser una víctima de *phishing*.

BYOD (*Bring your own device*)

Trabajando con equipo del trabajo (o propio) a distancia

Lo bueno:

- Mayor productividad al conocer sus dispositivos.
- Dispositivos más modernos y con mejor hardware.
- Usuarios familiarizados con sus sistemas.
- Mayor flexibilidad.
- Reducen costos a las compañías.

Lo malo:

- Puede haber fuga de información al estar fuera de la gestión de la compañía.
- Vulnerables al estar fuera de políticas de la empresa.
- Dispositivos perdidos/robados.
- No existen los controles que tendría la empresa sobre estos dispositivos.

Aplicaciones recomendadas

Box/ Egnyte: almacenamiento en la nube.
El *software* comercial más recomendable es **Google Drive.**

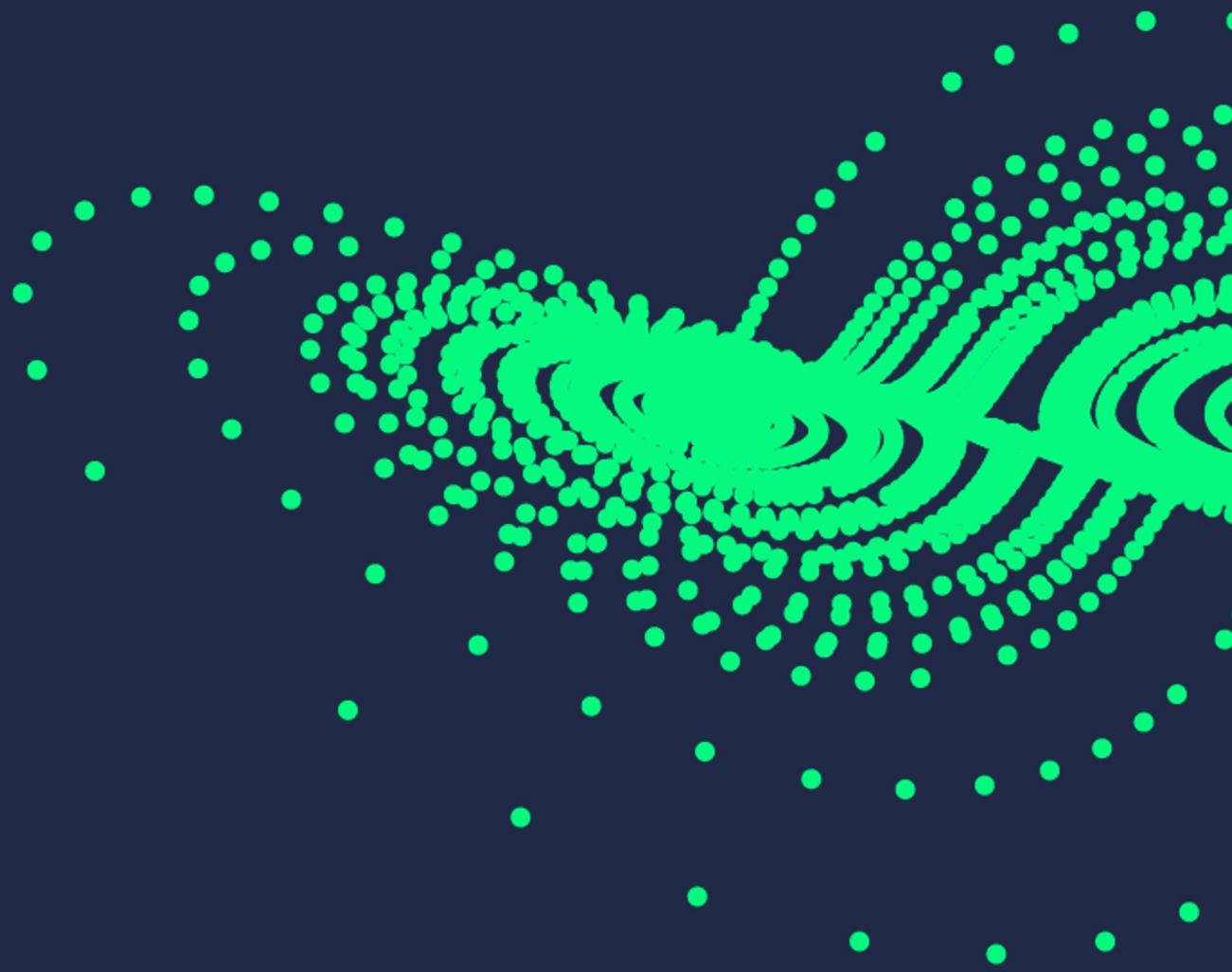
Lockdown / NetGuard: Firewall móvil.

iVerify: *Checklist* de seguridad y privacidad.

KeepSafe: Resguardo de documentos sensibles (imagen y video).

metabaseq.com
contact@metabaseq.com

METABASE Q



When your security works, your future works

Build a better future with Metabase Q

contact@metabaseq.com
+52 55 2211 0920

// Better Base, Better Future