Cuando los Ejecutivos Viajan, el Riesgo Digital Viaja con Ellos

Dispositivos comprometidos, escuchas no autorizadas y exposición física fuera del entorno digital de confianza de la organización.

RISCCO | 5 de Junio de 2026 | 8 minutos | 1881 palabras

Contenido

1. El problema y los riesgos.
2. Pasos a seguir si pierdo el dispositivo
3. Arquitectura de recuperación y continuidad.
4. Reducir las probabilidades.
5. ¿Cómo RISCCO puede ayudar?

1. El problema y los riesgos

Cada vez que un Ejecutivo viaja, la información sensible de la organización viaja con él.

Fuera de la oficina, los controles se detienen.

En el momento en que el Ejecutivo sale de la oficina y se encuentra en el aeropuerto, taxi, hotel o restaurante, la mayoría de los controles de seguridad que protegen al resto de la organización dejan de aplicarle.

Rutinario, no teórico.

Según el Lost & Found Index 2026 de Uber, los teléfonos, billeteras, pasaportes y laptops siguen estando entre los objetos más olvidados — un recordatorio de que el riesgo en viajes ejecutivos es rutinario, no excepcional.

Un dispositivo. Toda la organización.

Un solo teléfono o laptop puede contener los datos más sensibles de una empresa — o de una institución de gobierno —, las credenciales y el poder de decisión. El atacante ya no necesita llegar a la oficina — solo al Ejecutivo, una vez, en cualquier lugar.


La red más peligrosa suele ser la que parece más conveniente.
Wi-Fi
Conéctate
Disfruta de internet de alta velocidad

1. El problema y los riesgos

Riesgos	Salas VIP Aeropuerto	Taxis, ride-share o Aviones	Restaurantes Cafés	Habitación o lobby de Hotel
Robo o pérdida de dispositivos en tránsito. Los dispositivos se pierden o son robados. Un solo dispositivo perdido que contenga credenciales de acceso, correo sin conexión o archivos sin cifrar puede convertirse en una brecha de seguridad.	✓	✓	✓	✓
Redes Wi-Fi comprometidas y redes no seguras. Los hackers pueden crear puntos de acceso Wi-Fi fraudulentos que se hacen pasar por uno original. Un Ejecutivo que se conecte puede exponer, sin saberlo, credenciales de acceso e información sensible de la organización y personal.	✓	✓	✓	✓
Estaciones públicas de carga USB comprometidas. Un puerto, cable o adaptador de carga fraudulento puede exponer un dispositivo al robo de datos o malware mientras el Ejecutivo carga un teléfono, laptop o Tablet en un lugar público.	✓	✓	✓	✓
Manipulación de dispositivos desatendidos en habitaciones de hotel. Las habitaciones de hotel son accedidas rutinariamente por personal autorizado. Un dispositivo dejado desatendido está expuesto a manipulación física, acceso no autorizado o alteración de software.				✓
Teléfono o dispositivo olvidado en un taxi, ride-share o Avión. Un dispositivo olvidado puede contener información de la empresa o personal, y permitir acceso directo a datos y sistemas privados.		✓		

Nota: *"Dispositivos" incluye laptops, teléfonos, tablets, audífonos, relojes inteligentes y lentes inteligentes.*

RISCCO

¿Qué hacer si el dispositivo ya no está?

2. Pasos a seguir si pierdo el dispositivo

La velocidad supera a la perfección. *Los primeros 15 minutos determinan si esto se convierte en un incidente recuperable o una brecha de seguridad.*

Primeros 15 Minutos

1. **Activar el borrado remoto.** Llamar al personal de TI o Seguridad de la organización para que lo guíen en el procedimiento respectivo. Si lo anterior no es posible, hágalo usted mismo. Ingrese con sus credenciales a su cuenta en https://www.icloud.com/ (Iphone) y si es Android, revise la documentación de la marca de su teléfono.
2. **Restablecer credenciales primarias desde un dispositivo limpio.** Correo, SSO, VPN, gestor de contraseñas, portales financieros.
3. **Empezar a utilizar el teléfono de "backup".** El teléfono de "backup" (se menciona página 8), empiece a utilizarlo para aprobar inicios de sesión o autenticación MFA. Si no tienes un teléfono de "backup", llamar a persona de TI o seguridad and who's everyone else hey E definitelyncia. La ausencia de un teléfono de "backup" hace más lento todo el proceso de volver a estar operativo.
4. **Presentar la denuncia en la Policía**. En el operador del taxi, aerolínea u hotel siempre solicitarán el número de denuncia para el seguro, bloqueo por parte de la operadora telefónica y/o cualquier otro trámite de emergencia.

Perdido, robado y manipulado, se actua de forma distinta

PERDIDO *(taxi, restaurante, salas VIP)*

La recuperación aún es posible. Monitorear la señal de ubicación del teléfono (Find My – Iphone o Find My Device - Android) y tratar el dispositivo como comprometido y quizás recuperable hasta demostrar lo contrario.

ROBADO

Asumir que el dispositivo está comprometido. Activar el borrado remoto. Restablecer credenciales de acceso, presentar una denuncia policial y alertar a la compañía y/o amistades sobre cualquier transacción sensible en curso.

MANIPULADO O FUERA DE LA VISTA *(inspección en aduana, migración o para acceder una oficina)*

Si tiene duda sobre la manipulación del dispositivo, no conectar a la red corporativa hasta que personal de TI o seguridad lo revise. Utilizar el teléfono de "backup" en su lugar.

Consejo: La tarjeta de recuperación de bolsillo. *Lleve una tarjeta impresa tamaño billetera con: teléfono directo de TI, el móvil del Oficial de Seguridad, el número de su asistente, la credencial maestra del gestor de contraseñas (si tiene) y los códigos de recuperación de las 2 o 3 cuentas más críticas que no estén ya protegidas por el teléfono de "backup". Use seudónimos de cuenta (no su nombre real). Revise y actualice la tarjeta cada seis meses. El primer instinto tras una pérdida es restaurar la conectividad a cualquier costo. Sin una tarjeta de recuperación es muy complicado y frustrante.*

RISCCO

3. Arquitectura de recuperación y continuidad

Un teléfono de “backup” hace más que ayudarle a estar conectado. Le permite seguir trabajando, pero solo si el teléfono lo mantiene listo.

El teléfono de “backup” en la caja fuerte del hotel debe tenerlo listo, no mantenerlo vacío.

El teléfono de “backup” solo es útil si se mantiene preparado: sincronizado cuando sea posible, con las aplicaciones críticas instaladas, probado periódicamente y con los métodos de recuperación documentados. Contactos, calendario y correo pueden mantenerse sincronizados; aplicaciones como WhatsApp, Signal, banca móvil y MFA deben configurarse o validarse previamente según las restricciones de cada plataforma

Cuando el teléfono principal se pierda, el de “backup” no es un dispositivo vacío que haya que configurar, es el teléfono que le permite de forma rápida volver a estar conectado trabajando.

- Si se pierde el teléfono principal, con el teléfono de “backup” se restablece voz, MFA, aplicaciones de bancos, WhatsApp y correo en quince minutos. El viaje continúa.
- Si lo que se pierde es el laptop, el teléfono de “backup” es la oficina móvil. Correo, calendario, documentos, videollamadas, mensajería, todo desde el dispositivo.
- Si pierde ambos (teléfono principal y laptop), el teléfono de “backup” es el salvavidas que hace las llamadas, trabaja con las aplicaciones importantes y sigue en contacto con la oficina y su familia.

El teléfono de “backup” y su costo real. Dos teléfonos. Dos líneas. Dos facturas mensuales. La objeción es predecible. Pero el costo de un teléfono de “backup” nunca ha superado el costo de estar incomunicado en la habitación de un hotel extranjero, sin soporte de TI, sin MFA, sin mensajes, sin una forma de llamar a casa, en el momento exacto en que el Ejecutivo necesita todo eso.

Un teléfono de “backup” no es un gasto. Es el seguro más barato que un Ejecutivo comprará jamás. Para un Ejecutivo cuyas decisiones mueven transacciones, votos de junta, entre otros, el costo es un error de redondeo frente a una sola hora de estar incomunicado.

4. Reducir las probabilidades

Tres niveles. Elija el que su organización pueda realmente sostener.

NIVEL 1
No negociable

Cada viaje. Cada Ejecutivo.

Fortalecer la seguridad del dispositivo

- Cifrado de disco completo verificado antes de viajar.
- Cubiertas de cámara web y filtros de privacidad en cada dispositivo.

Preparación para la recuperación

- Teléfono de “backup” configurado, sincronizado y probado.
- Códigos de recuperación impresos y almacenados por separado (tarjeta de recuperación de bolsillo).

Disciplina al usar redes

- No utilizar Wi-Fi público para trabajo sensible salvo use un VPN.
- Apagar Wi-Fi y Bluetooth cuando no se usen.
- No utilizar cargadores tipo USB públicos. Use cargador personal.

Custodia física

Nunca dejar los dispositivos desatendidos. Utilice la caja fuerte de la habitación para el teléfono de “backup”. Nunca deje encendido el laptop si no podrá vigilarlo.

NIVEL 2
Viajes sensibles

Cuando el viaje lleva información que la organización no puede permitirse perder o que terceros no autorizados accedan.

- Charlas regulares o panfletos de concienciación sobre seguridad en viajes para los Ejecutivos.
- De ser posible, laptop dedicada de viaje cargada solo con los datos y aplicaciones esenciales para el viaje.
- Con ayuda del personal de TI y seguridad, eliminar credenciales de acceso en caché y archivos de correo sin conexión antes del viaje.
- Bloqueo automático (30–60 segundos) en el teléfono y 5 minutos para el laptop.
- Verificar con personal de TI que la configuración del borrado remoto está activa antes del viaje.

NIVEL 3
Destinos Riesgo-Alto

Fronteras con inspectores, entornos de inteligencia hostil, vigilancia persistente.

- Viajar con una laptop que tenga una imagen del disco reinstalada, sin datos históricos ni identidad de marca que identifique a la organizacional
- Utilice sellos antimanipulación en cada dispositivo; inspeccionar cuidadosamente antes de reutilizar el dispositivo.
- Si el dispositivo fue revisado o inspeccionado por terceros, a su regreso, que el personal de TI o seguridad lo revise antes de conectarlo a la red de la organización.
- Tratar cualquier dispositivo al cual le haya perdido la vista, como comprometido.

Cada nivel incluye al anterior. *El Nivel 3 supone el Nivel 2; el Nivel 2 supone el Nivel 1.*

RISCCO

5. ¿Cómo RISCCO puede ayudar?

Dos artículos. Un perímetro.

Ayudándolo a:

1) Construir un protocolo de viajes ejecutivos
2) Crear una matriz de riesgos y controles
3) Brindar sesión de orientación ejecutiva de concienciación.

Compartiendo Artículos Ejecutivos para mitigar el riesgo:

DENTRO DEL EDIFICIO (OFICINA)

Sus reuniones confidenciales no son privadas

Escucha no autorizada, grabación sin consentimiento y espionaje digital en juntas, comités y agencias de gobierno. *Aceder aquí.*

RISCCO — Enero de 2026

FUERA DEL EDIFICIO

Cuando los Ejecutivos Viajan, el Riesgo Digital Viaja con Ellos

Dispositivos comprometidos y exposición física fuera del entorno de confianza de la organización.

RISCCO — Junio 2026

Amenazas distintas, mismo objetivo: proteger la conversación, la decisión y los datos dondequiera que esté el Ejecutivo. La mayoría de las firmas escribe artículos. RISCCO escribe una doctrina, un artículo a la vez.

Una conversación de 30 minutos es el próximo paso.

Antonio Ayala I., CEO — **aayala@riscco.com**

RISCCO

Bibliografía

Imágenes

1. https://openai.com/

Fuentes

1. https://www.uber.com/nz/en/newsroom/lost-found-index-2025/
2. Kaspersky — DarkHotel APT campaign: https://www.kaspersky.com/about/press-releases/darkhotel-aptattacks-high-profile-executives-through-hotel-wi-fi
3. FCC — Cybersecurity Tips for International Travelers: https://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers
4. FBI — Public advisory on juice jacking: https://www.fbi.gov/contact-us/field-offices/denver/news/tech-tuesday-avoiding-juice-jacking
5. CISA — Cybersecurity While Traveling: https://www.cisa.gov/news-events/news/cybersecurity-while-traveling
6. NIST — Guidance on telework and travel security https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/telework-and-travel

CONTACTOS

Panamá, Centroamérica y El Caribe

Antonio Ayala I.
CEO
aayala@riscco.com

Rubén Fernández
Gerente de Consultoría
rfernandez@riscco.com

Marinelda Morales
Gerente Comercial
mmorales@riscco.com

República Dominicana y Puerto Rico

Eury Valdez
Asesor Comercial
efvaldez@riscco.com

El Salvador, Guatemala, Honduras, Costa Rica y Nicaragua

Jeniffer Escoto
Asesor Comercial
jescoto@riscco.com

Acerca de RISCCO

RISCCO es una firma de consultoría internacional e independiente, comprometida con transformar la forma en que las organizaciones gestionan el riesgo y adoptan la Inteligencia Artificial. Combinamos un enfoque riguroso en GRC (Gobernanza, Riesgo y Cumplimiento) con analítica de datos avanzada e Inteligencia Artificial para ayudar a nuestros clientes a anticipar riesgos, fortalecer la gobernanza y resolver desafíos complejos. Con sede en Panamá y presencia en seis países, en 2026 cumplimos 17 años sirviendo a más de 200 organizaciones líderes en Centroamérica y el Caribe.

Rigor internacional. Ejecución ágil. Impacto medible.
Pensamos como estrategas. Ejecutamos como especialistas.

riscco.com