RISCCO

IT Risk & Security
Internal Audit

10 Años
2009-2019

RESULTADOS

Sondeo sobre la privacidad de mensajes sensitivos de la organización vía "Chats”.

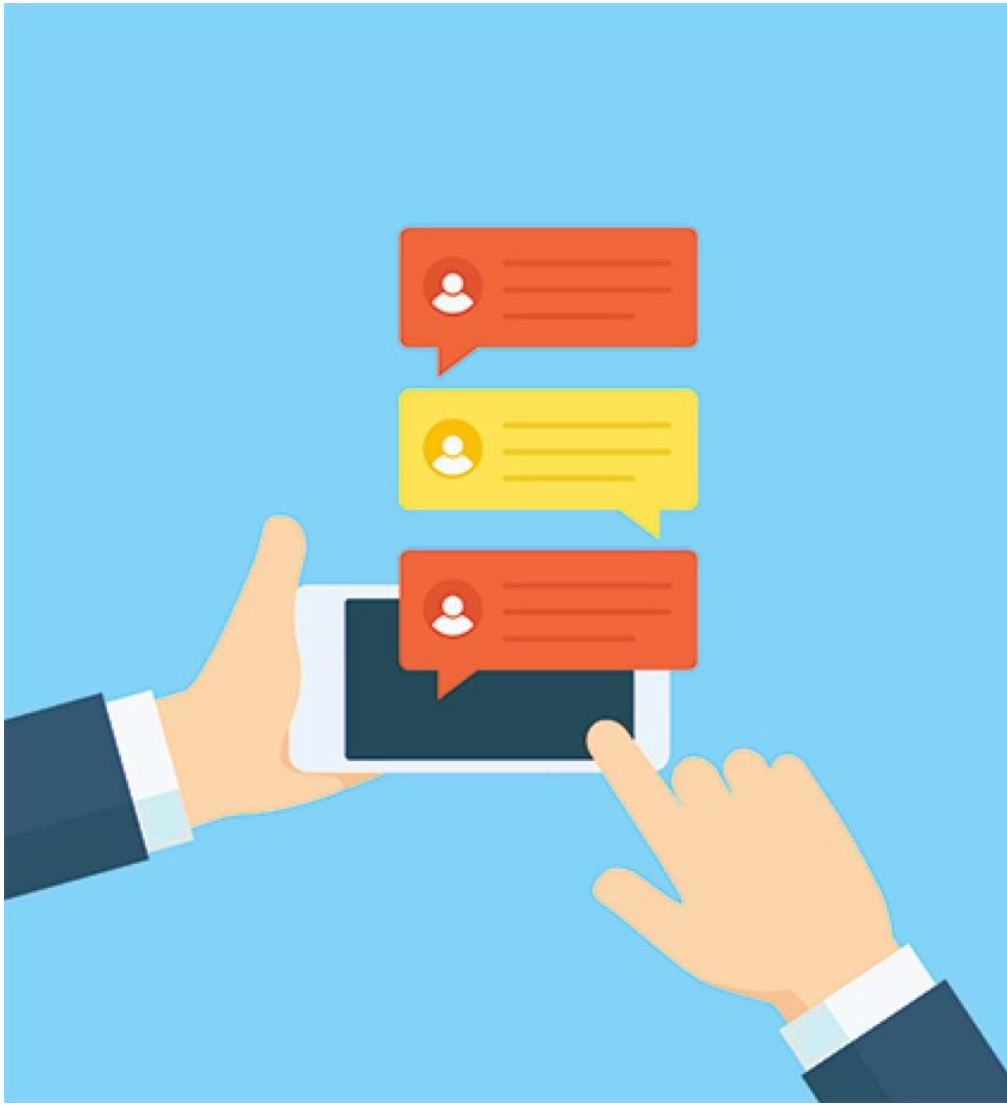
25 de julio de 2019
Punto de Vista

CONTENIDO

a. El peso de la filtración de “chats” confidenciales.

b. ¿En qué consiste el problema?

c. Consejos y buenas prácticas.



© 2009 – 2019. Todos los derechos reservados.

a. El peso de la filtración de “chats” confidenciales.

Al momento de emitir este documento *(25 de julio de 2019, 8am. hora Panamá)*, hacía pocas horas que el Gobernador de Puerto Rico anunciaba su renuncia al cargo en medio del llamado “escándalo del chat”. Evento devastador, inédito (en la isla), delicado y que deja lecciones que cualquier Ejecutivo debe valorar.

¿Por qué?

Porque se filtraron a los medios 889 páginas de “chats” de un grupo creado en la aplicación ***Telegram*** entre el Gobernador y su círculo íntimo de colaboradores. No es que “hackearon” la cuenta o el teléfono del Gobernador. Se infiere de las noticias que un miembro del grupo del “chat”, filtró los mensajes.

Ahora bien, piense en su organización. ¿Se ha preguntado cuántos “chats” con temas confidenciales de su organización pueden en este momento estar en grupos de “chats” entre sus colaboradores?

Si cree que en los grupos de “chats” utilizados por sus colaboradores no existe información confidencial, piénselo de nuevo. Quizás la realidad sea peligrosamente diferente.

© 2009 – 2019. Todos los derechos reservados.

b. ¿En qué consiste el problema?

- Abuso a todos los niveles, del uso de herramientas como ***Whatsapp*** y similares, para intercambiar asuntos confidenciales de la organización.

- Ausencia de una política o protocolo que instruya a los colaboradores sobre, en el contexto de la organización, qué se puede y qué no se puede enviar por “chats”.

- Poca o limitada concienciación a los colaboradores sobre las implicaciones que se filtren a terceros “chats” confidenciales.

- Equivocada tranquilidad producto de que herramientas como ***Whatsapp*** y similares, difícilmente pueden ser “hackeadas”. Si bien lo anterior es relativamente cierto, eso no tiene nada que ver con que un colaborador resentido filtre comunicaciones confidenciales a terceros.

© 2009 – 2019. Todos los derechos reservados.

RISCCO

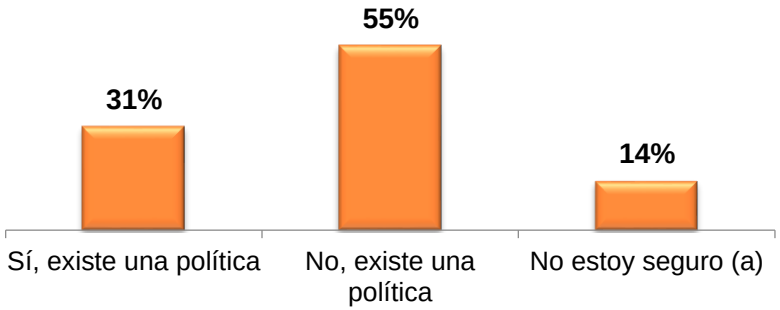
b. ¿En qué consiste el problema?

El 22 y 23 de julio de 2019 realizamos un sondeo sobre este tema a 420 Ejecutivos en Panamá.

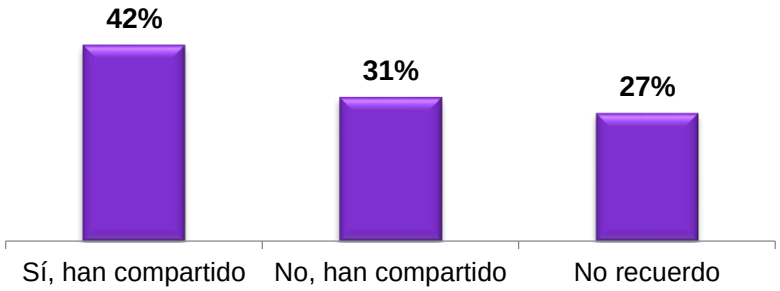
Las respuestas de 117 participantes evidencian que existen espacios importantes de mejoras.

Que el 42% haya indicado que recordaba que compañeros compartieron temas confidenciales vía “chats” es preocupante, más aún, si el 69% confirmó que no existe o no recuerda que exista una política al respecto.

¿Conoce si en su organización existe alguna política para cuáles temas sensitivos y/o confidenciales no se puede utilizar los "chats" de su teléfono?



¿Recuerda si en los últimos dos años compañeros de trabajo han compartido vía "chats" temas sensitivos y/o confidenciales de la organización?



© 2009 – 2019. Todos los derechos reservados.

b. ¿En qué consiste el problema?

Si a lo anterior se le adiciona que el 87% indicó no conocer o recordar de la existencia de algún control para identificar cuándo se envíen “chats” confidenciales, tiende angustiar.

En frío, es muy posible que en “chats grupales” existan temas confidenciales hoy día de su organización, sin que los que dirigen la organización lo sepan.

Las consecuencias de la filtración de mensajes confidenciales de su organización sería igual o más devastador que la situación que enfrentó el ex Gobernador del país caribeño.

© 2009 – 2019. Todos los derechos reservados.

c. Consejos y buenas prácticas

Si es un asunto confidencial de su organización, preferiblemente no utilizar “chats” grupales o individuales para ventilarlo.

Si inevitablemente tiene que enviar “chats” con asuntos sensitivos de su organización:

1. Defina y comunique una política y sanciones sobre el uso de “chats” grupales para asuntos confidenciales. Que la misma establezca las excepciones y condiciones, cuando se puede hacer.

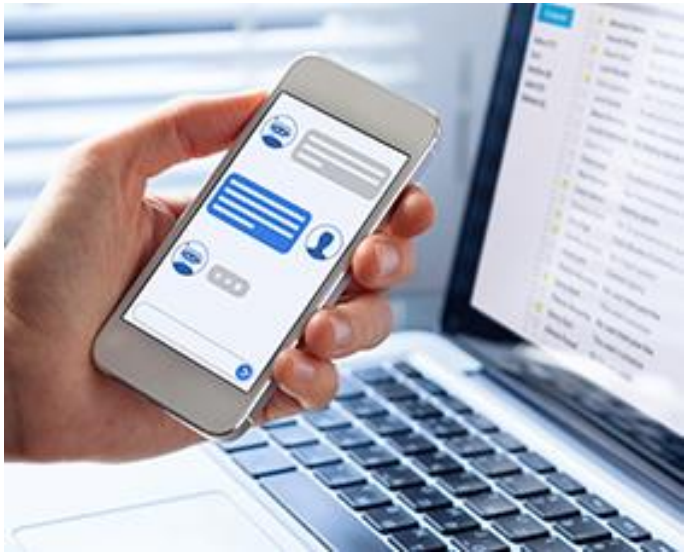
2. Eduque al personal sobre la política con muchos ejemplos.
   La política como tal, no garantiza nada.

© 2009 – 2019. Todos los derechos reservados.

c. Consejos y buenas prácticas

3. Utilice apps como ***Signal*** o similares, la cual al activar un parámetro en la configuración, una vez leído el mensaje, lo borra automáticamente.

4. Habilite la opción para encriptar los datos almacenados en su *smartphone*.



5. Si el *smartphone* que utiliza el colaborador es de la organización, solo para asuntos de la compañía, cada cierto tiempo revise el dispositivo para validar el cumplimiento de la política.

© 2009 – 2019. Todos los derechos reservados.

CONTACTOS

RISCCO
IT Risk & Security
Internal Audit

10 Años
2009 - 2019

Antonio Ayala I.
t: 279-1410 Ext. 104
aayala@riscco.com

Raúl Lezcano
t: 279-1410 Ext. 108
rlezcano@riscco.com

riscco.com

Es una compañía panameña, independiente y dedicada de manera exclusiva, a la consultoría en riesgo tecnológico, peritajes informáticos, seguridad de información y auditoría interna; compuesta por profesionales con el conocimiento y credibilidad necesaria para traducir aspectos muy técnicos a un lenguaje simple y con sentido de negocio. Con diez (10) años de haber iniciado operaciones, RISCCO cuenta en su cartera de clientes con compañías privadas e Instituciones del Estado Panameño, líderes en su ramo.

© 2009 - 2019 RISCCO. Todos los derechos reservados.