RISCCO

IT Risk & Security
Internal Audit

TELETRABAJO:

Consejos y buenas prácticas de seguridad de información.

#QuedateEnCasa

RISCCO | 27 marzo 2020 | 6 minutos | 813 palabras |

CONTENIDO

1. Nuestro punto de vista.
2. Consejos y buenas prácticas.

1. Nuestro punto de vista

Cuarentena, casos de COVID-19 en aumento, economía en el piso, pérdida de empleos, por mencionar solo algunas consecuencias.

Lamentablemente, a lo anterior hay que adicionar los riesgos y amenazas de ciberseguridad y de privacidad de datos, que enfrentan las personas y las organizaciones con el teletrabajo.

En marzo de 2020, la Organización Mundial de la Salud, fue atacada por *Hackers* que trataron, sin éxito, de filtrarse en sus sistemas. En adición, el 14 de marzo el grupo de *Hackers Maze* publicó datos personales de miles de ex pacientes después de que la Institución médica del Reino Unido *Hammersmith Medicines Research (HMR)*, se negara a pagar el rescate exigido por los *Hackers*.

En estos tiempos, los *Hackers* toman ventaja de que el control no está en la lista de prioridades de muchas personas en cuanto al teletrabajo, razón por la cual sugerimos algunas buenas prácticas y consejos de seguridad de información.

2. Consejos y buenas prácticas

a. SEA PROACTIVO

- Cumpla las políticas de seguridad de información corporativas. Recuerde, está en su casa pero trabajando para la organización.
- Sea desconfiado de abrir *emails-chats* sensacionalistas con la última información sobre COVID-19. Piense que podría ser la puerta de entrada para infectar su dispositivo digital.
- Reporte a la mesa de ayuda o soporte técnico de la organización, cualquier actividad sospechosa o inusual en su dispositivo digital.

b. CONTRASEÑAS

- Utilice contraseñas fuertes para acceder a la red corporativa de al menos 10 caracteres que incluyan: letras mayúsculas, letras minúsculas, números y caracteres especiales.
- Habilite una contraseña de acceso al computador (estamos en casa pero pueden haber niños, mascotas, etc.).
- En caso no lo haya hecho recientemente, cambie la contraseña de acceso al WIFI de la casa.

Mantenga la seguridad física del dispositivo digital. En caso no lo vaya a utilizar, mejor apáguelo o bloqueé su acceso.

2. Consejos y buenas prácticas

c. REDES Y ACCESO

- Utilizar VPN *(Virtual Private Netkwork)* para conectarse a la red corporativa. Cuando no la vaya a usar por cierto tiempo, desconecte la conexión VPN.
- Utilice en la red WIFI de su casa el protocolo de conexión WPA2 o WPA3.
- Si va utilizar el dispositivo digital para un fin personal, preferentemente desconéctese de la red corporativa.

d. RESPALDO A LOS DATOS (*BACKUPS*)

- Salvo que los documentos en los que trabaje sean almacenados directamente en los servidores de la organización, realice *backups* regularmente de sus dispositivos digitales utilizados para teletrabajo.

2. Consejos y buenas prácticas

e. PARA LAS ORGANIZACIONES

- Defina y comunique una política de teletrabajo (sencilla, clara y directa).
- Informe a los colaboradores sobre nuevos esquemas de ataques relacionados con COVID-19.
- Establezca una línea de soporte técnico para ayudar a los colaboradores con problemas técnicos.
- Establezca controles de seguridad estrictos sobre la base que cualquier conexión remota a la red corporativa puede ser un evento hostil, no un colaborador haciendo su trabajo.
- Que las conexiones de los colaboradores sea al menos con doble factor de autenticación.
- Considere dar acceso remoto a los colaboradores en horarios específicos y no las 24 horas.
- Asegurar que los dispositivos digitales utilizados para conectarse a la red corporativa (ya sean de la organización o de lo colaboradores) tengan *antivirus, antimalware* y *firewall* actualizados.

Nota:
Algunos consejos son del U.S. Federal Trade Commission (FTC); National Institute of Standards and Technology (NIST)

CONTACTOS

IT Risk & Security
Internal Audit

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 once (11) años de haber iniciado operaciones, RISCCO cuenta en su cartera de clientes con compañías privadas e Instituciones del Estado Panameño, líderes en su ramo.