Volumen 1 | Número 3

Mayo/2020

Los desafíos de ciberseguridad frente al teletrabajo

El teletrabajo presenta ventajas, pero también riesgos de ciberseguridad. Actualmente la gran mayoría de los colaboradores están trabajando de forma remota y están expuestos a las vulnerabilidades en videollamadas y en correos electrónicos. En consecuencia, la experiencia actual indica que es altamente recomendable la implementación de estrategias de mitigación frente a estos riesgos de ciberseguridad.

Resiliencia Organizacional y ciberseguridad

Gran parte de las compañías están desarrollando cierto nivel de resiliencia para asegurar la continuidad operacional, sin embargo ha aumentado la amenaza de ataques informáticos

Estamos frente a campañas de manipulación de la información que están resultando efectivas para quienes cometen delitos cibernéticos como es el ***phishing***, aprovechando el nivel de preocupación de todos respecto a la pandemia, sus consecuencias, las precauciones, avances en la investigación de posibles vacunas, entre otros. Estos mensajes, generalmente a través de correos electrónicos o redes sociales, están dirigidos a un grupo demográfico específicos. Los colaboradores hacen clic en los enlaces que tienen esos mensajes, abren archivos adjuntos que normalmente no harían y luego siguen haciendo sus cosas. Al hacerlo, están infectando dispositivos, volviendo a escribir credenciales y renunciando accidentalmente a ellas. Están de esta forma entregando información clave sobre su organización.

Existen estrategias de mitigación frente a estos riesgos de ciberseguridad en tiempos de pandemia y teletrabajo?

Estrategias de mitigación de riesgos de ciberseguridad

Actualmente están muy en boga los webinars (seminarios vía web) y se puede aprovechar para entregar diferentes consejos de seguridad a los empleados periódicamente (semanal o quincenalmente). Esta medida puede tener un efecto positivo tanto en la vida laboral como personal de los empleados, facilitando que ellos puedan compartir los principales consejos de seguridad de información.
Otra medida recomendable es que las empresas fijen videollamadas específicas para resolver problemas de conexión o de otro tipo que estén sufriendo los colaboradores, al mismo tiempo que se reitera la inconveniencia de que almacenan sus datos incumpliendo la normativa de suo de dispositivos de memoria USB, discos duros portátiles y espacios diversos en la nube.

La determinación de la estrategia adecuada, actividades a desarrollar y la oportunidad de éstas resultará clave para abordar las vulnerabilidades actuales y futuras en este periodo pandémico. Podemos apoyar a su empresa a definir e implementar la estrategia adecuada.

La importancia del Teletrabajo “seguro”

Teletrabajo seguro es conveniente para la empresa y para gran parte de los colaboradores

La resiliencia organizacional en aspectos de ciberseguridad es un desafío para las empresas, pero puede tener un impacto relevante en la motivación de los colaboradores que se sienten cómodos y adecuados a esta nueva modalidad de desarrollar el trabajo.

Definir los procesos y colaboradores que pueden proyectarse más allá de la pandemia en la modalidad de teletrabajo, ya sea en forma permanente o en forma flexible, será parte de las decisiones de la alta dirección.

Proveer un ambiente de trabajo, en que la seguridad de información y las vulnerabilidades de ciberseguridad estén bajo control, será imprescindible en toda organización moderna.

Contáctenos

En KRO Solutions somos un equipo muldisciplinario y estamos dedicados precisamente a los procesos de consultoría que apoyen a las empresas en las estrategias de ciberseguridad adecuadas a sus procesos de negocios y a las características de sus colaboradores. Podemos agendar una videollamada para que conversemos sobre las particularidades de tu empresa y visualizar distintas modalidades para enfrentar la situación actual.

nicolas.roca@krosolutions.com o hernan.gianini@krosolutions.com