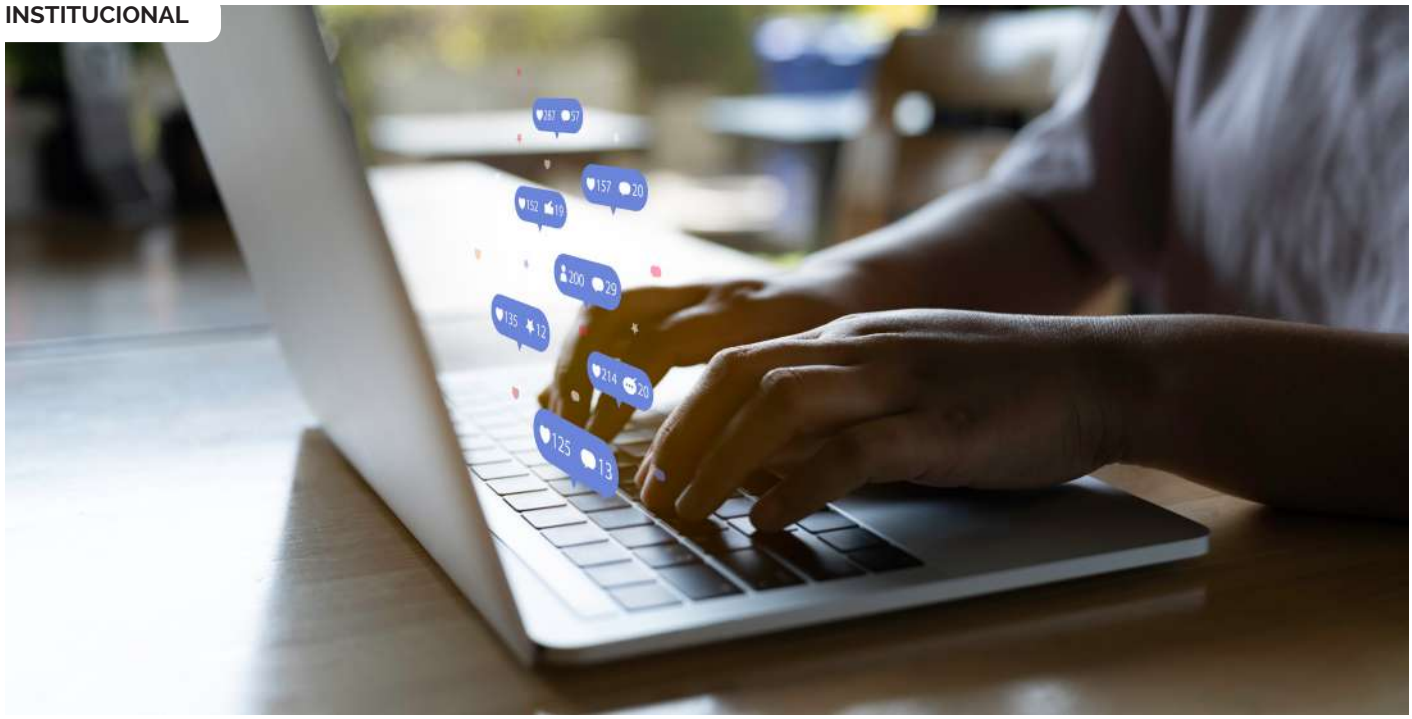

Trabajo remoto, **trabajo seguro**

Ante el impacto sanitario, económico y social del Covid-19, hoy más que nunca se han incrementado los pagos en línea y gestión de trámites de manera virtual. De igual manera, el trabajo remoto y el teletrabajo han cobrado protagonismo en el entorno empresarial, hasta el punto que organizaciones a nivel mundial ya se han adaptado completamente a esta modalidad.

Por ello, es importante no perder de vista el hecho de que nos enfrentamos a riesgos en el manejo de nuestra información personal, laboral y financiera, por lo que debemos implementar controles y estar muy atentos ante el previsible aumento de los ataques cibernéticos.

Conoce cómo identificar estos sistemas, para que no seas víctima de ciberdelincuentes:

Malware

Son programas informáticos diseñados o utilizados con el objetivo de infiltrase en estaciones de trabajo o servidores para causar algún daño o perjuicio como secuestro, hurto, alteración o eliminación de la información, cambios en el sistema operativo o para tomar control total del equipo, de manera remota.

Las principales maneras de infección de un malware son: archivos en correos electrónicos no solicitados, sitios web fraudulentos, sitios web legítimos pero infectados, redes sociales, redes P2P (descargas con regalo) dispositivos extraíbles como memorias USB, discos duros externos, entre otros.

¿Cómo puedes evitar un malware?

Usa siempre tu sentido común: nadie te regala un software legal, dinero, premios o suscripciones solamente por el hecho de hacer clic a un enlace. Recuerda que al hacerlo, lo más probable es que el delincuente esté verificando algo, robando las credenciales o información personal de tu equipo.

Ten siempre el sistema operativo y las aplicaciones al día, en cuanto a actualizaciones de seguridad corresponde. Si el sistema te indica que hay actualizaciones pendientes por instalar, procede y realízalas lo más pronto como te sea posible.

Cuenta con una solución antivirus/endpoint y mantenla actualizada, con el objetivo de proteger el sistema de amenazas informáticas que pudieran ingresas al computador o tu dispositivo móvil.

Evita el uso de dispositivos de almacenamiento extraíbles que vengan fuera de tu entorno. En caso que sean confiables, antes de usarlos realiza el análisis completo con la solución de antivirus.

Abstente de abrir correos electrónicos desconocidos, ejecutar archivos adjuntos y mucho menos, ingresar a los enlaces que estos contenidos nos invitan a visitar.

Mantén actualizado tu navegador Web

Evita la funcionalidad de autollenado o recordación de contraseñas que ofrecen los navegadores Web.

Realiza copias de seguridad de la información periódicamente. Esto debe realizarse de manera estricta, porque en caso de presentarse algún problema con tu computador, este se formatea y se vuelve a instalar.