

SEGURIDAD DE LA INFORMACIÓN EN TIEMPOS DE PANDEMIA

NOTI 301 – Julio de 2020

Algunas de las medidas de precaución recomendadas:

1. Claves seguras y fuertes.
2. Proteja su información personal.
3. Verifique y revise la seguridad de las páginas que visita.
4. Sea reservado con su información personal.
5. Manténgase actualizado en las últimas modalidades de fraude.

La Pandemia nos ha confrontado con retos sin precedentes en todos los aspectos de la gestión empresarial y de la gestión de riesgos. La crisis nos ha demostrado a todos, pero particularmente a los administradores de riesgos y auditores, que cuando lo inesperado se presenta, solo podemos tratar con la incertidumbre si estamos equipados con los recursos, conocimiento y experiencia adecuados.

Como respuesta a la nueva situación, los departamentos de Auditoría y Control Interno han debido adaptarse a las restricciones de movilidad, recurriendo a formas antes impensables para verificar el cumplimiento estricto de los procedimientos en las sedes apartadas de la oficina principal.

Pero deben ser todos los colaboradores de la empresa quienes se comprometan con la nueva forma de trabajo, más segura, más confiable y con un nivel de eficiencia

parecido al que se tenía anteriormente. Debemos comenzar con la seguridad en el trabajo que involucra medios electrónicos; o sea, a todos.

A continuación repetiremos las medidas de precaución recomendadas, las cuales son fáciles de seguir.

1. Crear claves de acceso seguras y fuertes

Además de usar claves complejas, difíciles de adivinar, aproveche siempre que pueda el dispositivo de doble clave que ofrecen algunos sistemas. Con este paso extra de verificación, su información no será tan accesible en casos de rupturas de seguridad o ciberataques. Considere adquirir administradores de claves como Dashlane, Keeper o 1password.

Los colaboradores de las empresas deben comprometerse con la nueva forma de trabajo, haciéndola más segura, más confiable y con un nivel de eficiencia equivalente o superior al que se tenía anteriormente.



Fuente:

<https://www.eleconomista.es/tecnologia/noticias/9554010/11/18/Como-crear-la-contrasena-perfecta-claves-para-estar-protegido-en-Internet.html>

2. Nunca repita sus claves

No solo hay que crear claves fuertes, hay que asegurarse de no repetirlas en diferentes plataformas. Resulta obvio que si una clave se repite en varios lugares, su pérdida o hurto puede ser desastrosa.

3. Proteja cuidadosamente su información personal

No suministre información personal sin necesidad. Los sitios Web que requieren de datos personales, como fecha de nacimiento o dirección casi siempre son falsos, ya que los portales de venta no necesitan de esta información para procesar sus compras.

4. Verifique y revise la seguridad de las páginas que visita

Con el fin de confirmar que el sitio Web que visita es seguro, verifique que tenga el ícono de un candado cerrado a la izquierda de la URL (Localizador Uniforme de Recursos) del sitio. Si no lo ve, vuelva a verificar si está realmente visitando el lugar que busca. Los delincuentes registran sitios con nombres parecidos a los reales, para aprovechar cualquier error de digitación de su parte.

Es el momento de ser creativos, no de entrar en pánico. Entendiendo que si se deja la puerta abierta, el fraude entrará a nuestras empresas tarde que temprano, debemos buscar medidas alternativas de control que nos permitan no solo ejercer una adecuada supervisión sobre las operaciones remotas, sino además enviarles a nuestros colaboradores, proveedores y clientes el mensaje de tener todo bajo control en la empresa, aun en estas circunstancias adversas.

5. Considere métodos alternativos de pago

Algunas opciones de pago son más seguras y privadas que otras. Por ejemplo, si usted tiene la opción de pagar con PayPal, GooglePay o una plataforma similar de pago en nombre de terceros, no tendrá que suministrar su información de tarjeta débito o crédito. Si estas opciones no están disponibles, pagar con tarjeta de crédito ofrece más seguridad que hacerlo con una de débito.



Fuente:

<https://tecnologiaaldia.wordpress.com/2013/08/26/10-claves-para-navegar-seguros-por-internet/>

Por: Alejandro Morales, Gerente General, ASR S.A.S.

Carrera 43B N° 16-41
Medellín, Colombia
+57 4 266 33 42
asr@asr.com.co
<http://www.asr.com.co/>

6. Si comparte con alguien su log in, que no debe hacerlo, mantenga el mismo estándar de seguridad sobre las claves.

Considérelo muy bien antes de decidirse a compartir el acceso a sus cuentas con otra persona. La popularidad en el uso de servicios en línea durante la pandemia ha hecho que muchas personas decidan compartir sus claves de acceso con amigos y familiares. Antes de hacerlo, asegúrese de que estas personas comprenden los riesgos de hacer públicas estas claves.

7. Manténgase actualizado

Los bancos y otras organizaciones como la ACFE (de cuya publicación extractamos apartes del presente NOTI), se encuentran en la tarea de enviar a sus clientes

alertas sobre las principales formas de fraude, insistiendo en la necesidad de permanecer alertas frente a señales sospechosas. Solicite a su banco el envío de alertas de cada transacción que sea hecha con sus productos.

8. Negocie solo con vendedores confiables

Una promoción o aviso publicitario recibido en sus redes sociales no tiene porqué ser considerado como auténtico y genuino. A los delincuentes no les queda difícil insertar avisos fraudulentos, burlando los controles de los operadores de las redes sociales. Asegúrese de contar con el mayor nivel de privacidad en sus redes, eliminando la opción de seguimiento satelital o localizador que la mayoría de estos ofrecen.

9. Sea reservado con su información personal

Por alguna razón incomprensible, a muchas personas les encanta retratar su vida personal y privada paso a paso, segundo a segundo. Dónde está, qué restaurantes visita, dónde compra, etc. Esta información es la materia prima para los delincuentes. Por favor, revise bien la importancia y la razonabilidad de ubicar todos los aspectos de su vida en una cartelera pública y las implicaciones que ello puede tener en su seguridad. Con frecuencia,

esta información es utilizada por los defraudadores para resetear sus claves y apoderarse de sus productos.

10. Manténgase actualizado en las últimas modalidades de fraude

Manténganse usted y su organización informados. Discuta y haga reuniones virtuales con su equipo de trabajo, para mantenerlos al día en materia de prevención. Haga extensiva esta información al grupo familiar de los trabajadores que laboran desde sus casas.

Con estas recomendaciones será posible mejorar la seguridad de la información de las empresas, evitando así ser víctimas de quienes siempre están al acecho de cualquier falla en sus sistemas.

asr@asr.com.co