KRONOS
Investigación y Consultoría

Email: contacto@kronosltda.com
Website: www.kronosltda.com
Tel: 3014821541

Políticas de seguridad y ciberseguridad

Hemos definido una política de Seguridad de la Información y Ciberseguridad, implementándola con los lineamientos y mejores prácticas que tienden a preservar y proteger la confidencialidad, integridad, disponibilidad, privacidad y auditabilidad de la información; todo esto para el óptimo manejo y administración de los recursos informáticos, y apoyo a los objetivos estratégicos del negocio.

Trabajamos constantemente para dar seguridad a la información del negocio y de nuestros clientes, dando cumplimiento a las leyes y regulaciones vigentes. Así mismo, recordamos a los usuarios de nuestro portal, que es de su responsabilidad la protección y seguridad de estos datos. A continuación, sugerimos tener en cuenta las siguientes recomendaciones al acceder a nuestro sitio web y Portal de Clientes:

- Cambia tu clave de acceso a internet al menos una vez cada 30 días o cuando sospeches exposición de esta.
- No uses claves fáciles de identificar. Por ejemplo: fechas o aniversarios, placas del auto, números consecutivos, entre otros.
- Memoriza tus claves, nunca las escribas o compartas con otras personas.
- No permitas que terceros conozcan o visualicen tus claves.
- Recuerda que la clave de acceso a internet es como la llave de tu casa, el que la tenga entra.
- No hagas transacciones en sitios que no sean de tu absoluta confianza, pues en ellos pueden grabar tus números de cuenta, usuarios y claves, sin que te des cuenta.
- En ningún caso debes facilitar tus claves a nadie, incluso aunque manifiesten solicitarlas en nombre de KRONOS INVESTIGACIÓN Y CONSULTORÍA S.A.S. por cualquiera que sea el medio utilizado (telefónicamente, correo electrónico o en persona).
- Debes actualizar tu navegador de internet para obtener mejores ventajas en cuanto a seguridad y servicios de navegación.

Email: contacto@kronosltda.com
Website: www.kronosltda.com
Tel: 3014821541

- Para mayor seguridad, después de utilizar los servicios de internet, cierra el navegador para evitar algún uso indebido.
- Asegúrate de tener antivirus instalado y actualizado en tu computador personal.
- No abras correos electrónicos de remitentes con direcciones extrañas, sospechosas o no habituales ya que pueden contener virus o software espía.
- No hagas clic en los enlaces que están dentro de un correo electrónico para ingresar a una página web, digita la URL en el navegador.
- Evita completar y enviar formularios recibidos por correo electrónico solicitando información confidencial.
- Verifica que el Firewall (cortafuego) de tu computador esté correctamente configurado. Asesórate con un técnico de tu confianza.
- Si sospechas que algún correo electrónico tiene intenciones fraudulentas o ha sido víctima de suplantación de identidad, repórtalo inmediatamente a nuestra línea de servicio al cliente: 3014821541.

Fraudes en internet

Con el fin de informar sobre los diferentes riesgos informáticos relacionados con fraude a través de internet o cibercrimen, los cuales cada vez son más comunes y sofisticados a continuación, mencionamos los más conocidos y algunas medidas para evitarlo:

Phising

El phishing es una modalidad de estafa diseñada con la finalidad de robar tu identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes de páginas en internet.

Email: contacto@kronosltda.com
Website: www.kronosltda.com
Tel: 3014821541

Medidas para evitar ser engañado con phishing

- Nunca respondas a solicitudes de información personal a través de correo electrónico. Si tienes alguna duda, ponte en contacto con nuestra línea de servicio al cliente: 3014821541.
- Sospecha de cualquier correo electrónico solicitando de manera urgente información financiera, personal o privada.
- Siempre introduce la dirección URL de la compañía https://www.kronosltda.com en la barra de direcciones. Es una forma de asegurarse que estás ingresando a nuestra página.
- Asegúrate de que el sitio web utiliza cifrado (https).
- En la página a la que requieres ingresar información confidencial, debe aparecer un ícono de candado cerrado, lo que indica que es una página segura. Haz doble clic sobre el ícono del candado para ver el certificado de seguridad.
- Si no estás seguro de la legitimidad y seguridad de la página, no introduzcas ninguna información personal. Sé prudente y abandona el sitio web.

Keyloggers o registrador de claves

Son herramientas generalmente de software, aunque también los hay de hardware, que permiten grabar el texto que escribe una persona desde el teclado del computador. Estos programas son usados por los delincuentes para capturar todo lo que escribe la persona (víctima) y lo envía a una dirección de correo electrónico configurado por el delincuente. Los keylogger se instalan y funcionan de manera 'invisible' (el usuario no se da cuenta).

Es muy común que estos programas los instale la delincuencia en computadores de uso público como café Internet, para robar los datos de autenticación de los usuarios a los servicios WEB bancarios (robo de identidad). Una vez obtenida esta información los delincuentes ingresan y desfalcan las cuentas efectuando pagos generalmente de servicios públicos, compras de minutos de celular, entre otros.

Email: contacto@kronosltda.com
Website: www.kronosltda.com
Tel: 3014821541

Medidas para evitar ser engañado por keyloggers

- No realices transacciones en línea desde computadores o lugares poco seguros, como un café internet.
- Para evitar que te instalen un programa de estas características en el computador de tu casa, es necesario instalar un firewall, software que controla todo lo que entra y sale del computador, y un programa antivirus o antiespía que ayuda igualmente a evitar que te puedan instalar ese tipo de programas invisibles para el usuario.
- Consulta frecuentemente los saldos de tus cuentas, para que en caso de que identifiques cualquier anomalía puedas informar oportunamente al banco con el que tienes la cuenta para proceder a bloquear el servicio.

Spyware o software espía

El spyware es un software que recopila información de un computador como números de tarjetas de crédito, números de identidad, tendencias del usuario y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

Un spyware típico se autoinstala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el computador y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados. Muchas empresas utilizan este tipo de software para detectar tendencias de navegación o para generar publicidad no requerida (SPAM) directamente en los computadores de los usuarios.

Medidas para evitar ser engañado con software espía

- Utiliza un Firewall, por ejemplo, el firewall de Windows.
- Actualiza el sistema operativo, instalar los últimos parches de seguridad ayudará a reducir los riesgos de seguridad.
- Ajusta la configuración de seguridad de tu navegador.
- Instala software antivirus o antispyware.
- Descarga e instala programas únicamente de sitios web de confianza.

Email: contacto@kronosltda.com
Website: www.kronosltda.com
Tel: 3014821541

- Utiliza software legal.

Ingeniería social

Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos, esta técnica es utilizada por investigadores privados, criminales o delincuentes informáticos para obtener información, acceso y/o privilegios que permiten realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

Los métodos utilizados para realizar ingeniería social pueden ser los siguientes:

- Una fase de acercamiento para ganarse la confianza del usuario, haciéndose pasar por un funcionario de la compañía, un cliente, proveedor, entre otros.
- Una fase de alerta para desestabilizar al usuario y observar la velocidad de su respuesta. Por ejemplo: este podría ser un pretexto de seguridad o una situación de emergencia.
- Una distracción, es decir, una frase o una situación que tranquiliza al usuario y evita que se concentre. Esta podría ser un agradecimiento que indique que todo ha vuelto a la normalidad, una frase hecha; en caso de que sea mediante correo electrónico o de una página web, la redirección a la página web de la compañía.

Medidas para evitar ser engañado por ingeniería social

- Utilizar el sentido común y analizar muy bien cada información recibida.
- No divulgues información que podría poner en peligro tu seguridad o la de la compañía.
- Confirma la identidad de la otra persona al solicitar información precisa (apellido, nombre, compañía, número telefónico).
- Si es posible, verifica la información proporcionada.
- Pregúntate qué importancia tiene la información requerida.