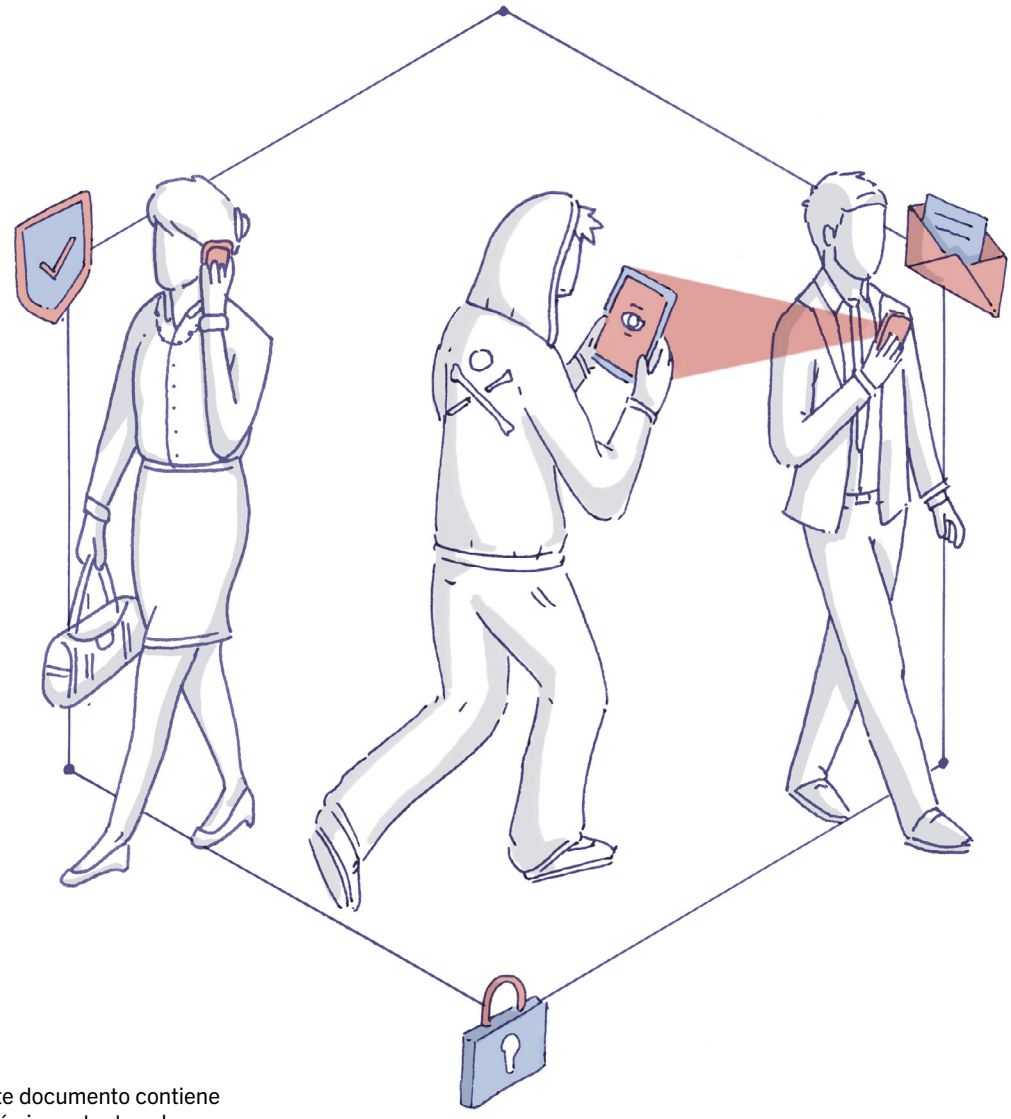
PICTET 1805

ENERO 2020

CIBERSEGURIDAD

PROTEGERSE DE LOS RIESGOS DIGITALES



El presente documento contiene información importante sobre los riesgos relacionados con las comunicaciones digitales y propone medidas fácilmente aplicables para reducirlos.

DATOS PERSONALES: RIESGOS EN AUMENTO

Los datos personales se han convertido en un nuevo tipo de materia prima. Permiten acceder a servicios gratuitos, tales como redes sociales, sistemas de correo electrónico o redes wifi públicas, a menudo sin que el usuario conozca las normas de seguridad utilizadas. Los que recogen los datos pueden explotarlos con fines comerciales, de manera legal o ilegal.

Por lo tanto, conviene ser especialmente prudente a la hora de comunicar información personal. Las filtraciones de datos son cada vez más frecuentes, aunque el comportamiento del usuario no tenga nada que ver. Se ha puesto de manifiesto la fragilidad de los gigantes digitales, como Facebook (87 millones de usuarios afectados por la filtración de datos a Cambridge Analytica) y Google (52 millones de personas afectadas por un fallo de seguridad en 2018).

El principal objetivo de Pictet es establecer, con un espíritu de colaboración, relaciones responsables con sus clientes. Deseamos asegurar la protección de nuestros clientes y, naturalmente, nos preocupan los riesgos relacionados con sus datos personales. En este sentido, queremos compartir nuestras recomendaciones en materia de ciberseguridad.

Los datos personales, tales como la identidad, la ubicación o las contraseñas, pueden caer fácilmente en manos de estafadores, que los usan para acceder a una cuenta o efectuar un chantaje. Algunas medidas sencillas pueden contribuir a reducir considerablemente ciertos riesgos. Este documento le ayudará a reforzar su seguridad digital (véanse páginas 4-5) y reaccionar de forma adecuada en caso de robo de datos (véase página 6). Le recomendamos que lea atentamente este folleto y lo conserve en un lugar de fácil acceso.

Enero 2020

¿CÓMO ACTÚAN LOS PIRATAS INFORMÁTICOS?

Al recopilar información confidencial, los ciberdelincuentes pueden acceder a las cuentas de sus víctimas o someterlas a un chantaje.

Los ciberdelincuentes compiten en ingenio para apropiarse de los datos personales de sus víctimas. A veces les basta con recoger información que se ha hecho pública por negligencia o por accidente. También pueden adivinar contraseñas, infiltrarse en sistemas informáticos o incluso usurpar una identidad.

Hay que saber que los estafadores utilizan mensajes que recurren a la emoción («su ordenador contiene un virus»), la empatía («un amigo en una situación difícil»), la urgencia («solicitud de reacción inmediata») o la promesa de ganancias («una oportunidad que hay que aprovechar»).

A continuación presentamos algunos ejemplos de robo de datos o de fraudes:

1. CUIDADO CON LOS DETALLES

Un correo electrónico de un remitente desconocido invita al usuario a acceder a una copia fraudulenta del sitio web de Pictet, alojada en una dirección parecida a la original, por ejemplo, picttet.com, plctet.com o pic-tet.com. De esta manera, es posible que la víctima aporte información que será utilizadaposteriormente por los ciberdelincuentes.

2. SECUESTRO DE DATOS

El usuario recibe de una persona cuya identidad ha sido usurpada un correo electrónico con un fichero adjunto. La apertura de este fichero va a bloquear el ordenador de la víctima. Un mensaje le informa entonces de que la única forma de desbloquear el ordenador es el pago de un rescate en una cuenta en criptomoneda. Esta amenaza se menciona con frecuencia en la prensa bajo el término de *ransomware*.

3. FRAUDE DEL CEO (SUPLANTACIÓN DE LA IDENTIDAD DE DIRECTIVOS)

El contable de una empresa recibe una llamada de un ciberdelincuente que se hace pasar por un superior jerárquico o un alto directivo de su empresa. Con el pretexto de una operación urgente (adquisición en el extranjero, inspección fiscal), el usurpador exige que se le comunique información confidencial.

RECOMENDACIONES EN MATERIA DE SEGURIDAD

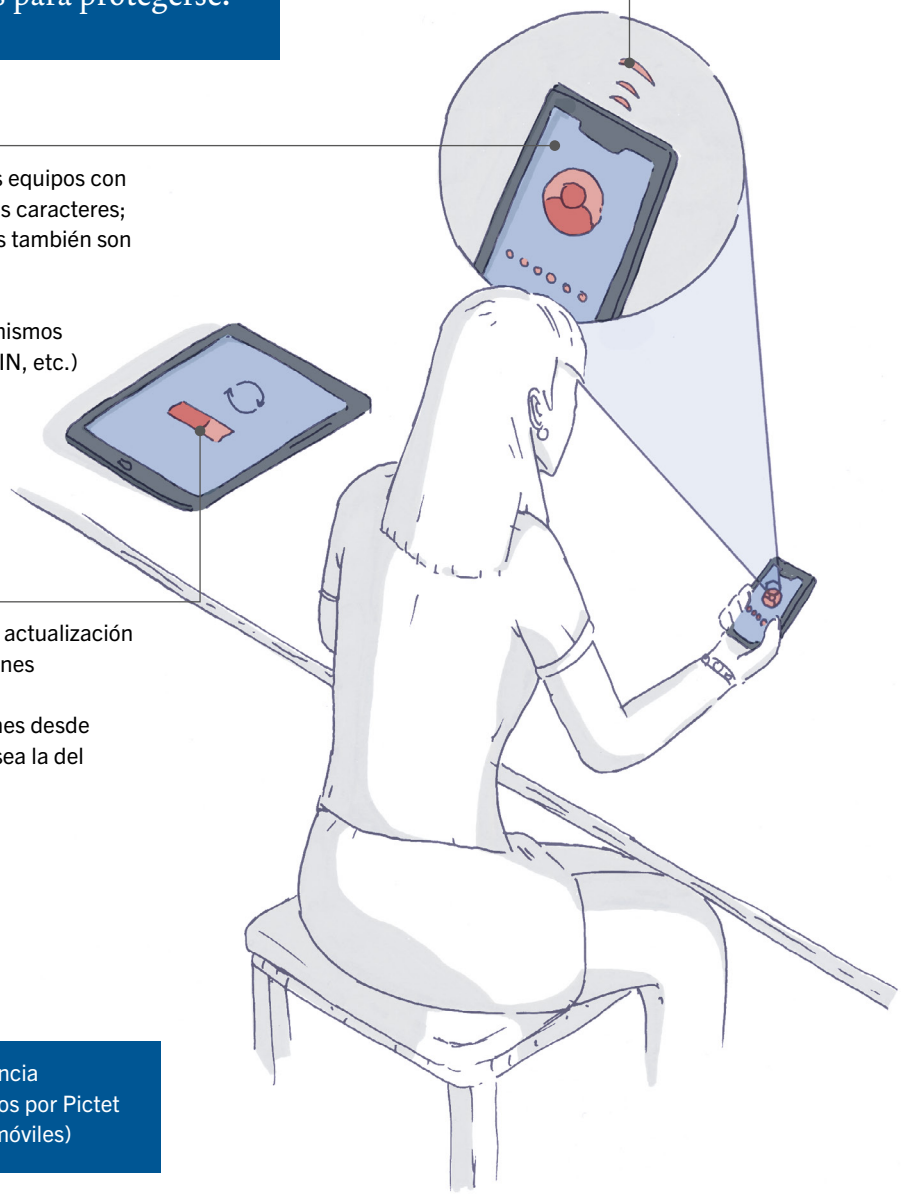
Numerosas medidas permiten evitar filtraciones o robos de datos y los riesgos de fraude. Explicamos aquí algunas soluciones para protegerse.

Activar las opciones que permiten borrar de forma remota los datos en caso de pérdida o robo de un dispositivo

No conservar información confidencial en los buzones de correo (contraseñas, operaciones financieras, etc.)

Proteger el acceso a sus equipos con un código de más de seis caracteres; los sistemas biométricos también son seguros

No desactivar los mecanismos de protección (código PIN, etc.)



Activar las funciones de actualización automática de aplicaciones

No descargar aplicaciones desde una plataforma que no sea la del fabricante

En todos los casos, dar preferencia a los canales seguros propuestos por Pictet (Pictet Connect, aplicaciones móviles)

Verificar las direcciones de los sitios web

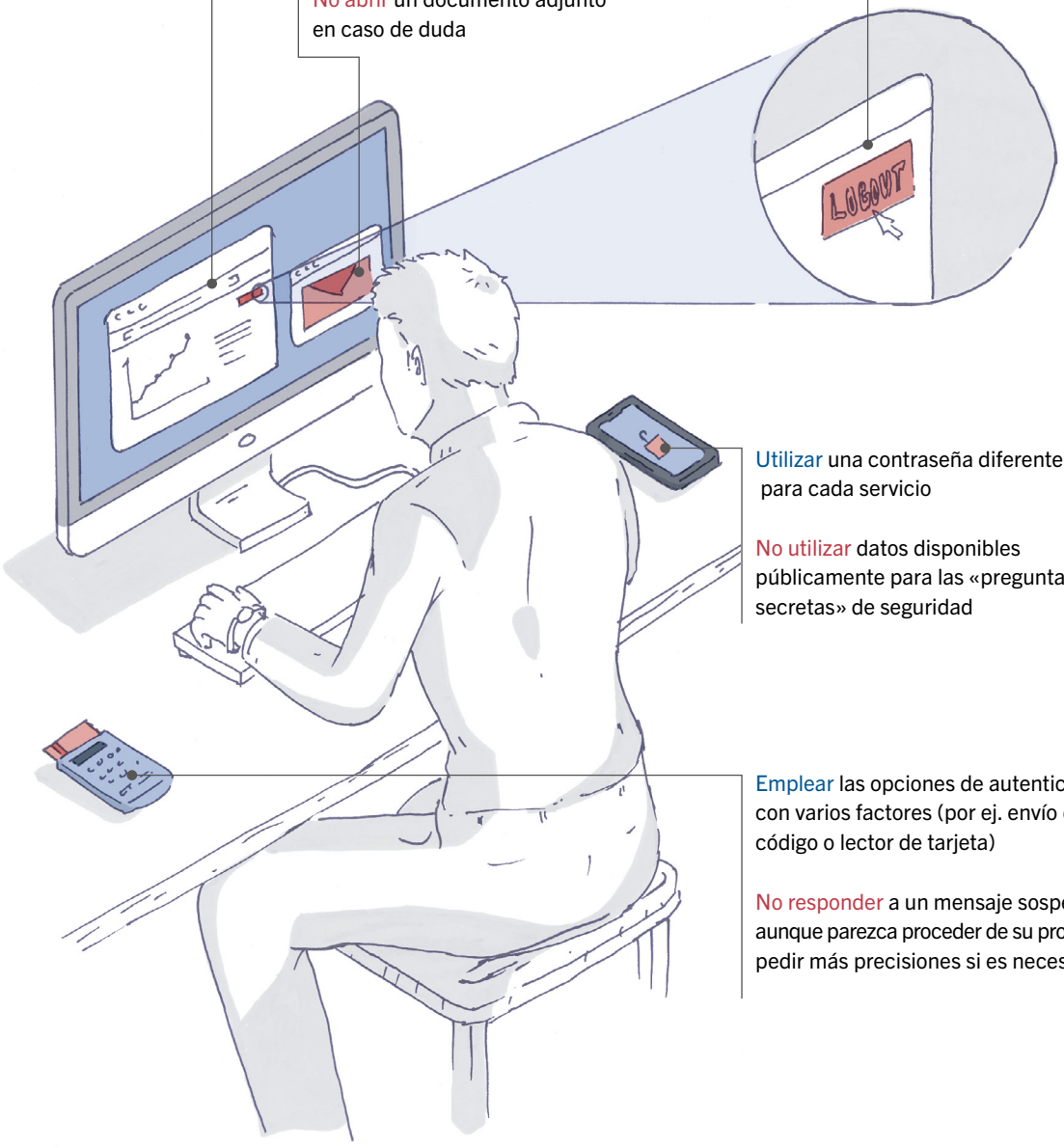
No divulgar información en un sitio que no sea seguro, especialmente al utilizar una red pública

Adoptar una actitud de relativa desconfianza ante correos no solicitados

No abrir un documento adjunto en caso de duda

Cerrar correctamente las sesiones mediante las funciones facilitadas

No dejar una sesión abierta sin vigilancia



Utilizar una contraseña diferente para cada servicio

No utilizar datos disponibles públicamente para las «preguntas secretas» de seguridad

Emplear las opciones de autenticación con varios factores (por ej. envío de un código o lector de tarjeta)

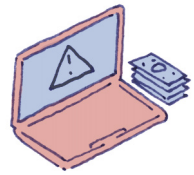
No responder a un mensaje sospechoso, aunque parezca proceder de su proveedor; pedir más precisiones si es necesario

¿QUÉ HACER EN CASO DE ROBO DE DATOS?

En caso de incidente, deben tomarse las siguientes medidas de inmediato.

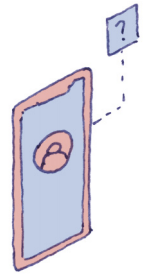
MI CORREO ELECTRÓNICO HA SIDO PIRATEADO

- Recuperar el acceso utilizando las instrucciones del proveedor y después modificar inmediatamente la contraseña (incluyendo la de cualquier otra cuenta para la que se esté usando la misma contraseña)
- Informar a allegados y contactos de que esa dirección de correo deja de ser fiable temporalmente
- Determinar las malversaciones que pudieran haberse llevado a cabo basándose en el contenido del buzón de correo (operaciones, datos confidenciales) y contactar con las partes afectadas
- Verificar o hacer verificar la configuración del buzón, en particular en lo que respecta a eventuales reenvíos automáticos de mensajes establecidos por los piratas informáticos



ME HAN PEDIDO UN RESCATE POR VÍA ELECTRÓNICA

- No pagar este rescate
- Ponerse en contacto inmediatamente con un experto informático



HE DADO INFORMACIÓN CONFIDENCIAL POR TELÉFONO A UNA PERSONA MALINTENCIONADA

- Modificar las contraseñas que podrían verse afectadas
- Informar a socios y allegados que podrían verse afectados
- Bloquear el número de teléfono de la persona malintencionada y no volver a responder a posteriores intentos de contactar con usted

¿CÓMO RECONOCER UN MENSAJE QUE PROVIENE DE UN ESTAFADOR?

No existe un método 100% seguro, pero algunas señales de alerta deberían llamar la atención de los usuarios.

Es importante desconfiar en particular de mensajes que:

- provengan de una dirección desconocida o inusual; es importante prestar particular atención al hecho de que una dirección fraudulenta puede tratar de imitar la de un contacto conocido;
- incluyan elementos sospechosos, resulten amenazadores o transmitan un sentimiento de urgencia;
- contengan promesas vagas o inesperadas;
- inciten a abrir un documento adjunto o hacer clic en un enlace para descubrir el contenido completo del mensaje;
- no mencionen claramente el destinatario del mensaje y no utilicen la dirección empleada habitualmente por el remitente.

Si un mensaje presenta una o varias de las señales mencionadas, no se trata necesariamente de un mensaje malicioso, pero conviene tomar precauciones antes de tratarlo.

Pictet
El grupo Pictet está dirigido por siete socios, que son a la vez propietarios y gestores. Los principios de sucesión dentro del grupo de socios y de transmisión del capital han permanecido sin cambios desde su fundación en 1805. El Grupo se dedica exclusivamente a la gestión de patrimonios, a la gestión de activos y al asset servicing. No ofrece créditos comerciales ni servicios de banca de inversión. Con unos activos bajo gestión o en depósito que ascendían a un total de 544.000 millones de CHF al 30 de junio de 2019, Pictet se encuentra hoy en día entre los principales actores independientes de Europa en el ámbito de la gestión de patrimonios y de activos.

El Grupo tiene su sede en Ginebra, donde comenzaron sus actividades, y cuenta con más de 4.300 empleados. El Grupo, que dispone de 27 oficinas, está también presente en Ámsterdam, Basilea, Barcelona, Bruselas, Dubai, Fráncfort, Hong Kong, Lausana, Londres, Luxemburgo, Madrid, Milán, Montreal, Munich, Nassau, Osaka, París, Roma, Singapur, Stuttgart, Taipei, Tel-Aviv, Tokio, Turín, Verona y Zurich.

Realización
Large Network

FSC
MIX
Paper
FSC® C002504

www.grupo.pictet