EL FRAUDE EN TIEMPOS DE CRISIS

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Mayo de 2020

EXPOSITORES

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

FCAdvisory
Forensic & Compliance Advisory SpA

Christian Caamaño, CFE
Socio Servicios Forensic y Compliance en FC Advisory
Académico UDP

Forensic & Cybercrime Investigation

Felipe Sánchez Fabre
Socio en Forensic & Cybercrime Investigation
Académico U.de Chile y USACH

FCAdvisory
Forensic & Compliance Advisory SpA

Pablo Alfaro, CFE
Socio Servicios Forensic y Compliance en FC Advisory
Académico USACH y UDP

AGENDA

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

- Introducción.
- ¿Por qué cometer fraude en crisis?
- Esquemas de Fraudes posibles.
- Perfil del defraudador.
- Esquemas de fraude en Covid-19.

- Escenario actual y desafíos.
- Aparición de nuevos riesgos.
- BEC modus operandi.
- Recomendaciones de controles operacionales.

- Escenarios de BEC y caso real.
- Controles de Ciberseguridad.
- Gestión de Evidencia digital..

INTRODUCCIÓN

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

INTRODUCCIÓN

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Menos ventas

Para mantener margen

Reducción de costos

Rescate de inversiones financieras

Disminución del ahorro

Reducción personal

Freno en contrataciones de personas y servicios

Caída (postergación) en proyectos de inversión

Percepción negativa del mercado

Dificultad de financiamiento

INTRODUCCIÓN

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

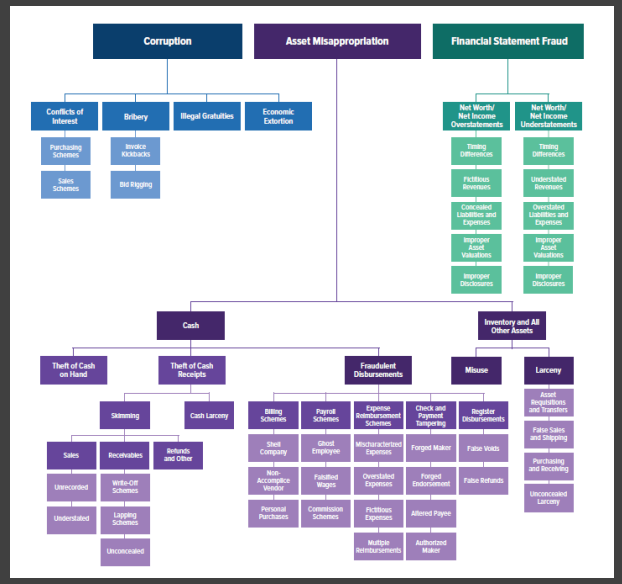
INTRODUCCIÓN

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Esquemas de Fraude

Esquemas de Fraude Ocupacional



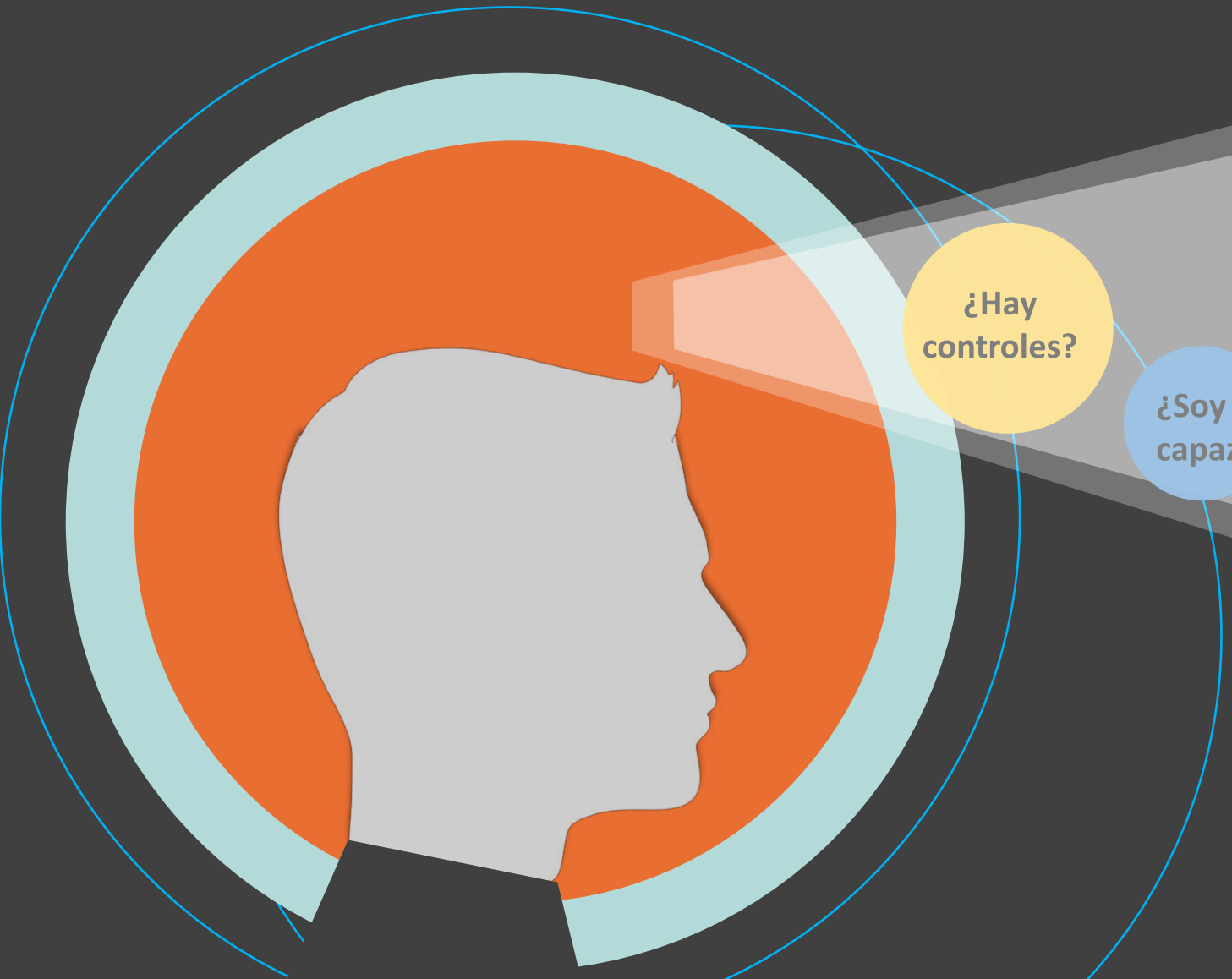
Esquemas de Fraude Externo

Esquemas de Fraude a las personas

¿POR QUÉ COMETER FRAUDE EN CRISIS?

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation



¿Hay controles?

¿Soy capaz?

¿Se están monitoreando o aplicando los contoles?

¿podré pagar mis deudas?

¿Mantendré mi empleo después de la crisis?

¿Es posible mantener la familia?

…de igual manera, tendré que buscar otra Fuente de ingresos.

¿Me descubrirán?

Esquemas de Fraudes posibles

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Reducción de costos

Menos ventas

Disminución del ahorro

Rescate de inversiones financieras

Dificultad de financiamiento

Percepción negativa del mercado

Presión de revertir ésto

Fraudes de estados financieros

Esquemas de Fraudes posibles

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Reducción personal

Miedos y presiones

Fraudes de Apropiación indebida

Freno en contrataciones de personas y servicios

Miedos y presiones

Fraudes externos

Esquemas de Fraudes posibles

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Reducción de costos

Caída (postergación) en proyectos de inversión

Freno en contrataciones de servicios

Presión de los proveedores por generar ingresos

Fraudes de Corrupción

Fraudes Externos

PERFIL DEL DEFRAUDADOR

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

ANTIGUEDAD (Pertenencia)

Los defraudadores ocupacionales con antigüedad laboral de al menos 6 años en sus organizaciones, causaron el doble de perdida que aquellos con menos antigüedad.

GENERO

Los hombres han participado en el 2/3 de veces, mientras que las mujeres un 1/3.

EDUCACIÓN

El 64% de los defraudadores tiene estudios universitarios o post grado.

EDAD

La edad ha estado directamente relacionada con el monto de la pérdida promedio en fraude ocupacional.

Reporte de las naciones, abril 2020

ACFE
Association of Certified Fraud Examiners

Esquemas en Época de Covid-19

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

PHISHING/SMSHING

WITH FRAUDSTERS IMPERSONATING GOVERNMENT AND HEALTHCARE OFFICIALS

75% OVERALL INCREASE | **48%** SIGNIFICANT INCREASE

FRAUDULENT VACCINES/CURES/CORONAVIRUS TESTS

65% OVERALL INCREASE | **40%** SIGNIFICANT INCREASE

CHARITY AND FUNDRAISING FRAUD

69% OVERALL INCREASE | **40%** SIGNIFICANT INCREASE

THIRD-PARTY SELLER AND BUYER SCAMS ON LEGITIMATE ONLINE RETAIL WEBSITES

63% OVERALL INCREASE | **35%** SIGNIFICANT INCREASE

BUSINESS EMAIL COMPROMISE

62% OVERALL INCREASE | **28%** SIGNIFICANT INCREASE

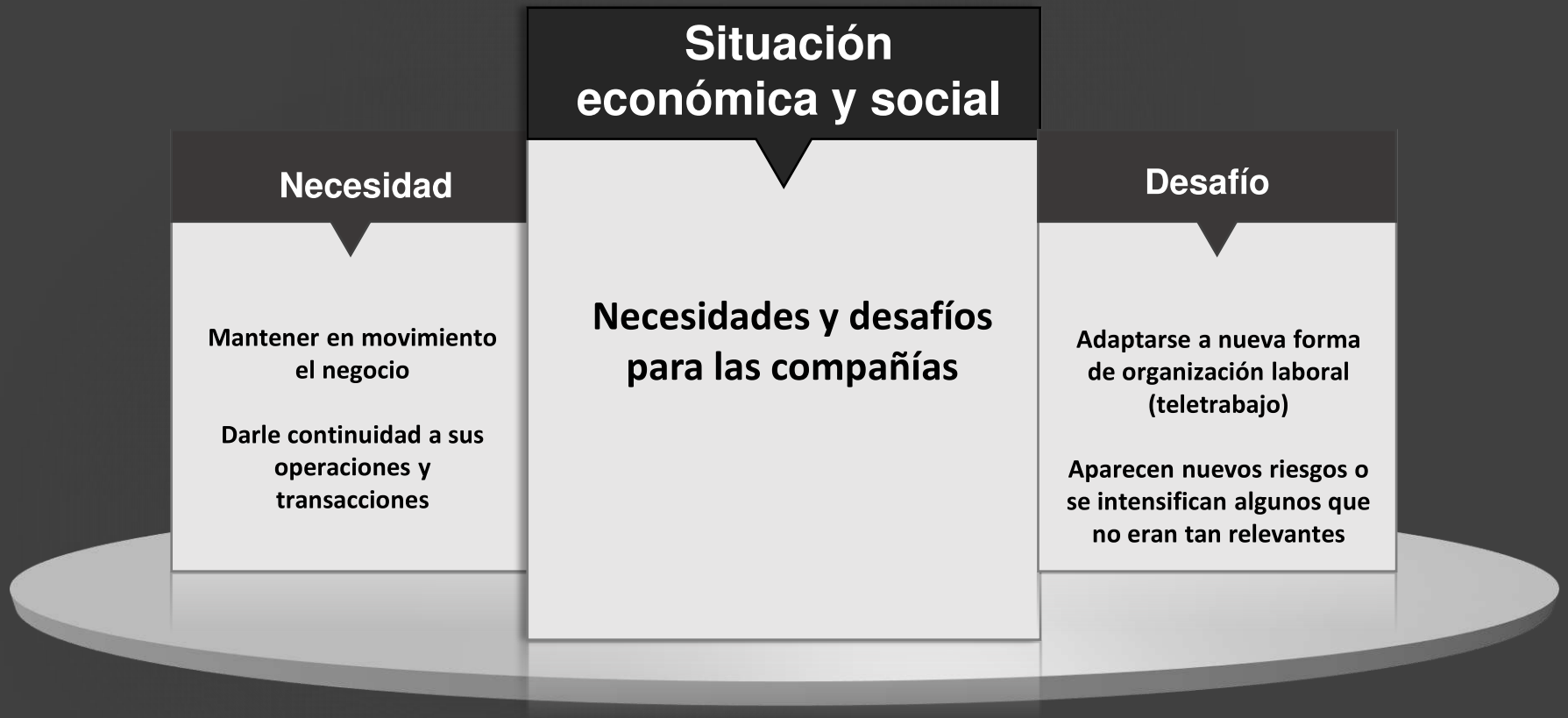
DATA BASED ON AN APRIL 2020 SURVEY OF 196 ANTI-FRAUD PROFESSIONALS.

ACFE
Association of Certified Fraud Examiners

Complejo escenario actual

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation



Es necesario identificar áreas / actividades claves donde podrían ser vulnerables

Condiciones Propicias

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Empresas en Shock

El tamaño del problema y lo impredecible de su duración crea escenario de incertidumbre, condicionado por la necesidad de mantenerse en pie.

Cambio Cultural

Empresas, especialmente aquellas que no tenían cultura de home office, todavía están tratando de ajustar su funcionamiento.

Transacciones en línea

Procesos de negocio cambian. Más demanda hacia trabajo y servicios de acceso remoto se transforma en la oportunidad para cometer delitos. Se detectan deficiencias en controles, procedimientos, sistemas y una baja percepción de ser descubiertos.

Saca ventajas

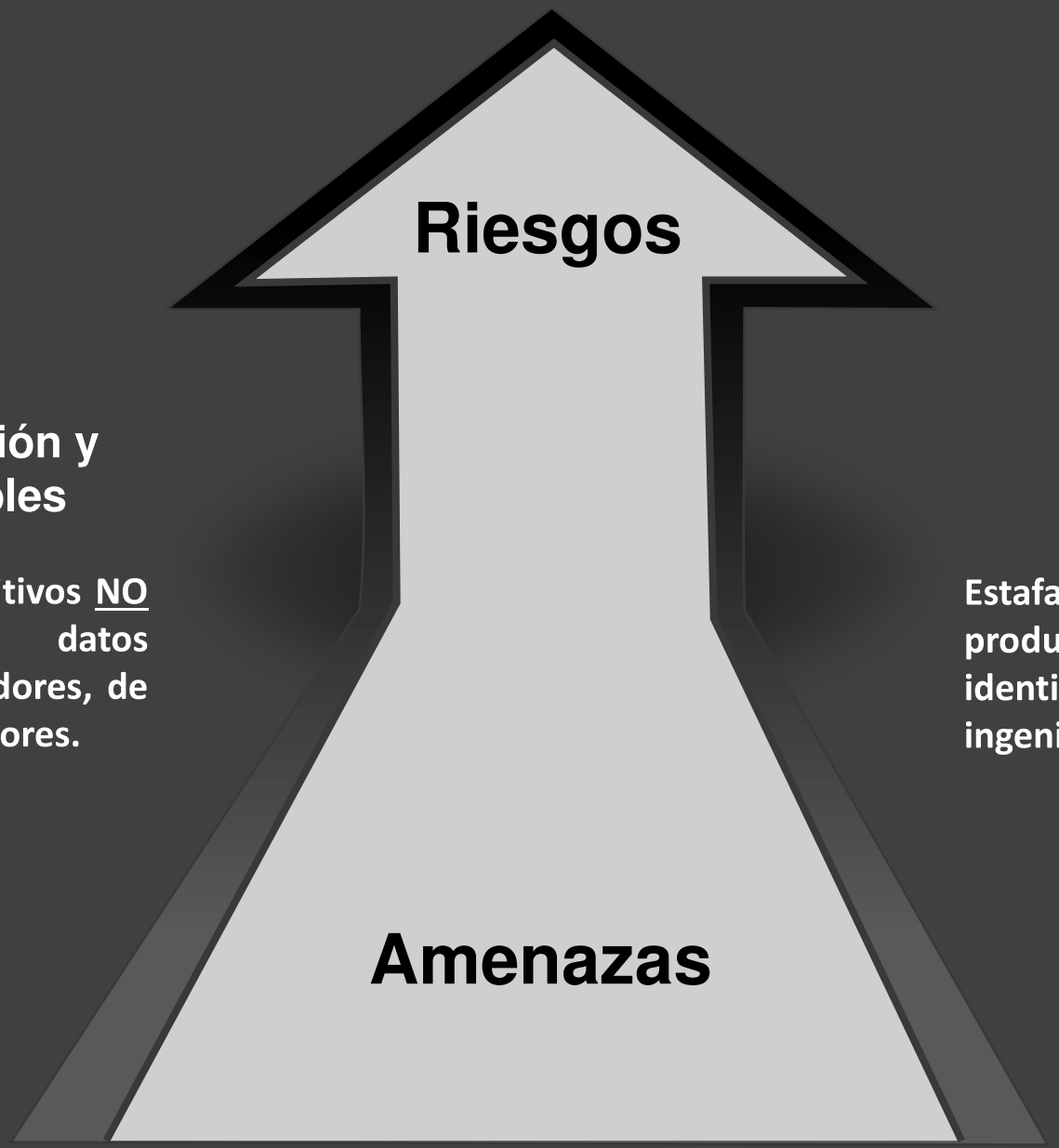
Delincuentes de cuello blanco sacan provecho económico de las necesidades de la población y las compañías. Surgen renovados esquemas irregulares. 1

1: Jenadem, PDI, 16.04.2020

NUEVOS FOCOS

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation



Seguridad de la información y Privacidad datos sensibles

Acceso a través de redes y dispositivos NO CORPORATIVOS, exponiendo datos confidenciales de clientes, proveedores, de la propia compañía y sus colaboradores.

Ciberseguridad

Estafas, fraudes, compra venta de productos falsos, suplantación de identidad, uso del comercio on-line, ingeniería social, phishing .

Interceptar comunicaciones para forzar el desvío de fondos

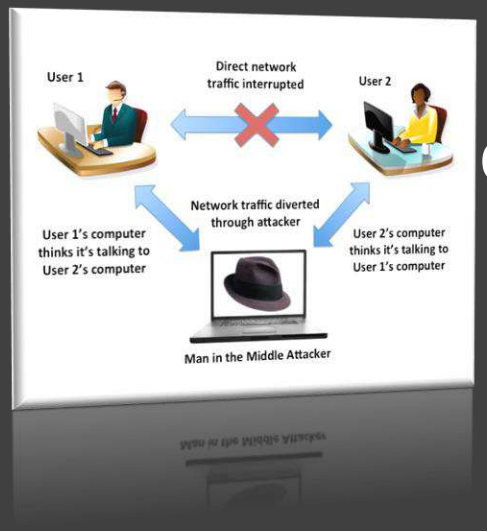
FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Man in The Middle (BEC)

- Equivale a una actividad de espionaje
- Un atacante se interpone entre dos transmisiones
- Se configuran herramientas programadas para "escuchar" las transmisiones
- Se interceptan y capturan datos definidos como valiosos
- Los datos se pueden modificar en el proceso de transmisión para engañar al usuario final
- La finalidad es que el usuario divulgue información confidencial.
- Atacante puede leer, insertar y modificar mensajes entre dos usuarios o sistemas
- Atacante debe poder observar e interceptar mensajes entre las dos víctimas

Un tercero intercepta, distribuye y modifica comunicaciones entre el emisor y el receptor



Consideraciones

- Cuentas @mail son usadas por un tercero desconocido para comunicarse simultáneamente con colaboradores de uno y otro lado (cliente-proveedor).
- Sin el conocimiento de ninguna de estas instancias o partes. El punto de inicio e inserción del esquema podría ser cualquiera de las dos partes (cliente o proveedor).
- El resultado es la apropiación de información clave tal como : datos bancarios necesarios para concretar pagos a proveedores en un banco situado en el extranjero.
- Se persigue el desvío de los fondos a una entidad y cuenta distinta a la original, ambas ligadas al atacante.
- En los pagos vía transferencia a cuentas bancarias en bancos internacionales las cuentas de correo electrónico del cliente son las preferidas, solicitándoles que remitan los pagos pendientes a una nueva cuenta bancaria, incluso modificando el beneficiario.

RECOMENDACIONES

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Específicas

1. Para modificar información clave de proveedores debe existir política y procedimiento formal (escrito), que debe respetarse en todo momento.

2. Este tipo de cambios deben ser autorizados por instancias superiores en la organización, debida y previamente definidas.

3. Solicitudes de este tipo, especialmente de proveedores, implican cambios relevantes que "SIEMPRE DEBEN ESCALARSE" internamente. Evitar decisiones autónomas.

4. Verificar DIRECTA Y VERBALMENTE con la parte "requirente" (proveedor). Evitar uso de correo electrónico ya que permite mantener el "engaño" fraguado por el atacante.

5. Poner atención a las banderas rojas:
1.- Dudar de correos electrónicos que evidencien errores ortográficos o gramaticales flagrantes (Ej: mayúsculas, oraciones rotas, redacción, entre otros).

6. 2- Poner atención a niveles anormales de presión o demandas urgentes de pago (Ej: dos o tres veces en un período de 24 horas).

3.- Poner atención al nombre de dominio del correo electrónico del remitente. Normalmente se utiliza una redacción o nomenclatura similar a las cuentas legítimas.

RECOMENDACIONES

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

1. Revisar y ajustar los procesos actuales. Foco en la continuidad del negocio, considerando la situación actual

2. Atentos al estado de “alerta” de sus colaboradores para enfrentar las amenazas, considerando contingencia y tensión actual = bajo nivel de respuesta, cometer de errores

3. Mensajes y recomendaciones permanentes respecto a: Las conexiones, comunicaciones, transferencia de información, respuestas a solicitudes de terceros, necesidad de escalar ante cualquier duda.

4. Identificar áreas y actividades claves potencialmente vulnerables: Tesorería, Mesa de Dinero, Compras, Mantención, Recursos Humanos

5. Revisar y adaptar regulación interna: Políticas, procedimientos, identificación rápida de riesgos y controles asociados a Fraude, Corrupción, Ciberseguridad.

6. Revisar capacidad de la compañía para enfrentar estas amenazas. Seré REACTIVO? ¿Recursos disponibiles (sistemas, mail, personas) ***READINESS***

Generales

Establecer un cuerpo de evidencia basada en hechos objetivos y verificables que facilite la toma de decisiones, causando el mínimo de disrupción en la operación del negocio.

Concientización

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

"You're going to be hacked. Have a plan."

Joseph Demarest, FBI cyber division chief.

20 de Octubre de 2014

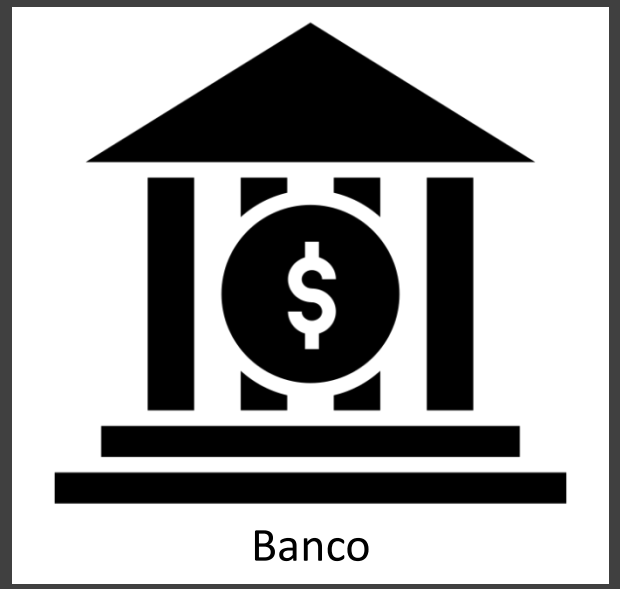
BEC - Comprimiso de Correo Comercial

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Proveedor

Comprador

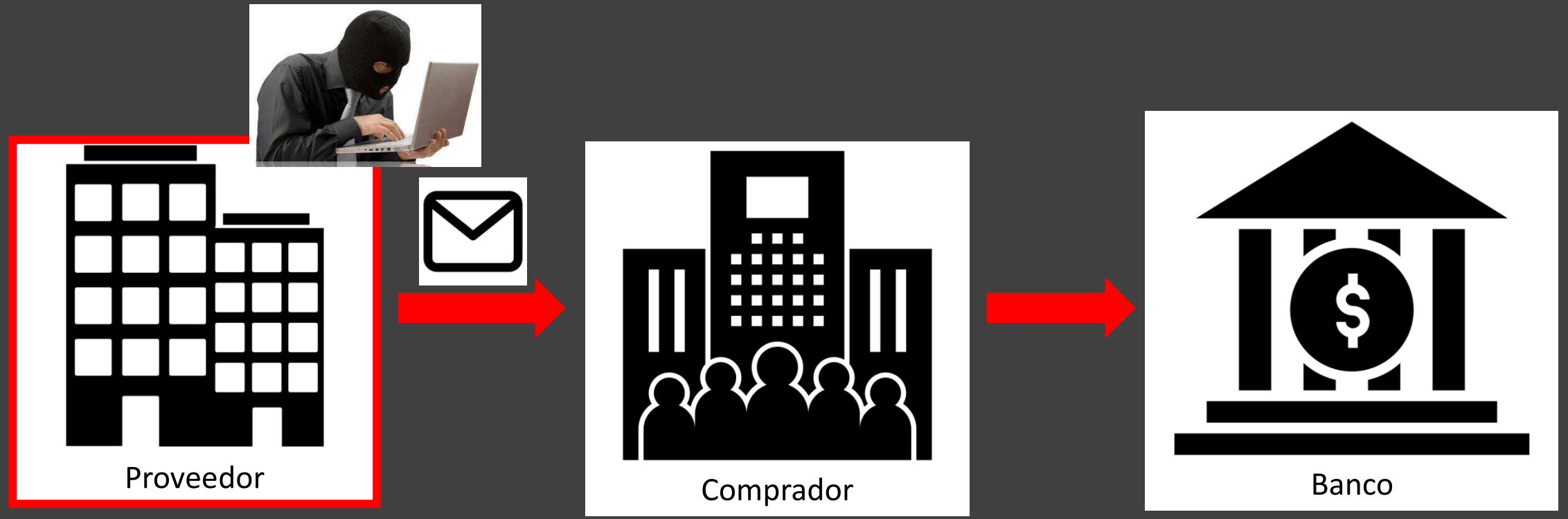


Banco

Escenario – Proveedor Intervenido

FCAdvisory
Forensic & Compliance Advisory SpA

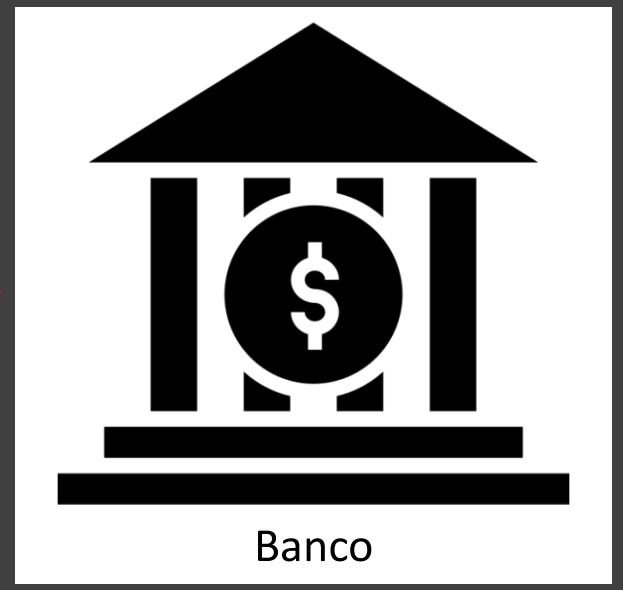
Forensic & Cybercrime Investigation



Escenario – Comprador Intervenido con simulación Proveedor

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation



Escenario – Comprador Intervenido con simulación Comprador

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

EL MUNDO
PIXEL. TECNOLOGÍA

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

TECNOLOGÍA

Un grupo de hackers valencianos aprovecha el estado de alarma para estafar 2,2 millones

Las empresas afectadas pertenecen a ámbitos como laboratorios, cooperativas, colegios privados, hoteles, energéticas, transportes o, incluso, nóminas de particulares.

OPERACIÓN HOMES

Este tipo de estafa consiste en **atacar las cuentas de correo electrónico de las empresas** para obtener datos de facturas pendientes, cuentas bancarias y clientes potenciales.

Dada la situación económica, con multitud de personas sin posibilidad de trabajar o que han perdido su empleo, estos hackers utilizaron a más de **60 personas en situaciones límite** como tapadera, como mulas digitales que sirvieran de testaferro para sus crímenes y que ahora podrían ser acusadas junto a ellos.

https://www.elmundo.es/tecnologia/2020/05/13/5ebc056e21efa0eb5c8b45d6.html

Controles de Ciberseguridad

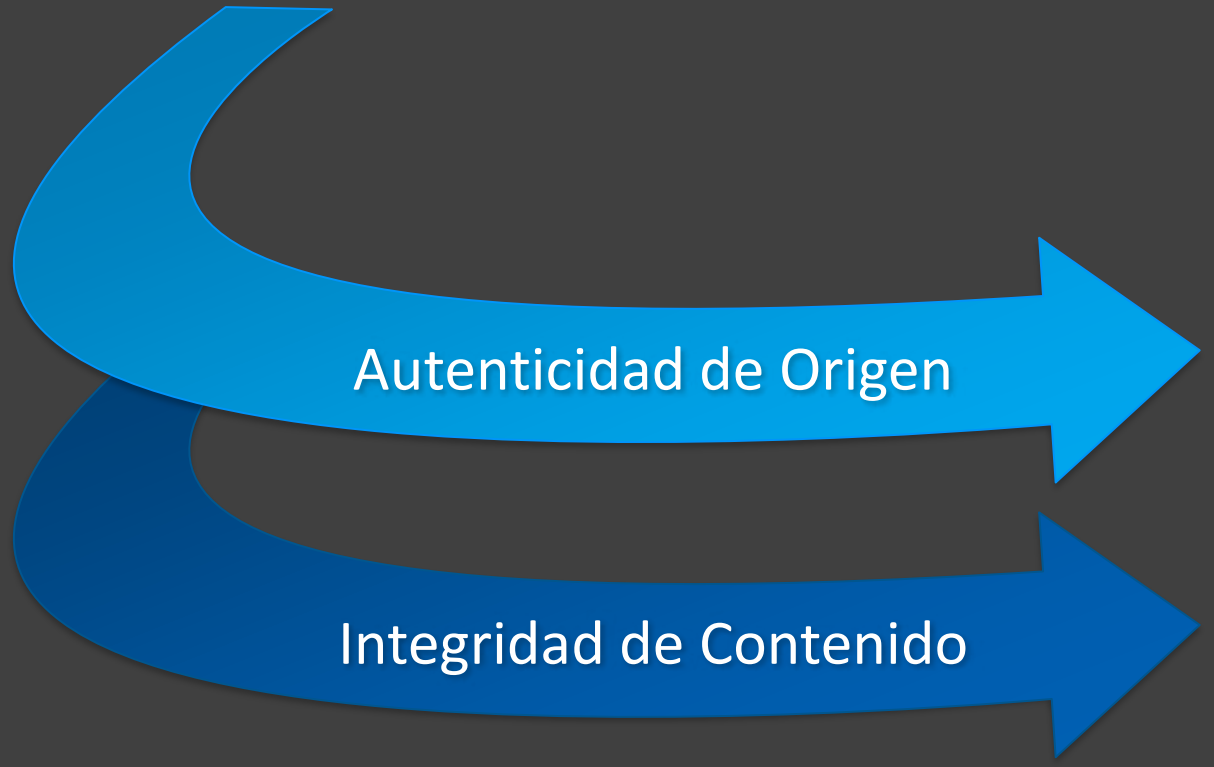
FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Controles Técnicos de Ciberseguridad

FCAdvisory
Forensic & Compliance Advisory SpA

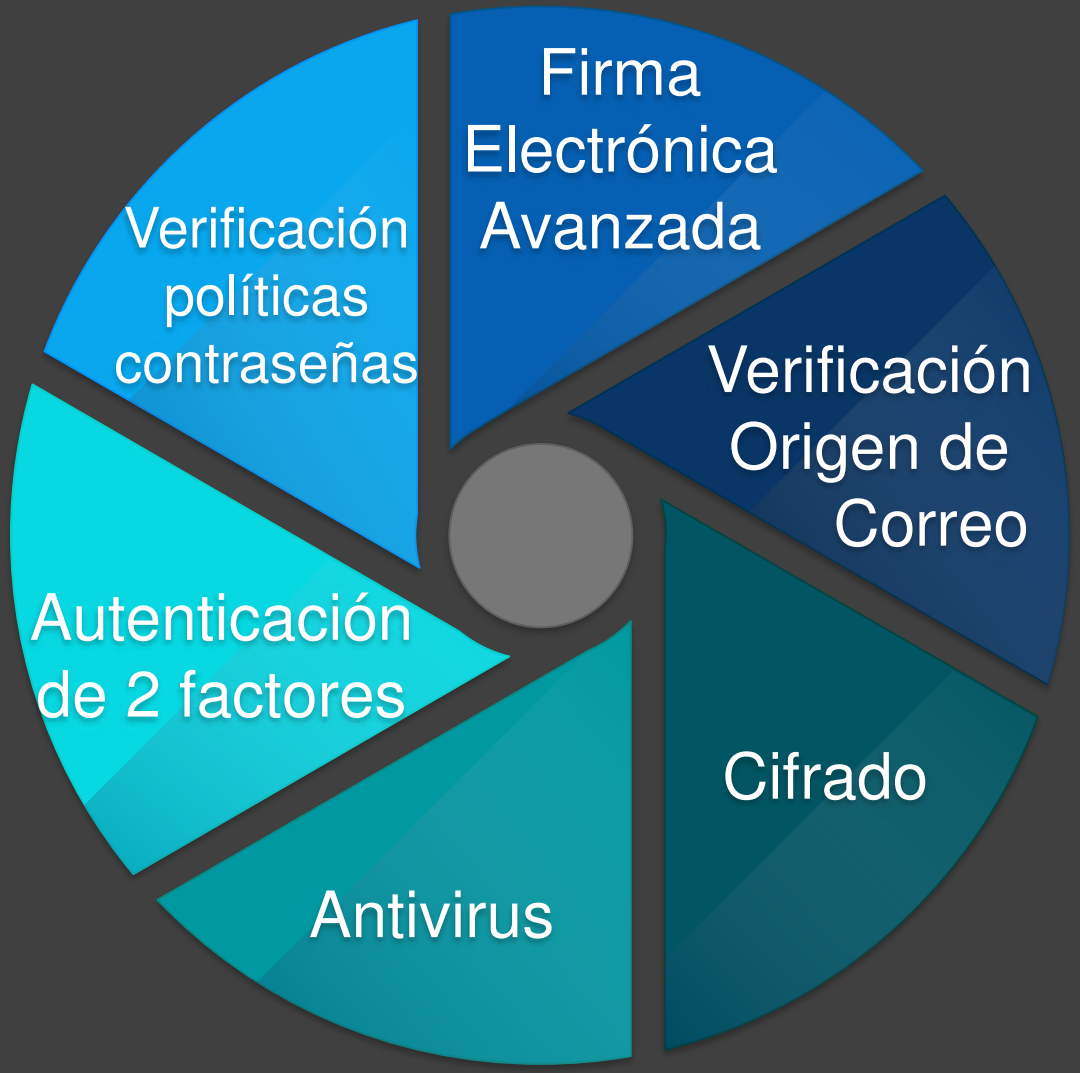
Forensic & Cybercrime Investigation



Controles Técnicos de Ciberseguridad

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation



Gestión de Evidencia Digital

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Gestión de Evidencia Digital

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

Existencia

Nivel de Detalle

Información consistente

Periodo Resguardo

Modo Y Lugar Resguardo

Servicios internos, externalizados y tecnologías contratadas (Ej: Firewall ISP y Cloud)

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation

¿ Preguntas ?

Contacto

Pablo Alfaro
+569 9572 9484
palfaro@fcadvisory.cl

Christian Caamaño
+569 5405 4018
ccaamanos@fcadvisory.cl

Felipe Sánchez
+569 9228 6839
fsanchez@fci.cl

FCAdvisory
Forensic & Compliance Advisory SpA

Forensic & Cybercrime Investigation