PREMIOS EIKON 2025

A LA EXCELENCIA EN COMUNICACIÓN

CATEGORÍA 8: *ISSUES MANAGEMENT*

CAPÍTULO GENERAL
REGIÓN ARGENTINA

Caso: CIBERDELITOS
“Cuando el delito se disfraza con tu marca”

Responsable: Camuzzi – Dirección de Relaciones Institucionales

Un mensaje urgente, un descuento tentador. Un canal que parece oficial.
En segundos, una estafa se concreta… hay una persona perjudicada y, con delincuente anónimo, la marca queda en el centro de la escena.

La suplantación de identidad en servicios públicos evolucionó hacia esquemas digitales sofisticados que utilizan la credibilidad corporativa como vehículo del delito.

Cuando eso ocurre, se pone en juego ese valor intangible tan preciado: la confianza.

El problema: el delito, disfrazado de marca

La suplantación de identidad no es un fenómeno aislado ni exclusivo de un sector. En la Argentina, se consolidó en los últimos años como una de las principales modalidades delictivas, especialmente en ámbitos como servicios públicos y entidades financieras, donde la confianza del usuario es un activo central.

El delito utiliza la marca, la capilaridad territorial y la relación de confianza para construir credibilidad y facilitar el engaño.

Históricamente, esta suplantación de identidad era presencial: en el caso de Camuzzi falsos operarios se presentaban en domicilios haciendo referencia a emergencias operativas, como fugas de gas, que empujaban a los vecinos a abrir sus puertas y, desprevenidos, ser robados por los delincuentes literalmente disfrazados con overoles y cascos. Esta modalidad de entradera migró a esquemas de fraudes digitales vía mail, redes sociales, WhatsApp y llamadas.

Los datos permiten dimensionar con claridad el alcance del problema. Aunque no tenemos datos 2025, según la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), en 2024 se registraron más de 34.000 reportes de delitos informáticos, lo que representa un crecimiento interanual del 21,1%.

Sin embargo, estas cifras deben leerse como un piso y no como una medida total del fenómeno: existe un volumen significativo de casos que no se denuncian, ya sea por desconocimiento, falta de canales claros o por la percepción de baja recuperación del daño.

En consecuencia, el universo real de víctimas es sensiblemente mayor, lo que refuerza la idea de estar frente a un problema estructural, en expansión y con un alto nivel de subregistro.

El fenómeno se aceleró significativamente en los últimos años, impulsado por el crecimiento sostenido de los procesos de digitalización. Antes de la pandemia, entre 2019 y comienzos de 2020, se registraban apenas 2.581 reportes. Con la virtualización de la vida cotidiana, los casos se dispararon a más de 22.000 en 2021, consolidándose luego en niveles superiores a los 30.000 reportes anuales.

Este punto marca un hito clave: la pandemia no solo amplió los canales digitales, sino también el terreno para el delito.

En paralelo, Camuzzi atravesaba su propio proceso de transformación digital. A partir de 2018, con el lanzamiento de la Oficina Virtual, y especialmente desde 2021 con campañas intensivas

de virtualización, la compañía logró migrar masivamente la relación con sus usuarios hacia entornos digitales. Hoy, el 98% de los clientes utiliza canales digitales y una proporción creciente de las gestiones se realizan de forma online, en un esquema de evolución tecnológica permanente.

Sin embargo, este avance —clave para mejorar la experiencia de usuario— también amplificó la superficie de exposición al riesgo, en línea con lo que ocurría a nivel país.

Al mismo tiempo, las modalidades delictivas se volvieron más sofisticadas. El phishing tradicional evolucionó hacia esquemas combinados —vishing (llamadas), smishing (mensajes) y suplantación de números oficiales— que utilizan datos reales, lenguaje institucional y situaciones de urgencia para construir credibilidad y concretar el engaño. Esta evolución no fue ajena a Camuzzi, donde los casos comenzaron a replicar esta misma lógica y complejidad.

Hoy, en Argentina, gran parte de los fraudes se origina en canales móviles y de mensajería, donde la interacción es inmediata y las posibilidades de verificación son más limitadas.

En este contexto, Camuzzi -como empresa distribuidora de gas natural en 370 localidades de 7 provincias argentinas- presenta condiciones que amplifican la exposición al riesgo:

- Operación de gran escala, con presencia en el 45% del territorio nacional
- Alcance en comunidades pequeñas y localidades con menor nivel de sensibilización frente a estas modalidades delictivas
- Más de 2,2 millones de usuarios
- Alto nivel de digitalización del vínculo (98% de usuarios digitalizados)
- Interacciones frecuentes vinculadas a pagos, gestiones y atención

Esta combinación ubica a la compañía en un lugar particularmente crítico:

Una marca masiva, confiable y cercana,
en un entorno donde el delito se
“aprovecha” de estos atributos para actuar.

Por eso, los primeros casos registrados en 2023 no fueron interpretados como episodios aislados, sino como la manifestación local de un fenómeno estructural en expansión.

El crecimiento del problema generó impactos concretos:

- Usuarios vulnerados económicamente
- Desconfianza en la presentación de nuevos canales oficiales
- Aumento de consultas operativas
- Demandas legales
- Exposición mediática y emociones negativas asociadas a la marca

La decisión: gestionar con foco en la prevención

Camuzzi decidió no adoptar una postura reactiva, sino abordar el fenómeno desde la prevención, porque un usuario informado es menos vulnerable, y un sistema que combina información, articulación, herramientas y acción institucional reduce el problema.

Objetivos:

- Proteger a los usuarios reduciendo la capacidad de acción del delito
- Preservar la confianza en la marca y mitigar el riesgo reputacional

Con tal fin, diseñamos un enfoque integral basado en tres ejes, teniendo al primero como el preponderante:

Prevención:
Informar, educar y generar conductas de alerta.
Desarrollar herramientas preventivas.

Articulación:
Coordinar acciones con plataformas, autoridades y usuarios.

Denuncia:
Desarrollar herramientas de denuncia, para evitar el subregistro.
Transformar casos aislados en procesos judiciales con trazabilidad.

La premisa:
disuadir, desactivar y denunciar.

Prevención: usuarios en modo “alerta”

La prevención no podía limitarse a una campaña masiva ni a acciones aisladas. Requería una lógica de intervención inteligente, capaz de combinar alcance, oportunidad y pertinencia. Una campaña con suficiente continuidad, sin generar agotamiento en el receptor.

El objetivo fue transformar al usuario en un actor activo dentro del sistema de protección, por lo que el mensaje debía brindar herramientas concretas para:

- Conocer las modalidades de fraude
- Detectar señales de alerta
- Actuar frente a situaciones sospechosas



La estrategia se estructuró bajo una lógica clara, a dos niveles:

- **Intervenciones de alcance masivo**, para instalar el problema, sensibilizar y generar conocimiento general en toda el área de concesión.

- **Acciones focalizadas y geolocalizadas**, activadas ante la detección de “olas de fraude” en localidades específicas.

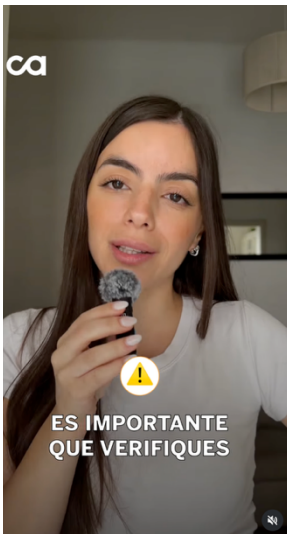
Este enfoque de segmentación permitió evitar la sobreexposición y el desgaste del mensaje y, al mismo tiempo, aumentar la relevancia y efectividad de la comunicación, llegando al usuario adecuado en el momento en que el riesgo era más alto.

Este modelo se replicó de manera consistente en todos los frentes de comunicación:

- **Prensa:**
  Campañas de difusión de comunicados generales para todo el territorio, combinadas con comunicados específicos cuando se detectaban incrementos de casos en localidades puntuales.

Entrevistas radiales y televisivas en medios locales, especialmente en contextos de mayor alerta, con mensajes adaptados a cada comunidad.

- **Ecosistema digital:**
  Una estrategia continua que integró:
  - Redes sociales (contenidos orgánicos y pauta)
  - E-mail marketing a la base de usuarios
  - Campañas digitales geolocalizadas
  - Información web



Evolución creativa: cercanía y credibilidad

Durante 2024 y 2025, las piezas priorizaron captar la atención mediante recursos creativos que invitaran a consumir mensajes preventivos, evitando tanto la monotonía como la banalización del riesgo.

En 2026, la estrategia evolucionó hacia contenidos con lógica de UGC (User Generated Content), reforzando la identificación y credibilidad.

Este enfoque permitió construir una narrativa más cercana, conectada con la experiencia real de los usuarios y alejada del discurso institucional.

Ofrecer una herramienta concreta para prevenir

Como evolución natural de la estrategia de prevención, Camuzzi incorporó un componente clave orientada a la detección temprana del fraude: el Sistema de Validación del Personal.

Esta plataforma permite a los usuarios verificar, en tiempo real, la identidad de cualquier persona que se presenta como colaborador de Camuzzi, tanto en interacciones presenciales como remotas. De esta manera, se busca desactivar uno de los principales mecanismos del fraude: la apropiación de la identidad corporativa para generar confianza.



El lanzamiento de esta solución fue acompañado por una campaña específica, integrada al ecosistema comunicacional de prevención, bajo un concepto rector:

“Conocé quién está del otro lado”

La comunicación se implementó siguiendo la misma lógica estratégica que el resto de las acciones con integración en prensa, medios, redes sociales y e-mail marketing

El objetivo no fue únicamente dar a conocer la herramienta, sino instar a un comportamiento: que los usuarios adopten la verificación de identidad como un paso previo en cada interacción.

Articulación y denuncia: del caso aislado a la acción coordinada

Si la prevención permitió reducir la vulnerabilidad, el segundo eje de la estrategia se enfocó en atender a los usuarios una vez afectados, y articular con otros actores involucrados para el seguimiento de los casos, a partir de una respuesta coordinada, trazable y sostenida en el tiempo.

Para evitar la denuncia dispersa y crear un sistema articulado impulsamos un esquema de trabajo con actores clave:

- Plataformas digitales (META)**,** para la detección, reporte y baja de perfiles falsos que utilizaban la marca
- Fiscalías, para canalizar los casos dentro del sistema judicial
- Usuarios, promoviendo un rol activo en la detección temprana y denuncia de situaciones sospechosas

Asimismo, como uno de los principales obstáculos en la gestión de este tipo de delitos es el alto nivel de subregistro, lo que limita la posibilidad de intervención y reduce la visibilidad real del problema, para abordar esta brecha, en 2025 Camuzzi desarrolló un nuevo canal específico de denuncia, orientado a facilitar el reporte por parte de los usuarios.

En paralelo, la compañía promovió activamente que los usuarios formalicen las denuncias ante las autoridades competentes, acompañando el proceso y facilitando la derivación hacia los organismos correspondientes.

Este trabajo permitió transformar eventos individuales en procesos judiciales con trazabilidad, consolidando un abordaje más estructural del problema.

Resultados y aprendizajes

La estrategia permitió:

- +200 perfiles falsos denunciados y desactivados en Meta.
- 700.000 usuarios alcanzados.
- 1,9 millones de impresiones (+114%).
- +30 acciones de prensa.
- 40+ denuncias judiciales.
- 3.200 validaciones realizadas por los usuarios sobre la identidad de los colaboradores (200 semanales).
- 140 denuncias de fraude trazados desde el lanzamiento del canal de denuncias.

Los resultados no solo evidencian alcance, sino un cambio de comportamiento: **el 60% de los casos reportados corresponden a intentos de fraude detectados a tiempo,** lo que indica una mayor capacidad de los usuarios para identificar situaciones sospechosas.