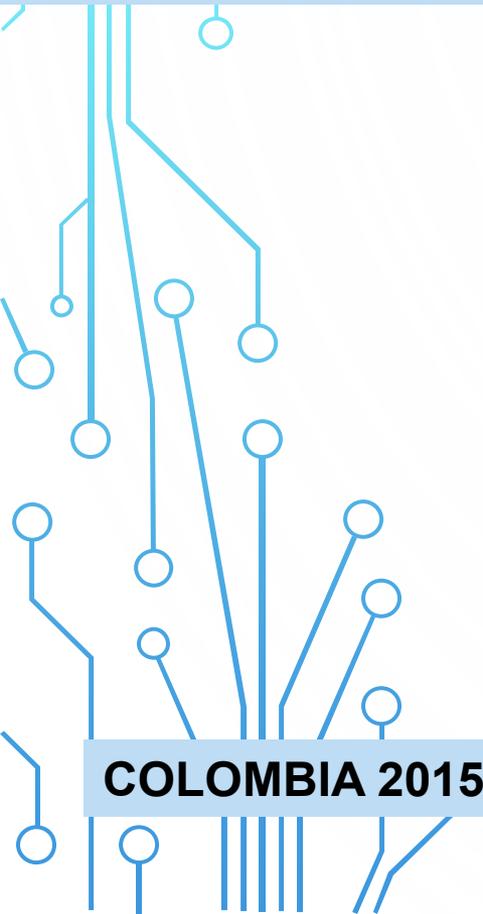




CYBERDRILL 2015

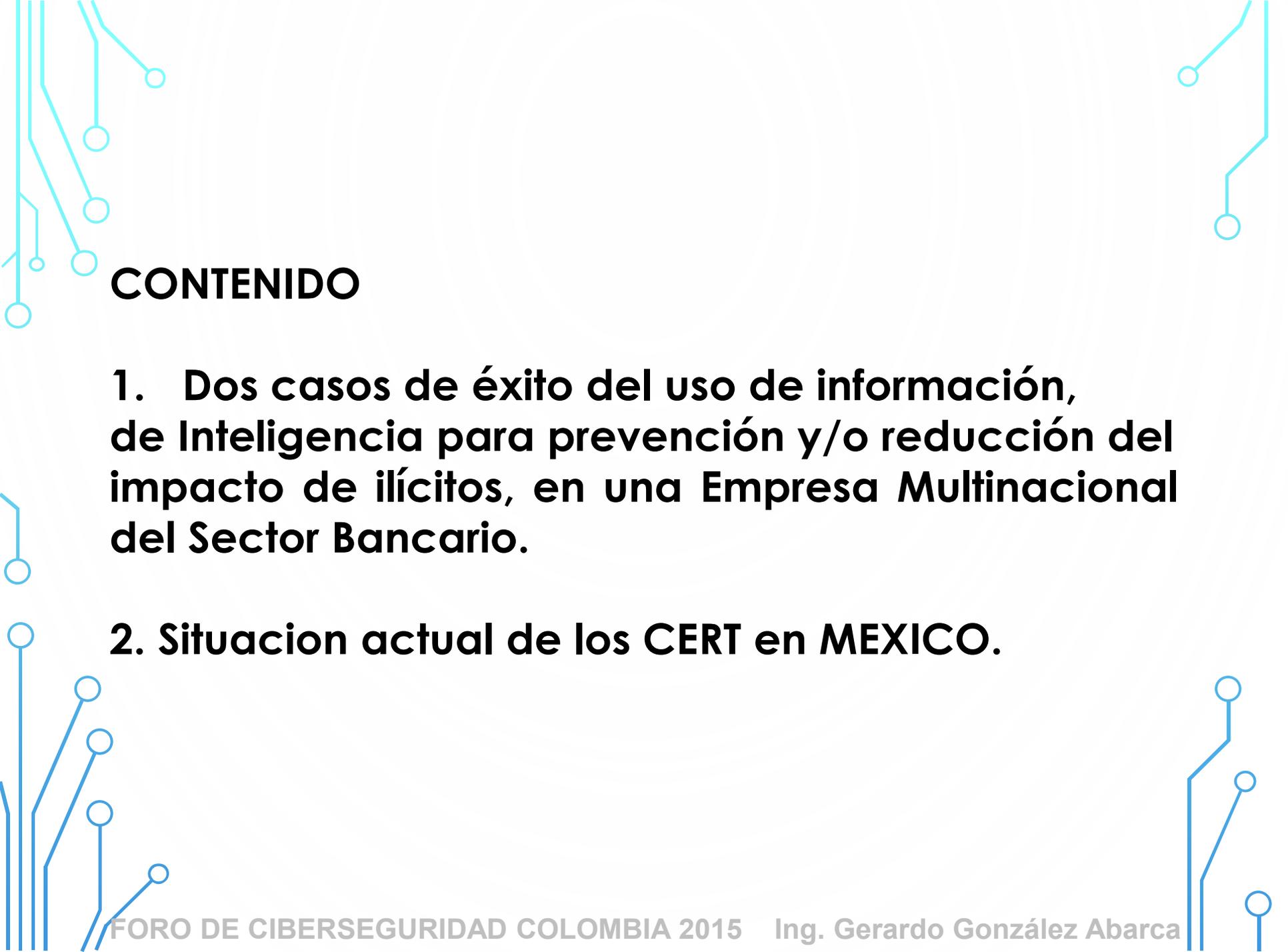
Universidad de los Andes BOGOTA.



COLOMBIA 2015

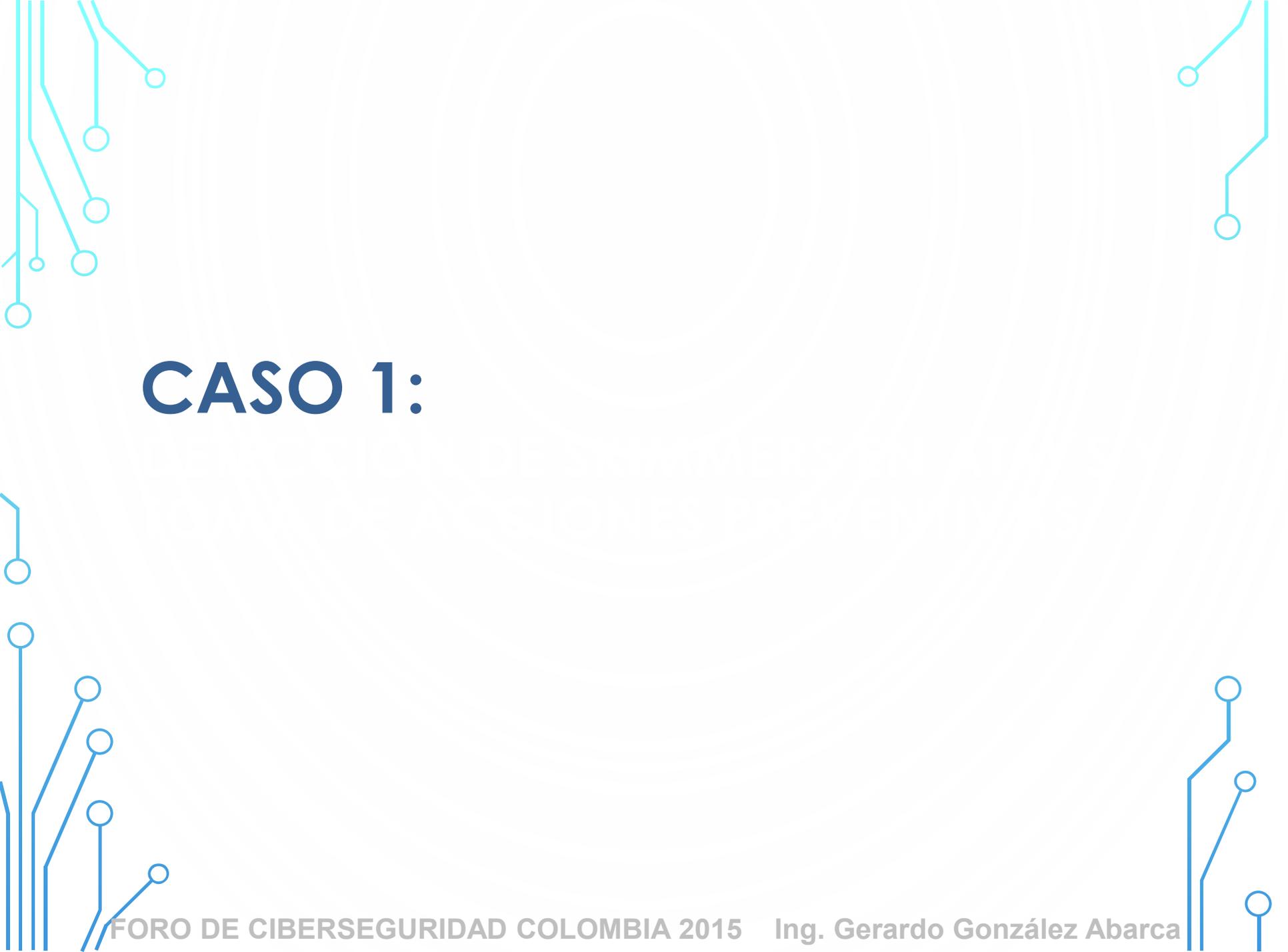
**Ing. Gerardo F. González
Abarca
CIME México**

**Agosto 3, 4 y 5 de
2015**

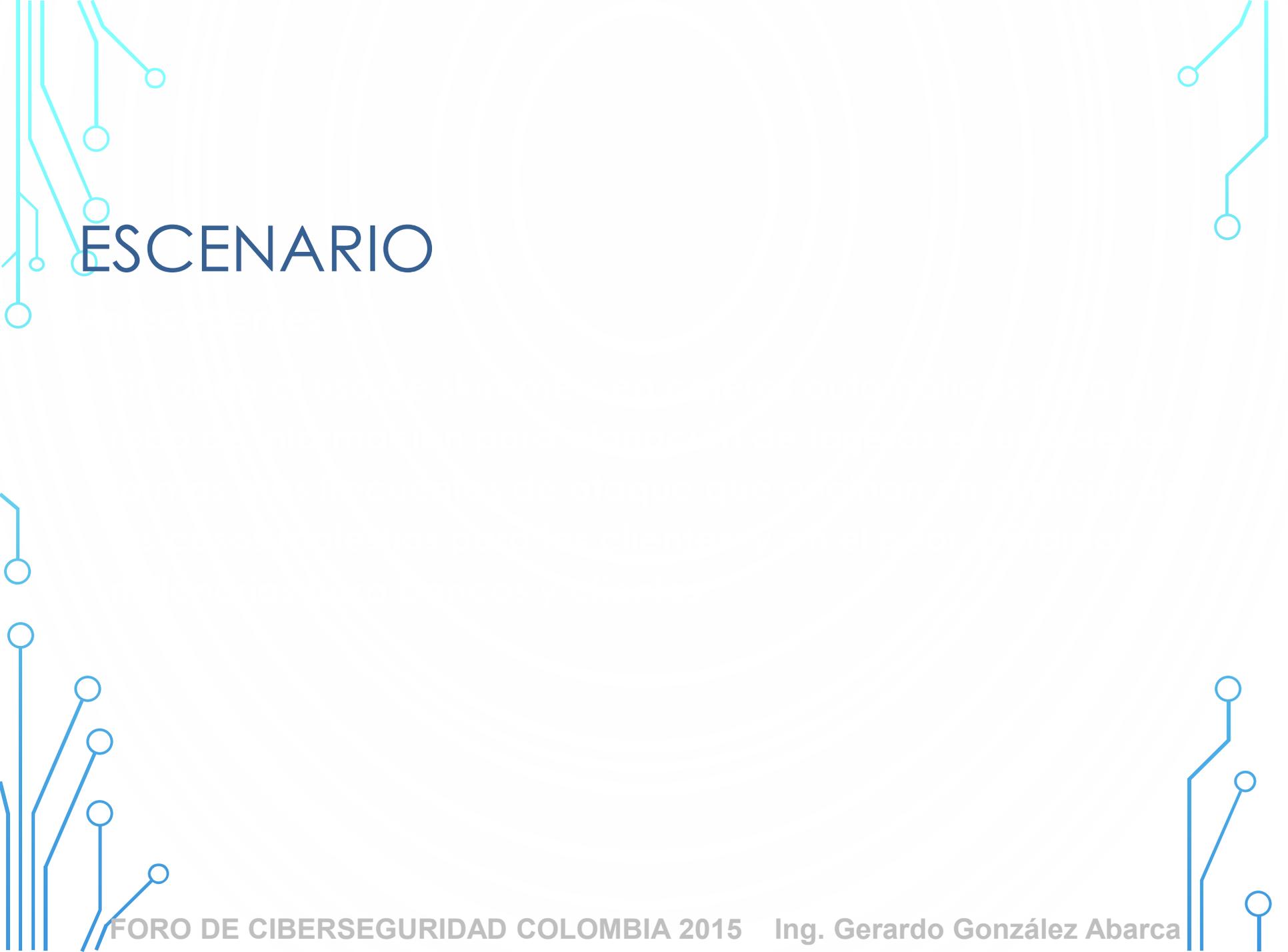


CONTENIDO

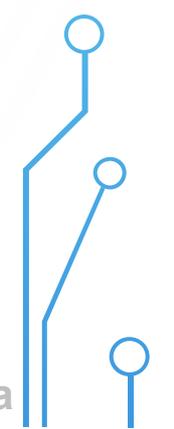
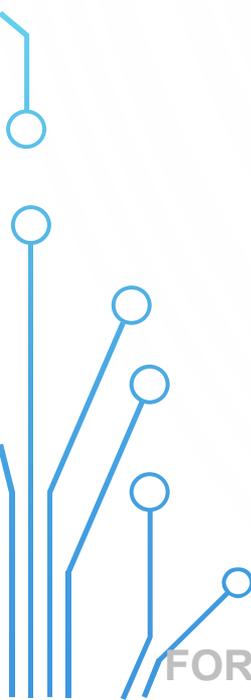
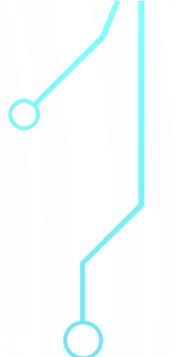
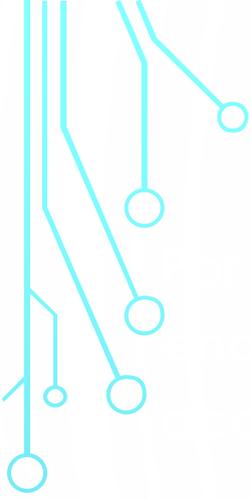
- 1. Dos casos de éxito del uso de información, de Inteligencia para prevención y/o reducción del impacto de ilícitos, en una Empresa Multinacional del Sector Bancario.**
- 2. Situación actual de los CERT en MEXICO.**

The slide features decorative circuit-like lines in the corners, consisting of thin blue lines with small circles at various points, resembling a network or data flow diagram.

CASO 1:



ESCENARIO





¿QUÉ SUCEDE CUANDO SE COLOCA UN SKIMMER EN UN ATM?



**Colocación del skimmer y regleta/
cámara**

**Prueba del skimmer introduciendo
una tarjeta varias veces en forma
consecutiva, sin concluir la
operación (Ej. no captura de NIP).**

**Registro de las operaciones del
defraudador y clientes en el skimmer
y en logs.**

**Retiro del skimmer después de
algunas horas ó días.**

¿QUÉ SUCEDE CUANDO SE COLOCA UN SKIMMER EN UN ATM?



Colocación del skimmer y regleta/
cámara

Prueba del skimmer con
tarjeta varias veces
consecutiva, sin éxito
(Ej. no captura de datos)

Registro de las operaciones
del defraudador y cliente
en logs.

Retiro del skimmer y regleta
horas ó días.

NUMERO DE CUENTA : XXXXXXXXXXXX1197
CAJERO: 000004872 C.F.PASE 2
MERIDA, YUC

OPERACION:1035-01450 04/05/2011 20:56:39
EL CLIENTE **CANCELO * PANTALLA COMISION ***

NUMERO DE CUENTA : XXXXXXXXXXXX1197
CAJERO: 000004872 C.F.PASE 2
MERIDA, YUC

OPERACION:1036-01451 04/05/2011 20:57:07
EL CLIENTE **CANCELO EN * CAPTURA DE PIN ***

NUMERO DE CUENTA : XXXXXXXXXXXX1197
CAJERO: 000004872 C.F.PASE 2
MERIDA, YUC

OPERACION:1037-01451 04/05/2011 20:57:29
EL CLIENTE **CANCELO * PANTALLA COMISION ***

METODOLOGÍA

Lectura de skimmers incautados

Registro de la primer tarjeta de skimmers en lista negra (LN)

Búsqueda de tarjetas de LN en logs de cajeros automáticos (diario)

Revisión de hallazgos o hits de LN.
Confirmación de patrón: "Operaciones sucesivas canceladas"

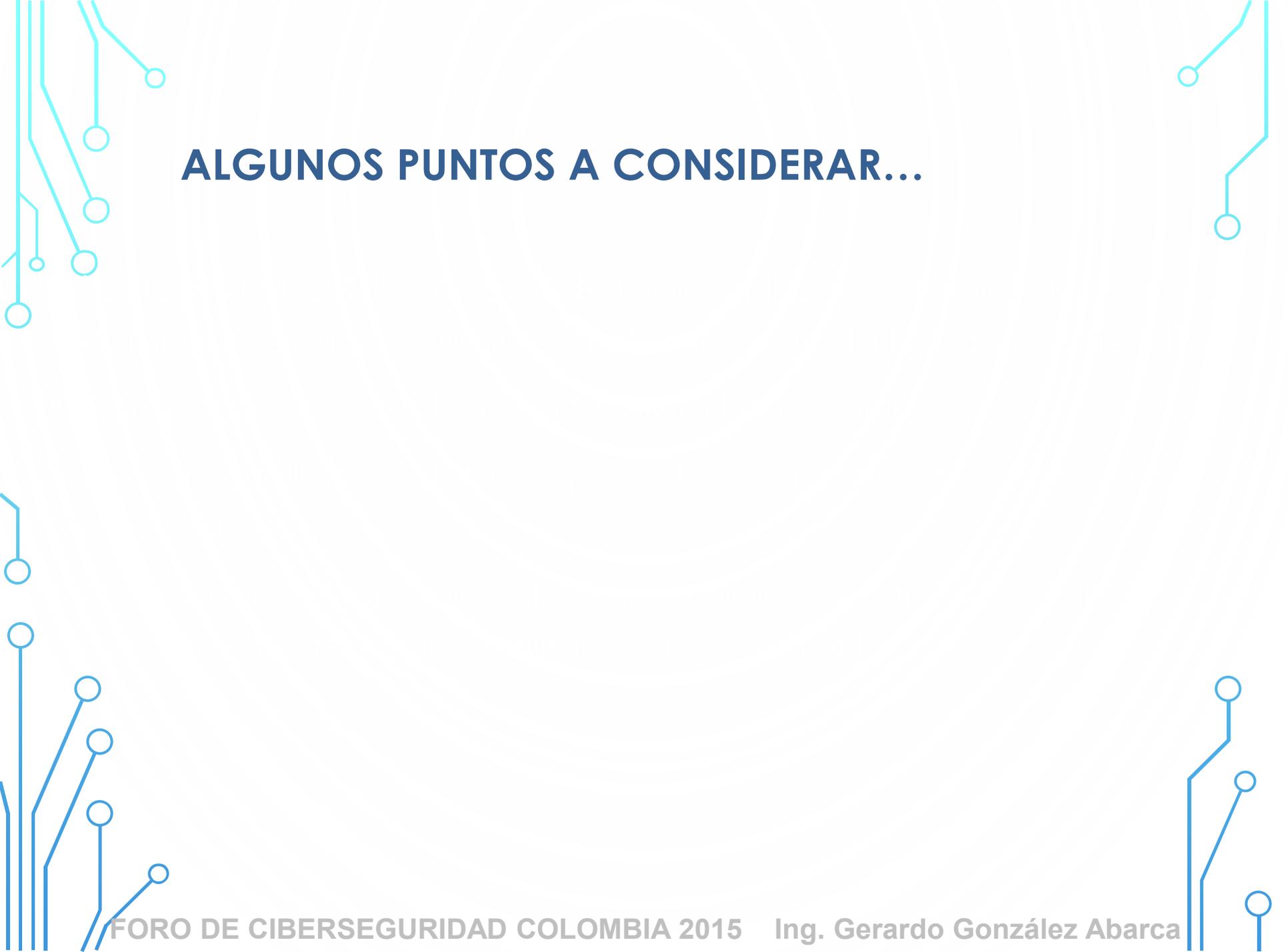
Identificación de tarjetas usadas después de cada hallazgo (hasta 24 horas después)

Ejecución de acciones preventivas sobre tarjetas identificadas

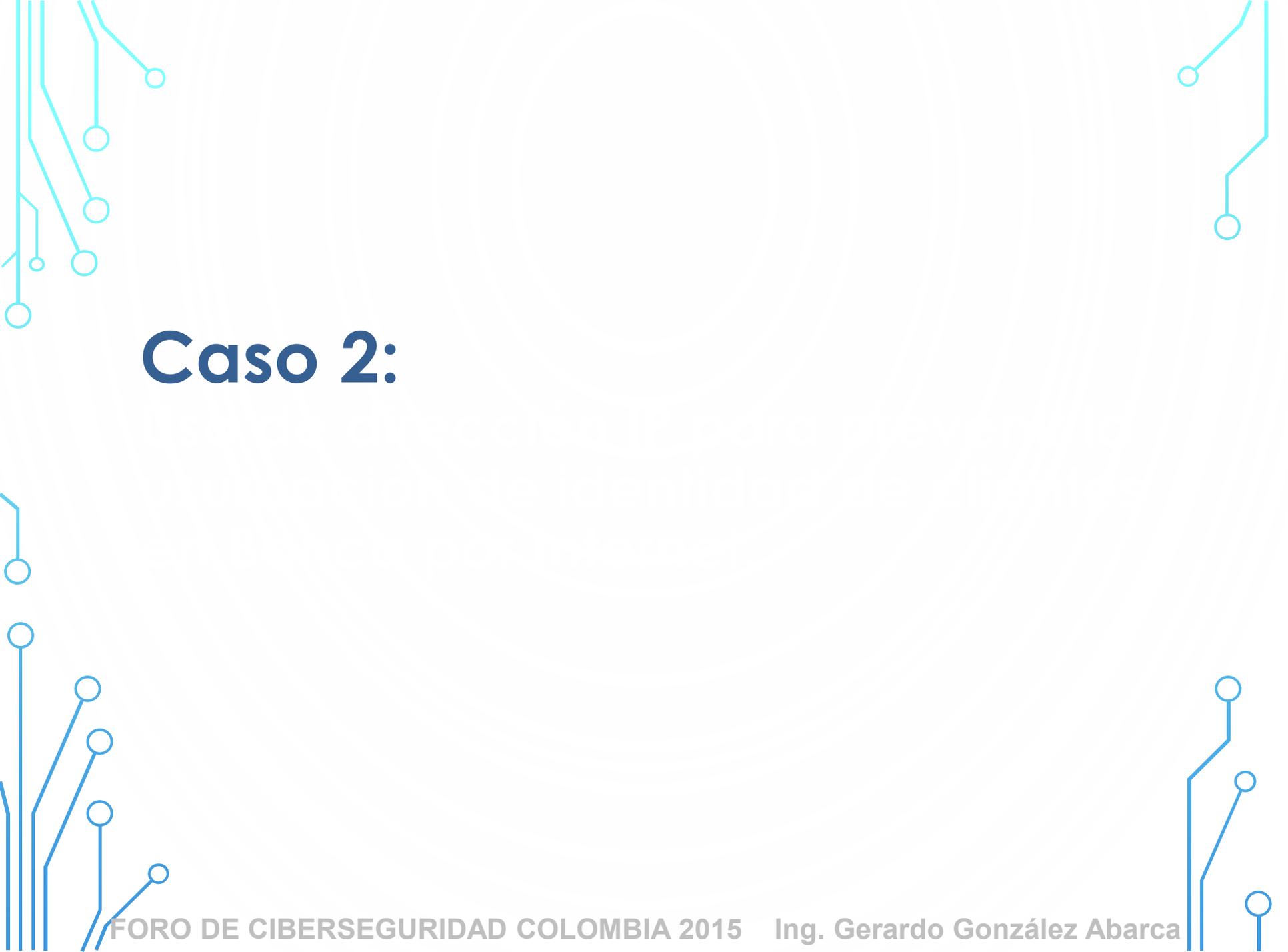
RESULTADOS

Periodo de monitoreo: 6 Meses

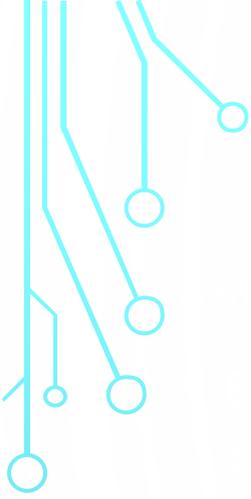
# ATMs con skimmers	24
Tarjetas en riesgo de ser clonadas	4,613
Fraude Prevenido (USD)	\$ 2,194,071

The slide features decorative circuit-like lines in the corners, consisting of thin blue lines with small circles at various points, resembling a network or data flow diagram.

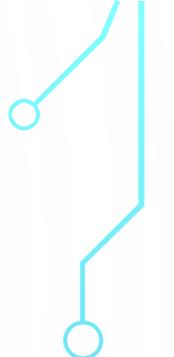
ALGUNOS PUNTOS A CONSIDERAR...

The slide features decorative circuit-like lines in the corners, consisting of thin blue lines with small circles at various points, resembling a network or data flow diagram. These lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners of the slide.

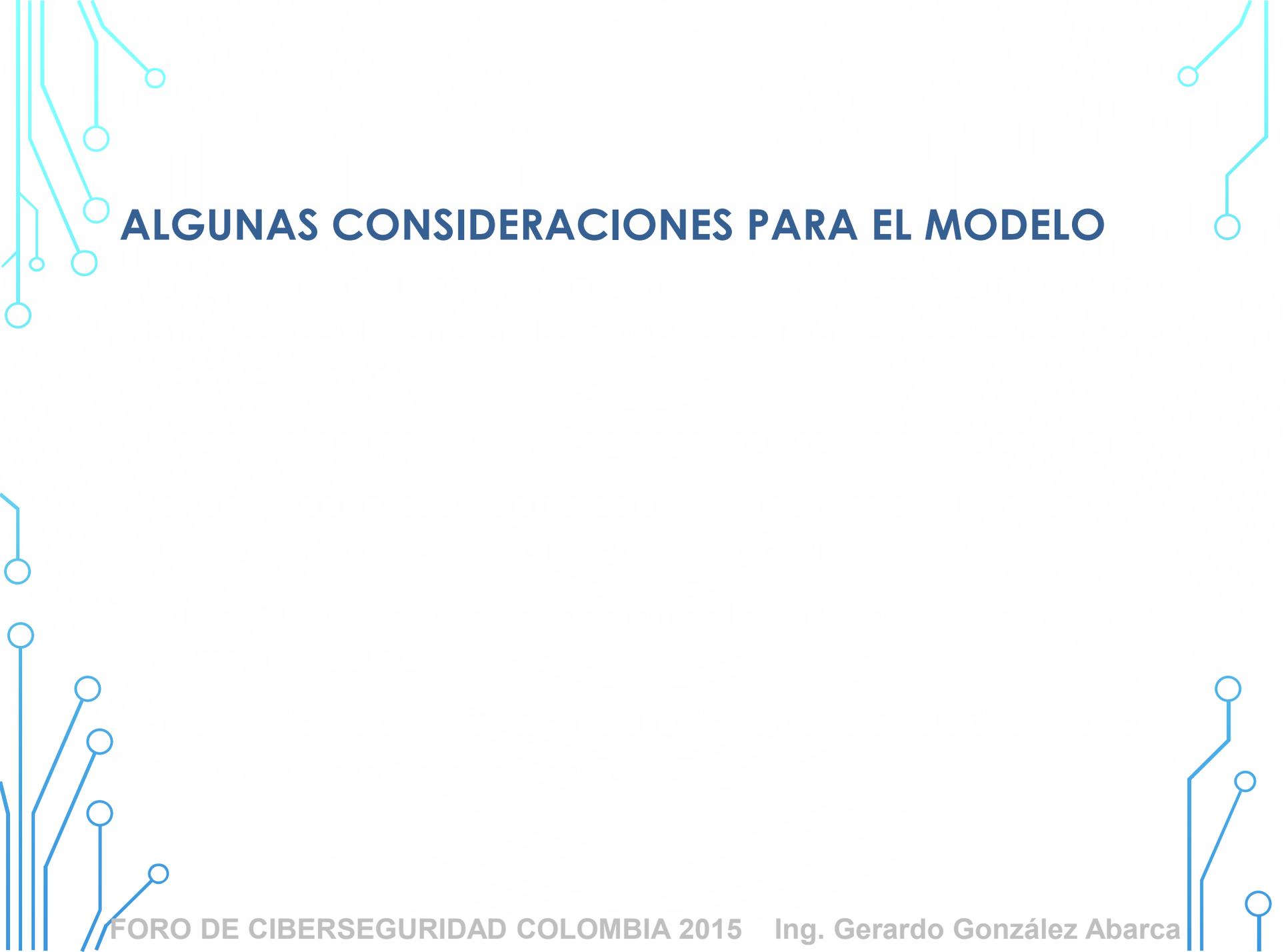
Caso 2:



ESCENARIO

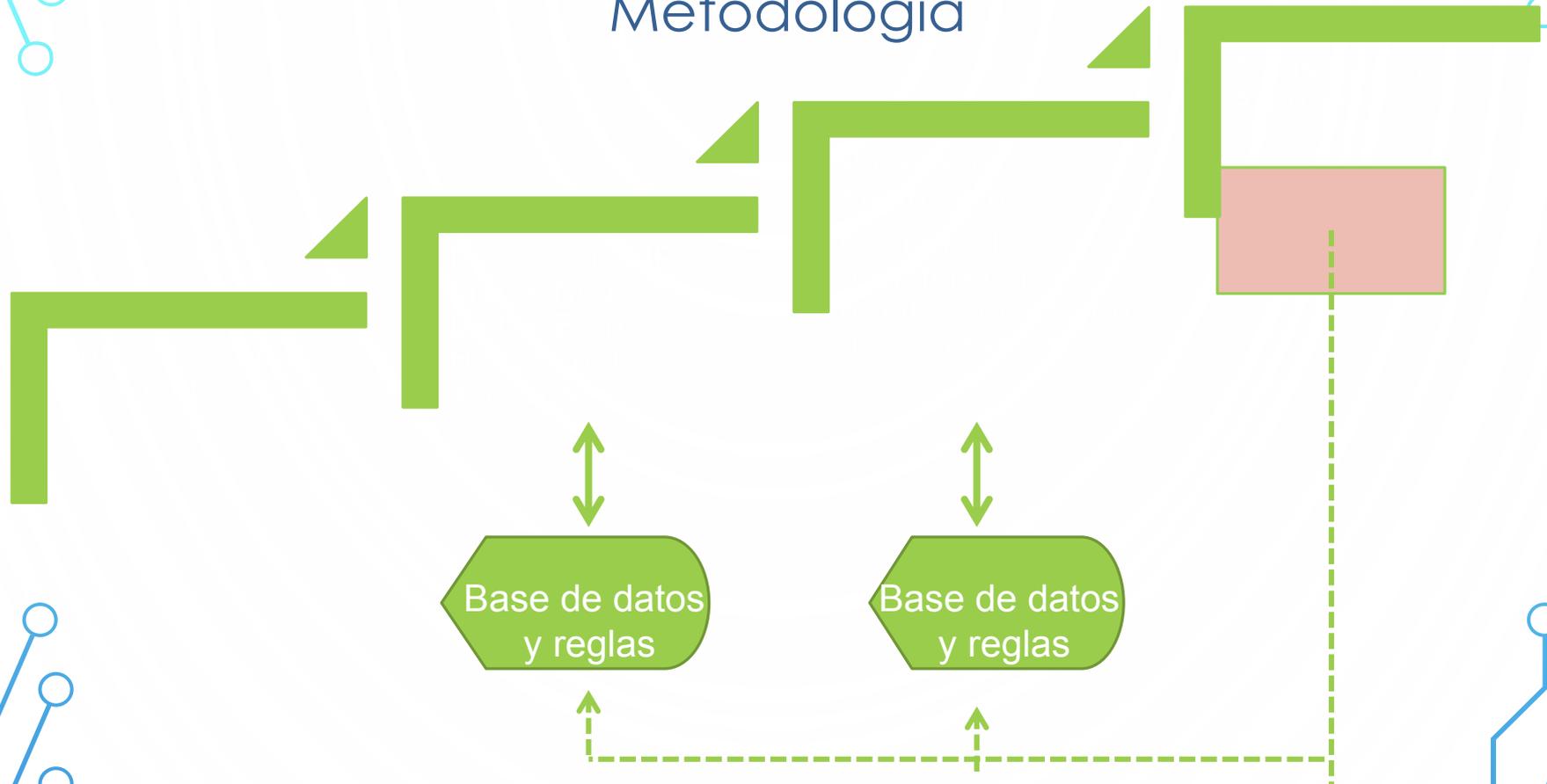


Caso de estudio

The slide features decorative circuit-like lines in the corners. The top-left and bottom-left corners have light blue lines, while the top-right and bottom-right corners have dark blue lines. These lines consist of straight segments connected by right-angle turns, ending in small circles.

ALGUNAS CONSIDERACIONES PARA EL MODELO

Metodología



Resultados

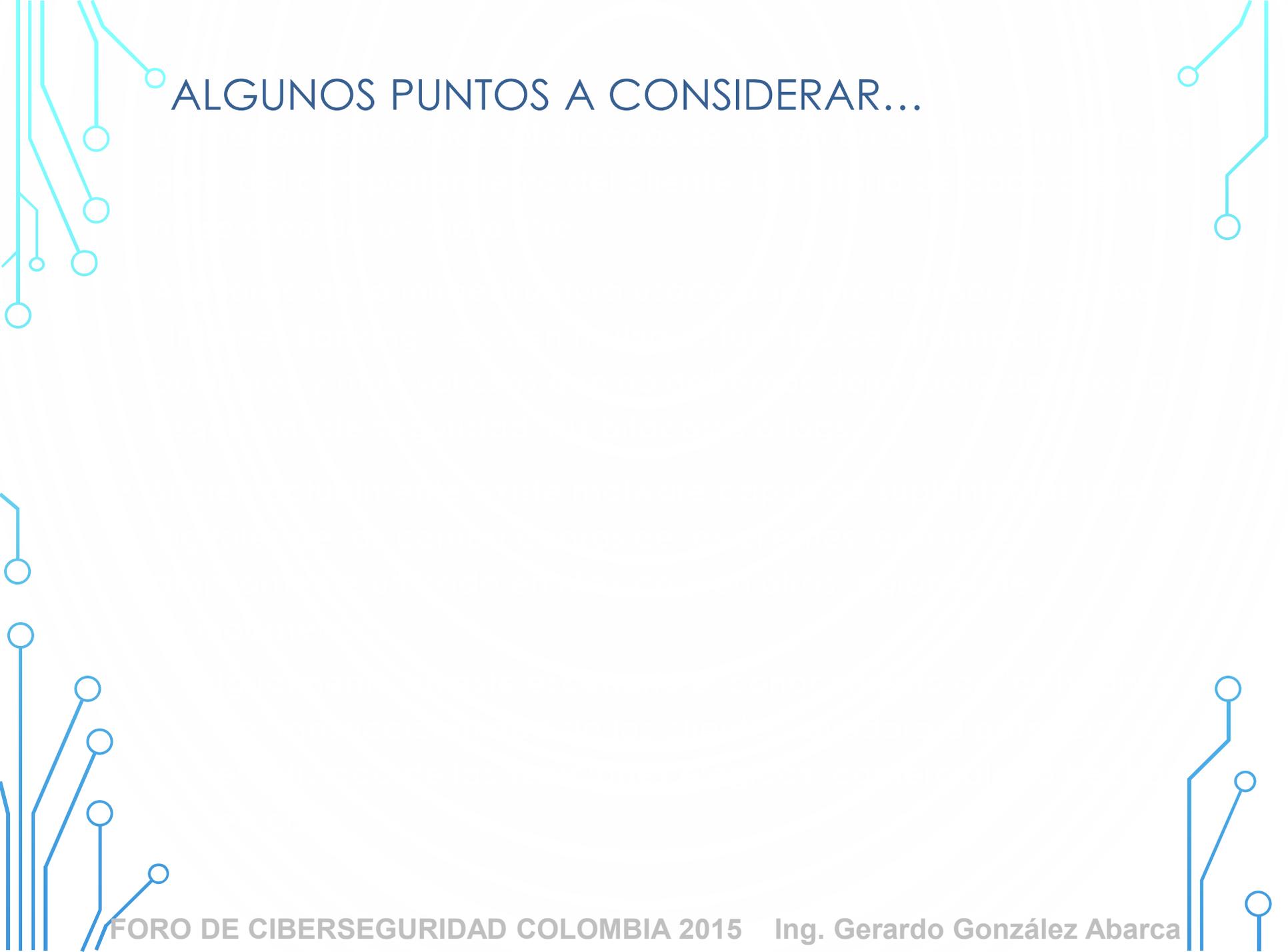
Reducción de niveles de fraude en más del 90%

Reducción de los falsos positivos en más del 50%

Reducción de los montos transaccionales de monitoreo

Mejoras al enfoque de los analistas de fraude

Mejor conocimiento de los perfiles de transaccionalidad del cliente



ALGUNOS PUNTOS A CONSIDERAR...

2. SITUACION ACTUAL DE LOS CERT EN MEXICO.

DE LOS CASOS DESCRITOS ANTERIORMENTE, PODEMOS APRECIAR QUE EN TERMINOS GENERALES LOS GRANDES GRUPOS EMPRESARIALES EN MEXICO, IMPLEMENTAN SUS PROPIOS SISTEMAS DE MONITOREO Y SEGURIDAD.

EXISTEN CERT ESPECIALIZADOS, TANTO DEL GOBIERNO FEDERAL DEL SECTOR SEGURIDAD COMO DE LAS ENTIDADES EDUCATIVAS PUBLICAS Y EMPRESAS PRIVADAS MULTINACIONALES QUE BRINDAN SUS SERVICIOS.

A CONTINUACION ENLISTO LAS WWW DE ALGUNAS DE ELLAS:

WWW.CNS.GOB.MX COMISION NACIONAL DE SEGURIDAD. GOBIERNO.

WWW.CERT.UNAM.MX UNAM. EDUCACION. GOBIERNO FEDERAL.

WWW.MNEMO.COM PROVEEDOR DE SERVICIOS. EMPRESARIAL

WWW.SCITUM-CSIRT.COM.MX PROVEEDOR DE SERVICIOS. EMPRESARIAL

The image features decorative blue circuit-like lines in the corners, consisting of vertical and horizontal lines with small circles at the ends, resembling a stylized PCB or network diagram.

GRACIAS POR SU ATENCION.