CCP.I/DEC. 234 (XXVII-15)[1]

CLASIFICACIÓN DE FRAUDE Y PRÁCTICAS ANTIRREGLAMENTARIAS EN LAS TIC

La XXVII Reunión del Comité Consultivo Permanente I: Telecomunicaciones/Tecnologías de la Información y la Comunicación (CCP.I),

DECIDE:

1. Solicitar a los Estados Miembros que diligencien la encuesta adjunta en el Anexo a la presente Decisión, hasta la XXVIII Reunión del CCP.I., para efectos del levantamiento de información sobre clasificación de fraude y prácticas antireglamentarias.

2. Designar a la Relatoría sobre Control de Fraude, Prácticas Antirreglamentarias en Telecomunicaciones la recopilación de la información con los resultados de la encuesta; y a presentar los resultados de la encuesta en la XXIX Reunión del Comité.

ANEXO I A LA DECISIÓN CCP.I/DEC. 234 (XXVII-15)

CLASIFICACIÓN DE FRAUDE Y PRÁCTICAS ANTIRREGLAMENTARIAS EN LAS TIC

País/Administración: _____

Nombre de quien diligencia: _____
Entidad/Institución _____
Datos de contacto:
Teléfono_____ e-mail _____

Objetivo: Relevar la situación actual en cada uno de los Estados Miembros de los 9 casos de Fraude más relevantes, tomando como fundamento la primera Matriz de Riesgo donde se tomaron los impactos y las ocurrencias de las 34 Tipologías de Fraude acordadas en el XXV Reunión del CCP.I.

Siendo las maniobras más riesgosas y con mayor impacto:

1. Robo de Celulares
2. Bypass – Reoriginamiento
3. Clonación de teléfonos celulares (Clonning)
4. SPAM
5. Fuga de equipos terminales móviles
6. IRSF (Fraude tercer país)
7. Fraude en suscripción al servicio
8. Fraude interno
9. Fraude de PBX

[1] CCP.I-TIC/doc. 3688/15

1. Completar la información de cada una de las maniobras antes mencionadas en el archivo adjunto:

Relevamiento de Fraudes

2. Según la Primera versión de la Matriz los nueves tipos de Fraude más relevantes son los que están en esta consulta, y en el orden mencionado. Según la experiencia de su país, ¿los tipos de Fraude coinciden?

SI ☐ NO ☐

3. En caso de que la respuesta anterior haya sido que NO por favor menciones los tipos de Fraude que no están contemplados entre los 9 más relevantes.

4. Teniendo en cuenta el nivel de riesgo de 1 a 9, ¿coincide con la valorización de la primera Matriz?

SI ☐ NO ☐

5. En caso que NO por favor ordenar las tipologías según la realidad de su país.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____

6. Por favor desarrolle todo lo que considere necesario sobre cada una de las 9 tipologías, referente a la realidad de las mismas en su país. Teniendo en cuenta, el impacto, las medidas de detección, las medidas de mitigación.

7. ¿Cuáles considera serían las mejores prácticas para cada una de las tipologías que existen en su país, para la mitigación del Fraude?

8. Por favor deje un correo de contacto para poder consultar cualquier duda que surja de las respuestas.

Nombre: _____
Correo electrónico: _____@_____

ANEXO II A LA DECISIÓN CCP.I/DEC. 234 (XXVII-15)

DEFINICIONES DE FRAUDES Y PRÁCTICAS ANTIRREGLAMENTARIAS MÁS RELEVANTES

1. **Robo de Celulares.**
   Existen bandas dedicadas al robo de dispositivos móviles con el objeto de revender los mismos para que sean usados dentro o fuera del territorio nacional normalmente en otros operadores, actualmente es un problema grande debido a que estos equipos son remarcados con números de identificación que los hacen aparecer como otro equipo ante la red del operador evadiendo de esta forma los controles de inactivación de terminales robados en las bases de los operadores.

2. **Bypass – Reoriginamiento:**
   La modalidad de Bypass consiste en transmitir tráfico del servicio de larga distancia Nacional o Internacional a través de redes de operadores sin título habilitante para la prestación de dichos servicios, una vez el tráfico es puesto en el punto de interés de destino, allí se realiza la modalidad de reoriginamiento que consiste en cambiar el origen de la comunicación que es de carácter Internacional simulándola como realizada entre operadores locales o de Intrared, esta modalidad se da para el servicio fijo o móvil. El negocio del defraudador consiste en ganarse la diferencia existente entre el precio de comunicación internacional y el tráfico local para el caso de fijos o de Intrared para el caso de móviles, adicionalmente por lo general estos defraudadores no tienen obligaciones regulatorias, no pagan impuestos y perciben sus ingresos en el exterior. Tipos de bypass: entrante, saliente, reoriginamiento local, nacional o internacional o móvil.

3. **Clonación de teléfonos celulares (Clonning):**
   Los defraudadores interceptaban los números ESN (Equipment Serial Number) a través de equipos de recepción de radio. Teniendo dichos números, los reprogramaban en otros equipos desde los cuales realizaban llamadas a cargo del suscriptor con el ESN original.

4. **SPAM**: Correo no deseado, por este intermedio el timador intenta bombardear a listas de usuarios con correos no solicitados, muchas veces contenido programas que se auto instalan e incluso pueden dañar el contenido de los computadores, los defraudadores muchas veces los utilizan como medio de propagación de virus entre otros.

5. **Fuga de equipos:**
   El defraudador se suscribe en planes de telefonía móvil en donde los equipos son subsidiados, con el objeto de obtener el terminal, los cuales son tomados por delincuencia organizada y puestos normalmente en otros países en el que el precio de estos equipos es mucho mayor, con el objeto de beneficiarse económicamente de la diferencia de precio del equipo.

6. **IRSF International Revenue Share Fraud:**

En este caso, tras el fraude de suscripción, se realizan llamadas de larga duración a destinos internacionales con alto costo (generalmente a naciones que se corresponden con pequeñas islas o rangos de numeración de servicios satelitales). Las llamadas no alcanzan a los destinos geográficos que les corresponderían, sino que son encaminadas por una operadora intermedia hacia un tercer proveedor que posee un servicio de pago compartido (p.ej. audio texto).
En ciertos casos este enrutamiento se realiza incluso sin el consentimiento del propietario del bloque de numeración. De esta forma el proveedor del servicio de pago compartido obtiene el beneficio de estas llamadas, a la vez que no pagará a la operadora con la que posee la suscripción fraudulenta. Este tipo de fraudes ha sido ampliamente documentado por GSMA, habiéndose elaborado listas negras de numeraciones fraudulentas o sospechosas.

7. **Fraude de suscriptor:**
   El usuario entrega documentación falsa o mediante suplantación, para la solicitud y suscripción de un servicio de telecomunicaciones con el objeto de usufructuarlo generalmente para no pago o realizar otros tipos de fraude de manera clandestina.

8. **Fraude Corporativo o Interno:**
   Consiste en el fraude realizado por personal interno de la empresa, con la intención de utilizar incorrectamente los recursos de la empresa para propósitos personales o de terceros, involucra los privilegios y conocimientos técnicos que tiene el defraudador, entre los que se encuentran:
   1) Apropiación de bienes para usufructo personal o de terceros.
   2) Venta o uso para propio beneficio de información privilegiada.
   3) Venta de accesos a bienes o servicios proveídos por las compañías para usufructo de terceros.
   4) Acceso a los sistemas de la cadena de prestación del servicio para cambiar información de uso de servicios propios o de terceros.
   5) Abuso de servicios o facilidades provistas para manejo interno de la compañía en beneficio propio o de terceros.
   6) Acceso y uso de facilidades de red de clientes para beneficio propio o de terceros.
   7) Divulgación de información de procesos y vulnerabilidades identificadas para beneficio de terceros.
   8) Favorecimiento a terceros en procesos de oferta, selección y contratación de servicios o compra de bienes y activos de la compañía, para beneficio propio, de conocidos o familiares.

9. **Fraude de PBX:**
   Esta es una facilidad de las centrales de PBX que normalmente se le asignan a los ejecutivos de las compañías accesos remotos con códigos a las plataformas que les permite realizar comunicaciones de todos los servicios (local, larga distancia nacional, larga distancia internacional, móvil, acceso a Internet, entre otros), a través de ingeniería social o de manera inescrupulosa estos accesos son conocidos por terceros quienes usufructúan el servicio haciendo que finalmente la compañía pague la factura de servicios no usados para su beneficio. Este tipo de fraude se está incrementando con PBX IP, por la facilidad de acceso que posee desde cualquier parte del mundo y muchas veces la poca protección de estos elementos por parte de los usuarios.