NOTA DE PRENSA
N° 102-2022

OSIPTEL: desde el 12 de enero de 2023 será obligatorio uso de contraseña única para la contratación y reposición de chips móviles

- Durante webinar sobre seguridad de las telecomunicaciones, ente regulador recordó que empresas deben entregar esta clave de seguridad a usuarios de los servicios.

Para evitar casos de suplantación de identidad en las contrataciones nuevas, cambio de titularidad y reposición de chip móvil, desde el próximo 12 de enero de 2023, será obligatorio el uso de la contraseña única, de acuerdo a las medidas dispuestas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).

Así lo dio a conocer el presidente ejecutivo del OSIPTEL, Rafael Muente Schwarz, durante el desarrollo del webinar "Amenazas y desafíos de la seguridad en las telecomunicaciones", donde se revisaron diversas medidas, tanto en el aspecto ciudadano como en el institucional, para minimizar o neutralizar las actividades delictivas en las telecomunicaciones.

Indicó que la contraseña única es una clave personalizada que las empresas operadoras deben entregar obligatoriamente, desde el 12 de junio de este año, al momento de la contratación de un nuevo servicio o en cualquier otro en el que la identidad del abonado sea validada a través del sistema de verificación biométrica o del correo electrónico que este indique.

Se trata de un mecanismo de seguridad adicional a la verificación biométrica de huella dactilar, que busca evitar suplantaciones de identidad y contrataciones no solicitadas. También se implementará la reactivación de reposición del SIM card en un lapso de cuatro horas y no de manera inmediata como es hasta ahora, así como la validación biométrica para los vendedores del sector telecomunicaciones, entre otras medidas.

"Hoy en día existen muchos elementos tecnológicos que están involucrados en estos tipos de comportamientos que buscan obtener dinero ilícitamente. Desde OSIPTEL hemos actuado con celeridad en estos aspectos. Es importante que se sigan implementando directivas desde el ámbito personal e institucional para salvaguardar los datos personales de los ciudadanos", señaló Muente Schwarz.

Por su parte, el director de Fiscalización e Instrucción del OSIPTEL Luis Pacheco, enfatizó que el control biométrico a través de la huella dactilar sigue siendo una medida de seguridad robusta, pues posibilita la verificación de la identidad con la base de datos del RENIEC, antes de la contratación del servicio de acuerdo a la normatividad vigente "No hay que descartar los lectores de biometría dactilar; por el contrario, hay que reforzar este mecanismo de seguridad y emplear lectores de huella viva, que son más precisos y ayudan a descartar las huellas de plástico", señaló.

Además, se indicó que, como parte del paquete de medidas implementadas para prevenir la suplantación de identidad, el OSIPTEL dispuso limitar a cinco el número de intentos de verificación biométrica por persona en el día y por trámite.

Limpieza del registro de abonados

Por otro lado, el regulador señaló que viene realizando un proceso de limpieza del registro de abonados, que involucra más de 400 mil servicios telefónicos móviles, y cuya finalidad es validar la identidad de los titulares de dichos servicios, para lo cual se ha suscrito un convenio con el RENIEC y se ha contado con información proveniente de Migraciones-MININTER.

La limpieza del registro está a cargo de las empresas operadoras. En el supuesto que no corrijan la información, se evaluará la aplicación de medidas administrativas.

Enmascaramiento de llamadas

Otro modo de aproximación del delincuente con los usuarios, es haciéndose pasar por la propia entidad bancaria. Para ello utilizan la técnica de **"enmascaramiento de número llamante"**, que consiste en reemplazar el número de origen de la llamada por el número telefónico de la entidad bancaria, generando confianza en la víctima.

Aunque la problemática del enmascaramiento de llamadas está a cargo del Ministerio de Transportes y Comunicaciones (MTC), el regulador ha elevado una batería de propuestas para modificar los reglamentos que buscan bloquear el tráfico internacional de aquellas llamadas que tienen numeración local.

Venta ambulatoria

Tras brindar recomendaciones para no ser víctimas de las principales modalidades de delitos informáticos, el supervisor especialista del OSIPTEL, Marcos Zacarías, recordó que la contratación de servicios móviles en la vía pública está prohibida y constituye un alto riesgo para la seguridad de las personas.

"Exponer sus datos personales a través de un huellero biométrico portátil representa el mayor riesgo para la seguridad de la persona que contrata un servicio de telefonía de manera ambulatoria", enfatizó

Señaló que desde el 2020, OSIPTEL ha impuesto multas por 20 millones de soles, aproximadamente, a las empresas de telefonía móvil por infracciones relacionadas a fiscalizaciones de la venta de chips móviles en la vía pública.

El webinar gratuito "Amenazas y desafíos de la seguridad en las telecomunicaciones", contó con la participación de funcionarios y especialistas de entidades del sector público peruano, académicos, investigadores, gremios y asociaciones, estudiantes universitarios y público en general.

Lima, 28 de octubre de 2022