Panorama
Data Leak

digital

Panorama de Data Leak 2023

TLP:RED	TLP:AMBER	TLP:GREEN	TLP:CLEAR
No divulgar, restringido solo a participantes.	Divulgación limitada, restringida a la organización de los participantes y sus clientes.	Divulgación limitada, restringida a la comunidad.	Divulgación sin restricciones.

A continuación, se exponen las tendencias gráficas en el que se detalla una comparativa de los ataques realizados en LATAM en los años 2022 y lo que va de 2023.

De esta forma con la información obtenida se puede obtener comparativas de diferentes periodos que nos permitan determinar cómo se ha desarrollado la tendencia y de esta forma anticipar posibles factores de riesgo.

Este año ha estado marcado por una constante renovación de foros en Deep y Dark Web, dada principalmente tras el Takedown por policías y en menor medida tras ataques entre administradores de los mismos en busca de demostrar capacidades o eliminar competencia.

Entre los casos más conocidos de TakeDown se destacan:

- Raid Forums (Takedown)
- Breached (Takedown)
- Exposed (Takedown)
- Genesis Market (Takedown)

Actores de amenaza

Dentro de los actores de amenaza que han realizado ataques a LATAM, incluido Chile, se observa una continua renovación de actores de amenazas, dado principalmente por algunos de los siguientes motivos:

- Actores que no se crean nuevos usuarios tras las caídas, renovaciones o surgimiento de nuevos foros de mercados underground en Deep y Dark Web.
- Usuarios creados únicamente para una serie de campañas específicas.
- Cambio de alias, no vinculable al perfil anterior para evitar seguimiento.

Por otra parte, existe un número de actores de renombre que persisten y se encuentran constante o esporádicamente activos bajo su mismo alias en diferentes fuentes para ser reconocidos y cada vez aumentar su estatus y credibilidad.

Independientemente de lo anterior, las motivaciones de estos ataques son principalmente:

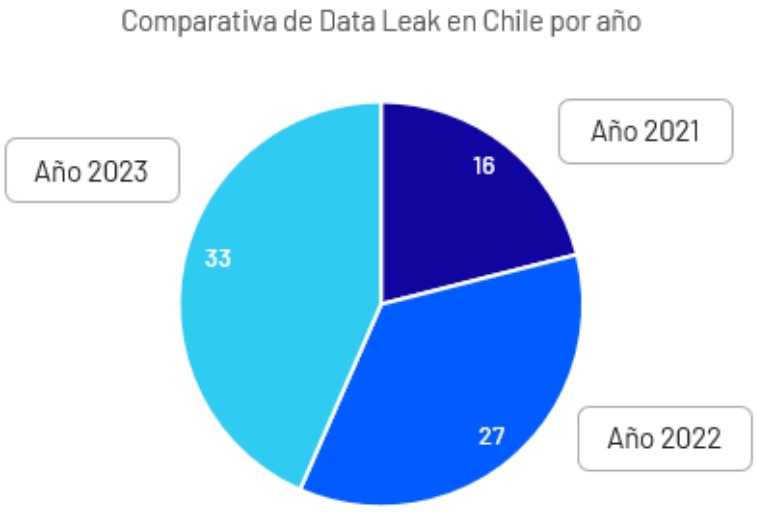
- **Financiera**: debido a las altas retribuciones monetarias que se pueden obtener por la venta de información sensible en internet y debido a esto, algunos actores necesitan mantenerse ligados a un usuario reconocible a través de múltiples canales de venta para aumentar su reputación y la confianza entre sus clientes.
- **Hacktivistas:** liberan información de forma gratuita pero debido a que no se logra generar una fuente de ingresos esta, se encuentra principalmente sustentada por ideales políticos o religiosos, donde el actor suele crear alias específicos para estas campañas con fin de evitar su seguimiento y/o rastreo.
- **Oportunismo:** también se podría catalogar como por gusto y/o hobbie, ya que son hallazgos que se realizan sin buscarlos de forma dedicada, sin embargo, llevar a cabo este tipo de actividades requiere gran constancia y cantidades de tiempo no remuneradas, por lo que suele estar ligada a actores que atacan vulnerabilidades críticas recientes, de fácil explotación, actores que tras mantenerse por grandes cantidades de tiempo en internet identifican vulnerabilidades en algún sitio o servicio web desde donde no dudan en extraer información.

Data Leak en Chile

Para el actual panorama de amenazas en Chile, se divide en diferentes puntos de análisis, pudiendo visualizar en primera instancia una comparativa anual de la cantidad de eventos ocurridos vinculados a organizaciones Chilenas para luego continuar con un desglose y descripción de los actores con mayor presencia durante 2023 junto a una breve descripción de sus actividades.

Comparativa anual

A continuación, se expone un gráfico en el que se detalla una comparativa de las exposiciones de datos realizadas en los años 2021, 2022 y en los primeros 9 meses de 2023.

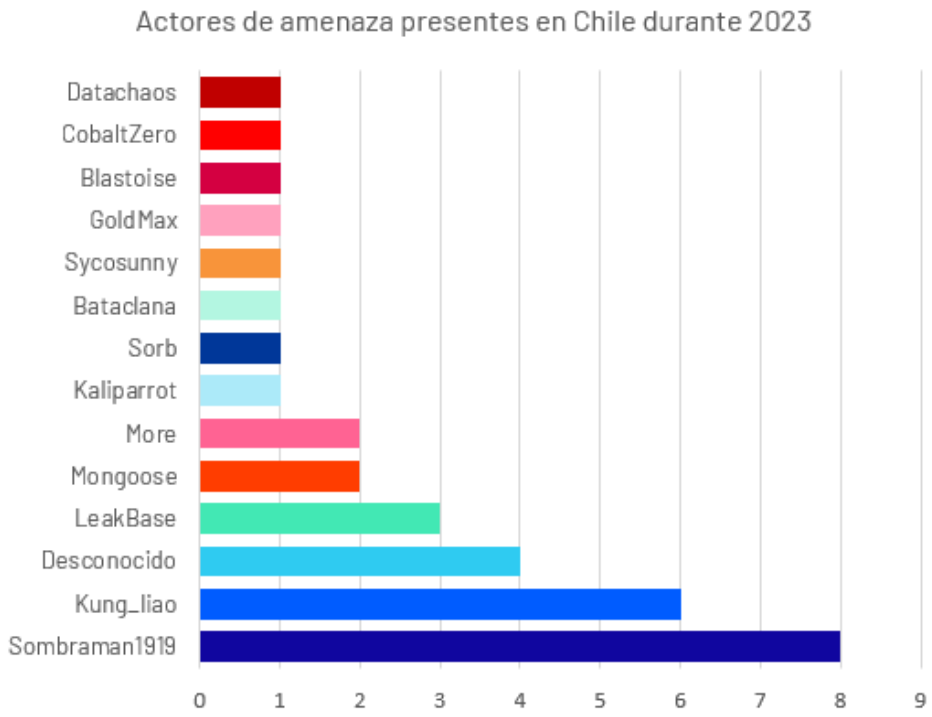


Del gráfico se puede apreciar que de 2021 a 2022 se produjo un incremento de un **69%** en la cantidad de eventos registrados, mientras que, por otra parte, en los 9 meses de transcurrido 2023 se aprecia un aumento del **22%** por sobre el total de eventos registrados durante 2022.

La actividad de actores de amenaza locales va en constante aumento y por consecuencia, es cada vez más común realizar este tipo de hallazgos en foros y mercados de Deep y Dark Web (DDW), principalmente por la familiaridad que tienen los atacantes con los sistemas comúnmente usados en Chile, el lenguaje utilizado y la brecha digital que va en constante disminución, permitiendo que cada vez exista mayor cantidad de profesionales y aficionados a la ciberseguridad con grandes conocimientos para llevar a cabo este tipo de actividades ilícitas con mayor sofisticación y en mayor volumen.

Data Leak en Chile 2023

Para el caso puntual de Chile, se identifican 33 eventos de filtraciones de datos, abarcados en 14 actores de amenaza diferentes, distribuidos de la siguiente forma:



A continuación, una breve descripción del TOP 3 de los actores de amenazas con mayor actividad en Chile durante el primer semestre de 2023, cabe destacar que para este TOP no se ha contabilizado a "Desconocido" ya que corresponden a alias no identificados tras una brecha de datos.

- **Ciberactor: Sombraman1919 [ONLINE]**
  - Cantidad de publicaciones realizadas:8 publicaciones
  - Motivaciones: Financiera
  - Actividad: 2012 - Actualidad
  - Alias: Se mantiene en el tiempo

Suele publicar muestras de sus bases de datos que posteriormente vende mediante su canal de Telegram, enfocado principalmente en compañías de telefonía móvil de LATAM.

- **Ciberactor: Kung_Liao [OFFLINE]**
    - Cantidad de publicaciones realizadas: 6
    - Motivaciones: Hacktivismo, Financiera
    - Actividad: Enero 2023 - Marzo 2023
    - Alias: Utilizado para campañas de corta duración.

Marcó tendencia a comienzo de año debido al ataque directo a instituciones nacionales de gobierno, su actividad fue breve, pero resultó ser de relevancia nacional.

- **Ciberactor: LeakBase [ONLINE]**
    - Cantidad de publicaciones realizadas : 3
    - Motivaciones: Demostración de capacidades, Financiera
    - Actividad: 2012 - Actualidad
    - Alias: Se mantiene en el tiempo

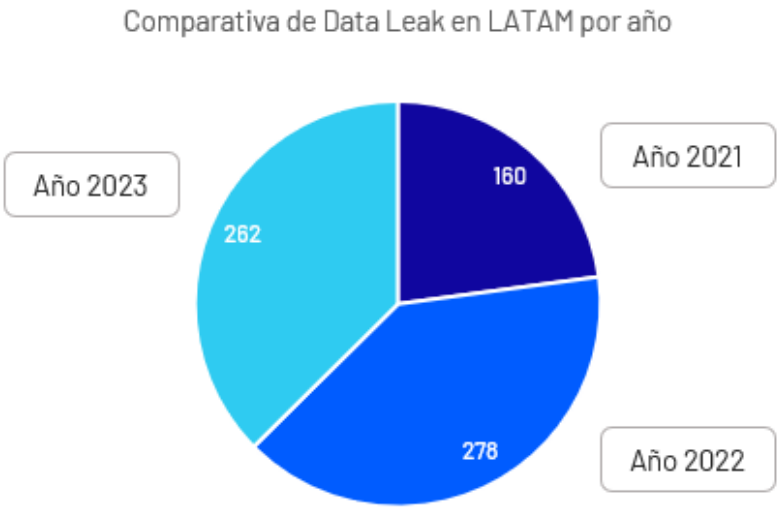
Activo hace gran cantidad de años, altamente reconocido en foros DDW y comparte información por su propio canal de Telegram e incluso mantiene su propio foro donde otros usuarios pueden compartir información.

Uno de los principales operadores de Chucky, quien también mantiene sus propios canales de difusión y una alta reputación.

Data Leak LATAM

Para el actual panorama de amenazas de LATAM, se divide en diferentes puntos de análisis, pudiendo visualizar en primera instancia una comparativa anual de la cantidad de eventos ocurridos vinculados a organizaciones de LATAM para luego continuar con un TOP de los actores con mayor presencia durante 2023.

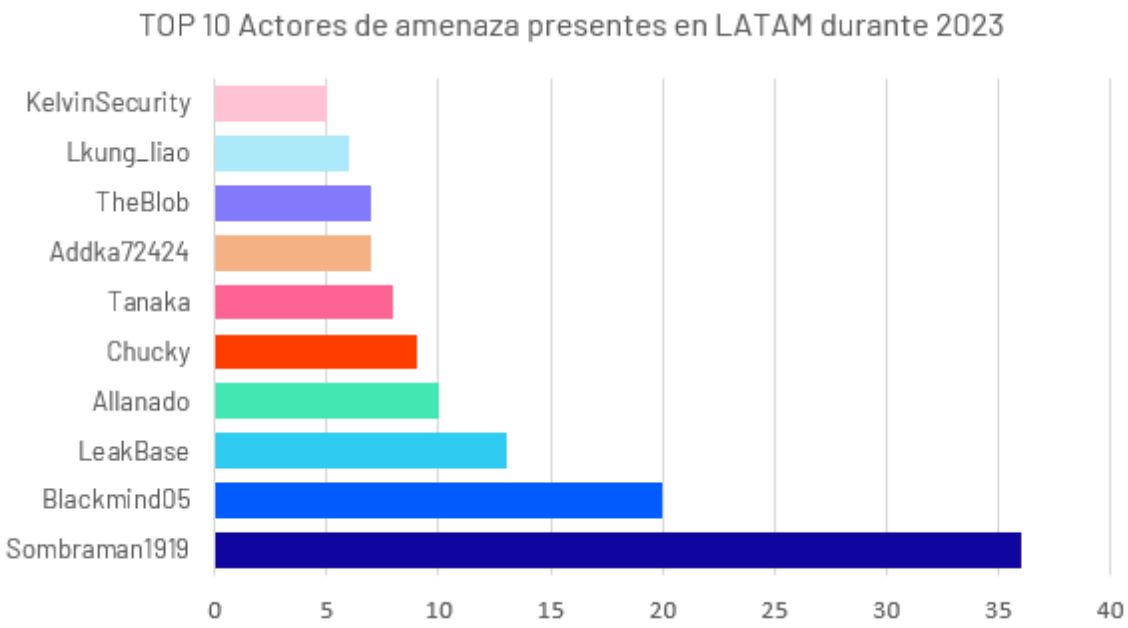
Comparativa anual



Del gráfico se puede apreciar que de 2021 a 2022 se produjo un incremento de un **73,7%** en la cantidad de eventos registrados, mientras que en los 9 meses de transcurrido 2023 ya se encuentra a un **94,9%** del alcanzar el total de eventos registrados durante 2022, por lo que se entiende que, al finalizar este periodo, podremos dimensionar la real brecha generada con este aumento, que, por consecuencia, aumenta las probabilidades de las organizaciones a ser afectadas.

Data Leak en LATAM 2023

Para el caso de LATAM (incluidos los 33 casos de Chile), se identifican 295 eventos de filtraciones de datos, abarcados en 119 actores de amenaza diferentes, distribuidos de la siguiente forma:



A continuación, una breve descripción del TOP 3 de los actores de amenazas con mayor actividad en LATAM durante el primer semestre de 2023 y dado que dos (sombraman y leakbase) de los 3 ya han sido presentados en el apartado de Chile, se describe el actor restante.

- **Ciberactor: Blackmind05 [ONLINE]**
  - Cantidad de publicaciones realizadas: 7
  - Motivaciones: Financiera
  - Actividad: 2012 - Actualidad
  - Alias: Se mantiene en el tiempo

Suele publicar muestras de sus bases de datos que posteriormente vende mediante su canal de Telegram, enfocado principalmente en la obtención de información personal de usuarios de bancos y de compañías de telefonía móvil de LATAM, presenta gran similitud con el actuar de Sombraman1919 y existen sospechas que trabajan de forma conjunta.

Países más afectados en LATAM 2023

En base al seguimiento realizado al panorama de Data Leak, es posible observar que los lugares donde existen más registros durante el primer semestre de 2023 corresponden a Brasil (99), México(77) y Chile (33), muy probablemente debido a la estabilidad de la moneda local y el desarrollo de la industria TI que cuenta con leyes y políticas tardías en la gran mayoría del territorio, lo que es conocido y muy bien utilizado por los actores de amenaza para proteger sus operaciones y así evitar seguimiento y/o sanciones legales.

Data Leak mundial

Noticias relevantes, nacionales e internacionales

Debido a la amplitud del panorama mundial, se extraen los hechos más relevantes ocurridos durante el año que han afectado a diferentes industrias, siendo principalmente afectados los servicios tecnológicos y de telecomunicaciones y en segunda medida, organizaciones vinculadas a entidades de gobierno.

Deep and Dark Web (DDW)

Take Down

Take Down [Dar de baja / Desmantelar]: Corresponde a cuando entidades de seguridad como policías u otro organismo, logra desbaratar una infraestructura tecnológica principalmente vinculada a mercados negros que se encuentran alojados algún sitio de internet, de esta forma en algunos casos se logra dar con la identidad real de los administradores para llevar a cabo su detención, mientras que en otras solo se logra capturar la administración del sitio, para su posterior peritaje que permita entregar antecedentes para identificar a otros involucrados y/o usuarios activos en ellas.

Entre algunos de los casos más relevantes se identifican a los siguientes foros y/o portales:

- Raid forums [Market y Hacking]
- Breached - Pompompurin (arrestado) [Market y Hacking]
- Exposed [Market y Hacking]
- Genesis market [Market y Hacking]

Data Leak a Foros/Market DDW

- **Data Leak [Fuga de datos]:** Corresponde a una fuga de datos mediante una exposición inadecuada de los mismos y accesible de forma pública, sin mediar un ciberataque para la obtención de la información y vinculado a errores de configuración y seguridad de los sistemas que alojan dicha data.
- **Data Breach [Brecha de datos]:** Corresponde a una fuga de datos por medio de un ciber ataque en donde se vulnera información confidencial mediante vulnerabilidades conocidas y/o desconocidas, lo que va a depender netamente de las capacidades del actor detrás del ataque.

Entre algunos de los casos más relevantes se identifican a los siguientes foros y/o portales:

- BidenCash [Carding]
- RaidForums [Market y Hacking]
- Breached [Market y Hacking]
- BreachForums [Market y Hacking]

Otros que, si bien son de menor relevancia, son constantemente vulnerados entre sus pares, principalmente con el objetivo de demostrar capacidades, desplazar a foros más pequeños y/o por rivalidades.

Todos es estos nombres recién mencionados, si bien pueden parecer desconocidos para muchos usuarios, corresponden a diferentes foros y portales de larga data y con gran reputación que han sido dados de baja durante el último año y que han servido para el intercambio, compra y venta tanto de conocimientos de hacking como de diferentes tipos de herramientas maliciosas, por mencionar algunas de la cosas que allí se transan, las cuales varían y pueden ser tanto de pago como entregadas de forma gratuita, convirtiéndose en un concentrador de todo tipo de intereses, principalmente ilegales, donde incluso actores de amenaza de renombre han ofrecido reclutar gente para sus operaciones.

Público

Empresa	Rubro
Dole	Alimentos
Pepsi	
City of Oakland	Entidades de Gobierno
City of Augusta	
New York City students	
Oregon (Moveit)	
Louisiana (Moveit)	
Manchester police officers	
Swedish Authority for Privacy Protection (IMY)	
Gobierno de Francia	
Colorado Department of Health Care Policy & Financing (HCPF)	
Colorado Department of Higher Education (CDHE)	
Colorado State University (CSU)	
Missouri's Department of Social Services	
UK Electoral Commission	
New York City Department of Education (NYC DOE)	
Google FI	Data Leaks a servicios o compañías de tecnología y telecomunicaciones
Verizon breaches	
I2VPN Leak en telegram	
T-Mobile (x2)	
AWS Lambda credentials	
Okta Data Leak	
Activision	
Free VPN Exposes records	
Razer	
Ubiquiti	
Western Digital	
Kodi	
MSI breach	
Dish Network	
Blackbaud	
AT&T	
Acer	
TELUS (canada telcom)	

Empresa	Rubro
Atlassian	
A10 Networks	
MailChimp	
NortonLifeLock	
Rackspace	
Razer	
Siemens Energy	
PharMerica	Salud y farmacia
major hospital in Seoul	
Brightline	
MCNA Dental	
HCA Healthcare	
Independent Living Systems (ILS)	
Mental health provider - Cerebral	
Community Health Systems (CHS)	
California medical group	
AmerisourceBergen	
Johnson & Johnson	
Capita	Finanzas y Criptofinanzas
Zacks Investment	
Coinbase	
Trezzor	
PayPal	
Credit Control Corporation (CCC)	Data Leak a industria bancaria e instituciones proveedoras de tarjetas
Data Leak ICICI Bank	
Data Leak Provider Deutcsche Bank	
Hatch Bank	
Deutsche Bank	
Dateleak airBaltic	Data Leak a aerolíneas
Air France / KLM	
American Airlines	
Southwest Airlines	
Scandinavian Airlines	
Volvo Data Leak	Data Leak a compañías automovilísticas
Honda	
Toyota	

Empresa	Rubro
Hyundai	
Ferrari	
Nissan North America	
Arnold Clark (Minorista más grande de Europa)	
Colorado State University	Data Leak a universidades
University data leak	
University of Manchester	
Open University of Cyprus	
Stanford University	
Sydney University	
Data Leak tiktok	Data Leak a RRSS
instagram	
yahoo	
Reddit	
Discord	
Caesars Entertainment	Entretención y retail
Forever 21	
Paramount	
Seiko	
Nickelodeon	
Apreciación	

Apreciación

De acuerdo a lo observado durante el presente documento, es posible evidenciar una constante alza en cuanto cantidad de Data Leak y nuevos actores de amenazas, generando de esta forma un fuerte interés en compañías tecnológicas, ya que la data allí capturada puede servirle a actores de amenazas para atacar también a los clientes de dicha organización, pudiendo expandir considerablemente la superficie de ataque y por tanto, las retribuciones monetarias, ya sea por la venta en mercados negros o por la extorsión hacia las víctimas.

Por otra parte, también se ha evidenciado un fuerte aumento de ataque a entidades de gobierno, siendo un caso memorable de esto, el ataque del grupo Guacamaya y que pese a que los eventos ocurrieron durante 2022, el impacto y relevancia ha golpeado fuertemente hasta el día de hoy a los afectados ya que en algunos casos de liberaron documentos que afectan la seguridad nacional y por consecuencia a todos los habitantes de dicho territorio, sentando precedentes para evitar que esto se vuelva a repetir.

Mientras que por el lado de los usuarios, es común que en las filtraciones de datos de todo tipo se involucren datos personales ya sea de colaboradores o clientes, conteniendo diferentes antecedentes como nombres completos, números de teléfono personales, direcciones, correos electrónicos, datos bancarios e inclusive fotos de documentos como carnet de identidad o pasaporte, que podrían dar pie incluso a la suplantación de identidad para llevar a cabo algún tipo de ataque a mayor escala como fraude, ataques BEC (Business Email Compromise) o convirtiendo a la persona afectada en un usuario VAP (Very Attacked People) lo cual tiene un impacto directo en su privacidad e inclusive podría llevarlo a problemas judiciales.

Con todos estos antecedentes es posible entender el gran interés de actores maliciosos por estos datos en un mundo donde la información digital es cada vez más valiosa tanto por su valor intrínseco o por su valor monetario, por lo cual año a año crece considerablemente tanto la gente con conocimientos de ciberseguridad como el interés de numerosos actores, donde todos tienen diferentes tácticas, técnicas, procedimientos y motivaciones, pero aun así todos convergen en un único objetivo, **extraer información sensible**, lo que se ha visto reflejado en gráficos de constante ascenso y que se espera continúen fuertemente en la misma dirección.

Acciones inmediatas:

- En el caso de identificar filtraciones es imperante tomar contacto con los usuarios identificados para gestionar la limpieza y eliminación del malware desde su equipo a la brevedad.
- En el caso de identificar filtraciones es imperante formatear el equipo afectado en su totalidad para eradicar la amenaza.
- Es importante conocer si el usuario afectado corresponde a un proveedor conocido y si cuenta con un equipo organizacional o con equipo propio para que cada uno según corresponda, actúe de acuerdo con sus protocolos de contención de amenazas.
- Las campañas de phishing se caracterizan por tener faltas de ortografía o errores en el diseño. Revisa el contenido con detención, y desconfía de correos con imperfecciones.

- Desconfía de los correos alarmantes. Si un mensaje le indica o incentiva a tomar decisiones apresuradas o en un tiempo limitado, probablemente se trata de phishing.
- Ingresa a los sitios oficiales de la institución a la que estás afiliado, realiza todos tus trámites desde allí, es más seguro que utilizar algún enlace en el correo, WhatsApp o SMS.
- No haga clic en ningún enlace ni descargue ningún archivo en un correo electrónico si no puede verificar la fuente de forma independiente. E incluso si el correo electrónico proviene de una fuente de confianza, verifique con ellos si realmente lo enviaron.
- No responda a correos electrónicos no solicitados de extraños y especialmente si le piden que proporcione algún tipo de información personal.
- Escanear todos los archivos adjuntos, antes de abrirlos, con un antivirus que detecte comportamientos para combatir los ransomwares.
- Actualizar los equipos con Windows a las últimas versiones.
- Nunca seguir la instrucción de deshabilitar las funciones de seguridad, si un correo electrónico o documento lo solicita.
- Disponer de sistemas antispam para correos electrónicos, de esta manera se reducen las posibilidades de infección a través de campañas masivas de malspam por correo electrónico.
- Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 "Concienciación con educación y capacitación en seguridad de la información" o NIST PR.AT-1: "Todos los usuarios se encuentran entrenados e informados", a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas, haciendo énfasis en cómo proceder al recibir correos de orígenes desconocidos, objeto prevenir que sus usuarios sean víctimas de entes maliciosos.


digital