CERT.ar

INCIDENTES INFORMÁTICOS

Informe Anual de Incidentes de Seguridad registrados en el 2023 por el equipo de respuesta ante Emergencias Informáticas Nacional.

Dirección Nacional de Ciberseguridad

Secretaría de Innovación, Ciencia y Tecnología
Jefatura de Gabinete de Ministros

Subsecretaría de Tecnologías de la Información

CERT.ar

Indice

1. Introducción 2

2. Incidentes informáticos registrados en el 2023 3

3. Nivel de severidad utilizado 5

4. Conclusión 6

5. Algunos datos del informe representados en gráficos 7

6. Glosario 11

Introducción

El Equipo de Respuesta ante Emergencias Informáticas nacional (CERT.ar) de la Dirección Nacional de Ciberseguridad registró 379 incidentes de seguridad informática durante el año 2023. Si bien la cifra representa un ligero aumento del 13% en comparación con el 2022, cuando se detectaron 335, es significativamente menor a los 591 casos del 2021.

Esta disminución puede atribuirse a una mayor conciencia y preparación de las entidades frente a las amenazas cibernéticas, así como a las medidas de seguridad implementadas. Este informe tiene como objetivo proporcionar una visión integral de las amenazas cibernéticas que han afectado a los sistemas y redes del Sector Público Nacional, así como destacar las tendencias y cambios significativos en comparación con los años anteriores.

Los reportes recibidos proceden de fuentes externas y de la información ingresada a través de los canales de comunicación del CERT.ar, es decir, a través del formulario de la página web **https://argentina.gob.ar/cert-ar**, y del mail **reportes@cert.ar**.

Continuando la tendencia del año anterior, el phishing sigue siendo la principal amenaza, representando el 75% de los incidentes reportados en el 2023. Respecto a su accionar, se observa una evolución en las técnicas empleadas y ataques más sofisticados a través de las redes sociales. Y para mitigar este tipo de amenaza, la concientización y educación en materia de seguridad cibernética se destacan como áreas clave.

En cuanto a los sectores más afectados, se evidenció que el de Finanzas y el del Estado[1] continúan siendo los blancos de ciberataques más elegidos, manteniendo de esta forma la tendencia observada en el 2022.

Este hecho subraya la importancia de fortalecer las medidas de seguridad en estas áreas específicas y de seguir implementando estrategias proactivas para garantizar la integridad de los sistemas y la protección de la información sensible.

Por otra parte, se menciona que, durante el transcurso del año 2023, el CERT.ar ha continuado desempeñando un papel crucial en la prevención, protección y resiliencia frente a posibles ciberataques. Se ha mantenido la colaboración con equipos CERT y CSIRT a nivel federal e internacional, compartiendo información relevante, indicadores de compromisos y protocolos de acción. Se trabajó de esa forma porque el Equipo considera que la cooperación global es siempre esencial para anticipar y mitigar amenazas en un entorno digital cada vez más complejo.

[1] A la categorización del sector Estado lo conforman oficinas de gobierno federales, provinciales o municipales que brindan a la ciudadanía diferentes trámites.

Asimismo, se destaca que este año el CERT.ar elaboró junto a la Dirección Nacional de Ciberseguridad una guía para notificar y gestionar incidentes, que pudieran afectar a los organismos estatales, a los diferentes CERTs de la Administración Pública Nacional y a todos aquellos que operen en el territorio argentino[2].

Por último, el CERT.ar reitera la importancia de la colaboración entre organismos gubernamentales, sectores privados y ciudadanos para fortalecer la ciberseguridad a nivel nacional. La detección temprana, la respuesta rápida y la mejora continua de las prácticas de seguridad son fundamentales para enfrentar las crecientes amenazas cibernéticas en un entorno digital que está en constante evolución.

Incidentes informáticos registrados en el 2023

Durante el período comprendido entre el 1 de enero y el 31 de diciembre de 2023, el CERT.ar registró en su plataforma de administración un total de 379 incidentes informáticos, cifra que aumentó en un 13% respecto a la del 2022, cuando se registraron 335.

La fuente de información o herramienta de comunicación más utilizada para realizar estos reportes fue el correo electrónico con 295 casos recibidos y validados. La segunda, con 64 hechos comunicados, fue por los diversos feeds -es decir, repositorios de información específica de distintos canales- en los cuales el CERT.ar participa. La tercera fue por medio del formulario web, donde se registraron 14 incidentes. Y, por último, 6 fueron reportados por otro medio de recepción, que no abarca ninguno de los 3 nombrados anteriormente. De los 379 casos, 12 se encuentran abiertos, es decir, que aún se está trabajando en los mismos, o se está esperando alguna respuesta de las entidades involucradas para cerrarlo, según el protocolo de procedimiento. Los 367 restantes están cerrados.

De acuerdo con la taxonomía utilizada por el CERT.ar, la totalidad de los incidentes registrados se divide en la siguiente categorización:

- Fraude: **288**
- Compromiso de la información: **60**
- Contenido abusivo: **8**
- Intrusión: **8**
- Contenido dañino: **6**
- Disponibilidad: **4**
- Vulnerable: **4**
- Obtención de información: **1**
- Otros: **0**

[2] https://www.boletinoficial.gob.ar/detalleAviso/primera/289746/20230706

Los casos de fraude, con 288 incidencias, representan el 76% del total de incidentes reportados, denotando que esta tipología fue el delito informático que más se registró durante el período mencionado.

Entre los tipos detectados, se incluyeron uso no autorizado de los recursos, derechos de autor, suplantación de identidad y phishing.

Y a los efectos de la administración de incidentes, se consideraron doce sectores denominados Alimentación, Estado, Energía, Finanzas, Hídrico, Nuclear, Químico, Salud, Espacio, Tecnologías de la Información y las Comunicaciones (TICs) y Transportes, y Otros.
Haciendo un análisis anual, el sector más comprometido de acuerdo con los incidentes reportados fue el de Finanzas con 117 casos, cifra que representa el 31% del total registrado.

El segundo sector más afectado fue el del Estado con 84 incidentes (22%), mientras que el sector denominado Transportes se ubica en el tercer lugar con 66 incidentes (17%).
Como se podrá observar, los sectores Finanzas y Estado superan el 50% de los incidentes anuales reportados (53%), a diferencia de los años anteriores que superaban el 70%.

Tipos de incidentes reportados en el sector Finanzas (117)

- **Phishing**: **117** incidentes, cifra que representa el 100% del total de los casos del sector Finanzas.

Tipos de incidentes más reportados en el sector del Estado (84)

- Modificación no autorizada de la información: **26** (31%)
- **Phishing**: **35** (42%).

Entre ambos acaparan más del 70% de los incidentes en el Estado.

Tipos de incidentes reportados en el sector Transportes (66)

- **Phishing**: **64** incidentes, cifra que representa el 97% del total de los casos del sector Transportes.
- Configuración errónea: **2** (3%)

Continuando con el detalle anual por sector, Otros, con 46 reportes, se ubica en el cuarto lugar, seguido por el sector de las Tecnologías de la Información y las Comunicaciones (TICs) con 31 incidentes. En tanto, el sector Salud tuvo 29 reportes, cifra que lo posiciona en el sexto lugar. Los sectores Alimentación y Energía registraron 3 incidentes cada uno, siendo los menos afectados. Se puede observar a nivel general que los incidentes estuvieron más repartidos en comparación a los años anteriores.

Al realizar una discriminación por tipo de incidente informático, el phishing fue el más registrado con 286 casos, cifra que representa el 75,5% del total reportado.

La modificación no autorizada de información se ubica en el segundo lugar con 50 incidentes reportados (13,2%), mientras que el acceso no autorizado a la información se posiciona en el tercero con 10 casos, dato que significa el 2,6% de la totalidad. El resto, es decir los 33 faltantes, representan el 8,7% de los tipos de incidentes y se dividen en forma decreciente entre:

- SPAM: **8** (2,12%)
- Compromiso de equipo/sistema: **6** (1,58%)
- Malware: **6** (1,58%)
- Configuración errónea: **3** (0,79%)
- Sistema vulnerable: **3** (0,79%)
- Compromiso de cuenta: **2** (0,53%)
- Suplantación: **2** (0,53%)
- Denegación de Servicio: **1** (0,26%)
- Escaneo de redes/análisis de tráfico: **1** (0,26%)
- Revelación de información: **1** (0,26%)

Nivel de severidad utilizado

Los criterios del nivel de severidad de un incidente están regidos por el tipo de incidente y la criticidad del recurso afectado. En tanto, el impacto del incidente se evalúa según el daño potencial y/o real adverso causado sobre las infraestructuras tecnológicas, los sistemas de información y la información que gestionan. También se tienen en cuenta los tiempos máximos aceptables para la gestión del incidente.

Y según el impacto que cause el incidente, se consideraron cuatro niveles de severidad, que son denominados como bajo, medio, alto y crítico.

Durante el período analizado, es decir el año 2023, 341 de los incidentes reportados (89,97%) fueron de severidad alta, seguidos de 18 de severidad crítica (4,75%), 17 de severidad media (4,49%) y 3 de severidad baja (0,79%).

Conclusión

Como se mencionó en la introducción del informe, al hacer una comparativa entre los últimos dos años, se puede observar un ligero aumento del 13% en la cantidad de incidentes reportados en 2023 en comparación con el año anterior. Esta pequeña variación puede atribuirse a una mayor conciencia y preparación -respaldada por medidas de seguridad implementadas- de las entidades frente a las amenazas cibernéticas.

Con respecto a la principal amenaza, se pudo observar que el phishing ocupó el primer lugar, representando el 75% de los incidentes reportados en 2023. Por tal motivo, la concientización y educación en seguridad cibernética se consideran críticas para mitigar este tipo de técnica de ataque. Los sectores Finanzas y Estado siguen siendo los más afectados, manteniendo la tendencia del año anterior. Este hecho destaca la necesidad de fortalecer las medidas de seguridad en estas áreas específicas y de implementar estrategias proactivas para garantizar la integridad de los sistemas y la protección de la información sensible.

Asimismo, se destaca que la implementación de normativas como la Decisión Administrativa 641/2021 y la Disposición 7/2021 han contribuido significativamente a la reducción de incidentes. Estas medidas han elevado los niveles de seguridad de la información en organismos estatales y han facilitado la detección temprana mediante la creación de puntos focales de ciberseguridad.

También se puede mencionar el esfuerzo de concientización realizado a través de cursos y charlas técnicas que brindó el equipo del CERT.ar -junto a la Dirección Nacional de Ciberseguridad- como otro factor que contribuyó a que la cifra de incidentes no creciera tanto. Estas últimas fueron dictadas para los Puntos Focales de Ciberseguridad[3], de marzo a noviembre, con el fin de reforzar conceptos vinculados a la seguridad de la información.

El objetivo de los encuentros online fue transmitir conocimiento y que además se compartan y debatan experiencias de gestión de incidentes para un bien común, ya que estos suelen ser cada vez más sofisticados.

Debido al daño que pueden causar actualmente los ciberataques, se espera que en el corto plazo la ciberseguridad se constituya en una de las prioridades de la agenda de trabajo de los organismos estatales y de las organizaciones en general. En ese sentido, el CERT.ar se pone a disposición de su comunidad objetivo para contribuir al logro de esa meta, ya que se necesita estar preparado lo mejor posible para enfrentar los desafíos de ciberseguridad, una disciplina en constante evolución.

[3] Un punto focal de ciberseguridad es un empleado de un organismo público que debe reportar a la Dirección Nacional de Ciberseguridad los incidentes de seguridad que se produzcan en su ámbito laboral.

Algunos datos del informe representados en gráficos

Distribución de los incidentes de acuerdo con las categorías establecidas

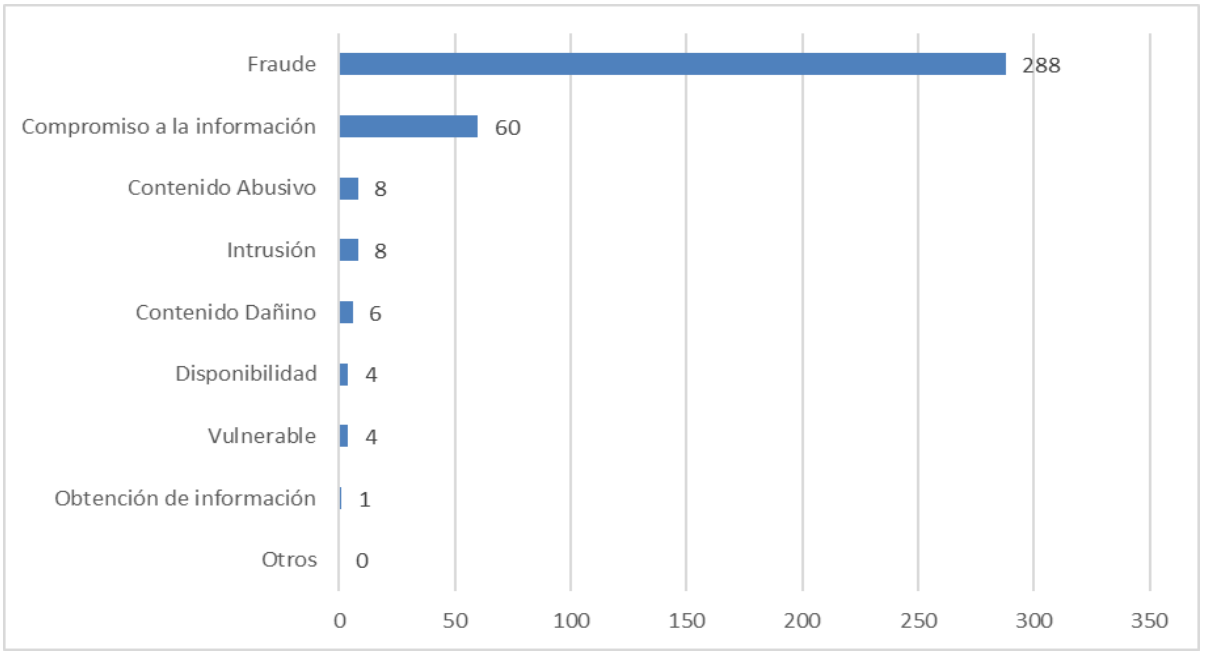

Gráfico 1

Distribución anual de incidentes por sector

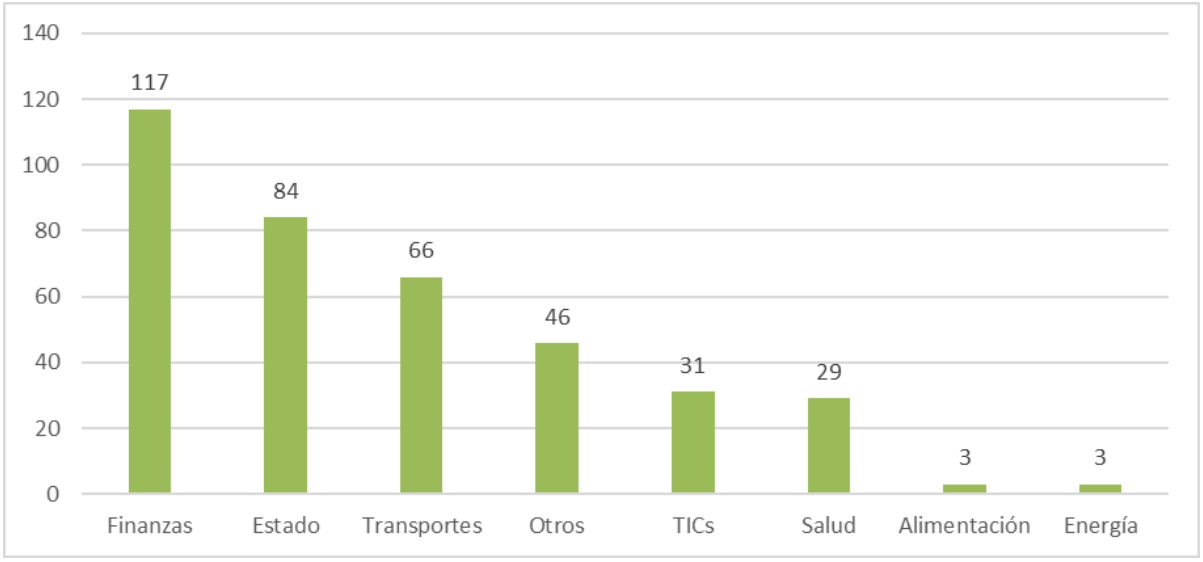

Gráfico 2

Representación de los incidentes según el nivel de severidad

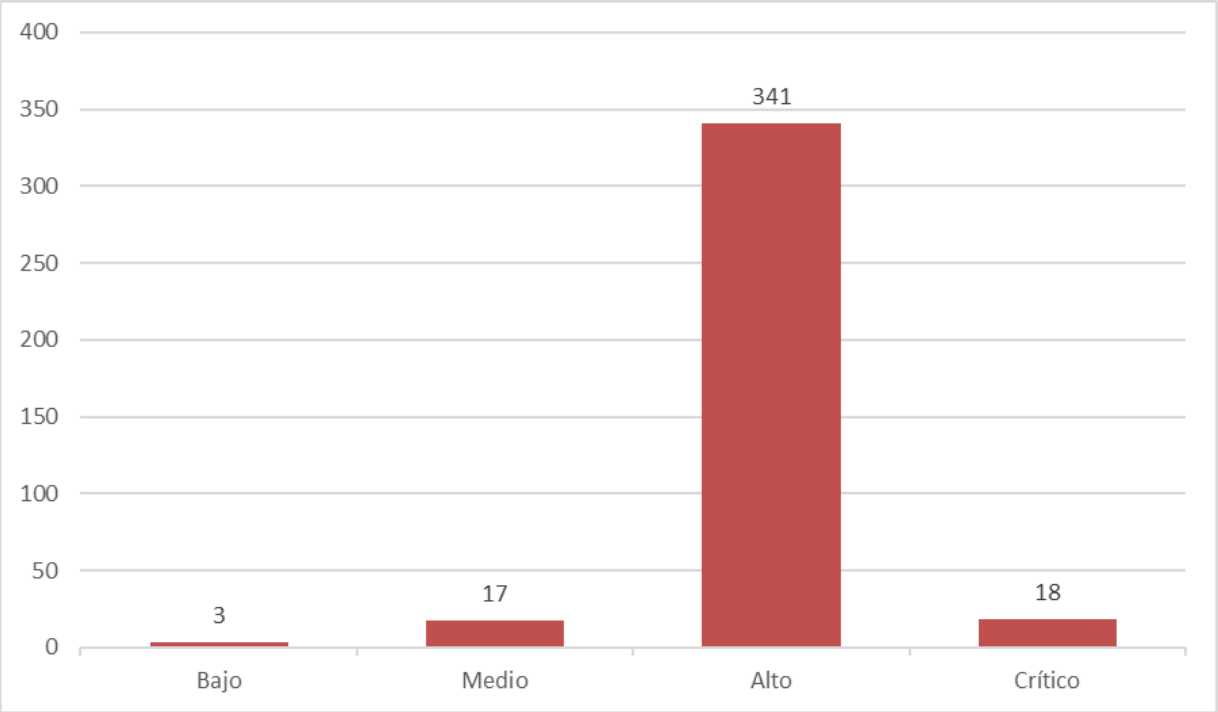

Gráfico 3

Distribución anual por tipo de incidente

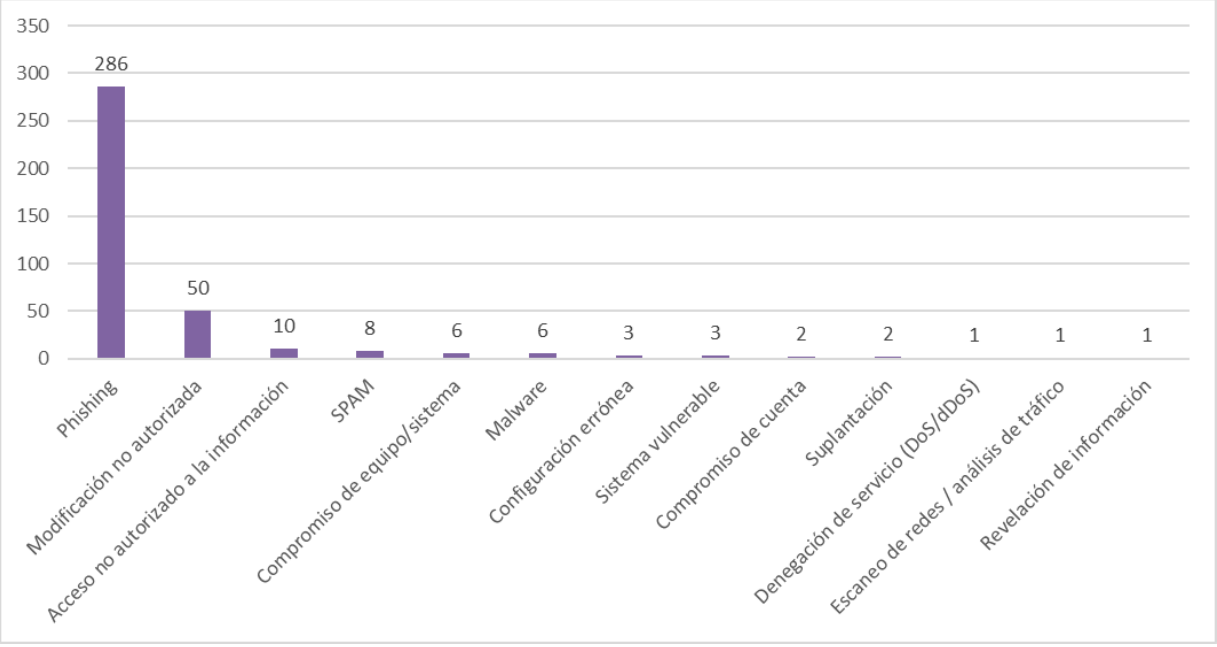

Gráfico 4

Comparativa de incidentes más reportados durante el 2023

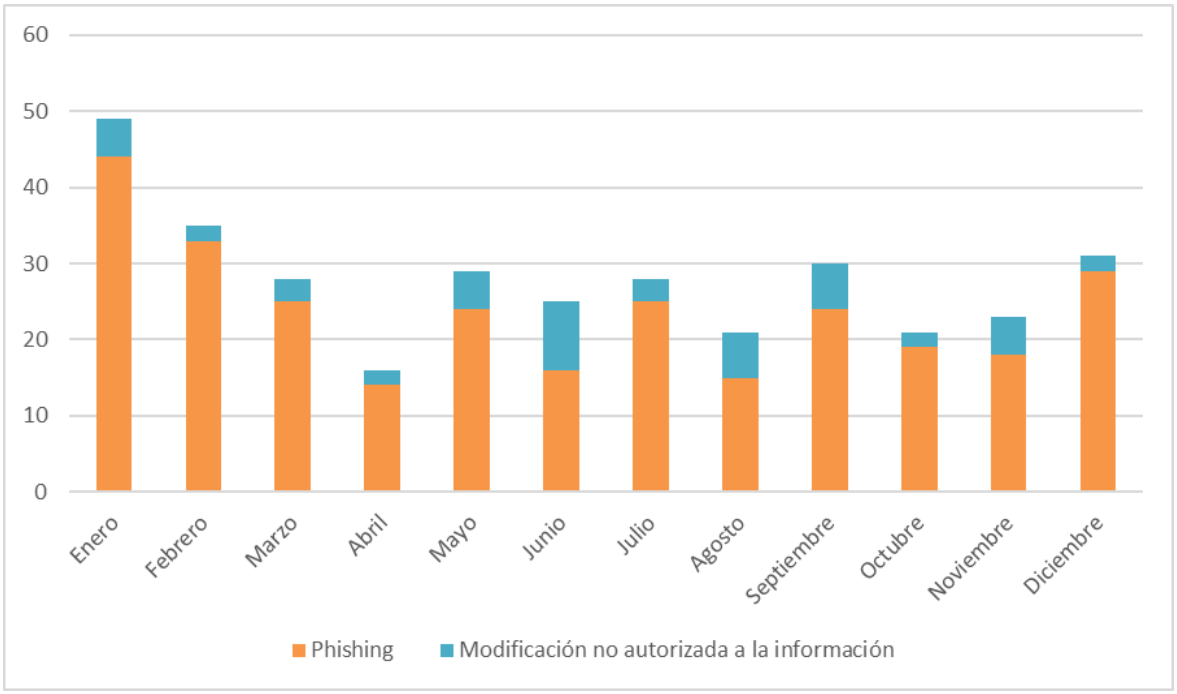

Gráfico 5

Distribución de incidentes reportados en el Estado

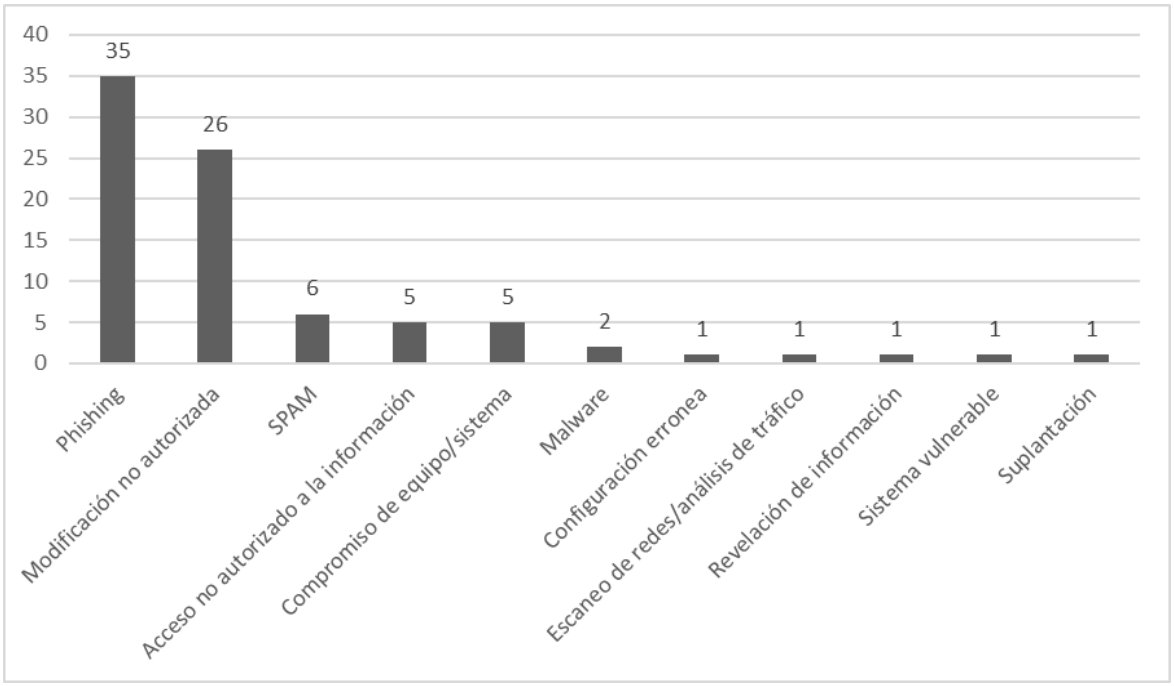

Gráfico 6

Representación de los incidentes según la fuente de información

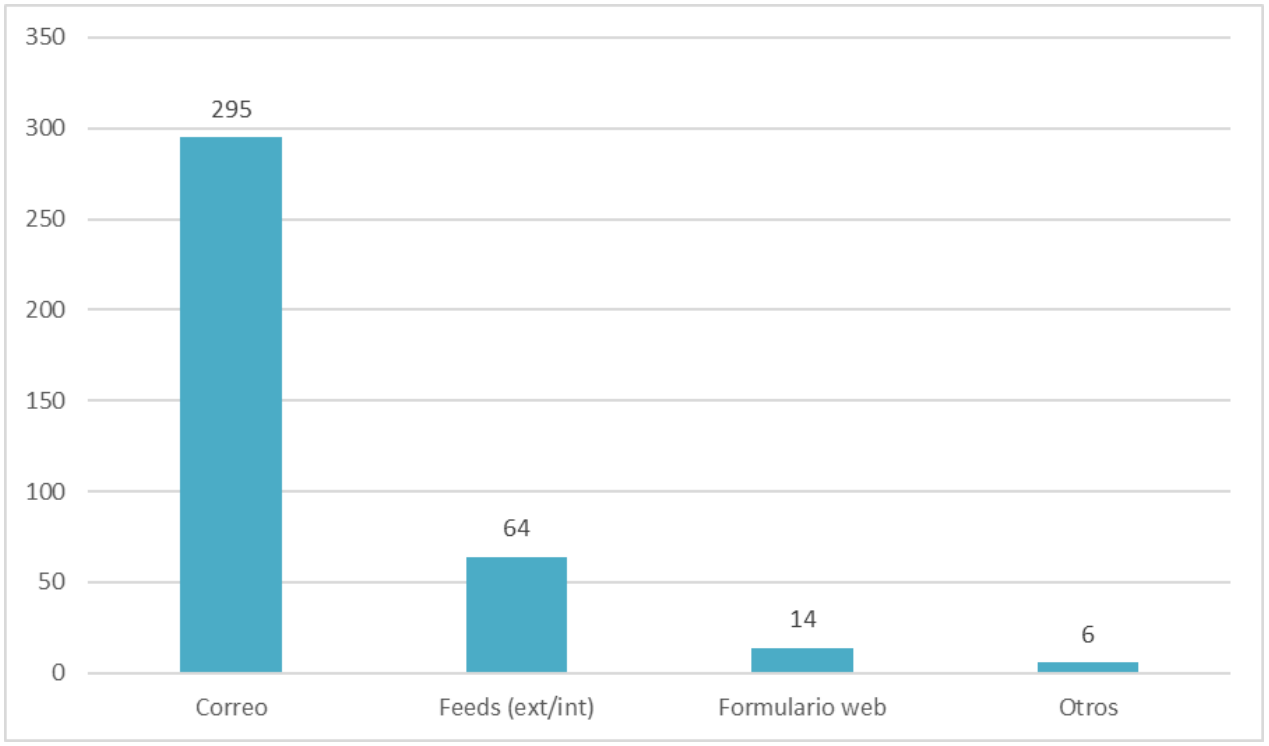

Gráfico 7

Glosario

CERT.ar: Equipo de Respuesta ante Emergencias Informáticas nacional de la Dirección Nacional de Ciberseguridad de Argentina.

Incidente de seguridad informática: cualquier suceso que pueda comprometer la seguridad de un sistema informático, sus datos o su infraestructura.

Phishing: técnica de ingeniería social que se utiliza para engañar a las víctimas para que revelen información confidencial, como contraseñas o números de tarjetas de crédito.

Fraude: delito informático que se comete con el propósito de obtener un beneficio económico o patrimonial indebido.

Modificación no autorizada de la información: ataques por ransomware, modificación de archivos, SQL, etc.

SPAM: correo electrónico masivo no solicitado.

Compromiso de la información: situación en la que se accede a información confidencial sin autorización.

Contenido abusivo: información que puede causar daño a las personas, como imágenes o videos de violencia o pornografía infantil.

Intrusión: acceso no autorizado a un sistema informático.

Contenido dañino: software malicioso o información que puede causar daños a los sistemas informáticos.

Vulnerable: sistema informático que tiene una o más vulnerabilidades que pueden ser explotadas por los atacantes.

Obtención de información: acción de recopilar información confidencial sin autorización.

Disponibilidad: capacidad de un sistema informático para estar disponible para su uso.

Severidad: nivel de daño potencial causado por un incidente de seguridad informática.

Decisión Administrativa 641/2021: norma que establece los Requisitos Mínimos de Seguridad de la Información para los organismos del Sector Público Nacional.

Disposición 7/2021: norma que instruye la creación del registro de Puntos Focales de Ciberseguridad.


JEFATURA DE GABINETE
REPÚBLICA ARGENTINA