Dirección Nacional
de Ciberseguridad

Incidentes Informáticos

Informe anual de incidentes de seguridad informática registrados en el **2022** por el **CERT.ar**

Argentina unida

Jefatura de Gabinete de Ministros
Argentina

Secretaría de Innovación Pública

Febrero 2023

CERT.ar

Introducción

El Equipo de Respuesta ante Emergencias Informáticas nacional (CERT.ar) de la Dirección Nacional de Ciberseguridad realiza tareas vinculadas con posibles ciberataques, que puedan afectar los sistemas y redes del Sector Público Nacional, para brindar mejoras en materia de prevención, protección y resiliencia. Además hace el seguimiento y la evolución de los hechos detectados o reportados con el fin de brindar asistencia técnica y administrativa.

Asimismo trabaja con diversos equipos CERT y CSIRT -que operan a nivel federal e internacional- en aspectos claves como las alertas tempranas, y comparte con ellos casos conocidos, indicadores de compromisos y protocolos de acción ante incidentes de seguridad.

Una de las funciones que tiene a su cargo el CERT.ar, es la de llevar un registro de estadísticas y métricas a nivel nacional. Por ese motivo, el Equipo realizó este informe sobre los incidentes de seguridad informática registrados en el 2022.

En ese sentido, se explica que este documento tiene como objetivo analizar y describir los 335 incidentes que fueron reportados al CERT.ar durante el año mencionado. El dato representa una disminución de casos del 46% en relación al 2021, cuando hubo un total de 591 incidentes registrados. En ese período anterior, la población mundial estaba conviviendo con el segundo año de la pandemia del Covid-19, una situación sanitaria que profundizó la modalidad del trabajo remoto y el acceso a herramientas digitales de usuarios que -en algunos casos- no poseían la instrucción tecnológica necesaria. Tal escenario favoreció a la perpetración de ciberdelitos en tanto generó un crecimiento de la superficie de ataques al haber más dispositivos conectados a Internet.

Los reportes recibidos de este nuevo informe 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.

Durante el transcurso del año, se pudo ver que continuó la migración hacia las plataformas digitales por parte de organismos estatales, industrias y usuarios particulares, como sucedió en los dos años anteriores.

Se registró una mayor cantidad de ataques orientados a organismos públicos, mientras que se produjo una disminución en la cantidad de casos sucedidos contra usuarios particulares y entidades privadas.

De la información obtenida, se observa que el phishing -mediante sus distintos vectores de ataque- representa el 72,2% de los incidentes reportados durante el año 2022, afectando a diversos organismos de la Administración Pública Nacional.

Los análisis han mostrado que se utilizaron diversas técnicas -como el phishing dirigido- que fueron implementadas en redes sociales y en campañas de creación masiva de dominios (Spam), donde se informa que la cuenta está comprometida y que necesita responder de inmediato haciendo clic en el enlace proporcionado, entre otros casos prácticos muy sofisticados para lograr convencer a la víctima.

Con respecto a los sectores definidos más afectados por diversos incidentes, el sector Finanzas y el sector Estado fueron los más comprometidos, al igual que sucedió en el 2021. Por tal motivo, se puede decir que ambos sectores continúan con la tendencia de ataques vista en el 2021.

Incidentes informáticos registrados en el 2022

Durante el período comprendido entre el 1 de enero y el 31 de diciembre del 2022, el CERT.ar registró en su plataforma de administración un total de 335 incidentes informáticos, cifra que representa un 43,3% menos de casos comparados con los del 2021, cuando se registraron 591.

La fuente de información o herramienta de comunicación más utilizada para realizar estos reportes fue el correo electrónico con 232 casos validados recibidos. La segunda, con 76 hechos comunicados, fue por los diversos feed -es decir, repositorios de información específica de diversos canales- en los cuales el CERT.ar participa. La tercera fue por medio del formulario web, donde se registraron 27 incidentes validados.

Del total de casos, hasta el 31 de diciembre del 2022, 323 fueron resueltos. Los 12 restantes continúan abiertos en dicho período ya que se encuentran en proceso de análisis o a la espera de alguna respuesta por parte de las entidades involucradas, según el protocolo de procedimiento establecido.

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

- **Indicio de fraude: 244**
- **Compromiso de la información: 63**
- **Contenido abusivo: 14**
- **Contenido dañino: 4**
- **Intrusión no autorizada: 3**
- **Disponibilidad[1]: 3**
- **Vulnerable: 3**
- **Otros: 1**

El indicio de fraude, con 244 casos, representa el 72,8% del total de incidentes reportados, siendo así el incidente informático más registrado durante el período mencionado. Entre los tipos detectados como indicio de fraude, se incluyeron el uso no autorizado de los recursos, suplantación de identidad y phishing.

A los efectos de la administración de incidentes, se tomaron en consideración siete sectores que son; Finanzas, Estado, Salud, Sectores no críticos, Transportes, Espacio, y el de las Tecnologías de la Información y las Comunicaciones (TIC).

Haciendo un análisis anual de los mismos, el sector más comprometido de acuerdo con los incidentes reportados fue el de *Finanzas* con 185 incidentes, cifra que representa el 55,2% del total registrado.

[1] Cuando un sistema o la información que contiene no son accesibles.

El segundo sector más afectado fue el de *Estado* con 71 incidentes (21,2%), mientras que el sector denominado *Sectores no críticos* se ubica en el tercer lugar con 33 incidentes (9,8%).

Como se puede observar, los sectores *Finanzas* y *Estado* -con 256 casos sumados entre ambos- superan el 70% de los incidentes anuales reportados (76,4%), al igual que en el año 2021, cuando hubo 449 casos (76%).

Tipos de incidentes más reportados en el sector del Estado	• **Modificación no autorizada de la información:** 39 incidentes, cifra que representa el 54,9% del total de los casos estatales. (En el 2021 también fue el más reportado con el 33,62%) • **Phishing:** 13 (18,3%). • **SPAM:** 6 (8,4%).

Tipos de incidentes más reportados en el sector de Finanzas	• **Phishing:** 182 incidentes, cifra que representa el 98,38% del total de los casos del sector Finanzas. (Mismo porcentaje que el año pasado). • **Denegación de servicios (DDoS/DoS):** 1 (0,54%) • **Acceso no autorizado a la información:** 1 (0,54%) • **Compromiso de equipo/sistema:** 1 (0,54%)

Continuando con el detalle anual por sector, *Salud* se ubica en el cuarto lugar con 27 reportes, seguido por el sector de *Transportes* que se posicionó en el quinto lugar con 10 incidentes. El sector de las *Tecnologías de la Información y las Comunicaciones (TIC)* se ubicó en el sexto lugar con 5 incidentes, mientras que los sectores *Alimentación* y *Energía* se posicionaron en el séptimo y último lugar al ser los menos afectados con 2 incidentes cada uno.

Al realizar una discriminación por tipo de incidente, el phishing fue el más registrado con 242 casos, cifra que representa el 72,23% del total reportado. La modificación no autorizada de información se ubica en el segundo lugar con 59 incidentes reportados (17,61%), mientras que el SPAM (comunicación masiva no solicitada) se ubica en el tercero con 14 casos, dato que significa el 4,18% de la totalidad. El resto, es decir el 5,98% de los tipos de incidentes, se divide en forma decreciente entre:

- Malware: 4 (1,19%)

- Acceso no autorizado a la información: 4 (1,19%)
- Compromiso de equipo/sistema: 3 (0,9%)
- Suplantación de identidad: 2 (0,6%)
- Configuración errónea: 2 (0,6%)
- Denegación de Servicio: 1 (0,3%)
- Otros: 1 (0,3%)
- Publicación de servicios vulnerables: 1 (0,3%)
- Sistema vulnerable: 1 (0,3%)
- Revelación de información: 1 (0,3%)

Nivel de severidad utilizado

Los criterios del nivel de severidad de un incidente están definidos 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-, la criticidad está relacionada con los activos de información afectados, la relevancia dentro de la continuidad del negocio y la operación de los sectores y organismos.

Además 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, 305 de los incidentes reportados (91,04%) fueron de severidad alta, 18 de severidad media (5,37%), 11 de severidad crítica (3,28%) y 1 de severidad baja (0,31%).

Conclusión

Al hacer una comparativa entre los últimos dos años, se puede observar una baja del 43,3% en los incidentes reportados, ya que en el 2021 se registraron 591 y en el 2022, 335. Tal situación pudo haber sucedido porque diferentes sectores de la sociedad volvieron al trabajo presencial, donde las infraestructuras internas tienen un mayor grado de control y administración centralizada que los accesos remotos y activos de información conectados y utilizados desde redes hogareñas.

Por otro lado, dicha baja se encuentra relacionada con diversos factores asociados a los aprendizajes y capacitaciones brindadas a lo largo del año para prevenir incidentes de seguridad informática, dentro de la estrategia de digitalización, protección e innovación del Estado. Dentro de este marco, se menciona la implementación de algunas normativas de la Dirección Nacional de Ciberseguridad de la Subsecretaría de Tecnologías de la Información.

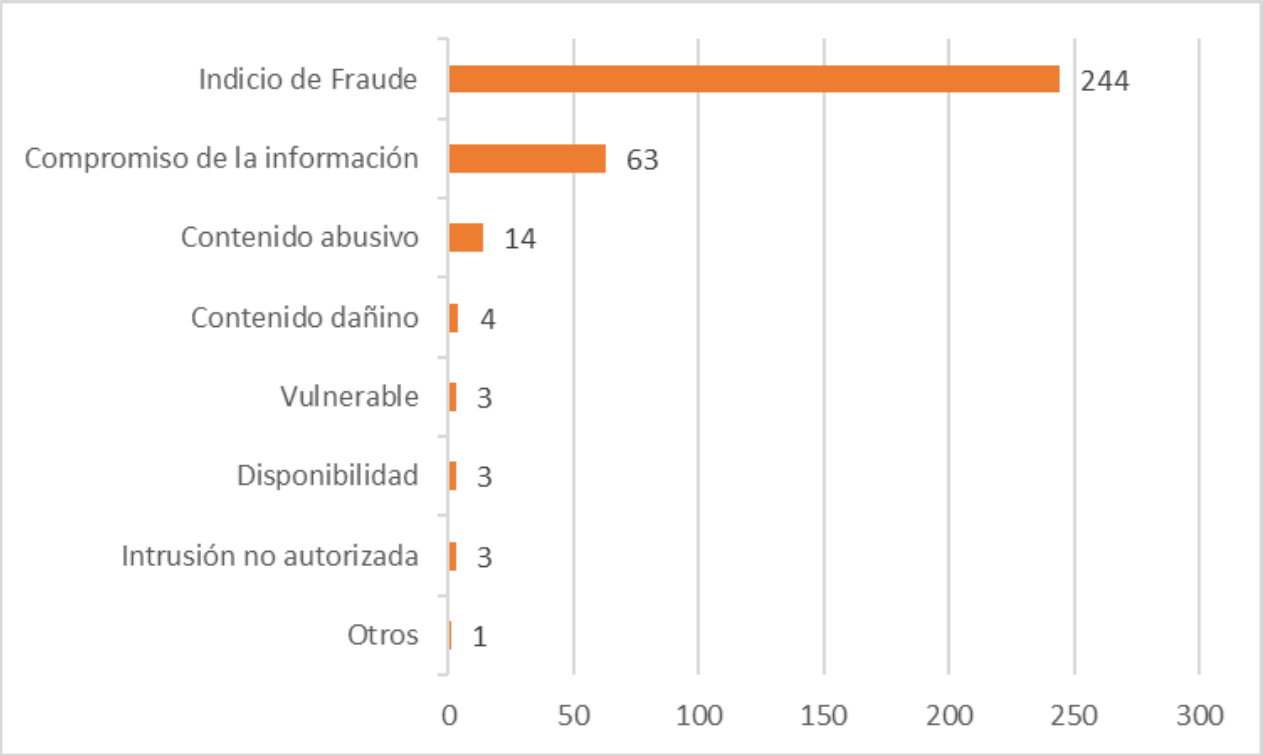
Por ejemplo la Decisión Administrativa 641/2021 -y sus complementarias- fue creada para elevar los niveles de seguridad de la información de los organismos del Sector Público Nacional, los principales receptores y productores de datos del país, donde las tareas realizadas en dicho periodo han evolucionado múltiples factores de protección, demostrado en los avances prácticos de la misma.

Cabe destacar que en comparación al 2021 se duplicaron los reportes en el formulario web, factor relacionado a las divulgaciones continuas en los otros canales utilizados por el CERT.ar para lograr una mayor agilidad en los reportes y las respuestas..

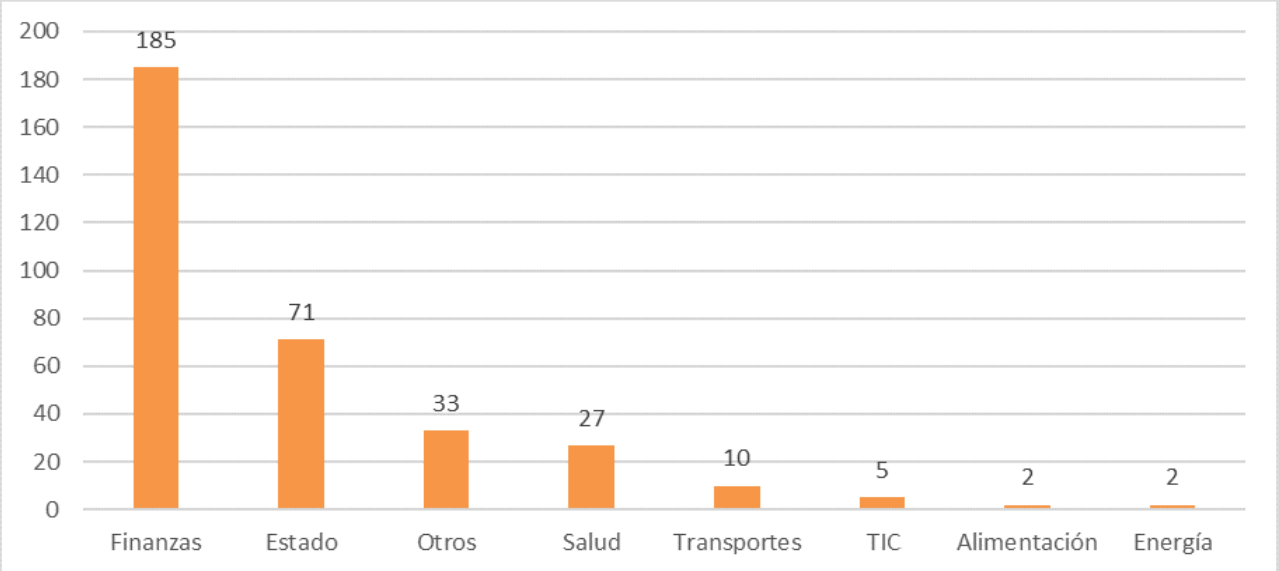
De todas maneras, si bien se redujo la cantidad de incidentes reportados, hubo un incremento en los incidentes considerados críticos, como por ejemplo los dirigidos a los Ministerios, que al ser entidades públicas, tuvieron gran visibilidad. De los datos relevados en el sector privado nos encontramos con una situación similar al verse disminuidos los incidentes reportados por phishing, pero aumentaron los incidentes por ransomware dirigidos. Esto presupone los vectores de ataques e intereses económicos y/o dañinos de los ciberatacantes.

Algunos datos del informe representados en gráficos

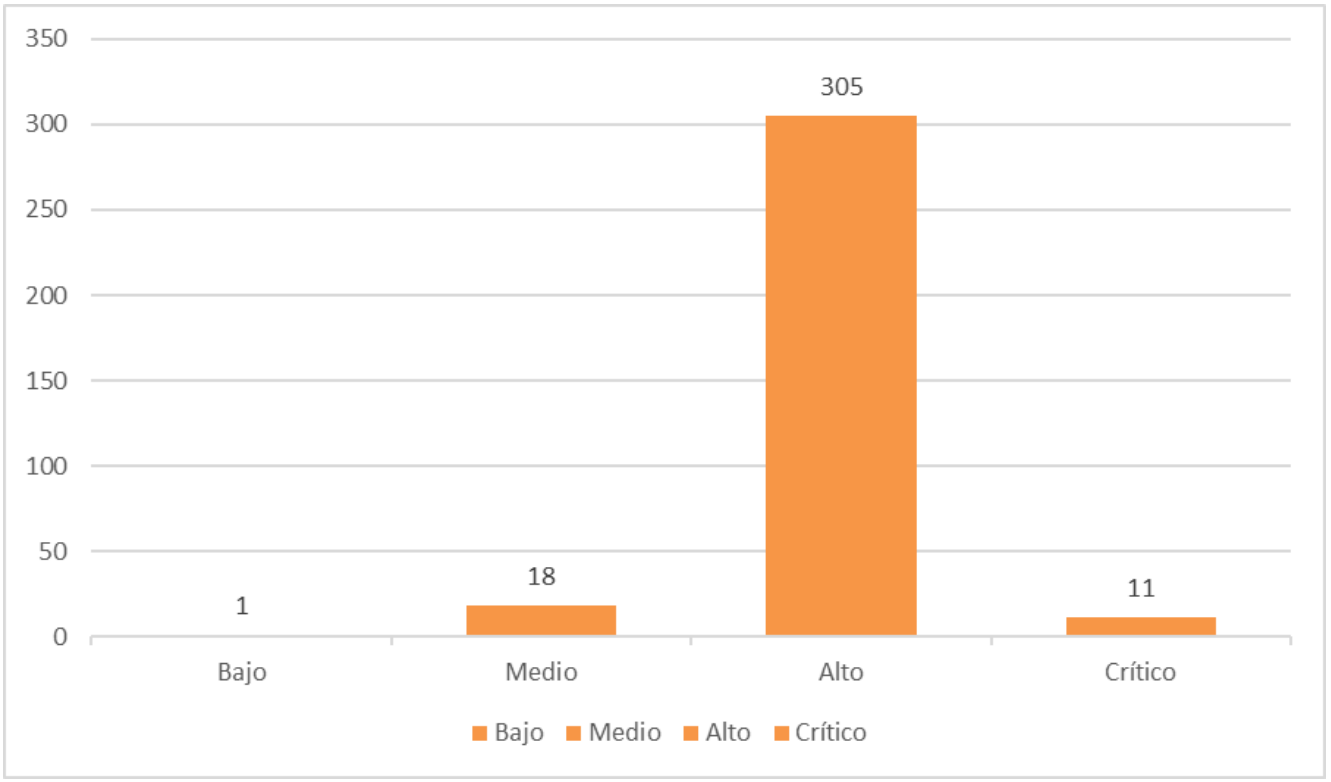
Distribución de los incidentes según las categorías establecidas



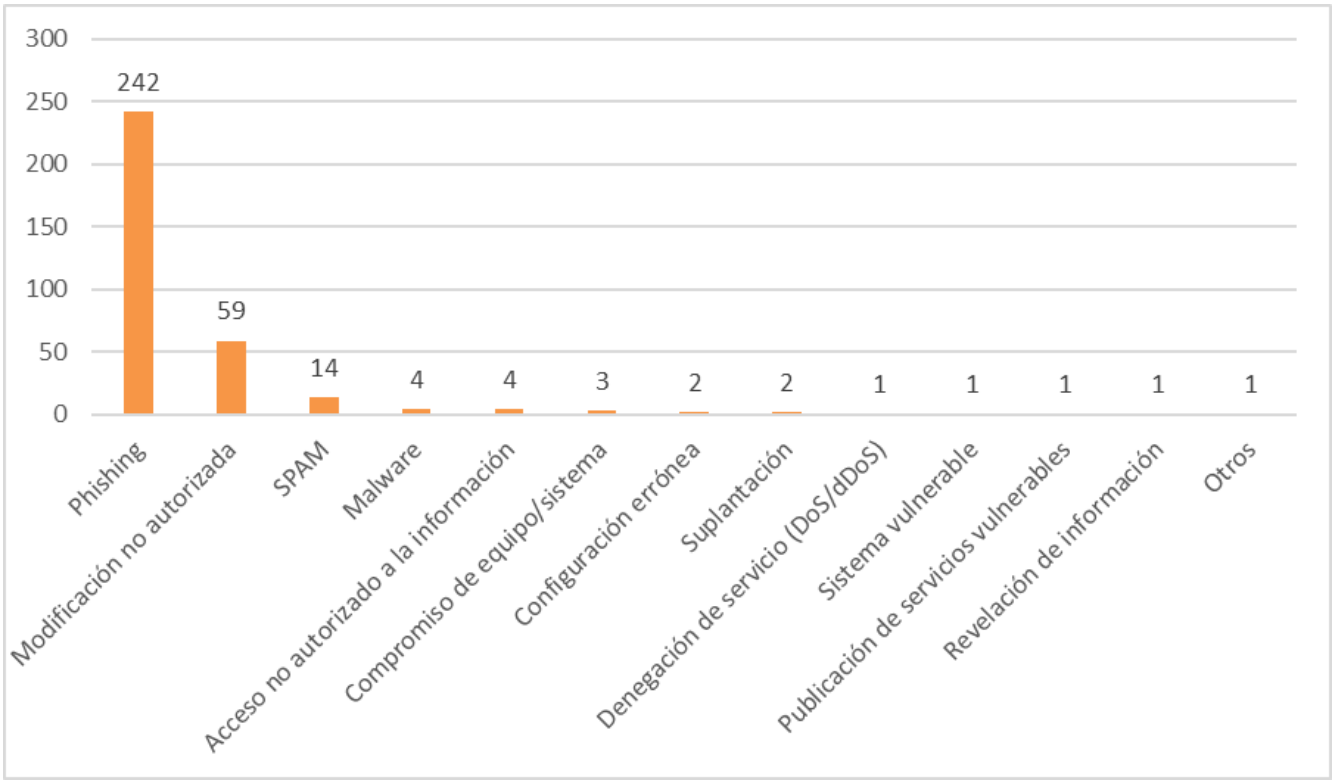
Distribución anual de incidentes por sector



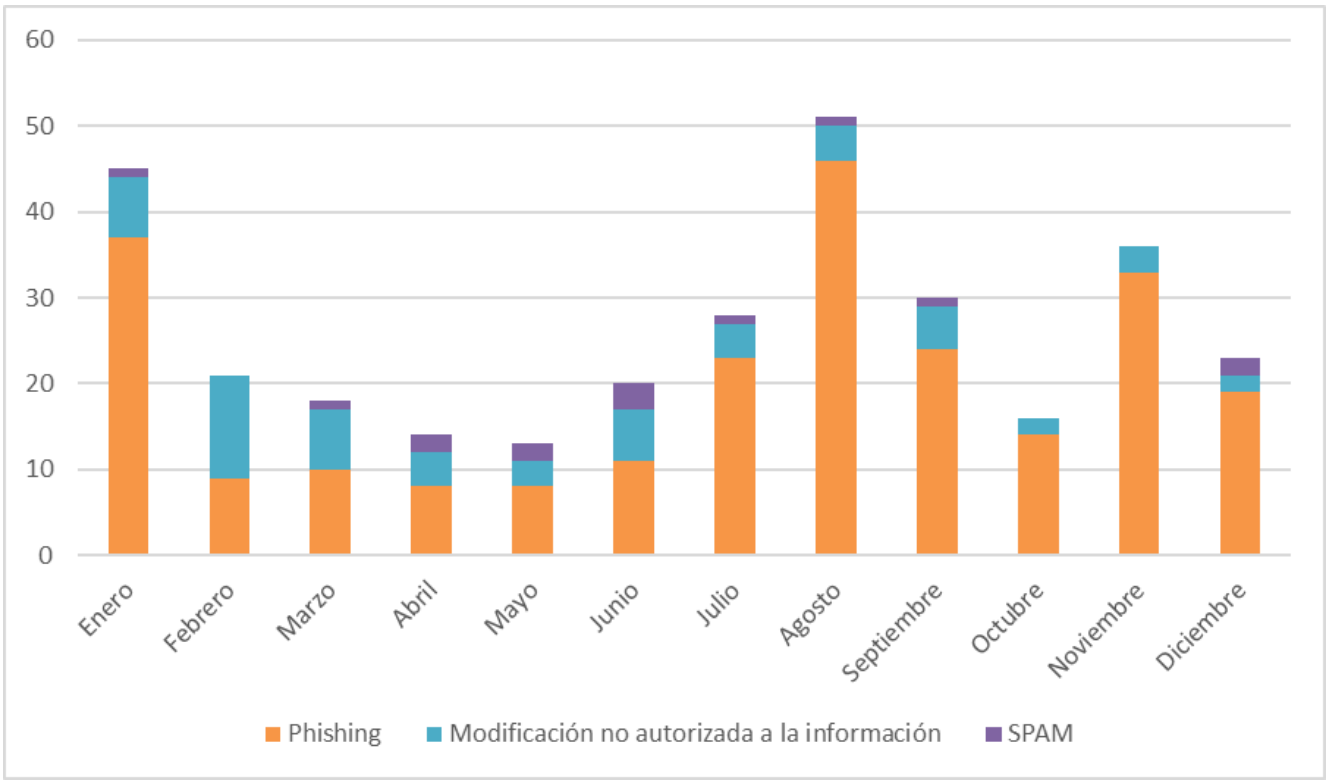
Representación de los incidentes según el nivel de severidad



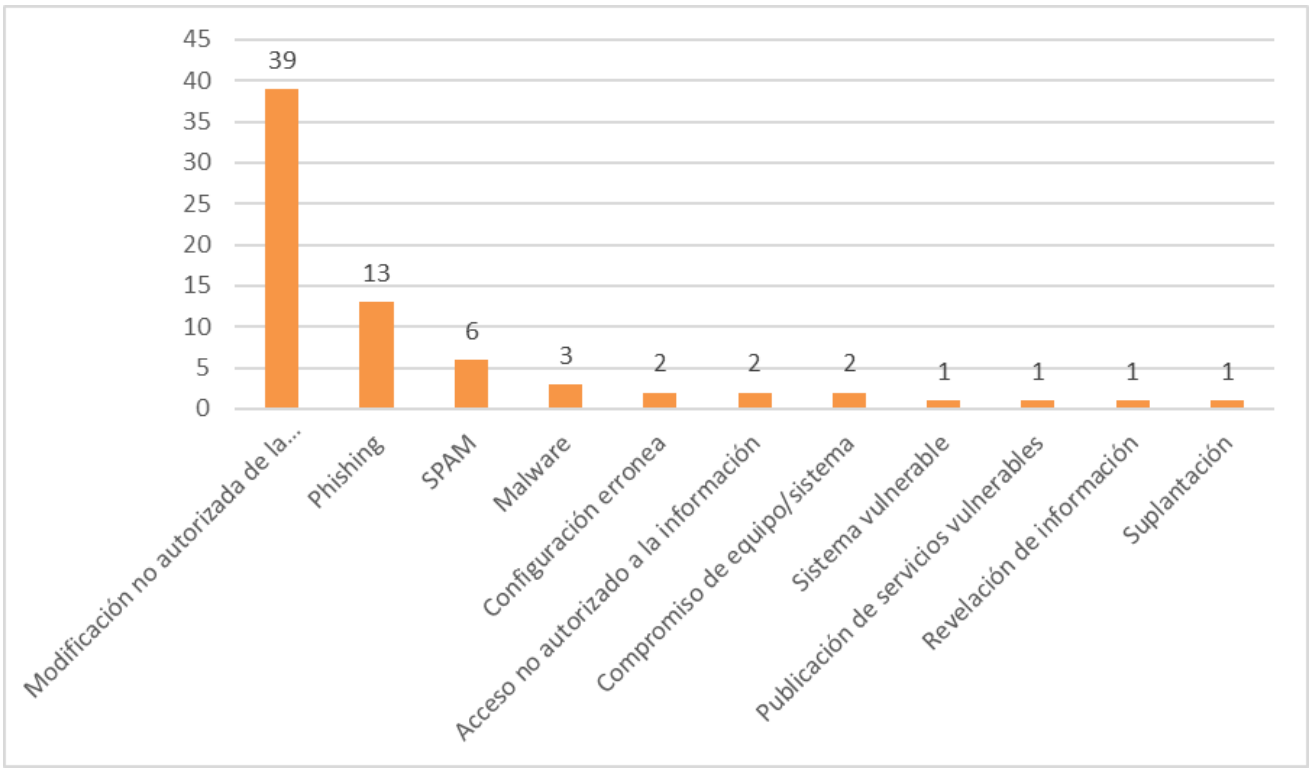
Distribución anual por tipo de incidente



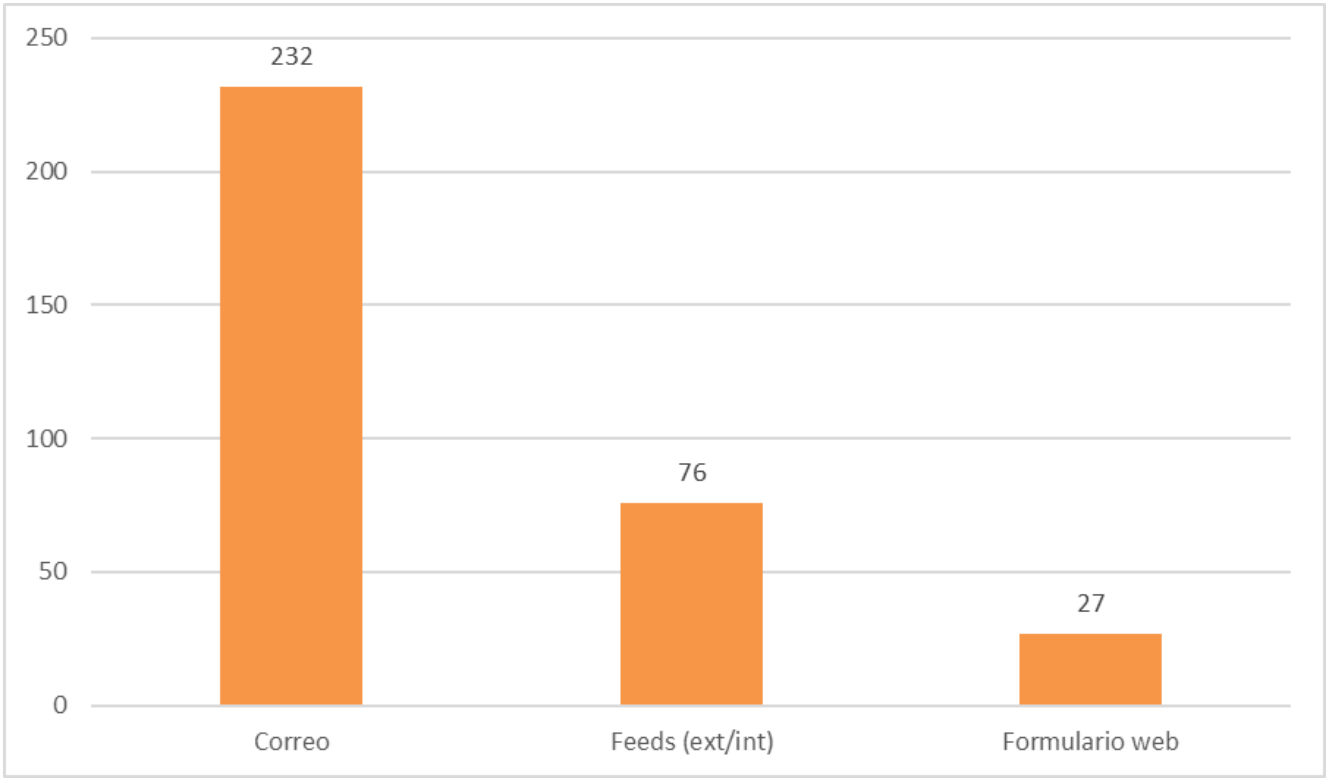
Comparativa de los tres incidentes más reportados del año



Distribución de incidentes reportados en el Estado



Representación de los incidentes según la fuente de información



Glosario

Incidente de seguridad de la información: se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información. Puede ser un evento que produzca un impedimento en la operación normal de un dispositivo, redes, sistemas o recursos informáticos. También puede ser una violación a la política de seguridad de la información de una organización. Lo que debe quedar claro es que un incidente no siempre es un delito, ya que todas las acciones de sus variantes no están tipificadas en el Código Penal argentino.

Phishing: suplantación de identidad para la sustracción de datos. Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas. Los ciberdelincuentes envían correos electrónicos falsos como anzuelo para “pescar” contraseñas y datos personales valiosos.

Ransomware: tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales mediante métodos de encriptación y que exige el pago de un rescate para poder tenerlos nuevamente disponibles.

Modificación no autorizada de la información: se produce por ataques de ransomware, modificación de archivos, o por inyectar código en una base de datos, que consiste en explotar una vulnerabilidad que le permite al atacante enviar instrucciones de forma maliciosa y malintencionada.

SPAM: correo electrónico masivo no solicitado.