Dirección Nacional
de Ciberseguridad

Incidentes Informáticos

Informe anual de incidentes de seguridad informática registrados en el 2021 por el **CERT.ar**

Argentina unida

Jefatura de Gabinete de Ministros
Argentina

Secretaría de Innovación Pública

Febrero 2022

CERT.ar

Introducción

El 2021 fue el segundo que se vivió en el contexto de la pandemia producida por el COVID-19. La priorización sobre el cuidado de la salud, que realizaron a nivel global algunos gobiernos nacionales, como el de Argentina, generó un aumento considerable de la actividad remota, en aquellos rubros y empleos que permitieron pasar del trabajo presencial al teletrabajo.

Asimismo, la ciudadanía utilizó también Internet y las Tecnologías de la Información y las Comunicaciones para seguir realizando distintas actividades, que van desde hacer operaciones comerciales hasta buscar cualquier tipo de entretenimiento.

Como sucedió en 2020, la web se llenó de trámites, inscripciones, transacciones bancarias, entre otros servicios que fueron rápidamente trasladados al ámbito virtual, donde no todas las organizaciones ni las personas usuarias estaban preparadas para esa migración.

Pero la urgencia en la entrega de esos servicios -imprescindible para la situación de emergencia existente-, sumado a la exigida incorporación de amplios sectores de la población no habituada al uso de las herramientas digitales, junto a otros factores, prepararon el escenario para que se produzca un aumento importante de los incidentes informáticos.

Cabe aclarar que un 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.

Este documento tiene como objetivo analizar y describir los incidentes que fueron reportados durante el 2021 en el **Centro Nacional de Respuesta a Incidentes Informáticos (CERT.ar) de la Dirección Nacional de Ciberseguridad.**

Estos reportes proceden de fuentes externas y de la información recibida en los canales de comunicación del **CERT.ar**, es decir, mediante el formulario de la página web argentina.gov.ar/cert-ar, y el mail reportes@cert.ar.

De la información obtenida, se observa que en Argentina se produjo un reflejo de lo que ocurrió a nivel internacional, donde el phishing -mediante sus distintos vectores de ataque- representa el 55% de los incidentes reportados durante el año 2021. Este tipo de incidente afectó principalmente a la comunidad objetivo del **CERT.ar** mediante diversas técnicas -como el phishing dirigido- implementadas en redes sociales y en campañas de creación masiva de dominios para realizar el ataque.

Asimismo, se menciona que, durante los últimos ocho meses del año 2020, los ataques más dañinos registrados fueron por ransomware (software malicioso), tendencia que continuó durante el 2021, afectando principalmente a organizaciones privadas y públicas.

Este tipo de ataque es de alto impacto, no sólo por el fraude que representa la obtención de rédito económico -mediante la solicitud de un rescate- sino también por el costo que significa la falta de disponibilidad de los recursos durante las etapas de análisis y resiliencia.

Y esta situación se agrava ante la posibilidad de una segunda etapa del ataque, que puede suceder por la venta de datos en la web profunda, o por la utilización de esa información personal para llevar a cabo otros ataques.

Durante el 2021, el ransomware fue la gran preocupación que se debatió en foros y ámbitos especializados, y se hizo presente en la comunidad objetivo del **CERT.ar**, mediante sus diferentes tipos y variantes como Sodinokibi, Avaddon, Clop, DarkRadiation, LockBit, OnePercent, Everest y Cuba, generando diferentes niveles de impacto.

Con respecto a los sectores más afectados por incidentes, el del Estado y el de las Finanzas fueron los más comprometidos, a diferencia del 2020, cuando el sector Salud fue el más perjudicado, mediante el SPAM y el phishing dirigido a instituciones sanitarias o al personal del sector. Para engañar a las víctimas, los ciberdelincuentes utilizaron la pandemia y prometieron accesos a insumos más económicos, planes de obras sociales con mejoras en la atención de pacientes con COVID, y hasta la compra de la vacuna en mercados alternativos, cuando aún no existía, etc.

Los ataques al sector de las Finanzas pueden residir en las alternativas que se ofrecieron -con un gran esfuerzo y prácticamente contra reloj- para continuar cumpliendo con los servicios en el marco de la pandemia. Así, con una propuesta más completa e integradora de atención remota mediante homebanking o nuevas formas de pago -para evitar la circulación de efectivo y el contacto personal-, se habilitó la posibilidad de ataques contra un usuario desprevenido y/o por una eventual vulnerabilidad de los recursos involucrados.

En cuanto al del Estado, la inmediatez de implementar el teletrabajo y otras alternativas laborales surgidas por la pandemia, para continuar brindando servicios a la ciudadanía, no permitieron la preparación necesaria de los recursos de información para ser accedidos de esta forma online, ni la concientización adecuada, masiva, acerca de la posibilidad de incidentes de seguridad.

Incidentes informáticos registrados en el 2021

Durante el período comprendido entre el 1 de enero y el 31 de diciembre del 2021, el **CERT.ar** registró en su plataforma de administración un total de 591 incidentes informáticos, cifra que superó en un 261,50% a la del 2020, cuando se registraron 226 incidentes.

De los 591 casos, 18 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 573 restantes están cerrados.

El **CERT.ar** utiliza la siguiente taxonomía en la tipificación de incidentes. A continuación, se detalla la cantidad deportada en cada categoría:

- Contenido abusivo: 57 incidentes
- Contenido dañino: 11
- Obtención de información: 2
- Intrusión: 26
- Disponibilidad: 11
- Compromiso de la información: 101
- Fraude: 331
- Vulnerable: 50
- Otros: 2

El fraude, con 331 casos, representa el 56% del total de incidentes reportados, dato que significa que 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 consideran siete sectores denominados Finanzas, Estado, Salud, Otros, Transportes, Espacio, y el de las Tecnologías de la Información y las Comunicaciones (TICs).

Haciendo un análisis anual, el sector más comprometido de acuerdo con los incidentes reportados fue el Estado con 235 incidentes, cifra que representa el 39,70% del total registrado.

El segundo sector más afectado fue el de las Finanzas con 214 incidentes (36,15%), mientras que el sector denominado Otros se ubica en el tercer lugar con 124 incidentes (21,11%).

Como se podrá observar, los sectores Estado y Finanzas superan el 70% de los incidentes anuales reportados, con 449 casos registrados entre ambos.

Durante el primer semestre, el sector más comprometido fue el Estado con 149 incidentes (43%), seguido por Finanzas que contabilizó un total de 98 incidentes (28%).

Distinta fue la situación que se observó en el segundo semestre, cuando el sector Finanzas reportó 116 incidentes (46%) y el Estado 86 (34%).

Tipos de incidentes más reportados en el sector del Estado

- Modificación no autorizada de la información: 79 incidentes, cifra que representa el 33,62% del total de los casos estatales.
- SPAM: 54 (22,98%).
- Phishing: 39 (16,60%).
- Sistemas vulnerables: 24 (10,21%).

Tipos de incidentes reportados en el sector Finanzas

- Phishing: 209 incidentes, cifra que representa el 97,66% del total de los casos del sector Finanzas.
- Denegación de servicios (Ddos/DOS): 2 (0,93%)
- Acceso no autorizado: 1
- Revelación de información: 1
- Ingeniería social: 1

Los últimos tres representan el 0,47% del total reportado en este sector.

Continuando con el detalle anual por sector, Salud, con 12 reportes, se ubica en el cuarto lugar, seguido por el sector de las Tecnologías de la Información y las Comunicaciones (TICs) con 4 incidentes. Los sectores Transporte y Espacio registraron 1 incidente cada uno, siendo los menos afectados.

Al realizar una discriminación por tipo de incidente informático, el phishing fue el más registrado con 327 casos, cifra que representa el 55,24% del total reportado.

La modificación no autorizada de información se ubica en el segundo lugar con 90 incidentes reportados (15,20%), mientras que el SPAM (comunicación masiva no solicitada) se ubica en el tercero con 57 casos, dato que significa el 9,23% de la totalidad. El resto, es decir el 20% de los tipos de incidentes, se divide en forma decreciente entre:

- Sistema vulnerable: 28 incidentes (4,73%)
- Revelación de información: 26 (4,39%)
- Compromiso de equipo/sistema: 21 (3,55%)
- Malware: 11 (1,86%)
- Denegación de Servicio: 7 (1,18%)
- Acceso no autorizado a la información: 7 (1,18%)
- Explotación de vulnerabilidades: 5 (0,84%)
- Suplantación de identidad: 5 (0,84%)
- Configuración errónea: 4 (0,68%)
- Otros: 1 (0,17%,)
- Escaneo de redes / análisis de tráfico: 1 (0,17%)
- Ingeniería social: 1 (0,17%)

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 2021, 467 de los incidentes reportados (79,02%) fueron de severidad alta, seguidos de 69 de severidad media (11,68%), 39 de severidad baja (6,60%) y 16 de severidad crítica (2,71%).

Conclusión

Como se mencionó al comienzo de la descripción de este informe, al hacer una comparativa entre los últimos dos años, se puede ver que hubo más de una duplicación de incidentes reportados, ya que en el 2020 se registraron 226 y en el 2021, 591.

Entre los motivos que permitieron registrar en el **CERT.ar** ese incremento importante, se citan dos normativas de la Dirección Nacional de Ciberseguridad de la Subsecretaría de las Tecnologías de la Información y las Comunicaciones, dependiente de la Secretaría de Innovación Pública.

Una es la Decisión Administrativa 641/2021, que establece los Requisitos Mínimos de Seguridad de la Información para los organismos del Sector Público Nacional. Esta medida apunta a promover una política pública que enmarque una conducta responsable en materia de seguridad de la información en los organismos estatales, sus agentes y funcionarios.

En otras palabras, busca elevar los niveles de seguridad de la información de los organismos estatales, los principales receptores y productores de datos del país.

La otra es la Disposición 7/2021, que instruye la creación del registro de Puntos Focales de Ciberseguridad. Esos Puntos son empleados de distintos organismos que deben reportar a la Dirección Nacional de Ciberseguridad los incidentes de seguridad que se produzcan en sus ámbitos laborales dentro de las 48 horas de haber tomado conocimiento de su ocurrencia o de su potencial ocurrencia.

Asimismo, la formalización de una postura del Gobierno nacional acerca del valor y la necesidad de asumir la ciberseguridad como una cuestión de Estado, soportado por las normativas antes citadas, colaboró con una mayor interacción entre el CERT nacional y su comunidad objetivo, promoviendo el reporte de incidentes de seguridad que aporta a la prevención y protección de los activos de información del Estado nacional.

Por otra parte, durante el corriente año, se prevé el establecimiento de una serie de medidas para el afianzamiento de esa relación, que seguramente redundará en una mayor cantidad de reportes y una mejor calidad de la información.

Algunos datos del informe representados en gráficos

Gráfico 1

Distribución de los incidentes de acuerdo con las categorías establecidas.

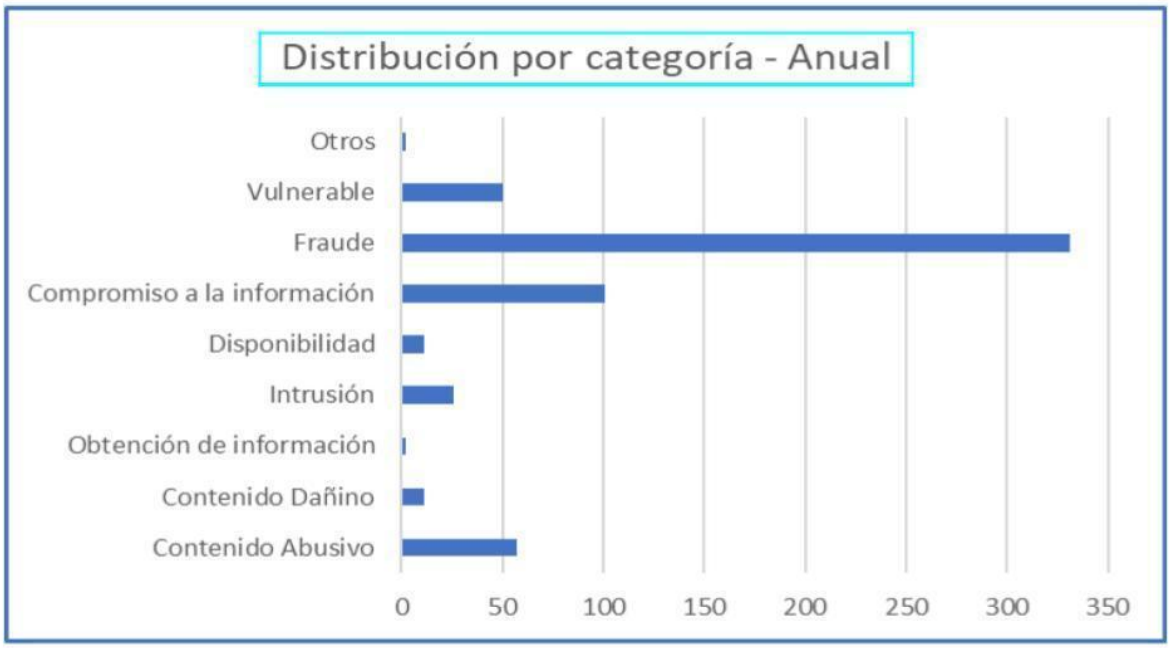

Gráfico 2

Distribución anual de incidentes por sector.

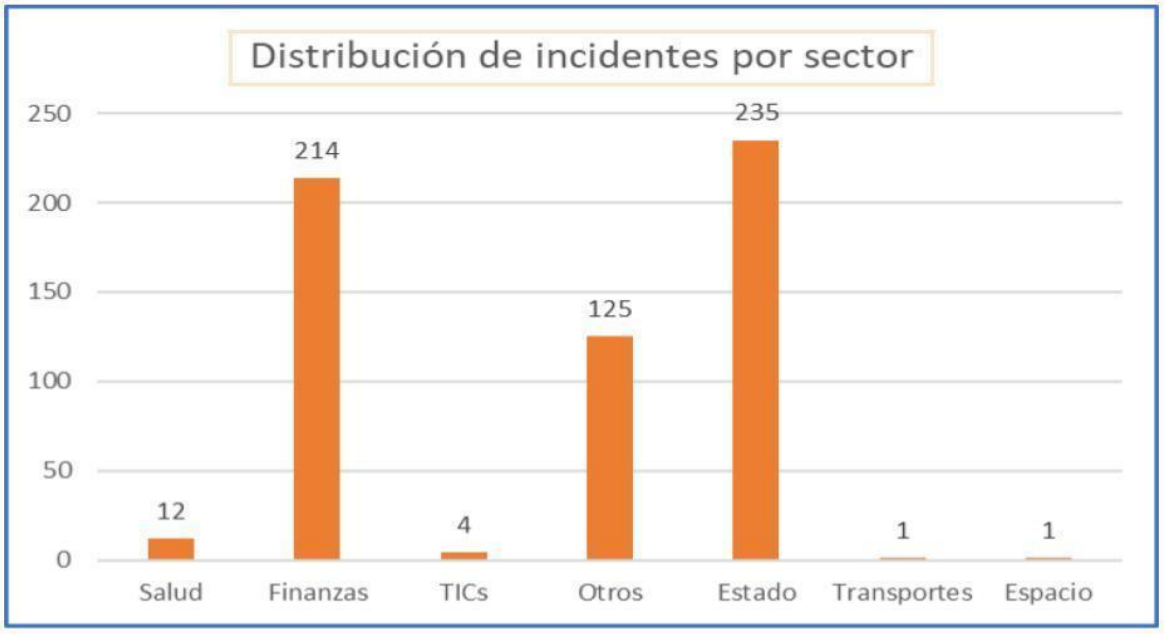

Gráfico 3

Incidentes distribuidos por sector en el primer semestre del 2021.

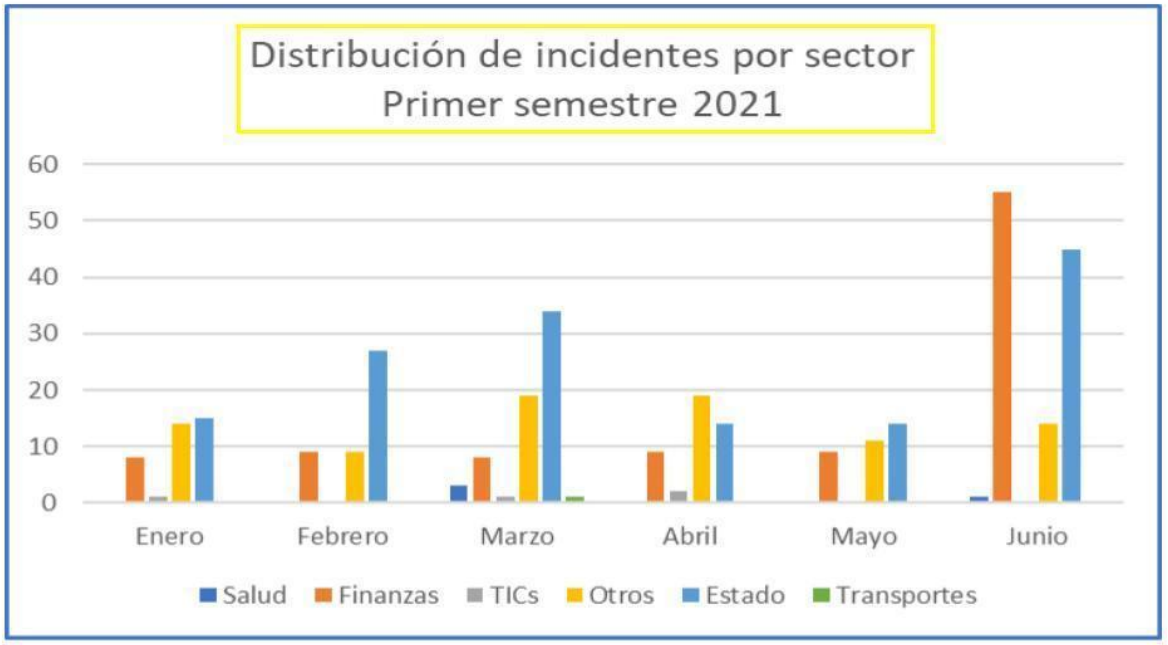

Gráfico 4

En el segundo semestre, se puede visualizar un cambio debido a que el sector Finanzas fue el más comprometido, seguido por el del Estado.

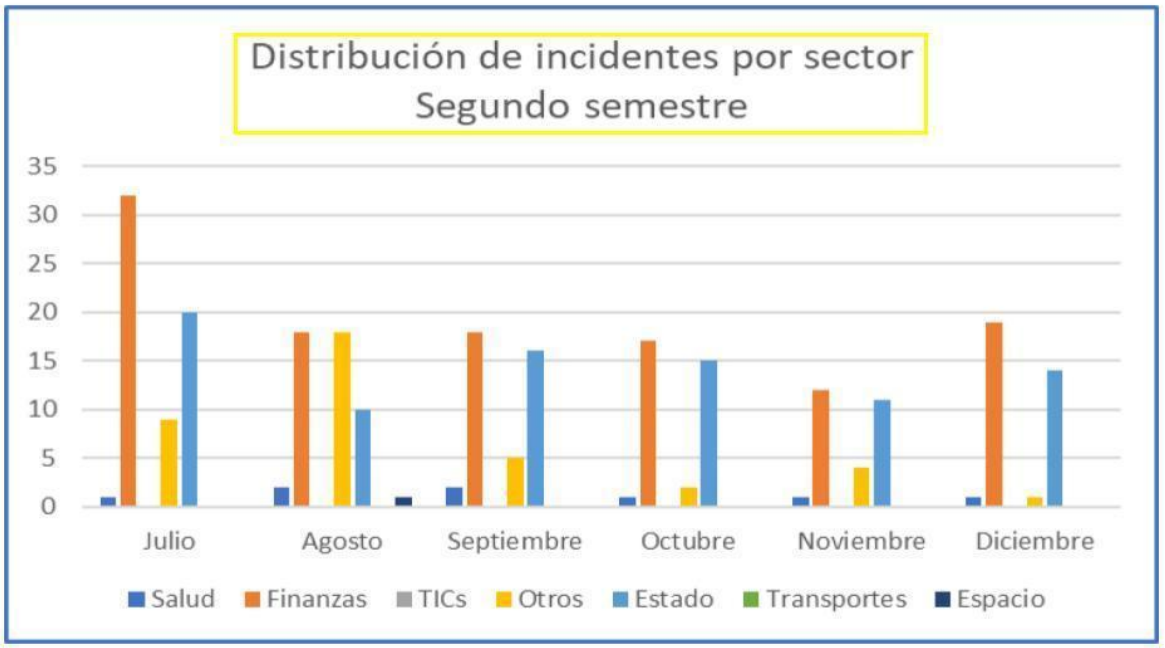

Gráfico 5

Representación de los incidentes según el nivel de severidad.

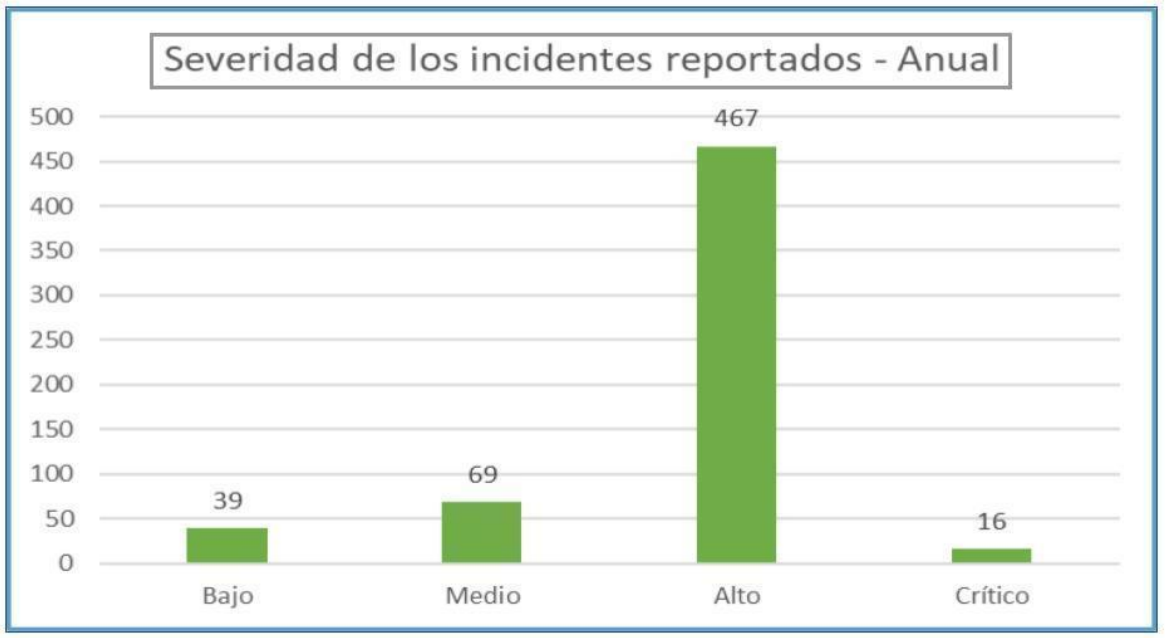

Gráfico 6

Representación de los incidentes según el nivel de severidad.
Distribución anual por tipo de incidente.

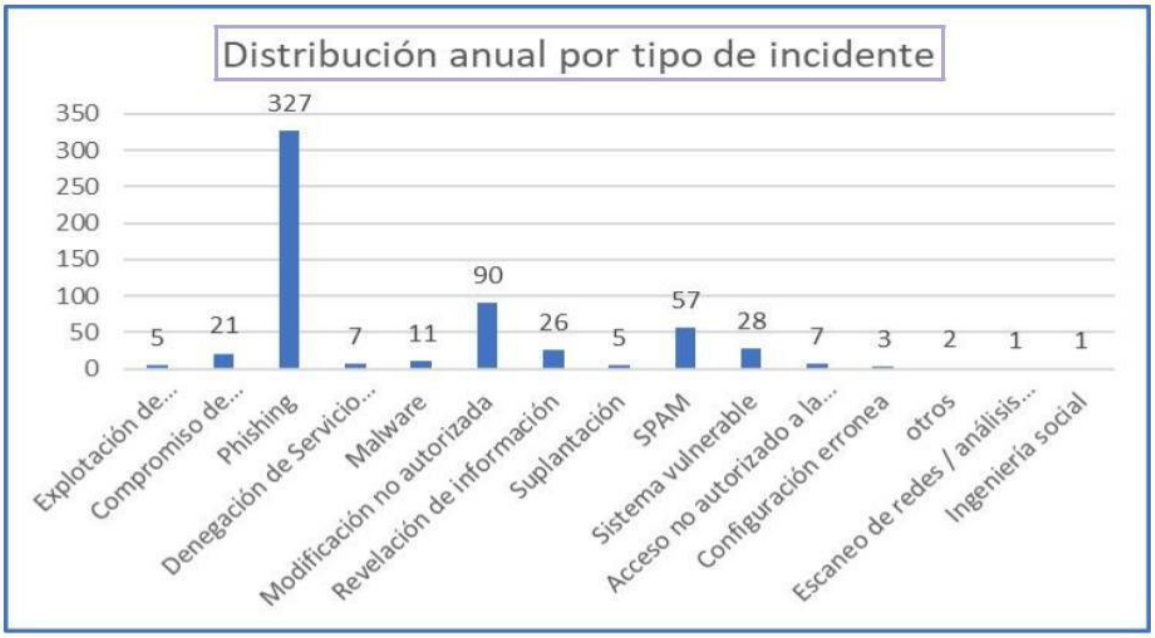

Gráfico 7

Distribución porcentual por tipo de incidente.

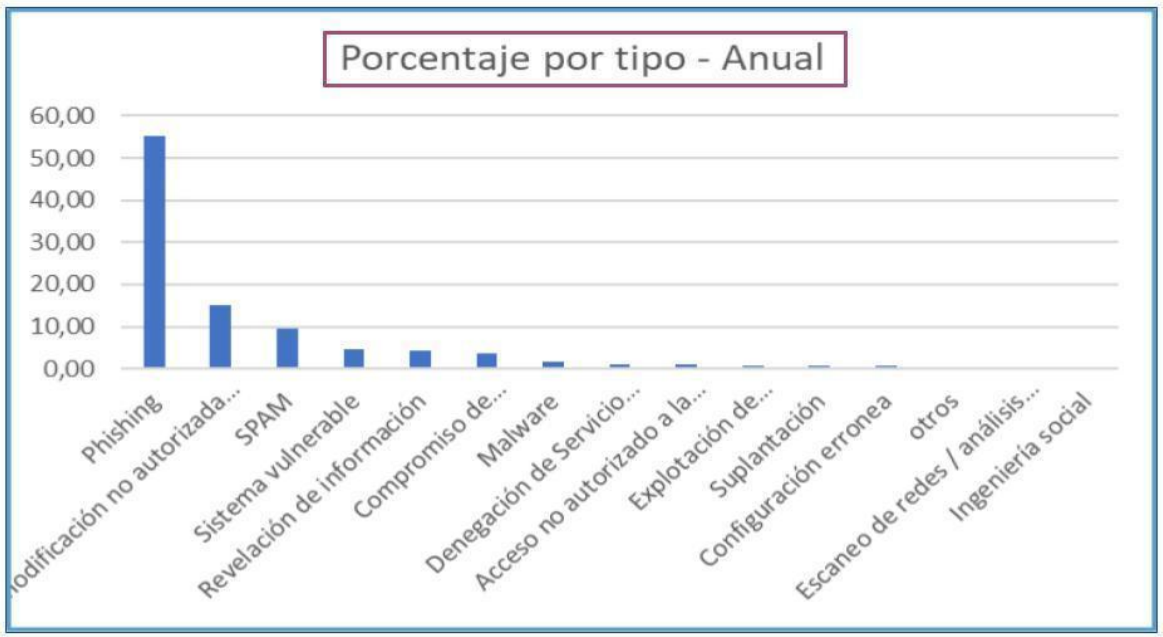

Gráfico 8

Comparativa de los tres incidentes más reportados durante el 2021.

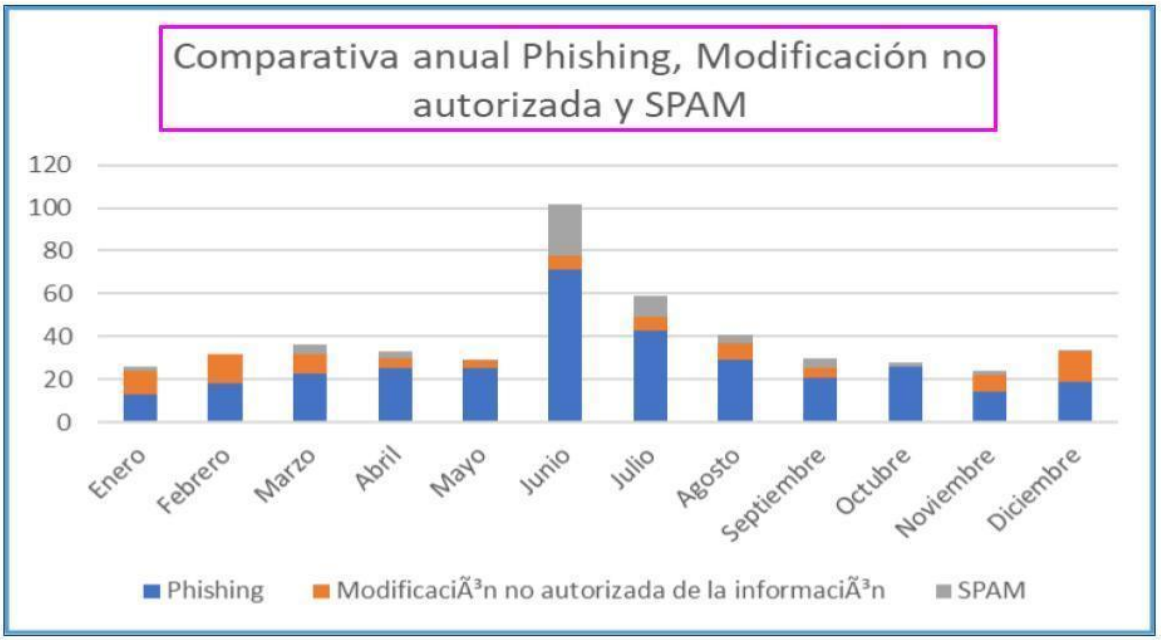

Gráfico 9

Distribución de incidentes reportados en el Estado.

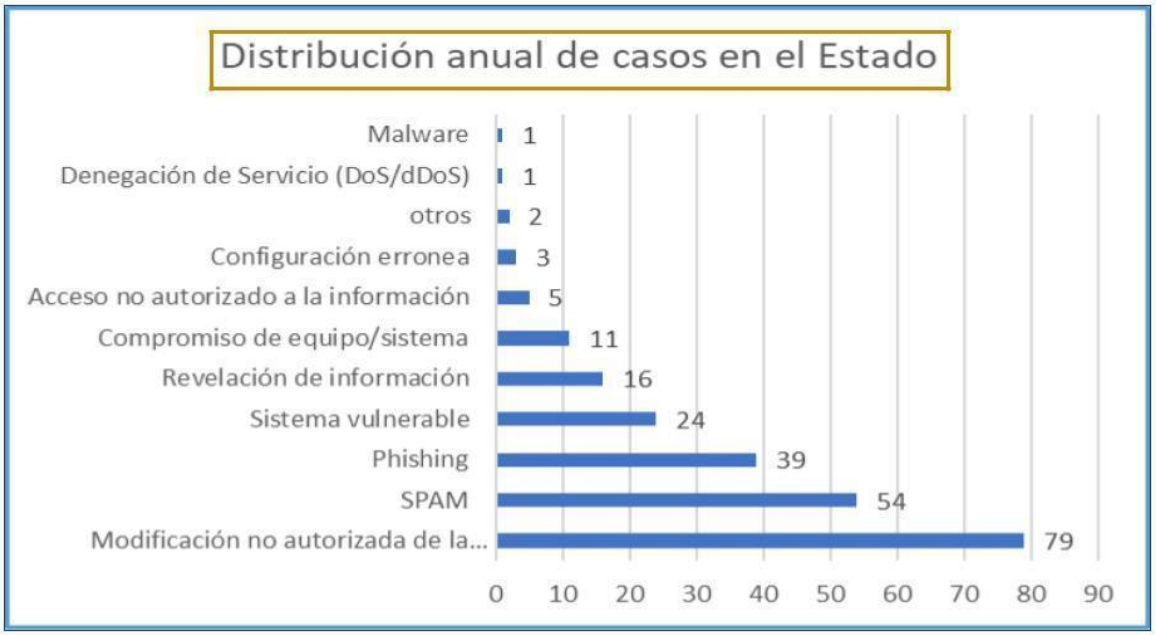

Gráfico 10

Comparativa de incidentes por semestre