JORNADAS FEDERALES DE CIBERSEGURIDAD

ING. ARIEL CESSARIO

Coordinador General del Equipo de Respuestas a Emergencias Informáticas de la República Argentina (CERT.ar) de la Dirección Nacional de Ciberseguridad

"LA GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES"

Santa Cruz Gobierno de la Provincia
UTN FACULTAD REGIONAL SANTA CRUZ
UNPA UARG
Jefatura de Gabinete de Ministros Argentina
Dirección Nacional de Ciberseguridad
Datastar
NUTANIX

Gestión de incidentes de seguridad informáticos en las organizaciones

Ariel Cessario
Dirección Nacional de Ciberseguridad
Mayo de 2022

Agenda

- Incidente de seguridad en el Estado
  - Conceptos y definiciones
  - Seguridad de la información
  - Plan de contingencia
- CERT Nacional
  - Antecedentes
  - CERT.ar
  - Acciones
  - Algunos datos

Conceptos y definiciones

- **CIBERESPACIO**: Entorno digital de redes, servicios, sistemas, personas, procesos u organizaciones interconectadas y todo lo que reside en el entorno digital o lo atraviesa
- **CIBERGUERRA**: Conflicto dentro del Ciberespacio.
- **CIBERDEFENSA**: Conjunto de acciones defensivas activas/pasivas, proactivas, preventivas y reactivas para asegurar el uso apropiado del Ciberespacio y negarlo al enemigo u otra inteligencia en oposición.
- **CIBERSEGURIDAD**: Salvaguarda de las personas, la sociedad, las organizaciones y las naciones de los riesgos cibernéticos y entendemos por salvaguardar a mantener los riesgos cibernéticos en un nivel tolerable.
- **CIBERCRIMEN**: Acción criminal dentro del Ciberespacio.
- **CIBERTERRORISMO**: Acción terrorista dentro del Ciberespacio.

Conceptos y definiciones

- **RED INFORMÁTICA**: Una red informática es un conjunto de computadoras que a través de distintos medios de comunicación se encuentran conectadas entre si, con el fin de compartir recursos, información y/o tareas específicas.
- **SISTEMA INFORMÁTICO**: podemos decir que un sistema informático son un conjunto de diversas técnicas utilizadas para la gestión, almacenamiento, tratado y resguardo de la información, que por medio de un lenguaje de programación, las computadoras permiten estas acciones a los usuarios.
- **MALWARE**: El malware es un software que tiene el propósito de perjudicar a un usuario, red informática o sistema, en forma directa o indirecta. Generalmente es conocido de forma genérica como virus informático.
- **RIESGO**: es la combinación de la probabilidad que ocurra un evento o incidente y su consecuencia o impacto, de que el mismo ocurra. El riesgo es una medición y es muy utilizado en las organizaciones para tener una posible magnitud frente a un ciberataque.

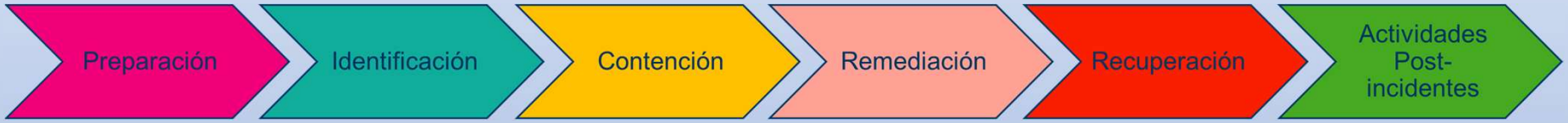
Conceptos y definiciones

Un **incidente de seguridad** informática es un evento inesperado y perjudicial en un sistema de computadoras, o red de computadoras, que puede comprometer o violar la confidencialidad, integridad y/o disponibilidad de la información.

Un **incidente de seguridad** informática puede ser causado mediante la explotación de alguna vulnerabilidad, un intento o amenaza de romper los mecanismos de seguridad existentes.

Ciclo de Vida

- El ciclo de vida de un incidente es el proceso vital desde la detección hasta la resolución del mismo.



- Por lo general, los ciclos suelen ser similares dependiendo el tipo, clasificación y la motivación del atacante.

Etapas

- **Preparación**: fase de preparación para atender el incidente. Aquellas actividades proactivas que permitan una mejor atención y respuesta frente a un incidente como se entrenamiento, procedimientos actualizados, herramientas, estándares e información útil para cada incidente.
- **Identificación**: medidas para limitar y aislar el impacto del incidente. Refiere a la capacidad de identificar o detectar un incidente, incluye el monitoreo, recolección de información, y toda aquella actividad que permita identificar los hechos, determinar el alcance e involucrar a las partes apropiadas.
- **Contención**: detección del incidente. Aquellas actividades que permitan evitar la propagación y efectos del incidente. Dependiendo el tipo de incidente se aislará el equipo de la red, se extraerán indicadores de compromiso, corrección de fallos, aplicación de parches, etc.

Tipos de Incidentes

VULNERABILIDAD

- Debilidad o falla en un sistema que pone en riesgo la seguridad de la información dejando que un atacante se haga con ella o no permita el acceso a las entidades autorizadas
- Puede tener distintos orígenes: fallo de diseño, errores de configuración o carencias de procedimientos (ej: Inyección de código SQL no autorizado)
- Por si sola, no causa daño alguno, pero posibilita que se materialice una amenaza sobre un activo afectado.

AMENAZA

- Violación de seguridad en potencia.
- Puede materializarse al explotar una vulnerabilidad para causar una infracción de la seguridad.
- Puede provocarse de manera intencional (ataque) o no intencional (amenaza natural o negligencia).

ATAQUE

- Acto intencionado y deliberado que viola la política de seguridad de una red o sistema.
- Puede ser de modo Activo (altera el sistema, recurso u operación) o pasivo (intenta aprender o utilizar información, pero no afecta directamente al sistema ni a su funcionamiento).

Clasificación de Incidentes

Clasificación	Método	Descripción
Contenido Abusivo	SPAM, delito de odio, abuso infantil.	Correos Electrónicos no solicitados Contenido discriminatorio y/o acoso Material que represente contenido relacionado al abuso infantil
Contenido Dañino	Malware	Distribución de malware, afectación de equipos, C&C.
Obtención no autorizado de información	Escaneo de redes, análisis de tráfico, ingeniería social	Envío de peticiones a un sistema, explotación de vulnerabilidades, obtención de tráfico de red por M0D
Intrusión	Ataque de fuerza bruta, ataques zero-D, compromiso de equipos/sistemas , robo	Intento o compromiso de un equipo o red de sistemas vía explotación de vulnerabilidad Recopilación de información personal sin un uso de la tecnología múltiples intentos de vulnerar credenciales Daño físico
Disponibilidad	Ataque por denegación de servicios, configuración errónea, sabotaje, interrupciones	DoS/DDoS Configuración débil o error de código involuntario
Compromiso de la información	Acceso o modificación no autorizada, pérdida de datos	Robo o suplantación de identidad Perdida de información por fallo de hardware

Tipo de adversarios y sus motivaciones

Conceptos y Definiciones

- **Remediación**: medidas para eliminar la amenaza. Actividades que permitan determinar las medidas de mitigación más eficaces las cuales dependerán del tipo de incidentes.
- **Recuperación**: procedimientos para volver a una operatoria normal. Actividades que permitan volver al nivel de operación a su estado normal, publicación de servicios; conexión del equipo a la red; restauración de archivos; reinstalación de sistemas; entre otros.
- **Post-incidente**: identificar e implementar medidas de mejora. Aquellas tareas que permitan identificar las lecciones aprendidas del incidente, mejorar los procedimientos, técnicas, etc.

Cooperación y Comunicación

"El 50 porciento de las organizaciones fueron atacadas.

El 50 porciento restante nunca se enteraron que fueron, o están siendo atacadas"

Cooperación y Comunicación

¿Qué SI?

- Comunicalo siempre.
- La información puede ser tu responsabilidad, pero no siempre es tuya.
- Apoyate en tus pares, tu consulta no molesta.
- Compartí experiencias.

¿Qué NO?

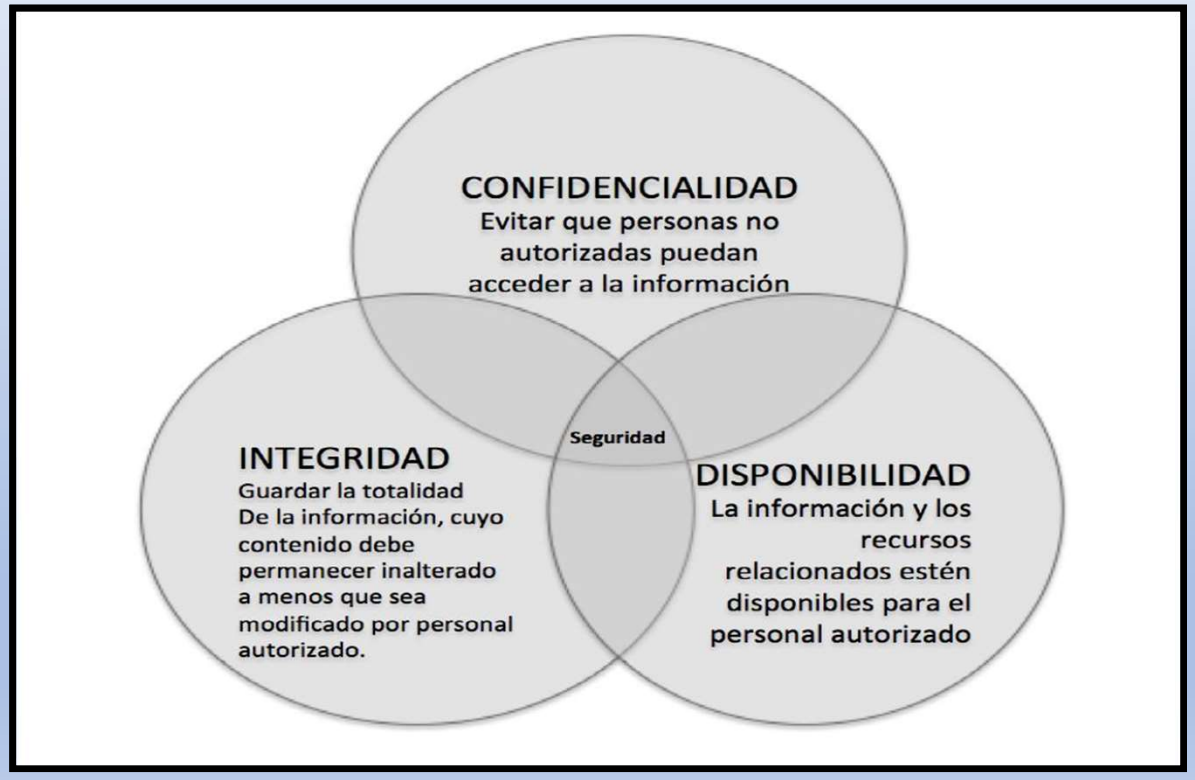
- No ocultes o modifiques los datos en la comunicación.
- No afirmes cosas que no tengas total seguridad.
- Por más que lo creas, no sos omnipotente; déjate ayudar.
- Nunca minimices los riesgos o los impactos del incidente.

Seguridad de la Información

Llamamos **información** a todo dato, o conjunto de estos, que son procesados y ordenados para su comprensión, con el fin de aportar nuevos conocimientos y valor agregado, para la administración y toma de decisiones.

Para garantizar dicha seguridad dentro de los sistemas y redes informáticas, se utilizan diversas técnicas que brinda protección y disponibilidad, tanto en el circuito de comunicación, como en el resguardo de la información.

Seguridad de la información



Seguridad de la Información

- **Seguridad desde el diseño**: actividad asociada a implementar técnicas de prevención y protección de la información, desde el inicio de un proyecto o desarrollo. En este punto, se tienen en cuenta estándares de comunicación segura, soberanía y gobernanza de los datos, leyes asociadas, etc.
- **Seguridad de las comunicaciones**: acciones que pueden implementarse en partes o en todo el circuito de comunicación, brindando distintos niveles de protección en cada una de las etapas.
- **Seguridad en el resguardo y tratado de la información**: acciones referidas a la seguridad de los medios que almacenan información, como así también los protocolos, estándares, procedimientos y actividades que brinden seguridad en el tratado de información (edición, eliminación, respaldo, compartimiento, etc.).

Seguridad de la Información

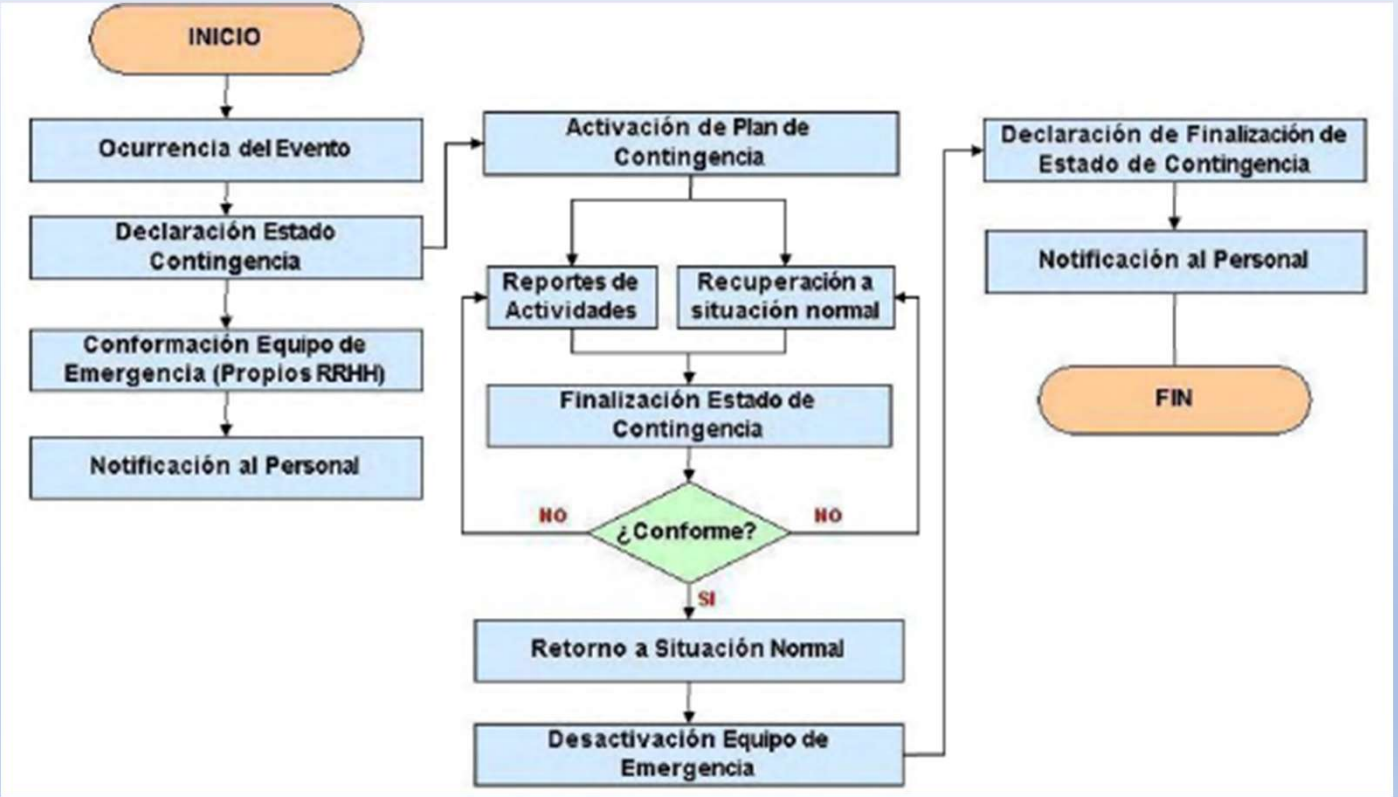
Plan de Contingencia - Importancia

- Evento con probabilidad de acontecer en un futuro.
- Tener prevención ante la incertidumbre.
- Posibilidad de minimizar un impacto negativo.
- Planear lo impensado.

Plan de Contingencia – Puntos Principales

- Roles y tareas definidas
- Identificación de los activos a proteger
- Análisis, manejo y aceptación del riesgo
- Compromisos de trabajo
- Revisión y adecuación

Plan de contingencia

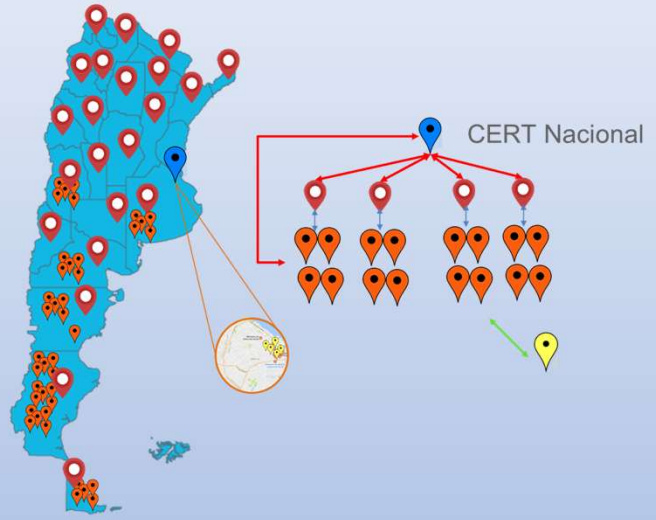


CERT - Antecedentes

- En el 2011 se crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (res. 580/2011 de Jefatura de Gabinete de Ministros)
- En el 2013 nace el grupo de trabajo “ICIC-CERT” con los objetivos de administrar información, centralizar esfuerzos, asesorar e interactuar con equipos de similar naturaleza sobre incidentes de seguridad informática, dentro del Sector Público Nacional (disp. 2/2013 de la Oficina Nacional de Tecnología de Información)
- Actualmente mediante la Disposición 1/2021 de la Dirección Nacional de Ciberseguridad se crear el actual equipo denominado **CERT.ar**, en la cual se focaliza y concentra las diversas funciones para la comunidad objetivo del equipo dentro del Sector Público Nacional.

Cert.ar

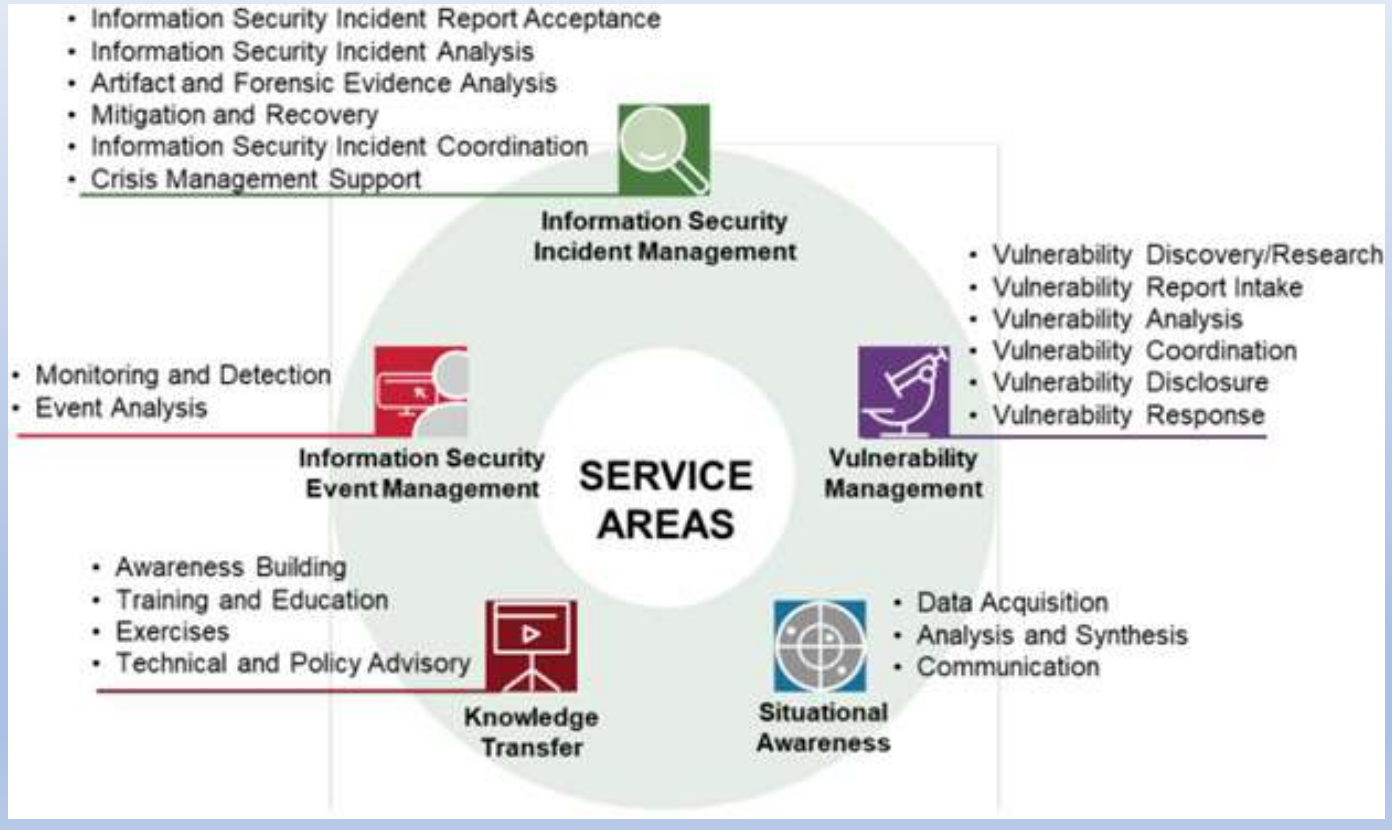
- Centralizar los reportes sobre incidentes de seguridad ocurridos en los sistemas y redes del Sector Público Nacional.
- Encausar posibles soluciones de los incidentes reportados, asesorando técnica y administrativamente.
- Promover la coordinación de las unidades informáticas para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad informática.
- Difundir información útil para incrementar los niveles de seguridad de las infraestructuras críticas de información.
- Interactuar y cooperar con la comunidad objetivo, CERT y SCIRTs del país.



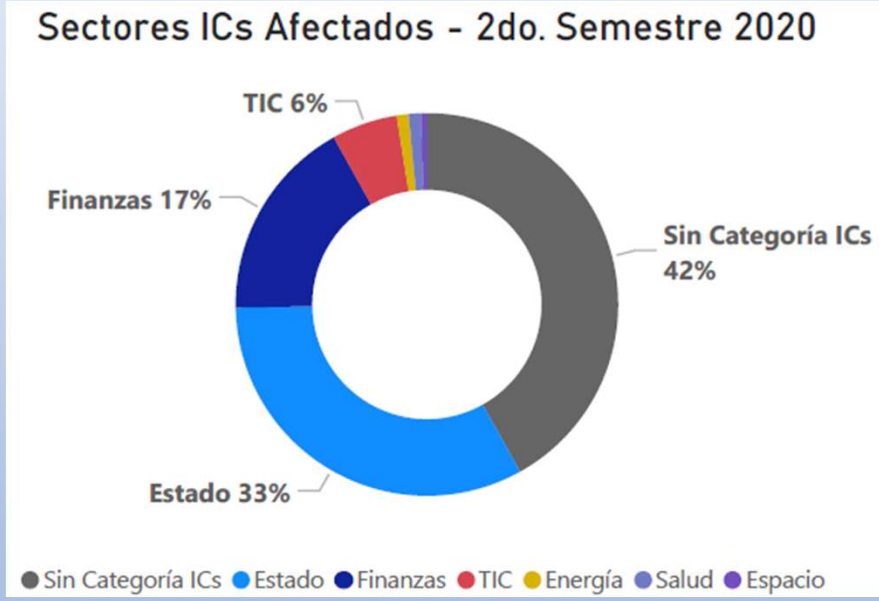
FIRST Improving Security Together

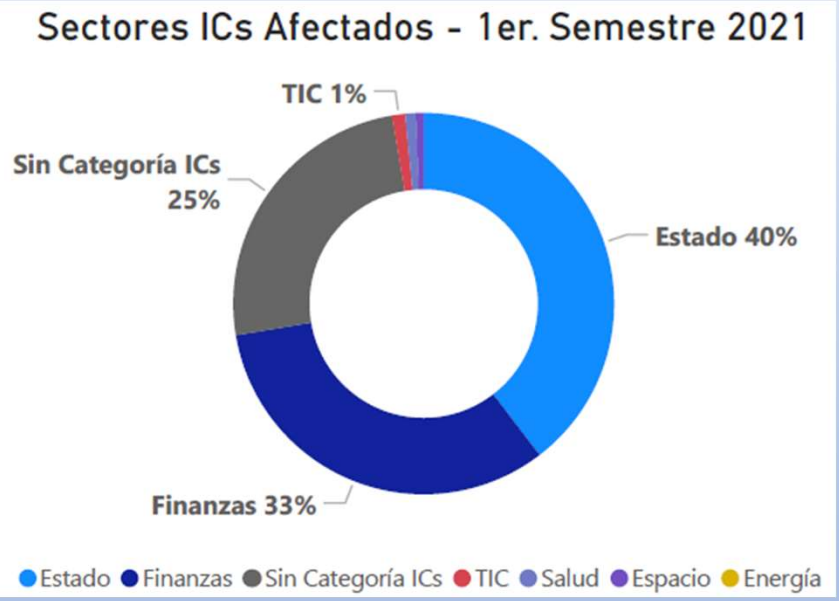
CSIRTamericas.org

CERT.ar - Acciones

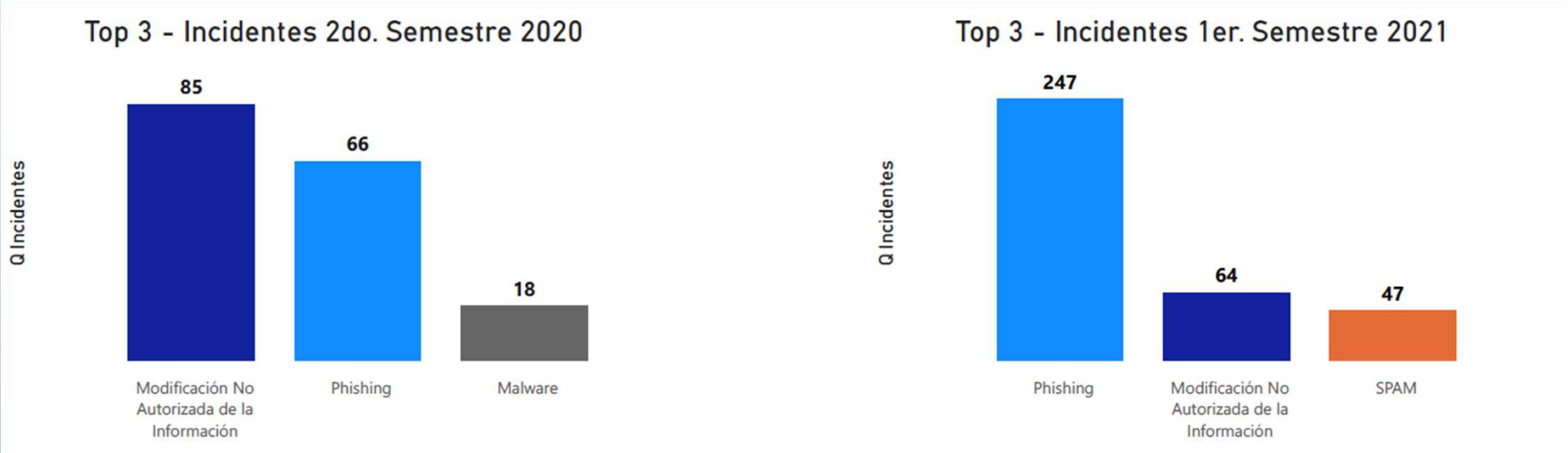


Cert.ar - Datos





Cert.ar - Datos



¡Gracias!

Ariel Luis Cessario

Dirección Nacional de Ciberseguridad

Mayo de 2022

EXTRAIDO DE

JEFATURA.SANTACRUZ.GOB.AR/CIBERSEGURIDAD2022/