CSIRT CUDI

Experiencias en el sector educativo mexicano

CSIRT

SIGESTIC'23

cudi

Mayo 2023

Antecedentes

- A finales de 2018, el consejo de administración de la Red Nacional de Educación e Investigación de México (RNEI) autoriza la conformación del CSIRT CUDI.
- A partir de 2019, se integra el primer equipo de trabajo del CSIRT CUDI para establecer los lineamientos sobre los que debe actuar.
- En 2019, por invitación de WARP *(Warning, Advice and Reporting Point)* de LACNIC y la Universidad Veracruzana se asiste a un taller de creación de un Equipo de Respuesta a Incidentes de Seguridad Cibernéticos.
- En 2019 con el apoyo del CSIRT CEDIA (Ecuador) se dan los primeros pasos para definir la comunidad objetivo, el modelo de organización y la autoridad sobre la que el CSIRT CUDI actuará.

Antecedentes

- ¿Por qué un CSIRT de la RNEI?
  - Infraestructura que conectaba a la mayoría de las universidades mexicanas (apoyada con una iniciativa de gobierno)
  - Malware cruzando por la red académica (Enlaces que de alguna manera se monitoreaban)
  - Ataques y malware circulando en la infraestructura de la propia RNEI (Ataques de DDoS, Escaneos, Phishing, Defacement, entre algunos otros).
  - Apoyo a las Instituciones de Educación Superior (IES) mexicanas en la gestión de incidentes de ciberseguridad.
  - Establecer colaboración y participación de la RNEI y las instituciones mexicanas con CSIRT de otras RNEI.

Antecedentes

- 2020 a 2022 Cambios en el entorno
  - Se termina el apoyo gubernamental para conectividad de las IES mexicanas
  - Inicia pandemia por COVID-19
    - Inicia la transformación de la educación hacia un aprendizaje digitalizado
    - Cambia la forma de tomar las clases
    - Mayor uso de internet
    - Incremento de la superficie de ataque
    - Riesgo mayor de ciberataques
  - Incrementa la inseguridad cibernética
    - Incremento en los ataques hacia el sector educativo (Malware, Phishing, Ransomware)
  - Surgen otros grandes retos de ciberseguridad en las IES

Antecedentes

- 2021 Cambios en la estrategia del CSIRT CUDI
  - Se lleva a cabo un primer ejercicio para conocer el “El estado de la Ciberseguridad en las IES mexicanas”
  - El ejercicio se compuso de dos fases:
    - Cualitativa
      - 3 Focus Group con 20 IES
      - Hablan de “viva voz” sobre los problemas que enfrentan en el trabajo diario
    - Cuantitativa
      - Se invita a 192 universidades
      - Responden la encuesta 171 (90%)
      - 3 secciones
        - Inventario de recursos y actividades de las áreas de ciberseguridad
        - Importancia de la comunicación y participación
        - Principales problemas que enfrentan

Antecedentes

- **Principales resultados Fase Cualitativa**

PROBLEMA	TOP 2 BOX
Inversión en ciberseguridad se ve como gasto	68.8%
Falta de presupuesto	66.4%
Falta de recursos humanos calificados	65.9%
Recursos humanos insuficientes	62.4%
Falta de normativas	45.8%

Presupuestos, recursos humanos y falta de normativas son los problemas más señalados

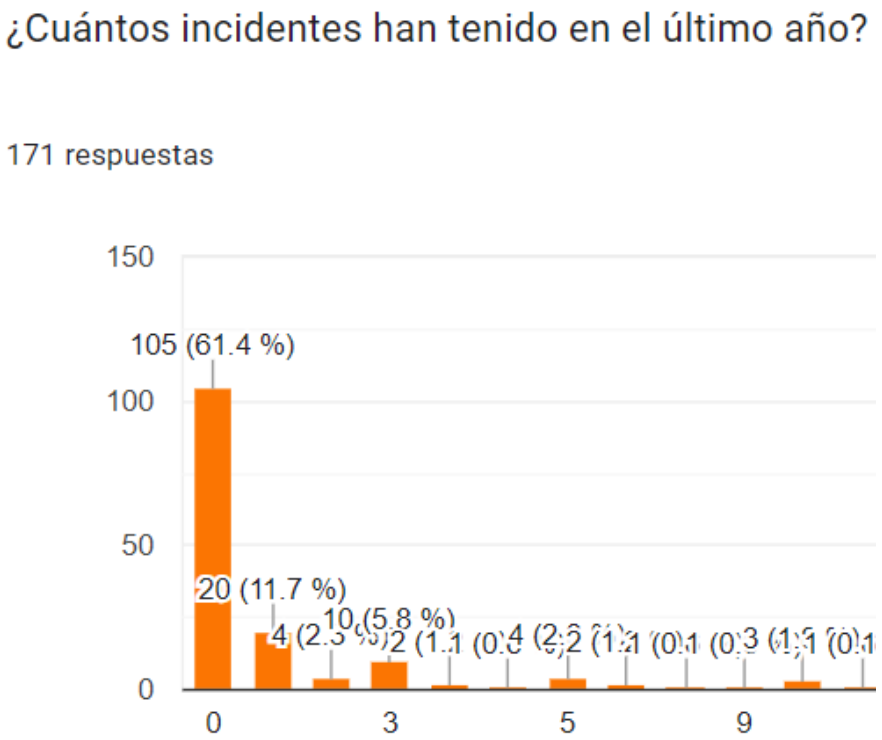
Antecedentes

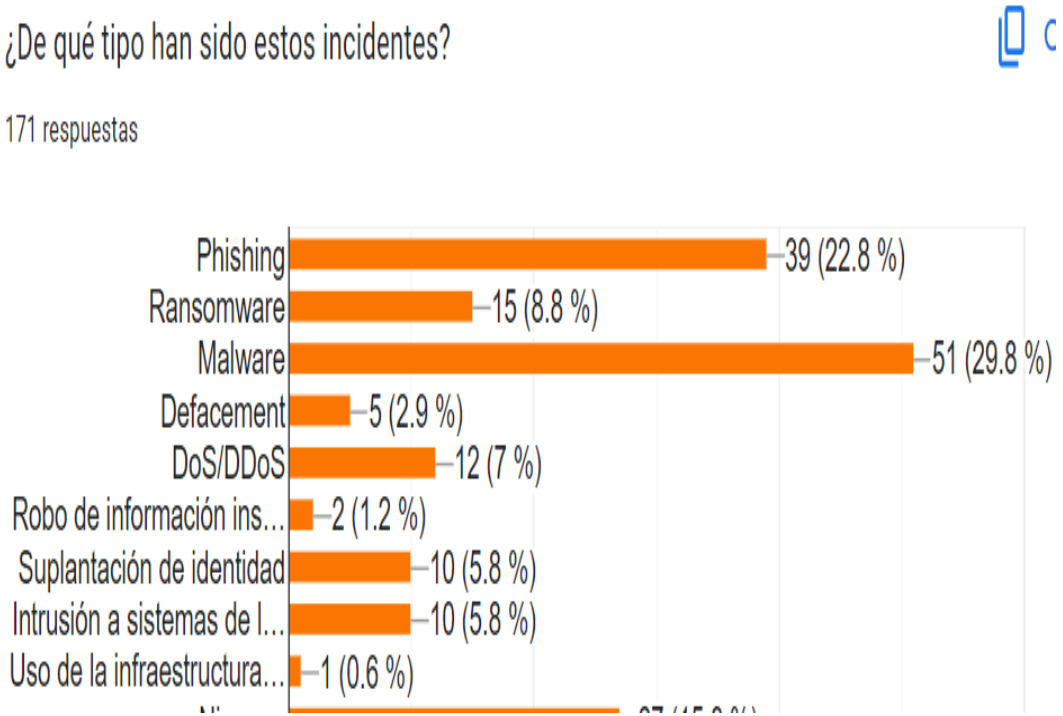
NO (%)	ACTIVIDAD
92.9	Plan de capacitación o certificación en ciberseguridad para directivos
90.0	Plan de capacitación o certificación en ciberseguridad para personal operativo
78.8	Implementado proceso de gestión y manejo de riesgos
75.1	Área de seguridad informática
69.4	Realiza pruebas de penetración al menos una vez al año
65.9	Plan de gestión de riesgos
64.0	Plan/proceso para recuperación de desastres
63.5	Programa de concientización para los usuarios
62.4	Realiza pruebas del código fuente
61.2	Realiza análisis de vulnerabilidad al menos una vez al año
60.6	NOC
57.1	Sistema de gestión de seguridad de la información
54.7	Realiza análisis de riesgo al menos una vez al año
52.4	Sistema de gestión de incidentes
51.2	Políticas de seguridad de la información
47.4	Sistema de seguridad para *endpoint*

- **Principales resultados Fase Cuantitativa**

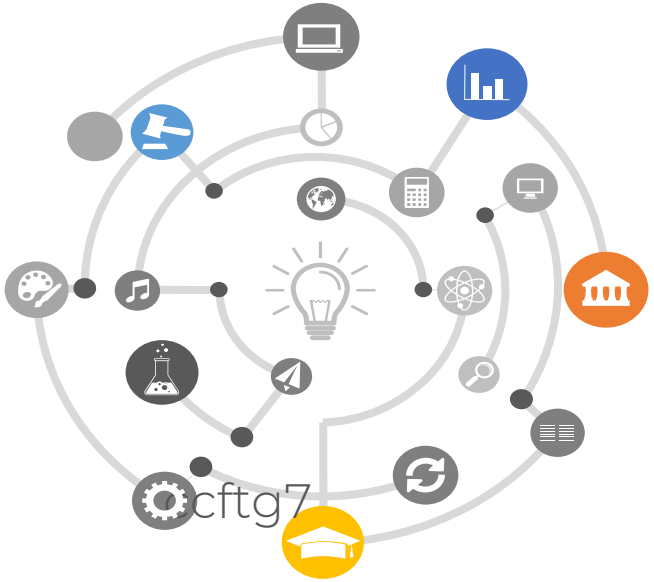
Antecedentes

Incremento en los ataques





Un objetivo más del CSIRT CUDI



- Proporcionar a las instituciones servicios, herramientas y capacitación en ciberseguridad.

Plan de acción

- Para ayudar a las universidades, el CSIRT CUDI diseñó un plan inicial bajo 4 ejes estableciendo líneas estratégicas de acción que contribuyan a la solución de los retos y problemáticas encontradas.

Ejes

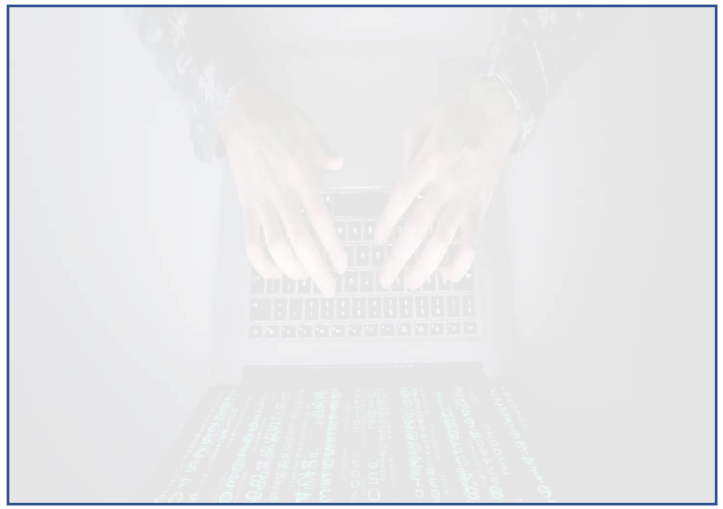
1. Herramientas

2. Formación

3. Servicios

4. Alianzas

Eje 1: Herramientas



Herramientas

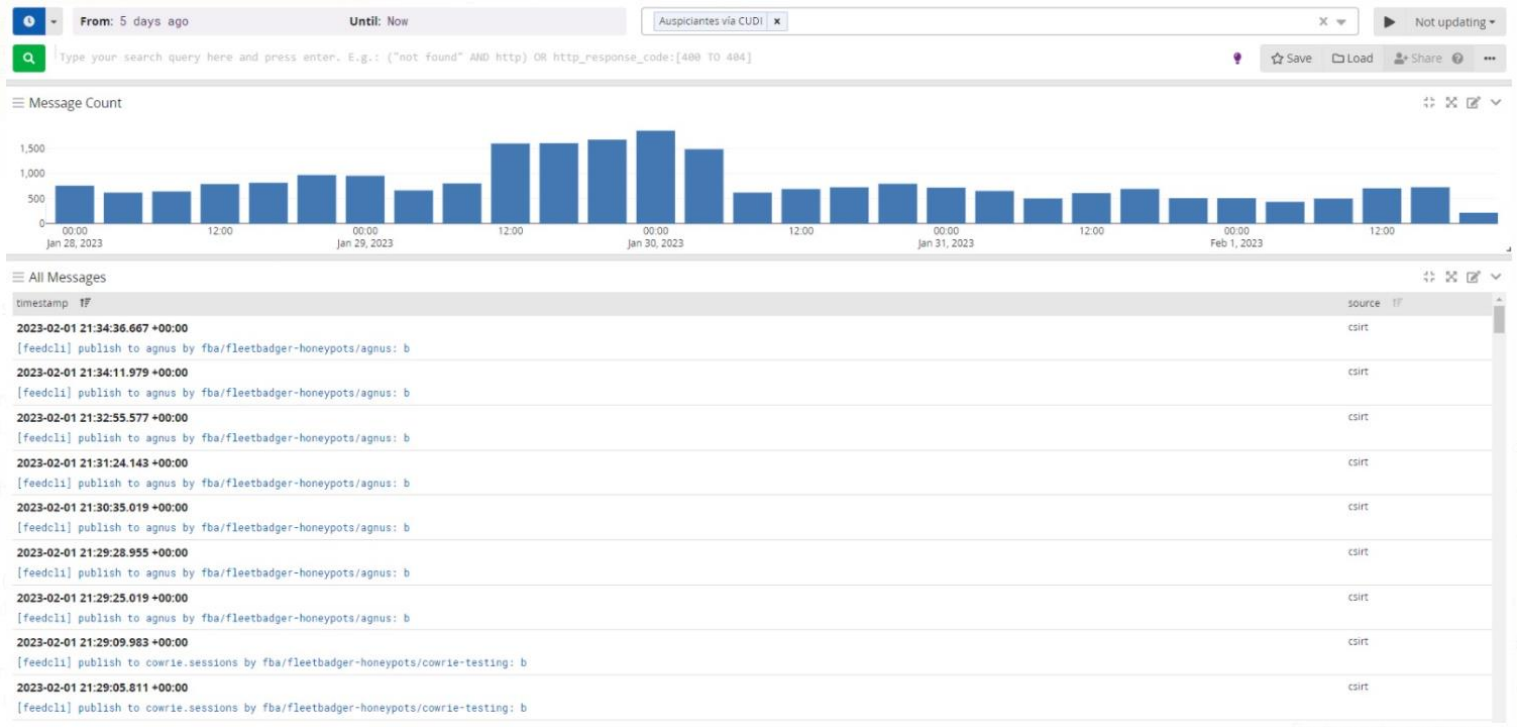
- Descripción y objetivo
  - Desarrollar y proporcionar herramientas (open source) que ayuden a la mitigación de los riesgos cibernéticos inherentes al uso de la infraestructura sobre todo en las instituciones pequeñas y medianas.
- Retos que ayuda a resolver
  - La falta de seguridad perimetral
  - Tener un mecanismo de conexión segura para los usuarios que requieran conectarse a la infraestructura de la institución
  - Contar con soluciones de monitoreo de red
  - Conocer de primera mano la amenazas que están circulando en las redes institucionales del país, y tomar acciones de prevención.

Herramientas

Firewall	Firewall
Antivirus Server	Antivirus para servidores
VPN	Open VPN, eduVPN
Monitoreo de dispositivos red	Nagios, Cacti,
Honeynet	Red Nacional de Sensores Universitarios CUDI

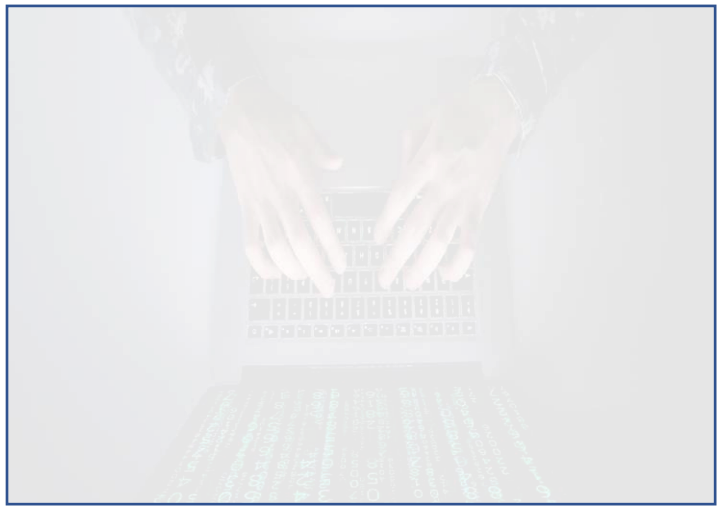
Herramientas

Red Nacional de Sensores Universitarios



- 10 Instituciones en producción
- 2 Instituciones en piloto
- Formación de un grupo de análisis multidisciplinario e interinstitucional
- Shadow Server
- Creciendo…

Eje 2: Formación



Formación

- Descripción y objetivo
  - Apoyar en la consolidación de perfiles especializados en ciberseguridad y redes.
- Retos que ayuda a resolver…
  - Disminuir la escasez de especialistas en ciberseguridad y redes en las áreas operativas y de dirección de TI
  - Falta de personal certificado
  - Falta de conocimiento para implementar modelos correctos de gestión de riesgos, recuperación de desastres, políticas, etc.
  - Que el personal operativo cuente con un mínimo de conocimientos en ciberseguridad y redes
  - Sensibilizar a áreas de TI sobre la importancia de la ciberseguridad
  - Colabora a resolver el problema de las limitaciones presupuestales de la institución para la formación de recursos humanos en ciberseguridad y redes

Formación

Cursos de capacitación de la RNIE

- Monitoreo de red básico e intermedio
- Ruteo básico e intermedio
- Implementación de OpenVPN
- Implementación básica de Sistema de gestión de incidentes (iTop)
- Taller y acompañamiento en la Creación de CSIRT institucionales

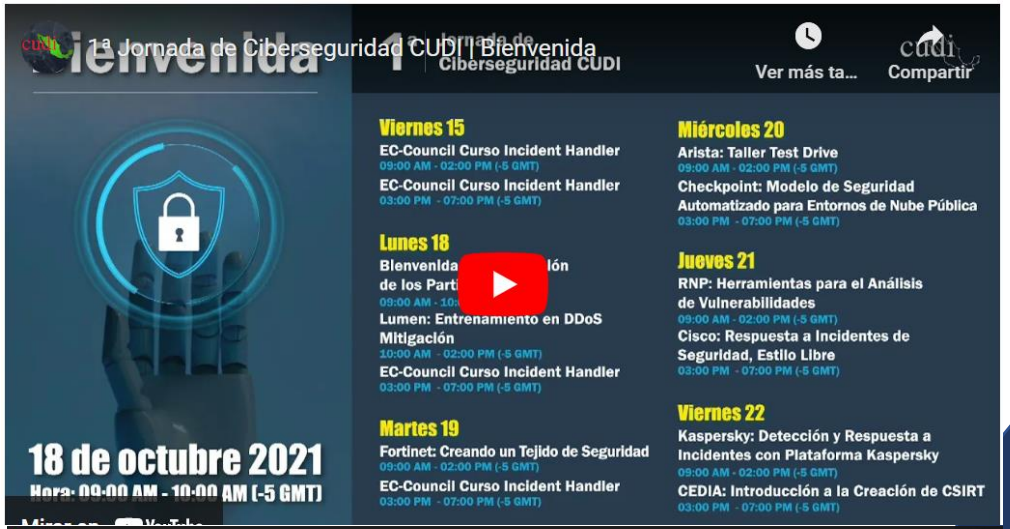
Cursos de certificación

Firmando algunos acuerdos con fabricantes

- Academia EC-COUNCIL
- Academia Fortinet
- Academia Hacking
- Cisco**
- CompTIA**

1ª Jornada de Capacitación en Ciberseguridad

Formación / Capacitación



1ª. Jornada de Capacitación en Ciberseguridad CUDI 2021

Participantes

Más de **350** usuarios de las áreas de ciberseguridad y TI de las IES registrados

245 Asistentes en línea (zoom)

30 Instituciones representadas

Participación de **4** Redes Nacionales de Educación e Investigación de América Latina

Cursos y talleres

9 Talleres o cursos de certificación

Duración

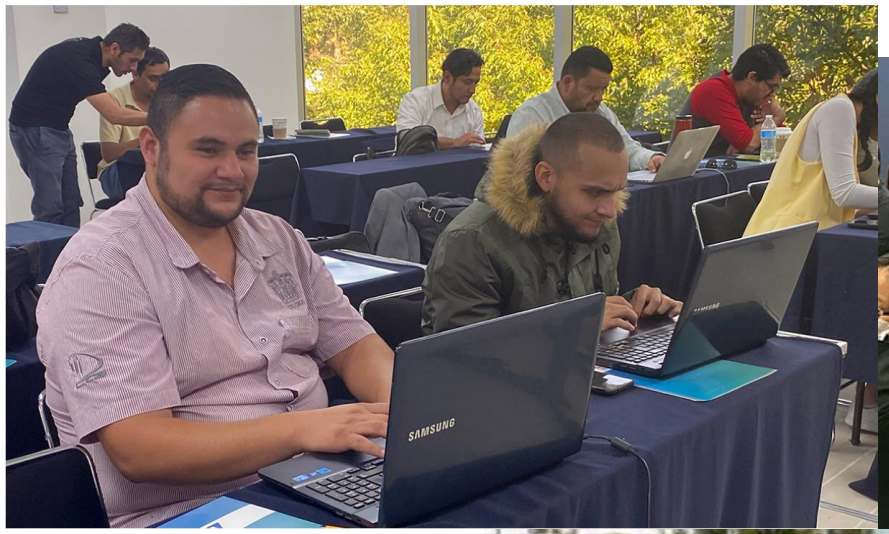
6 Días de capacitación

Un total de **48** Horas de capacitación sobre los temas de tecnologías de la información y la ciberseguridad

2ª Jornada de Capacitación en Ciberseguridad CUDI

Formación / Capacitación

2ª Jornada de Capacitación en Ciberseguridad CUDI 2022



Cursos, talleres y plenarias

22 Talleres o cursos de certificación

5 Sesiones Plenarias

Participantes

Más de **440** asistentes presenciales y por videoconferencia

41 Instituciones representadas

Participación de **5** Redes Nacionales de Educación e Investigación de América Latina y **2** organizaciones

Duración

5 Días de capacitación

Un total de **144** Horas de capacitación en los temas de tecnologías de la información y la ciberseguridad

4ª Jornada de Capacitación en Ciberseguridad CUDI

Formación / Capacitación

4ª Jornada de Capacitación en Ciberseguridad CUDI 2022

Cursos, talleres y plenarias

12 Talleres o cursos de certificación

5 Sesiones Plenarias

Duración

3 Días de capacitación

Un total de **84** Horas de capacitación en los temas de tecnologías de la información y la ciberseguridad

Primer Encuentro de CISOs de las Universidades Mexicanas

10 sesiones con perfil ejecutivo

35 CISOs de las principales universidades

SIGESTIC'23

Formación

Formación de CSIRT Institucionales

- Actualmente colaborando con dos universidades para la formación de su CSIRT Institucional
- Colaborando con la iniciativa del Gobierno Federal en el Área Cibernética para la implementación del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos

Eje 3: Servicios

Servicios

- Descripción y objetivo
  - Poner a disposición de las IES miembros CUDI servicios que ayuden a mantener la operación óptima de las áreas de redes y ciberseguridad
- Retos que ayuda a resolver…
  - Escasez de personal con conocimiento para realizar tareas de análisis de riesgo de ciberseguridad
  - Falta de programas de concientización hacia las comunidades académicas
  - Conectividad para los usuarios móviles.
  - Falta de personal con conocimiento para realizar tareas de diseño y configuración de redes.

Servicios

Análisis de vulnerabilidades

Sesiones de concientización

Análisis de brecha ISO 27000

Despliegue de eduroam

Asesoría para la conectividad
A la Red CUDI

Asesoría técnica de red

Servicios

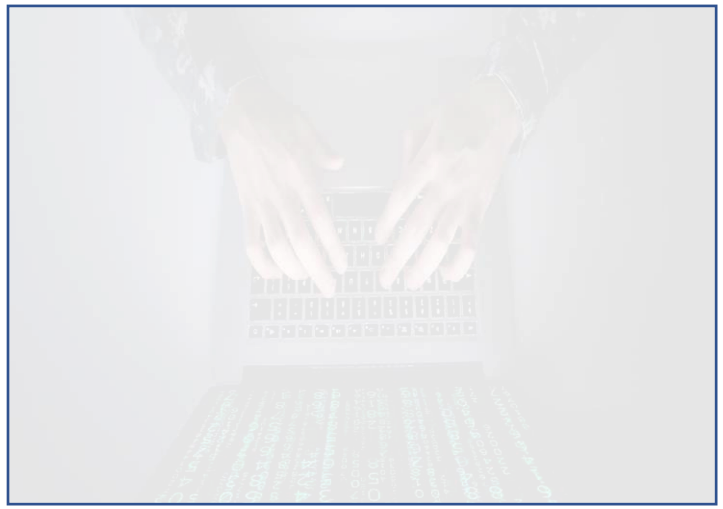
Análisis Vulnerabilidades

Dirección IP	Vulnerabilidades		
	Nivel de Riesgo		
	Alto	Medio	Bajo
	• → 146044-Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 : MySQL vulnerabilities (USN-4716-1) • → 145234-Ubuntu 18.04 LTS / 20.04 LTS / 20.10 : Linux kernel update (USN-4689-4) • → 143431-Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4658-1) • → 144750-Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4679-1)	• → 145007-Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 : Linux kernel vulnerability (USN-4694-1) • → 144944-Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 : tar vulnerabilities (USN-4692-1) • → 144869-Ubuntu 18.04 LTS / 20.04 LTS / 20.10 : Linux kernel vulnerabilities (USN-4689-2)	• → 33851-Network daemons not managed by the package system • → 145463-Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 : Sudo vulnerabilities (USN-4705-1)

Dirección IP	Vulnerabilidad	Analisis	Descripción	Severidad
	146044-Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 : MySQL vulnerabilities (USN-4716-1)	Caja Blanca	Múltiples vulnerabilidades encontradas en MySQL Server y Client, se anexan CVE de las vulnerabilidades encontradas: CVE-CVE-2021-2002 CVE-CVE-2021-2010 CVE-CVE-2021-2011 CVE-CVE-2021-2014 CVE-CVE-2021-2021 CVE-CVE-2021-2022 CVE-CVE-2021-2024 CVE-CVE-2021-2031 CVE-CVE-2021-2032 CVE-CVE-2021-2036 CVE-CVE-2021-2038 CVE-CVE-2021-2046 CVE-CVE-2021-2048 CVE-CVE-2021-2056 CVE-CVE-2021-2058 CVE-CVE-2021-2060 CVE-CVE-2021-2061 CVE-CVE-2021-2065 CVE-CVE-2021-2070 CVE-CVE-2021-2072 CVE-CVE-2021-2076 CVE-CVE-2021-2081 CVE-CVE-2021-2087 CVE-CVE-2021-2088 CVE-CVE-2021-2122 XREF USN:4716-1 Para mayor referencia de las vulnerabilidades, revisar el archivo	Alta
	431-Ubuntu 04 LTS / 20.04 : Linux kernel lnerabilities SN-4658-1)		Para mayor referencia de las vulnerabilidades revisar el archivo "Microscopia_caja_blanca_nbmnzg.pdf" página 9, sección "Description".	
			Múltiples vulnerabilidades encontradas en el Kernel de Linux, se anexan CVE de las vulnerabilidades encontradas: CVE-CVE-2020-0423 CVE-CVE-2020-4788 CVE-CVE-2020-10135 CVE-CVE-2020-14351 CVE-CVE-2020-14390 CVE-CVE-2020-25211 CVE-CVE-2020-25284 CVE-CVE-2020-25643 CVE-CVE-2020-25645 CVE-CVE-2020-25705 CVE-CVE-2020-28915 XREF USN:4658-1 Para mayor referencia de las vulnerabilidades revisar el archivo "Microscopia_caja_blanca_nbmnzg.pdf" página 11, sección "Description".	Alta

Análisis de vulnerabilidades a varias IES miembros CUDI

Eje 4: Alianzas



Alianzas

- Descripción y objetivo
  - Establecer convenios de colaboración con organismos que tengan entre sus fines el promover y fomentar programas que incrementen la ciber-resiliencia de las instituciones.
  - Establecer convenios de colaboración con fabricantes, que permitan obtener soluciones de ciberseguridad en hardware y software, a costos reducidos.
- Retos que ayuda a resolver…
  - Falta de soluciones de ciberseguridad para los endpoints
  - Refuerza las opciones para la implementación de ciberseguridad perimetral
  - Apoya en una mejor utilización del presupuesto de las IES

Eje 4: Alianzas

Organismos, Asociaciones y RNIEs

lacnic csirt
cedia
Internet Society
Red Ciberlac
LAC4 Latin America and Caribbean Cyber Competence Centre
GN
ANUIES - TIC
RedCLARA Cooperación Latino Americana de Redes Avanzadas

Fabricantes

EC-COUNCIL | ACADEMIA PARTNER
FORTINET Training Institute
LUMEN
ARISTA
KASPERSKY lab
cisco

Otras colaboraciones

Grupo Regional de Ciberseguridad de las RNEI de América Latina y el Caribe

eduLACSeg

- 2021 Firma de MOU
  - Miembros iniciales
    - CEDIA, CUDI, RedCLARA, REUNA, RNP
    - Actualmente participan 9 RNEI de los siguientes países: Brasil, Ecuador, Chile, Colombia, México, Costa Rica, Guatemala, Uruguay y Cuba
  - Objetivos
    - Formar un grupo de ciberseguridad regional
    - Establecer colaboración sobre ciberseguridad entre las NRENs y sus IES miembros
    - Desarrollar e implementar líneas de acción que contribuyan al desarrollo de un ecosistema de ciberseguridad en la región

Otras colaboraciones

Grupo Regional de Ciberseguridad de las RNEI de América Latina y el Caribe

- A partir del año 2020, tracks de ciberseguridad en encuentros TICAL
- Encuesta Regional del Estado de la Ciberseguridad en las IES
- eduLACSoc, proyecto formación de SOC's para las RNEI de LAC

eduLACSeg


merci
obrigado
danke
teşekkür ederim
sagolun
sukriya
hvala
gracias
taiku
arigato
terima kasih
ngiyabonga
grazie
mauruuru
kop khun krap
dakujem
go raibh maith agat
bedankt
dank je
tapadh leat

¿?