

LUNES 4 DE JUNIO
FOROS DE DISCUSIÓN - AUDITORIO

08:00 - 09:00	REGISTRO	
09:00 - 09:30	Sesión Bienvenida	
	Ministerio de Modernización	
	UNLP	
	Unión Internacional de Telecomunicaciones	Pablo Palacios
09:30 - 09:35	FOTO GENERAL Y CORTA PAUSA	
09:35 - 10:50	Sesión Concienciación	
	Ciberseguridad toma de decisiones: Infraestructura Crítica	ITC – Eduardo Cardozo
10:50 - 11:20	Positive Technologies Security - Dan Tara	
	Mitos y realidades sobre seguridad en redes SS7/LTE. Ataques en Infraestructura Nacional Crítica a través de portadores móviles.	
11:20 - 11:40	PAUSA CAFÉ	
11:40 - 13:00	Mesa de Discusión: Ciberseguridad en el sector Público	
	Moderador: UNLP	
	Ministerio de Modernización	Hugo Miguel
	Secretario de País Digital	Raúl Martínez
	Ministerio de Defensa	Alfredo Parodi
	Ministerio de Seguridad	Pablo Lázaro
	ISOC	Shernon Osepa
13:00 - 14:00	PAUSA ALMUERZO	
14:00 - 15:30	Mesa de Discusión: Ciberseguridad en el sector Privado y Financiero	
	Modeador: ITC	
	Banco de la Nación Argentina	Fernando Marson
	Banco Central de la Nación Argentina	Gustavo Pereyra
	Banco Central de la Nación Argentina	Marcela Pallero
	International Telecommunications Union	Marwan Ben Rached
15:30 - 16:00	PAUSA CAFÉ	
16:00 - 17:00	Mesa de Discusión: La Academia y la Ciberseguridad	
	Moderador: Secretaría País Digital	
	Universidad Nacional de La Plata	Javier Díaz
	Universidad de Buenos Aires	Raúl Saroka
	ITC Uruguay	Eduardo Carozo
17:00 - 17:30	SESIÓN DE CLAUSURA	
	Ministerio de Modernización	
	UNLP	
	Unión Internacional de Telecomunicaciones	Pablo Palacios
19:00 - 21:00	ACTIVIDAD SOCIAL: Cocktail en Senado de la Provincia de Buenos Aires	

MARTES 5 DE JUNIO
CHARLAS TÉCNICAS - SALA 1

Capacidad: 30 a 50 personas

08:00 - 09:00	REGISTRO
09:00 - 10:30	Charla Técnica 1: Positive Technologies Security - Dmitry Kurbatov & Dan Tara
	Workshop sobre seguridad en señalización & Demo en vivo de ataques en redes SS7 – Historia y Desarrollo de redes de señalización (SS7/Diameter/GTP)
10:30 - 11:00	PAUSA CAFÉ
11:00 - 13:00	Charla Técnica 2: Positive Technologies Security - Dmitry Kurbatov & Dan Tara
	Workshop sobre seguridad en señalización & Demo en vivo de ataques en redes SS7 – Construyendo procesos de seguridad de señalización a escala completa en operadores y la regulación requerida para apoyarlo
	DEMO
13:00 - 14:00	PAUSA ALMUERZO
14:00 - 15:30	Charla Técnica 3: CYBR Score Comtech Telecommunications
	Análisis Ciber Defensa (CDA) y Laboratorio: Análisis de Protocolo (CDA); Detección de Intrusiones (CDA); Metodología de Manejo de Incidentes (CDA); Análisis de Defensa de la Red (CDA); Análisis de Ataque de Red (CDA); Colección Inteligente de Información Gathering (VAM); Ataque (VAM); Defensa (VAM).
15:30 - 16:00	PAUSA CAFÉ
16:00 - 17:30	Charla Técnica 4: CYBR Score Comtech Telecommunications
	Análisis Ciber Defensa (CDA) y Laboratorio: Análisis de Protocolo (CDA); Detección de Intrusiones (CDA); Metodología de Manejo de Incidentes (CDA); Análisis de Defensa de la Red (CDA); Análisis de Ataque de Red (CDA); Colección Inteligentes de Información Gathering (VAM); Ataque (VAM); Defensa (VAM).

MARTES 5 DE JUNIO
CHARLAS TÉCNICAS - SALA 2

Capacidad: 30 a 50 personas

08:00 - 09:00	REGISTRO
09:00 - 10:30	Charla Técnica 5: ITC Uruguay – Eduardo Carozo & Leonardo Vidal
	Ciberseguridad en Internet de las Cosas
10:30 - 11:00	PAUSA CAFÉ
11:00 - 12:30	Charla Técnica 6: ITC Uruguay – Eduardo Carozo & Leonardo Vidal
	Ciberseguridad y Ciudades Inteligentes
12:30 - 14:00	PAUSA ALMUERZO
14:00 - 15:30	Charla Técnica 7: Silensec - Almerindo Graziano
	Threat Intelligence
15:30 - 16:00	PAUSA CAFÉ
16:00 - 17:30	Charla Técnica 8: International Telecommunication Union - Marwan Ben Rached
	Ciberseguridad en Sistemas Financieros
17:30 - 18:30	SOLO PARA LOS EQUIPOS QUE PARTICIPAN EN EL CYBERDRILL
	Sesión preparatoria: CyberServices - Csaba Virág
	Sesión preparatoria para el CyberDrill

MARTES 5 DE JUNIO
CAPACITACIÓN TÉCNICA - FIRST - SALA 3

Título: Building threat Intel pipelines.

Nivel del Curso: Intermedio.

Experto: Paweł Pawliński – CERT Polonia.

Capacidad: 30 personas.

Paweł Pawliński es un especialista principal del CERT.PL. Su experiencia laboral incluye análisis de datos, trazo de amenazas y automatización. Es responsable del diseño e implementación de la plataforma n6 para compartir datos relacionados con ciberseguridad y por el diseño de sistemas a gran escala para monitoreo de ataques en Internet. Paweł es autor de publicaciones y capacitaciones enfocadas en la colección, análisis e intercambio de información de los CSIRTs.

Pre-requisitos:

1. Los participantes deben estar familiarizados con aspectos operacionales de un CSIRTs/SOCs incluyendo manejo, análisis y mitigación de incidentes. En particular, es crucial, un buen entendimiento de IoCs y otro tipo de información usado para defensa de redes.
2. Requerimientos de Software/hardware: Laptop, detalles TBA.

Abstracto:

El curso cubre diseño de procesos para manejar efectivamente una variedad de información útil para operaciones de seguridad. Los participantes aprenderán cómo seleccionar fuentes de información y cómo procesarla para obtener conclusiones. Se explicarán problemas relacionados con la evaluación, colección, análisis e intercambio de información. La capacitación incluye ejercicios prácticos en los cuales se presentarán varias herramientas de software libre para manejo de amenazas inteligentes y datos relacionados con incidentes.

08:00 – 09:00	REGISTRO
09:00 - 10:30	Charla Técnica 9: Introducción a los conceptos principales
10:30 - 11:00	PAUSA CAFÉ
11:00 - 12:30	Charla Técnica 10: Evaluación de fuentes de información, colección, preparación y almacenamiento de datos
12:30 - 14:00	PAUSA ALMUERZO
14:00 - 15:30	Charla Técnica 11: Toolset showcase - MISP, IntelMQ, The Hive
15:30 - 16:00	PAUSA CAFÉ
16:00 - 17:30	Charla Técnica 12: Toolset showcase - MISP, IntelMQ, The Hive

MARTES 5 DE JUNIO
CHILD ONLINE PROTECTION y CHARLAS TÉCNICAS - SALA 4

Capacidad: 50 a 80 Personas

CONCIENCIACIÓN A LA JUVENTUD SOBRE CHILD ONLINE PROTECTION	
08:00 – 09:00	REGISTRO
09:00 - 12:00	UNLP Manejo de Redes Sociales y Cyberbullying. Experiencias
	ICMEC - Pilar Ramirez Pornografía infantil, grooming, sexting y sextorsion, definiciones y aspectos legales
	Ministerio Modernización El Gobierno y sus acciones ³⁰
	Fundación REDES Violencia Digital
	UIT - Pablo Palacios Programa "Child Online Protection" - Consideraciones Generales
13:00 – 14:00	REGISTRO
14:00 - 15:30	Charla Técnica 13: ADACSI
	Gobierno y gestión de la Seguridad: Normas, estándares y buenas prácticas en Ciberseguridad
15:30 - 16:00	PAUSA CAFÉ
16:00 - 17:30	Charla Técnica 14: Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires – CAPA8 - (TBC)
	Gobierno y gestión de la Seguridad: El rol de los profesionales en la Ciberseguridad

MIÉRCOLES 6 DE JUNIO
CHARLAS TÉCNICAS - SALA 1

Capacidad: 30 a 50 personas

08:00 – 09:00	REGISTRO
09:00 - 10:30	Charla Técnica 15: Kaspersky - Andres Giarletta
	Parqueo de Capa 8
10:30 - 11:00	PAUSA CAFÉ
11:00 - 12:30	Charla Técnica 16: Kaspersky - Santiago Pontirolli
	Amenazas locales, problema global. Argentina y el panorama de amenazas actual - presentando con un enfoque local y las amenazas que afectan a Argentina y América Latina
12:30 - 14:00	PAUSA ALMUERZO
14:00 - 15:30	Charla Técnica 17: Deloitte - Julio Ardita
	Ataques a empresas desarrolladoras de aplicaciones de pago
15:30 - 16:00	PAUSA CAFÉ
16:00 - 17:30	Charla Técnica 18: Deloitte - Julio Ardita
	Ciber-Resiliencia en Organizaciones
18:00 - 20:00	ACTIVIDAD SOCIAL: Visita al Planetario UNLP

MIÉRCOLES 6 DE JUNIO
CHARLAS TÉCNICAS - SALA 2

Capacidad: 30 a 50 personas

08:00 - 09:00	REGISTRO
09:00 - 10:30	Charla Técnica 19: CyberServices , Csaba Virág
	Respuesta ante incidentes Ransomware
10:30 - 11:00	PAUSA CAFÉ
11:00 - 12:30	Charla Técnica 20: Marwan Ben Rached – Unión Internacional de Telecomunicaciones
	Detección proactiva de Incidentes de Ciberseguridad – Honeypots / Construir un CIRT basado en herramientas de software libre
12:30 - 14:00	PAUSA ALMUERZO
14:00 - 15:30	Charla Técnica 21: ISOC Cybersecurity SIG - Julio Balderrama
	Asegurando las infraestructuras críticas, el gran desafío
15:30 - 16:00	PAUSA CAFÉ
16:00 - 17:30	Charla Técnica 22: VHGroup - Emiliano Piscitelli
	Ingeniería Social - Hacking & Hardening HumanOS
18:00 - 20:00	ACTIVIDAD SOCIAL: Visita al Planetario UNLP

MIÉRCOLES 6 DE JUNIO
CAPACITACIÓN TÉCNICA - FIRST - SALA 3

Título: Building threat Intel pipelines.

Nivel del Curso: Intermedio.

Experto: Paweł Pawliński – CERT Polonia.

Paweł Pawliński es un especialista principal del CERT.PL. Su experiencia laboral incluye análisis de datos, trazo de amenazas y automatización. Es responsable del diseño e implementación de la plataforma n6 para compartir datos relacionados con ciberseguridad y por el diseño de sistemas a gran escala para monitoreo de ataques en Internet. Paweł es autor de publicaciones y capacitaciones enfocadas en la colección, análisis e intercambio de información de los CSIRTS.

Capacidad: 30 personas.

Pre-requisitos:

1. Los participantes deben estar familiarizados con aspectos operacionales de un CSIRTS/SOCs incluyendo manejo, análisis y mitigación de incidentes. En particular, es crucial, un buen entendimiento de IoCsy otro tipo de información usado para defensa de redes.
2. Requerimientos de Software/hardware: Laptop, detalles TBA.

Abstracto:

El curso cubre diseño de procesos para manejar efectivamente una variedad de información útil para operaciones de seguridad. Los participantes aprenderán cómo seleccionar fuentes de información y cómo procesarla para obtener conclusiones. Se explicarán problemas relacionados con la evaluación, colección, análisis e intercambio de información. La capacitación incluye ejercicios prácticos en los cuales se presentarán varias herramientas de software libre para manejo de amenazas inteligentes y datos relacionados con incidentes.

08:00 – 09:00	REGISTRO
09:00 - 10:30	Charla Técnica 23: Análisis de datos incluyendo fusión de información de múltiples fuentes
10:30 - 11:00	PAUSA CAFÉ
11:00 - 12:30	Charla Técnica 24: Aspectos prácticos de intercambio de información
12:30 - 14:00	PAUSA ALMUERZO
14:00 - 15:30	Charla Técnica 25: Tareas típicas de automatización usando software libre
15:30 - 16:00	PAUSA CAFÉ
16:00 - 17:30	Charla Técnica 26: Tareas típicas de automatización usando software libre
18:00 - 20:00	ACTIVIDAD SOCIAL: Visita al Planetario UNLP

MIÉRCOLES 6 DE JUNIO

CHARLAS TÉCNICAS- ISOC - SALA 4

Capacidad: 30 a 50 personas

08:00 - 09:00	REGISTRO
09:00 - 10:30	Charla Técnica 27: ISOC
	Trabajo de ISOC en Ciberseguridad, proyectos en la Región
10:30 - 11:00	PAUSA CAFÉ
11:00 - 12:30	Charla Técnica 28: ISOC
	Ciberseguridad en Internet de las Cosas
12:30 - 14:00	PAUSA ALMUERZO
14:00 - 15:30	Charla Técnica 29: ISOC
	Acuerdo mutuo sobre Normas y Seguridad en Ruteo
15:30 - 16:00	PAUSA CAFÉ
16:00 - 17:30	Charla Técnica 30: ISOC
	Seguridad en Comunidad de Redes inalámbricas
18:00 - 20:00	ACTIVIDAD SOCIAL: Visita al Planetario UNLP

JUEVES 7 DE JUNIO

CYBERDRILL

Capacidad: 60 personas

Distribución de la Sala: Distribución en forma de "U"

Escenarios Técnicos:

1. Unión Internacional de Telecomunicaciones;
2. Silensec;
3. CyberServices;
4. Universidad Nacional de La Plata;
5. Comtechtel (CyberScore).

Escenarios Gerenciales:

6. Kaspersky;
7. Deloitte.

08:00 - 08:30	REGISTRO
08:30 - 09:00	Introducción: International Telecommunications Union - Pablo Palacios / Marwan Ben Rached
	Introducción a los escenarios para Cyberdrill
09:00 - 10:30	Escenario 1: Silensec - Almerindo Graziano
	Threat intelligence utilizando reglas YARA
10:00 - 11:00	PAUSA CAFÉ
11:30 - 12:30	Escenario 2: Universidad Nacional de La Plata - Einar Felipe Lanfranco
	Analysis of a cryptocurrency mining malware
12:30 - 13:30	PAUSA ALMUERZO
13:30 - 15:00	Escenario 3: International Telecommunications Union – Marwan Ben Rached
	Simulación de Negocios para un banco grande con sucursales, negocios B2B y su propia red ATM. Kaspersky Interactive Protection Simulation (KIPS)
15:00 - 15:30	PAUSA CAFÉ
15:30 - 18:00	Escenario 4: Kaspersky
	Simulación de Negocios para un banco grande con sucursales, negocios B2B y su propia red ATM. Kaspersky Interactive Protection Simulation (KIPS)
18:00 - 21:00	ACTIVIDAD SOCIAL

VIERNES 8 DE JUNIO
CYBERDRILL

Capacidad: 60 personas

Distribución de la Sala: Distribución en forma de “U”

Empresas Expertas Participantes:

Escenarios Técnicos:

1. Unión Internacional de Telecomunicaciones;
2. Silensec;
3. CyberServices;
4. Universidad Nacional de La Plata;
5. Comtechtel (CyberScore).

Escenarios Gerenciales:

6. Kaspersky;
7. Deloitte.

09:00 - 11:00	Escenario 5: CyberServices – Csaba Virág
	Análisis Ransomware
11:00 - 11:30	PAUSA CAFÉ
11:30 - 13:00	Escenario 6: Deloitte - Francesco Binaschi
	Manejo de Ciber Crisis
13:00 - 14:00	PAUSA ALMUERZO
14:00 - 16:30	Escenario 7: Comtech Telecommunications Corp - Alan Gush & Phillip Stoner
	CTF Challenge
16:30 - 17:00	Sesión de Cierre
17:00 - 17:30	PAUSA CAFÉ
