

## BIO PABLO ROMANOS



Pablo Romanos es Ingeniero graduado por la Universidad de la Marina Mercante, y posgraduado por la Universidad Politécnica de Madrid (España) como "Esp. Redes, Aplicaciones y Servicios". También posee un MBA otorgado por la Universidad Abierta Interamericana y ha cursado el Programa Ejecutivo "Cybersecurity Leadership and Strategy" otorgado por la OEA y la Universidad Internacional de Florida (EEUU).

Es Director de la Diplomatura en Gestión de Ciberseguridad e Inteligencia para Smartcities, docente de Posgrado en Ciberseguridad en la Universidad UCEMA, Miembro del Comité Académico y docente en la Maestría en Ciberdefensa de la Universidad del Ejército, y docente en las Maestrías TIC y CIO en UADE.

Participa como miembro activo de los comités IRAM y es miembro del grupo de Expertos ISO Internacional. También ha formado parte de la Comisión Directiva de Cloud Security Alliance Argentina; miembro de ISSA Argentina y ha sido organizador de numerosas ediciones del OWASP Latam Tour.

En el ámbito de la investigación académica lidera proyectos de IoT, Robótica y Ciberseguridad. Es fundador de CROZONO, herramienta diseñada para conducir investigaciones haciendo uso de drones y robots para alcanzar el objetivo.

Desempeña su carrera profesional como especialista del Centro de Ciberseguridad (BA-CSIRT) y ha sido Gerente de Ciberseguridad de los Juegos Olímpicos de la Juventud - Buenos Aires 2018.

Ha sido orador en importantes conferencias de tecnología nacionales e internacionales como Black Hat Londres 2016, Ekoparty Security Conference 2015, 8dot8 2018, SEGURINFO, OWASP Latam Tour, ISO, IRAM e IEEE, entre otras.

<https://www.linkedin.com/in/pablormanos/>

@pablormanos



DESDE 2004 DEDICADOS A ASESORAR A INDIVIDUOS Y EMPRESAS EN DELITOS INFORMATICOS Y PROTECCIÓN DE DATOS  
Contacto: [info@identidadrobada.com](mailto:info@identidadrobada.com)

Home / Noticias / Pablo Romanos, fundador del proyecto CROZONO: "La ciberseguridad ha ido tomando gran relevancia con la gestión actual de gobierno"

## Pablo Romanos, fundador del proyecto CROZONO: "La ciberseguridad ha ido tomando gran relevancia con la gestión actual de gobierno"



El ingeniero electrónico Pablo Romanos, fundador del proyecto Crozono, un framework diseñado para ejecutarse en vehículos aéreos no tripulados (UAVs, drones en general), robots y prototipos comandados a distancia, con el objetivo de acceder a una red interna y adquirir evidencia forense relevante para una investigación judicial, dijo que la ciberseguridad "ha ido tomando relevancia en estos últimos años con la gestión actual de gobierno".

Investigador y Docente de BADE, Maestría TIC (Tecnología Informática y de Comunicaciones) y Maestría CIO (Dirección Estratégica de la Información), Pablo Romanos es Responsable de Planificación del Centro de Ciberseguridad (BA-CSIRT), y miembro del comité de ciberseguridad para los Juegos Olímpicos Buenos Aires 2018.



Ayudanos a convertir un error en la oportunidad de una familia. Dona tu página de Error 404



"Hace un tiempo que Argentina viene trabajando en temas de ciberseguridad, desde la creación en noviembre de 2016 del Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires con foco en la atención de ciberincidentes que afectan a los ciudadanos", expresó Romanos en la entrevista concedida a Ciberseguridad LATAM.



### ¿Cómo nace el proyecto CROZONO y cuál es su objetivo?

CROZONO nace a partir de un proyecto de investigación académica en la Facultad de Ingeniería de la Universidad de la Marina Mercante, con el objetivo de demostrar cuál es el comportamiento de los mecanismos de defensa perimetral frente a situaciones extremas.

Subscribe al Newsletter

Name:   
Email:

Subscribe



ÚLTIMO



El enorme ataque criptográfico a los routers de Cisco GP, se...



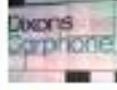
Capela: caso real de distribución de pornografía infantil por WhatsApp



Ciberdelincuentes infectan más de 200.000 routers Mikrotik con malware de Crypto...



Seguridad en dispositivos IoT: ¿cómo garantizarla?



La relación de datos de Google Carphone de 2017 fue peor...





Alerta para empresas y usuarios particulares de Internet

# Prueban que desde un drone se puede hackear una red Wi-Fi

Lo explicaron expertos en el marco de la cumbre de seguridad digital Ekoparty, que se desarrolla en el Konex.

Marcelo Bellucci  
mbellucci@clarin.com

Al traspasar el umbral del Centro Cultural Konex para ingresar a la tierra de la Ekoparty, las reglas sociales y los formalismos pierden vigencia. No es necesario saludar o ser simpático. Todos están atentos a su pantalla y no quieren saber qué está haciendo su vecino. Este encuentro anual reúne a consultores, programadores, técnicos, administradores de sistemas, nerds, curiosos y entusiastas de la tecnología que van allí para conocer los hallazgos más importantes en el ámbito de la seguridad informática.

En total, los casi 3.000 asistentes ocuparán las tres jornadas (tierra mañana) en alguna de las 22 charlas, 12 workshops o visitando los puestos de demostración de 22 sponsors. Entre las propuestas más atractivas se explica cómo aprovechar los drones para hackear, las fallas que expone el voto electrónico y la vulnerabilidad en sistemas de actualización de sistemas.

Como una regla no escrita, la primer recomendación que recibe el visitante es que "no se te ocurra conectarte al Wi-Fi, acá todos están haciendo pruebas y si encuentran un desperfecto, se van a divertir un rato. Si tenés un teléfono, lo mejor es dejarlo en modo avión".

Para demostrar que el ingenio combinado con la capacidad técnica puede lograr maravillas, Pablo Romanos, ingeniero en Electrónica, graduado de la Universidad de la Marína Mercante y Sheila Berta, una joven autodidacta de 20 años, adelantaron a Clarín la charla que presentarán mañana sobre cómo aprovechar drones o robots para penetrar en espacios inaccesibles.

"Nuestro primer desafío fue meter una computadora dentro de un cuadricóptero reducido. La solución fue recurrir a una Raspberry Pi, que es una PC reducida a una sola placa. Pero había más. Como el drone opera en la misma frecuencia que el Wi-Fi, al estar en el aire se producía interferencia y no lo podíamos controlar. Entonces, para alcanzar un piso 20, se nos ocurrió que lo podíamos hacer aterrizar y recién allí activar la conexión", explica Romanos.

Una vez que el drone quedó



Pericias. Especialistas y entusiastas ayer en Ekoparty, probando errores en sistemas informáticos. MAXIMILLA



Sheila Berta y Pablo Romanos. Exponen mañana en la cumbre hacker.



El día que llegó el futuro

Una réplica del DeLorean, el auto del filme Volver al Futuro 2, desfiló ayer por las calles de Telcío. En la película transcurre el año 1985, y los protagonistas viajan al futuro adelantándose a su tiempo 30 años, exactamente al 21 de octubre de 2015.

apoyado en un techo, la pregunta que se hicieron es: ¿Cómo meterse a la red de una empresa, sin teclado para controlarlo? "Desarrollamos un soft inteligente llamado Crozono que incorpora todos los ataques conocidos y de acuerdo a la protección de la red, decide la mejor opción. Si no funciona prueba otra, así hasta que rompa la defensa. Una vez que lo consigas, te abre la puerta para que puedas acceder desde tu ubicación remota", explica Berta. Esta operación, si los sistemas de seguridad son muy estrictos, puede tardar 15 minutos. Mientras que la autonomía del drone es de 20. Alcanzada esta marca, el aparato vuelve en forma automática hasta el punto de partida. Dicen que Crozono podría ser usado por la Policía para investigar pedófilos o acosaciones virtuales.

Coincidiendo con la fecha que Marty McFly llegó desde el pasado en la segunda parte de "Volver al Futuro", el logo de este año es Ekoparty: Back to Roots (volver a las raíces) con la tipografía del filme.

Otro de los que estuvo dando charlas fue Ondrej Vitek, jefe de operaciones de Avast, una empresa de seguridad que tiene 230 millones de usuarios en todo el mundo. "Las redes Wi-Fi, por su gran popularidad, son el centro de ataques de muchos delincuentes. El núcleo de este problema no son las redes sino los routers, que son fáciles de vulnerar y nadie se preocupa de mejorarlos. Pocos usuarios ingresan al soft de configuración y eso es algo que aprovechan quienes planean un ataque. Al controlar el router, pueden tomar posesión de los aparatos que se conectan a la red y también de la PC", concluye. ■



**INNOVACIÓN**

## CON DRONES EN ESCENA Y GRAN PARTICIPACIÓN, TERMINA HOY LA CUMBRE HACKER EN BUENOS AIRES

Es Etoparty, la conferencia que reúne a especialistas en seguridad informática de todo el mundo. Participaron más de 2.000 personas en el Centro Kones. Cómo hackear una red Wi-Fi con drones y la vulnerabilidad de la bolsa electrónica fueron algunos de los platos fuertes.

**Perfiles.** Especialistas y entusiastas ayer, en Etoparty, probando ensayos en sistemas informáticos, más fallas

14.5. Deiana Kles, Sergio, Etoparty, Hacker



Se está llevando a cabo hoy el tercer y último día de Etoparty, la cumbre internacional de expertos en seguridad informática, que ya se convirtió en una tradición de octubre en Buenos Aires. Este año participaron más de 2.000 personas en el Centro Cultural Kones. Los platos fuertes del evento fueron la charla en que se mostró cómo se puede usar drones para ingresar en áreas Wi-Fi, los casos de ciberterrorismo que recibe Corea del Sur desde sus vecinos del Norte, y cómo romper el sistema de bolsa electrónica usado en la Argentina.

Hay saltaron al escenario Pablo Romanos, ingeniero en Electrónica graduado de la Universidad de la Marina Mercante y Sheila Berta, una joven autodidacta de 29 años, que mostraron, en vivo, cómo se puede aprovechar drones o robots para penetrar en espacios inaccesibles.



Sheila Berta y Pablo Romanos. Expusieron en la cumbre hacker.

"Nuestro primer desafío fue meter una computadora dentro de un cuadricóptero reducido. La solución fue recurrir a una Raspberry Pi, que es una PC reducida a una sola placa. Pero había más. Como el dron opera en la misma frecuencia que el Wi-Fi, al estar en el aire se producía interferencia y no lo podíamos controlar. Entonces, para alcanzar un piso 20, se nos ocurrió que lo podíamos hacer aterrizar y recién allí activar la conexión", explicó Romanos a Next.

[http://next.clarin.com/innovacion/escenario-participacion-termina-buenos-aires\\_0\\_1454254848.html](http://next.clarin.com/innovacion/escenario-participacion-termina-buenos-aires_0_1454254848.html)



**ekoparty** @ekoparty [Seguir](#)

Ya terminó la charla de @pabloromanos y @SheilaBerta de la #Etoparty. ¡Gracias!

12:44 - 23 oct 2015

Una vez que el dron quedó apoyado en un techo, la pregunta que se hicieron es ¿Cómo meterlo a la red de una empresa, sin teclado para controlarlo? "Desarrollamos un soft inteligente llamado Crezono que incorpora todos los ataques conocidos y de acuerdo a la protección de la red, decide la mejor opción. Si no funciona prueba otra, así hasta que rompe la defensa. Una vez que lo consigue, se abre la puerta para que puedas acceder desde tu ubicación remota", agregó Berta.

Esta operación, si los sistemas de seguridad son muy estrictos, puede tardar 15 minutos. Mientras que la autonomía del dron es de 20. Alcanzada esta marca, el aparato vuela en forma automática hasta el punto de partida. Dicen que Crezono podría ser usado por la Policía para investigar pedófilos o accedidos virtuales.

**MEDIOS DE COMUNICACIÓN**

Nota Canal 9 – “Peligros de las Redes Sociales” Oct. 2013



<https://www.youtube.com/watch?v=50oDZxrn-w4>

Telenuvee “Cómo evitar el robo de claves” Feb. 2014.



<https://www.youtube.com/watch?v=W7bRXPgp64>

Nota Telenuvee “Drones en busca de pedófilos” Proyecto CROZONO. Ene.2016.



[https://www.youtube.com/watch?v=4\\_LuCJOusoE&t=83s](https://www.youtube.com/watch?v=4_LuCJOusoE&t=83s)

Nota C5N “Drones espías para combatir delito informático” Proyecto CROZONO. Mar.2016.



<https://www.youtube.com/watch?v=EbdWMCp1Ao>

Pablo Romanos, Especialista del Centro de Ciberseguridad BA-CSIRT del GCABA. Canal A24 - May 2017.



<https://www.youtube.com/watch?v=H7Gh61vRoWM&t=>

Evento IRAM "Día Mundial de la Normalización" Pablo Romanos Especialista en Ciberseguridad. Oct.2017



<https://www.youtube.com/watch?v=QallZjPT26I&t=>

Pablo Romanos, Especialista del Centro de Ciberseguridad BA-CSIRT del GCABA. Canal Metro - Abril 2018.



[https://www.youtube.com/watch?v=wp\\_tA0wGsvQ&t=76s](https://www.youtube.com/watch?v=wp_tA0wGsvQ&t=76s)

Pablo Romanos, Proyecto CROZONO. Canal Metro - Mayo 2018.



<https://www.youtube.com/watch?v=rtPsEKgFShs>

Facultad de Ingeniería

## La UdeMM se incorporó a una comunidad internacional de seguridad informática

Durante el pasado mes de mayo nuestra universidad pasó a formar parte de OWASP, una comunidad internacional formada por empresas y organizaciones educativas de todo el mundo, que trabaja en la creación de metodologías, herramientas y tecnologías informáticas.

A través de diversas charlas en la Facultad de Ingeniería, el Ing. Pablo Romanos (a cargo del proyecto), se ha trabajado de desarrollar los aspectos tecnológicos OWASP. Según el mismo explica "es importante que los docentes tengan conciencia de esto, porque influye cambios metodológicos en la forma de dar las clases y los alumnos a desarrollar software a los alumnos. No es lo mismo desarrollar generalista como hace la facultad de la capacitación, que incluir la seguridad desde el inicio del sistema, considerando en cada una de sus fases".

El Proyecto de Código Abierto de Seguridad en Aplicaciones Web (OWASP) -Open Web Application Security Project, es una comunidad formada por empresas, organizaciones educativas, y parti-

cipantes de todo el mundo. Junto con definir una comunidad de seguridad informática que incluye para, entre otros, métodos de trabajo, documentación, herramientas y tecnologías que se liberen y puedan ser utilizadas gratuitamente por cualquier persona o institución.

A este respecto el Ing. Romanos agrega que "OWASP es un nuevo tipo de entidad que al mercado de seguridad informática. Para hacer de personas corporativas fáciles que OWASP proporciona interacción informal, práctica y realizable sobre seguridad de aplicaciones informáticas. Esta comunidad no está afiliada a ninguna competencia específica, si bien apoya el uso de tecnologías de seguridad, y recomienda utilizar la seguridad de aplicaciones informáticas

considerando todas sus dimensiones: personas, procesos y tecnología".

Entre los documentos más relevantes de este proyecto se incluye la "Guía OWASP" y el ampliamente adoptado conjunto de estándares de "OWASP Top-10". OWASP cuenta con unos 80 capítulos locales por todo el mundo y más de 1000 miembros en las listas de correo del proyecto. Asimismo, ha organizado la serie de conferencias AppSec para mejorar la cooperación de la comunidad de seguridad de aplicaciones web.

Agenda: [www.owasp.org/index.php/Membership](http://www.owasp.org/index.php/Membership) padrones en los congresos y logos de todos los miembros que forman parte del OWASP en el mundo, incluyendo a partir de ahora a nuestra Universidad.



## CIBERATAQUES A LOS JUEGOS OLÍMPICOS y al G20

Presentación en diferentes medios de comunicación



*El Secretario Académico de Ingeniería, Mg. Ing. Pablo Romanos, durante su disertación como Especialista en Seguridad y Docente de la asignatura Seguridad Informática.*



## Conferencia sobre seguridad informática

Se llevó a cabo en nuestra universidad la tercera conferencia internacional OWASP Latam Tour 2014



*Algunos de los oradores en la conferencia internacional sobre seguridad informática*

**O**WASP es una comunidad abierta sin fines de lucro dedicada a formar y concientizar a las organizaciones a diseñar, desarrollar, adquirir, operar y mantener aplicaciones y sistemas seguros. Todas las herramientas de OWASP, documentos, foros y capítulos son gratuitas y abiertas a cualquier persona interesada en la mejora de la seguridad de aplicaciones.

Cabe destacar que el evento resultó ser un verdadero éxito, superando las ediciones anteriores, no solo por la calidad de los expositores de nivel internacional, sino por la audiencia que, dependiendo del horario, llegó a picos de casi 100 asistentes.

Debido a este éxito los organizadores de OWASP han invitado a la UdeMM a formar parte de la Red de Servicios de Tecnología Avanzada RENATA, red de la cual participan muchas universidades dentro del ámbito Latinoamericano. Esta red posibilita compartir contenidos multimediales (como por ejemplo conferencias remotas, telepresencia, transmisión de voz y video en directo, etc.).

Deseamos agradecer a los que de una u otra forma participaron de la organización del evento y contribuyeron para que todo salga según lo planificado.

**SEGURINFO 2007/2008**

Disertante sobre "Gestión de la Seguridad de la Información" – 2007 / 2008

[http://www.latinvia.com.ar/productos/categorias.cfm?desde=31&hasta=40&categoria=15&producto=89&nivel=1&ordenado=1&store\\_id=1&codalianza=3829&oferta=1](http://www.latinvia.com.ar/productos/categorias.cfm?desde=31&hasta=40&categoria=15&producto=89&nivel=1&ordenado=1&store_id=1&codalianza=3829&oferta=1)

[http://www.latinvia.com.ar/productos/productone.cfm?producto=89&nivel=2&categoria=21&Sku=SCAR6839&store\\_id=1&codalianza=3829](http://www.latinvia.com.ar/productos/productone.cfm?producto=89&nivel=2&categoria=21&Sku=SCAR6839&store_id=1&codalianza=3829)



**BLACK HAT ARSENAL EUROPE 2016 - LONDRES (REINO UNIDO)**

Speaker. CROZONO Project: "Leveraging autonomous devices as an attack vector on industrial networks"

<https://www.blackhat.com/docs/eu-16/materials/arsenal/eu-16-CROZONO-Framework-Leveraging-Autonomous-Devices-as-an-Attack-Vector-on-Industrial-Networks.pdf>



**EKOPARTY SECURITY CONFERENCE 2015**

Disertante - Presentación de Proyecto CROZONO: "Cracking the security perimeter with drones & robots"

<https://vimeo.com/album/3682874/video/147894742>







Mariano Barresi.



Carlos Benitez.

# Gestión integral de seguridad

**Durante un desayuno de trabajo, especialistas de Khu Technologies explicaron cuáles son las mejores prácticas tendientes a garantizar la seguridad de la información.**

**E**n las instalaciones del Hotel Madero By Sofitel, Khu Technologies, empresa especializada en soluciones de consultoría, infraestructura y servicios gestionados, realizó el primer encuentro de su "Ciclo de Desayunos de Seguridad de la Información". La temática abordada fue "Soluciones de consultoría para problemáticas comunes".

"Ante todo, es fundamental el análisis del riesgo; uno no puede implantar una solución para proteger determinados sistemas, si no conoce el riesgo existente y lo equilibra con el presupuesto que tiene para implementar dicha solución", expresó Mariano Barresi, Responsable Comercial de Khu Technologies, tras dar la bienvenida a los presentes.

"Nuestra solución de análisis de riesgo está soportada por dos pilares. Primero, la clasificación de la información. A su vez, dicha clasificación se soporta en el inventario de activos de información. Sin la existencia de un inventario, no se puede clasificar ni hacer análisis de riesgo", agregó.

Posteriormente, Pablo Romanos, Gerente de Organización de la Seguridad de

la compañía, expresó: "Actualmente, la seguridad es reactiva, se plantea una meta o fin a alcanzar y en ese punto finaliza el proceso. Los controles se aplican sobre los recursos IT, y el esquema se basa en restricciones y permisos. La responsabilidad en cuanto al mantenimiento de la seguridad es asignada a un grupo de empleados".

"Nuestra propuesta, en cambio –añadió– consiste en plantear un plan de gestión de seguridad de la información. Es decir, trabajar en una mejora continua, en forma

proactiva y planificada, con controles puestos no sólo sobre los recursos informáticos sino también sobre las personas y procesos".

"Cuando ocurre un incidente, en muchos casos no hay forma de saber quién fue la persona que debería haberlo previsto. También ocurre que el *time to market* se prioriza muchas veces ante la seguridad. Nuestra función es dar respuesta a estas situaciones", explicó.

Finalizada su charla, Carlos Benitez, Director de la Unidad de Negocios Seguridad de la Información de Khu Technologies, señaló algunas problemáticas comunes a las diferentes organizaciones, como por ejemplo, ataques sobre una de las aplicaciones, robo de datos personales, indeterminación ante incidente o errores, y el uso de criptografía en aplicaciones sin las medidas de seguridad correspondientes.

Según explicó Benitez, Khu Technologies ofrece a sus clientes consultoría, infraestructura y servicios para mantener la seguridad en un ciclo conformado por una serie de fases. La primera es la de relevamiento. A través de entrevistas mantenidas con los principales responsables, se obtienen métricas que serán el punto de partida de la información a analizar en las siguientes fases, que son: Análisis, plan de acción, plan estratégico de seguridad, análisis de riesgos, inventario de Activos, clasificación de la información y compliance (metodología y experiencia plasmadas en una herramienta específica que permite conocer de manera rápida, efectiva y precisa el nivel actual de cumplimiento de estándares y buenas prácticas de seguridad).

El encuentro finalizó con la exposición de un caso práctico. Durante la misma, Gustavo Aguirre, Chief Information Officer (CIO) de Osde, explicó las distintas acciones emprendidas por su empresa con el objeto de garantizar la integridad y seguridad de la información. ●



Pablo Romanos.



Gustavo Aguirre.



**CIENCIA.** Electrónica y computación, los chicos aprenden por medio de experimentos.

## EDUCACION

PARA CHICOS DE 4 A 18 AÑOS

# El juego de saber

Un taller para despertar vocaciones e iniciarse en la ciencia preferida.

**N**o usan anteojitos redondos, ni guardapolvos blancos, ni se peinan con una raya al medio. Tampoco utilizan un lenguaje incomprensible para el resto de los chicos de su edad, que como ellos, tienen entre 4 y 15 años. Pero saben cómo funciona un volcán, cómo incuba una gallina sus

huevo, cómo programar un robot, cómo fabricar una radio o cómo sacar fotos sin cámara.

Lo cierto es que todo es posible en el taller de Miniciencia. Las áreas son seis —computación, robótica, electrónica, carpintería, ciencia y fotografía— y en cada una de ellas los chicos, guiados por profesores, se plantean una duda, cuentan sus hipótesis a priori y luego, como en un juego, las llevan a la práctica para observar el resultado final.

Las actividades son interminables: programar juegos y canciones en computadoras, utilizar software, provocar reacciones químicas, armar circuitos eléctricos, sacar y revelar fotos, construir objetos en madera, e incursionar, siempre a través de la experiencia, en la astrología, la zoología —con el minizoo—, la botánica, la anatomía y la física.

“Los chicos participan de una clase- invitación, donde conocen todas las áreas. Luego eligen las que más les gustan, haciendo un nivel por año, y cursando una materia por semana”, dice Lidia de Scheingart (45), licenciada en química y directora del taller.

Claro que no todo es sólo para los más chicos, sino que también adolescentes de 18 años pueden participar en algunas actividades e incluso, los padres comparten dos clases anuales dirigidas exclusivamente por sus hijos.



Un minizoo, tres laboratorios, una sala de equipos y un gran número de aulas están a total disposición de los pequeños genios, que deben tener como principal requisito ganas de aprender jugando. “Para los profesores, además, estos talleres son un verdadero desafío. No sólo tienen que enseñar sino también respetar las preguntas de los chicos, escuchar sus afirmaciones y tener mucha paciencia para no imponer sus conocimientos sin antes dejar que ellos experimenten” —concluye Scheingart—.

Foto: Osvaldo Dubiel



**ROBOTICA.** Nueva experiencia (12q). En el minizoo: investigar la conducta animal, ante el hembra y con: especies (ab).



## I FERIA DE LOS INVENTOS y EXPOUNIVERSIDAD - EXPOSITOR DE ROBOT DE DISEÑO PROPIO – (1990-1999)

Diseño y construcción de robot autónoma, controlado por computadora, equipado con sensores de reconocimiento y cámara de video. Reportaje en TV, ATC (11-1997).

Entre el 11/8 y el 5/9 se realizó en las instalaciones de la Sociedad Rural Argentina la cuarta edición de ExpoUniversidad, destacándose el stand de la UdeMM, no sólo por la calidad de su atención, sino también por la incorporación de un simpático robot que aportó la Facultad de Ingeniería.

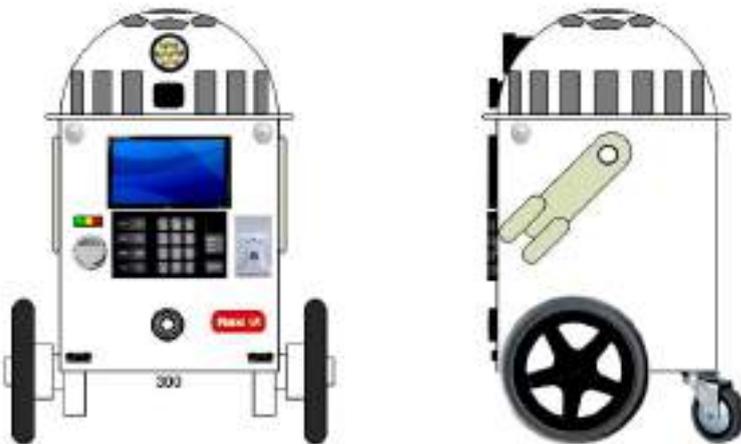


Nuestro stand (y el robot) en ExpoUniversidad '99



## DISEÑO Y CONSTRUCCIÓN DE ELECTRÓNICA DE AVANZADA Y SOFTWARE ESPECIALIZADO (1990-Presente)

- Pantallas táctiles para ser instaladas en patrulleros o móviles policiales que permiten en tiempo real la identificación de individuos y consulta de datos personales (DNI, domicilio, antecedentes, etc.).
- Luminaria solar que permite importantes ahorros de energía y garantiza el cuidado del medioambiente. Apta para reemplazar de forma parcial, luminarias en vía pública, rutas, autovías, etc.
- Barreras ferroviarias solares para ser instaladas en pasos a nivel rurales o donde no llega el suministro eléctrico. Permiten la detección temprana de la formación ferroviaria, evitando accidentes.
- Robots para vigilancia de espacios privados y publicidad en congresos y eventos. Monitoreo desde Internet, pudiendo interactuar con el robot de forma remota, mediante su CPU, su servidor web y sus sensores de temperatura, humo e incendios, de detección de gases complejos, cámara HD de visión infrarroja, pantalla táctil, voz y video.



Perim. =  $\pi \cdot D_{\text{diám.}}$   
Perim. =  $3.14 \cdot 300$   
Perim. = 942.3 mm

