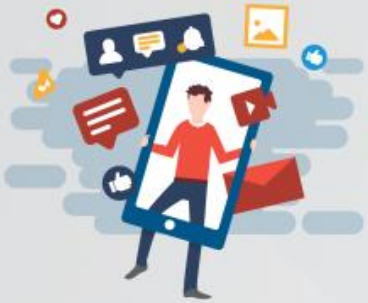
PELIGROS EN LAS REDES SOCIALES



Las redes sociales son espacios para el encuentro de personas en Internet, donde comparten mensajes de texto, imágenes, videos y fotografías, esté atento:

1 Personas extrañas pueden acceder a información personal para hacer uso indebido.

2 El contenido visualizado en las redes sociales puede ser inapropiado para menores.

3 La edad mínima de acceso recomendada para el uso de redes sociales es de 13 años.

Sugerencias de Seguridad al utilizar Redes Sociales

- **NO** agregue contactos que no conozca.
- **NO** brinde sus datos personales a personas desconocidas.
- **NO** visite páginas de contenidos no aptos para su edad.
- **AVISAR** inmediatamente a los adultos si encuentra contenido inapropiado.
- **AJUSTE:** perfiles de privacidad, para que sean solo para contactos conocidos.
- **NO** ofenda a otras personas ni responda a provocaciones.
- **NO** conteste mensajes a extraños, no abra mensajes desconocidos.
- **EVITE** encuentros con personas que únicamente conoce por Internet.
- **USE** contraseñas largas con números y letras. No se las proporcione a ninguna persona, ni las apunte en un lugar que alguien pueda verlas.
- **NO** envíe o comparta información con contenido sexual, no comprometa su integridad y dignidad.

COSTA RICA GOBIERNO DEL BICENTENARIO 2018 - 2022 | OEA Más derechos para más gente | micitt MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

sutel · uccaep · Hacienda · OIJ · ABRIENDO DATOS · CONSEJO NACIONAL DE RECTORES · SULÁ BATSÚ · PRODHAB

CIBERSEGURIDAD PARA NO TECNÓLOGOS

1 **En un mundo digital, todos somos responsables de la ciberseguridad. Enfrentarse a las ciberamenazas ya no es solamente una cuestión de especialistas en tecnología.** Requiere de la intervención de todos.

2 **Los delincuentes tienen nuevas oportunidades para robar y cometer fraude con la revolución digital.**
No se deje engañar por los ciberdelincuentes, Protéjase.

3 **Hay muchas formas en las que un ciberataque puede ejercer un impacto negativo en usted.**

- **Phishing**

- **Ciberbullying**

- **Malware**

- **Suplantación de identidad**

4 **Prepárese para responder ante el cibercrimen:**

- Infórmese de nuevos riesgos en la era digital.
- Falta de protección en los dispositivos tecnológicos.
- Recuerde que a usted le puede pasar.

5 **Los mejores sistemas no pueden bloquear todas las amenazas, prepárese e infórmese sobre riesgos y consecuencias de un ciberataque y sus medidas para contrarrestarlo.**

COSTA RICA GOBIERNO DEL BICENTENARIO 2018 - 2022 | OEA Más derechos para más gente | micitt

sutel · uccaep · Hacienda · OIJ · ABRIENDO DATOS · SULA BATSÚ · PRODHAB

CÓMO UTILIZAR CONTRASEÑAS SEGURAS

1

Pas****

Las contraseñas deben de utilizarse como la ropa interior

No debes dejarlos donde los demás pueda verlos.

*****

Deberías cambiarlos regularmente.

No deberías compartirlos

2

Las contraseñas son como el cepillo de dientes, es personal y debes de cambiarlo máximo cada 90 días.

*****

90 Días

COSTA RICA
GOBIERNO DEL BICENTENARIO
2018 - 2022

OEA Más derechos para más gente

micitt MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

sutel · uccaep · Ministerio de Hacienda · OIJ · ABRIENDO DATOS · CONSEJO NACIONAL DE RECTORES · SULÁ BATSÚ · PRODHAB

SEGURIDAD EN EL USO DE DISPOSITIVOS MÓVILES:

1 Hable con sus hijos sobre el uso apropiado del teléfono móvil.

2 Utilice un software de seguridad para su teléfono.

3 Utilice antivirus en sus dispositivos móviles.

4 Proteja el celular con una contraseña o patrón.

5 Tener cuidado con los accesos en las redes públicas.

6 Actualice el sistema operativo en el dispositivo móvil.

COSTA RICA GOBIERNO DEL BICENTENARIO 2018 - 2022 | OEA Más derechos para más gente | micitt MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

sutel uccaep Ministerio de Hacienda OIJ ABRIENDO DATOS CONSEJO NACIONAL DE RECTORES SULÁ BATSÚ PRODHAB

SEGURIDAD EN EL USO DE INTERNET EN LOS HOGARES

1 Extreme la seguridad si le solicitan datos de su cuenta, nunca revele información personal.

2 Extreme la seguridad en sitios web que requieren instalación de software.

3 Utilice antivirus en sus dispositivos electrónicos, para mayor seguridad.

4 Al utilizar navegadores web instale los parches de seguridad correspondientes al producto.

COSTA RICA GOBIERNO DEL BICENTENARIO 2018 - 2022 | OEA Más derechos para más gente | micitt MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

sutel | uccaep | Ministerio de Hacienda | OIJ | ABRIENDO DATOS | CONSEJO NACIONAL DE RECTORES | SULÁ BATSÚ | PRODHAB

CIBERSEGURIDAD EN EL USO DE DISPOSITIVOS MÓVILES EN EL ENTORNO LABORAL

1 **Configure claves seguras de acceso en los dispositivos móviles que utilice en su trabajo** (PIN, patrón o huella).

2 **Evite descargar y almacenar material de trabajo en tu dispositivo móvil.**

3 **Recuerda evitar las redes WiFi públicas para acceder a la información laboral y herramientas de trabajo.**

4 **No debes enviar tus contraseñas mediante aplicaciones móviles o almacenarlas mediante notas o fotografías en tu dispositivo móvil.**

5 **Recuerda no dejar tu dispositivo móvil desbloqueado y sin supervisión.**

COSTA RICA GOBIERNO DEL BICENTENARIO 2018 - 2022 | OEA Más derechos para más gente | micitt MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

sutel uccaep Ministerio de Hacienda OIJ ABRIENDO DATOS CONSEJO NACIONAL DE RECTORES SULÁ BATSÚ PRODHAB

PROTECCIÓN DE DATOS PERSONALES

¿Qué garantiza la Ley 8968 y su Reglamento a las personas?

1

Los datos personales le pertenecen al titular y únicamente pueden ser recopilados y transferidos bajo su consentimiento.

2

El consentimiento informado puede ser revocado en cualquier momento, usted tiene derecho a acceder, actualizar, rectificar o eliminar su información.

3

Usted decide como y a quien compartir sus datos personales, desconfíe de páginas web o personas desconocidas. Usted es el responsable de proteger sus datos personales.

4

Toda persona tiene derecho de conocer el tratamiento que se le dará a su información y exigir que sea utilizada de forma segura.

5

Los datos solo pueden ser utilizados cuando sean actuales, veraces, exactos y adecuados al fin para el que fueron recolectados.

COSTA RICA GOBIERNO DEL BICENTENARIO 2018 - 2022 | OEA Más derechos para más gente | micitt MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

sutel | uccaep | Ministerio de Hacienda | OIJ | ABRIENDO DATOS | CONSEJO NACIONAL DE RECTORES | SULÁ BATSÚ | PRODHAB

QUÉ ES UN MALWARE

Programas informáticos que afectan la funcionalidad de los equipos tecnológicos.

Se clasifican de diferentes formas:

Virus

Malware o software malicioso que tiene la capacidad de reproducirse y transmitirse por la red para ocasionar alteraciones en el funcionamiento de la computadora.

Troyano

Malware o software malicioso que a menudo se disfraza de software legítimo para obtener acceso o información de la computadora de la víctima.

Rootkit

Conjunto de herramientas de software maliciosas que se instalan en el sistema operativo de manera oculta y permiten el acceso privilegiado continuo a una computadora.

COSTA RICA GOBIERNO DEL BICENTENARIO 2018 - 2022 | OEA Más derechos para más gente | micitt MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

sutel | uccaep | Ministerio de Hacienda | OIJ | ABRIENDO DATOS | SULÁ BATSÚ | PRODHAB

PHISHING

El exceso de confianza puede convertirle en víctima...

¡SEA UNA PERSONA PRECAVIDA!

1 **Preste atención a la procedencia de los correos electrónicos:**
Cuidado si proviene de un desconocido, puede ser usado por ciberdelincuentes para obtener datos confidenciales.

2 **No proporcione a nadie, de manera verbal ni escrita, las claves o nombres de usuario de sus cuentas bancarias.**
Ninguna entidad se las solicitará.

3 **Cuando ingrese a páginas de bancos, digite en la barra de acceso la dirección oficial:**
No lo haga mediante buscadores porque se corre el riesgo de ingresar a sitios falsos de apariencia similar.

4 **Mantenga actualizados los antivirus en los dispositivos electrónicos, para tratar de evitar que, por medio de algún archivo malicioso o del sistema, roben información sensible.**

COSTA RICA
GOBIERNO DEL BICENTENARIO
2018 - 2022

OEA Más derechos para más gente

micitt MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

sutel · uccaep · Ministerio de Hacienda · OIJ · ABRIENDO DATOS · Consejo Nacional de Rectores · Sulá Batsú · PRODHAB

PROTECCIÓN DE DATOS BIOMÉTRICOS

Proceso tecnológico que hace identificable a la persona de forma única según sus características físicas, mediante fotografías, huellas dactilares, entre otras.

1

La seguridad de los datos personales constituye un pilar fundamental para realizar un efectivo tratamiento.

2

Todo responsable y encargado que realice tratamiento de datos personales biométricos deberá establecer y mantener medidas de seguridad administrativas, físicas y lógicas.

3

Las bases de datos utilizadas para almacenar datos personales biométricos deben establecer condiciones que garanticen su seguridad e integridad.

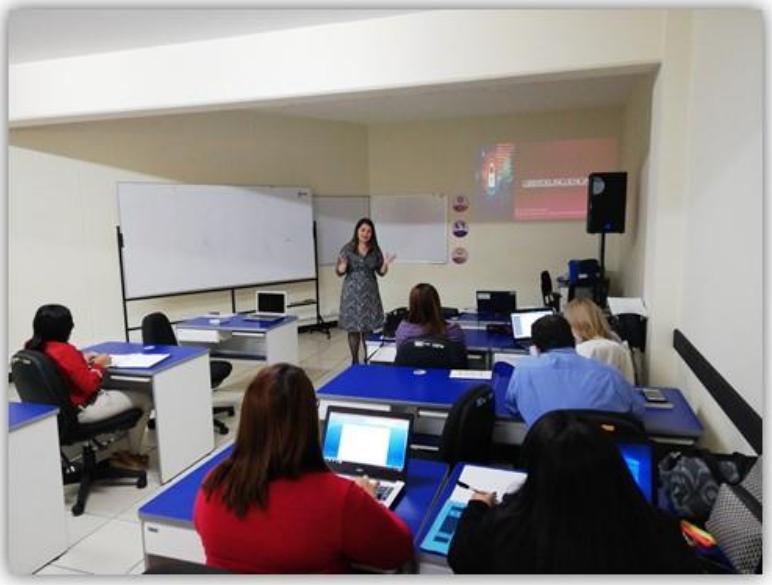
COSTA RICA GOBIERNO DEL BICENTENARIO 2018 - 2022 | OEA Más derechos para más gente | micitt

sutel · uccaep · Hacienda · OIJ · ABRIENDO DATOS · SUGEBAISU · PRODHAB

De: Área de Prensa - Ministerio Público <prensamp@Poder-Judicial.go.cr>
Enviado el: miércoles, 24 de abril de 2019 14:59
Asunto: FISCALES Y FISCALAS SE ESPECIALIZAN EN MATERIA DE CIBERDELINCUENCIA

Comunicación Interna | Ministerio Público

FISCALES Y FISCALAS SE ESPECIALIZAN EN MATERIA DE CIBERDELINCUENCIA



UCS. 24 de abril de 2019. *Ciberdelincuencia en casos de crimen organizado*, es el curso que se desarrolla entre el 23 y el 25 de abril en Unidad de Capacitación y Supervisión del Ministerio Público, dirigido a fiscalas y fiscales de diversas fiscalías territoriales.

El curso tiene como propósito que las personas participantes desarrollen competencias en cuanto a los conocimientos sobre el fenómeno criminal de Ciberdelincuencia, como el concepto, las características, y los riesgos, así como el uso de la Ingeniería Social.

También se pretende especializar al personal en el abordaje adecuado de los delitos como violación de datos personales, suplantación de identidad y sitios web, redes sociales, bitcoins, web oscura, delitos sexuales a través de la web, normativa, utilidad de las telecomunicaciones y rastreo de datos móviles, para una mayor eficacia en la persecución criminal.

El curso es impartido por la fiscala especializada en fraudes, Sharon Rodríguez Segura, así como Francisco Picado Cambronero, del Instituto Costarricense sobre Drogas (ICD) y César Alpízar Murillo, del Instituto Costarricense de Electricidad (ICE), quienes son especialistas en el tema.

Ante el desarrollo de las tecnologías y la utilización de estas por parte de redes criminales, la fiscala adjunta de la UCS, Mayra Campos, destaca la importancia de capacitar a fiscales y fiscalas en este tema, de manera que los nuevos fenómenos delictivos no resulten desconocidos, sino que, por el contrario, se cuente con la información para su abordaje de manera eficiente. En tal sentido, la Fiscala Adjunta destacó que también es importante la coyuntura con otras instituciones públicas, como ICD y el ICE.

Oficina de Prensa
Ministerio Público

Ministerio Público de Costa Rica
@FiscaliaCR
Ministerio Público de Costa Rica
prensamp@poder-judicial.go.cr
2248 3172

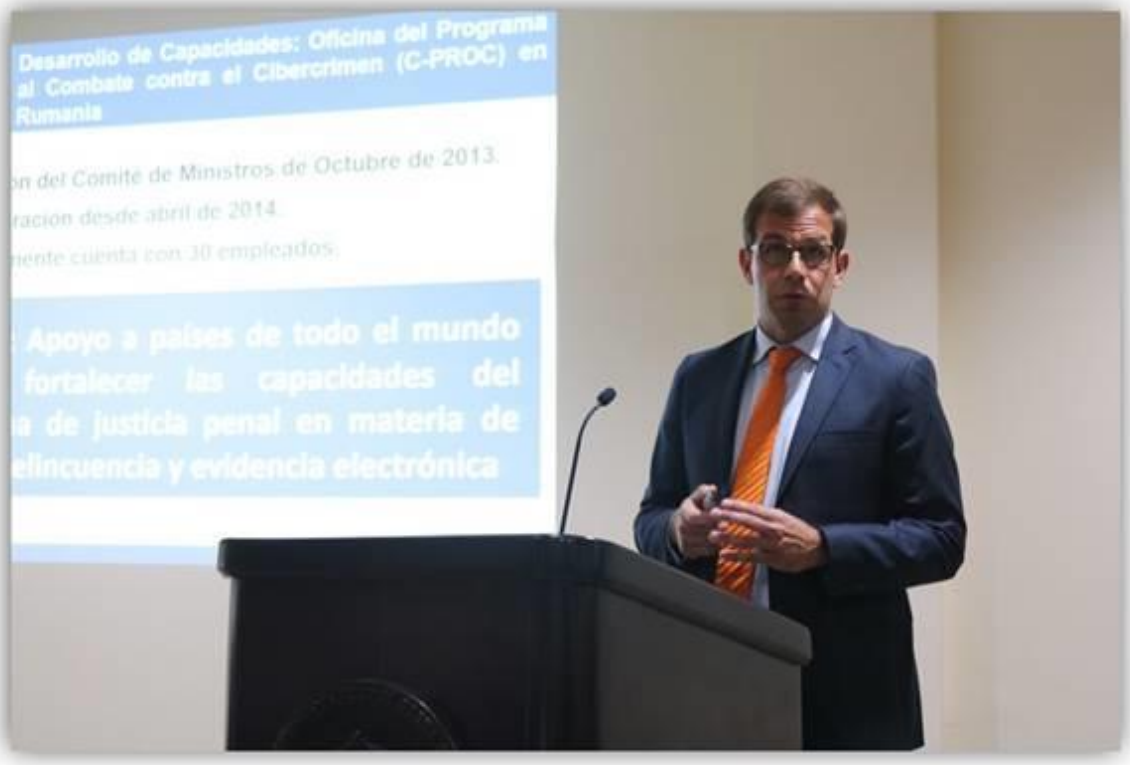
De: Área de Prensa - Ministerio Público <prensamp@Poder-Judicial.go.cr>
Enviado el: lunes, 13 de mayo de 2019 13:10
Asunto: CAPACITACIÓN PERMITE AL MINISTERIO PÚBLICO MEJORAR INVESTIGACIONES DE CIBERDELITOS

Comunicación Interna | Ministerio Público

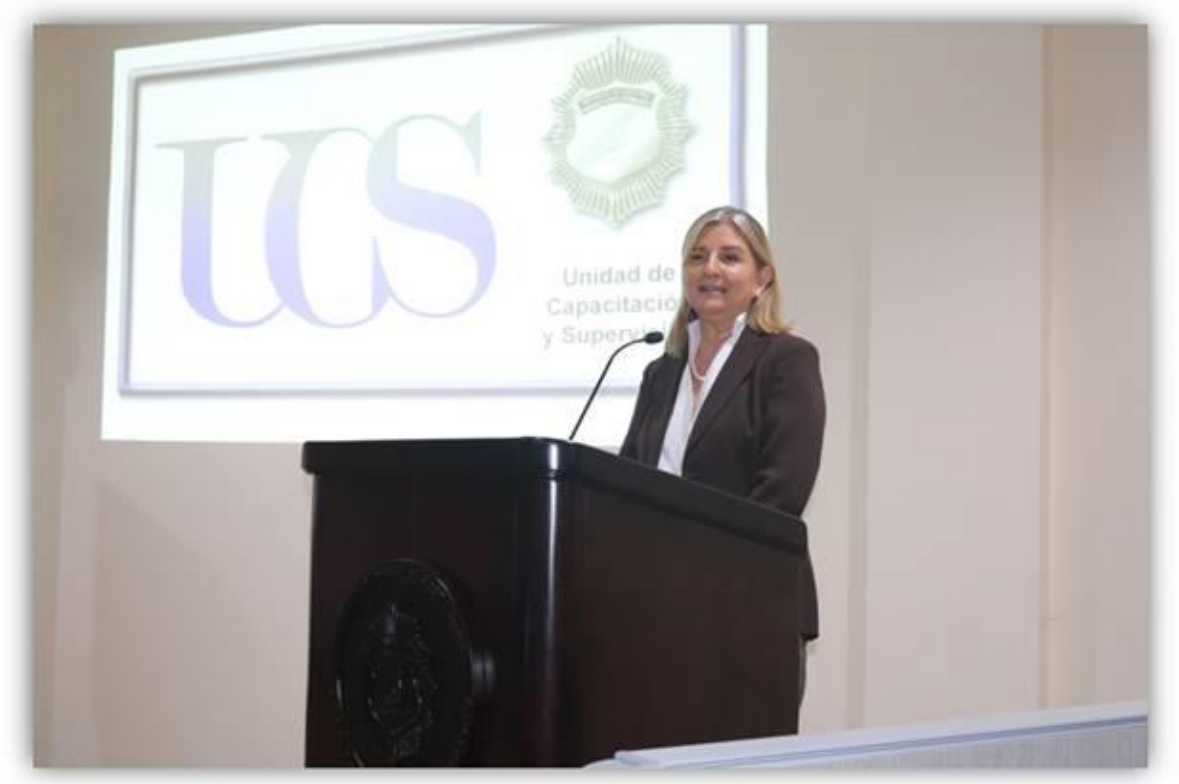
CAPACITACIÓN PERMITE AL MINISTERIO PÚBLICO MEJORAR INVESTIGACIONES DE CIBERDELITOS

Sharon Hernández Coto
shernandezco@poder-judicial.go.cr

13 de mayo del 2019. Un grupo de 18 fiscales y fiscalas participan del curso avanzado "Delitos Cibernéticos y Pruebas Electrónicas", la cual se realiza entre hoy y el próximo miércoles, en las instalaciones de la Unidad de Capacitación y Supervisión (UCS) del Ministerio Público.



Esta actividad es parte del Proyecto del Consejo de Europa GLACY+ (Acción Global sobre Cibercrimen, por sus siglas en inglés), el cual apoya a Costa Rica



en el fortalecimiento de la adecuada aplicación del Convenio de Ciberdelincuencia. La primera capacitación se llevó a cabo entre el 11 y 15 de febrero anterior.

“Estar en el Proyecto GLACY+ es muy beneficioso, porque les permite formar parte de una comunidad de países que están estrechamente
vinculados y que están activamente trazando líneas de investigación en el ciberdelito”, explicó Cristos Velasco, experto internacional del Consejo de Europa.

Durante la capacitación, los participantes profundizarán sus conocimientos en los temas de monedas virtuales, darknets (la red oscura del internet), evidencia electrónica y, además, analizarán algunos casos que podrían atender en las investigaciones. Los cursos están a cargo de los señores Uwe Rasmussen, Antonio Pina y Cristos Velasco, tres expertos en materia de ciberdelincuencia.

De acuerdo con la fiscala general de la República, Emilia Navas Aparicio, en la actualidad, los dispositivos electrónicos son utilizados para cometer un delito,

pueden registrar algún ilícito, o bien, son una herramienta para la resolución de casos.

“La Fiscalía General considera que es un tema básico, indispensable y necesario para todo el trabajo que hacen los fiscales y fiscalas; es por eso que hemos venido apoyando este tema con capacitaciones, para que un mayor grupo de funcionarios y funcionarias del Ministerio Público participen en este tipo de actividades”, señaló Navas.

Capacitación técnica especializada. Según explicó Mayra Campos Zúñiga, fiscala adjunta de la UCS, este tipo de temas es una prioridad para la institución,
ya que, al tratarse de un tema novedoso, se requiere reforzar las competencias de los fiscales y las fiscalas para que puedan desempeñar su trabajo de la manera correcta.

“Es sumamente importante que el personal se prepare y se actualice, sobre todo en este tipo de delincuencias, que requiere no solo un conocimiento de

carácter técnico sino la aplicación de una normativa internacional. Solo, a través de la capacitación, podremos cumplir con las labores que nos encomienda la Ley", añadió la fiscala adjunta de la UCS.

Tras finalizar la capacitación, el próximo jueves y viernes se realizará la Misión Consultiva, en la que se pretende realizar un análisis de la legislación costarricense, en relación con el Convenio de Ciberdelincuencia. Este trabajo será en conjunto con letrados de la Sala III, el Organismo de Investigación Judicial, el Instituto Costarricense de Electricidad, el Ministerio de Ciencia, Tecnología y Telecomunicaciones, Asamblea Legislativa, la Procuraduría General de la República y la Agencia de Protección de Datos de los Habitantes.

Oficina de Prensa
Ministerio Público

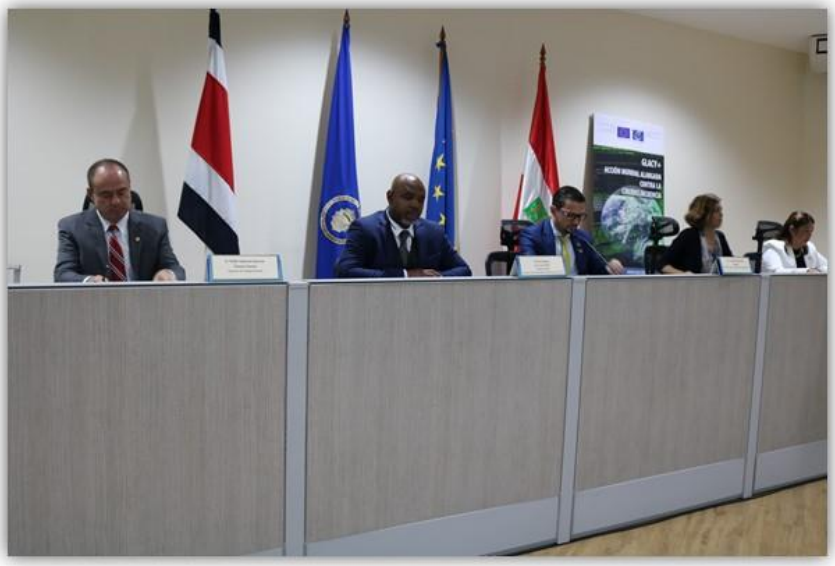
Ministerio Público de Costa Rica
@FiscaliaCR
Ministerio Público de Costa Rica
prensamp@poder-judicial.go.cr
2248 3172

De: Área de Prensa - Ministerio Público <prensamp@Poder-Judicial.go.cr>
Enviado el: viernes, 17 de mayo de 2019 15:42
Asunto: MINISTERIO PÚBLICO PARTICIPA EN ANÁLISIS SOBRE CIBERDELINCUENCIA Y LEGISLACIÓN COSTARRICENSE

Comunicación Interna | Ministerio Público

MINISTERIO PÚBLICO PARTICIPA EN ANÁLISIS SOBRE CIBERDELINCUENCIA Y LEGISLACIÓN COSTARRICENSE

Sharon Hernández Coto
shernandezco@poder-judicial.go.cr

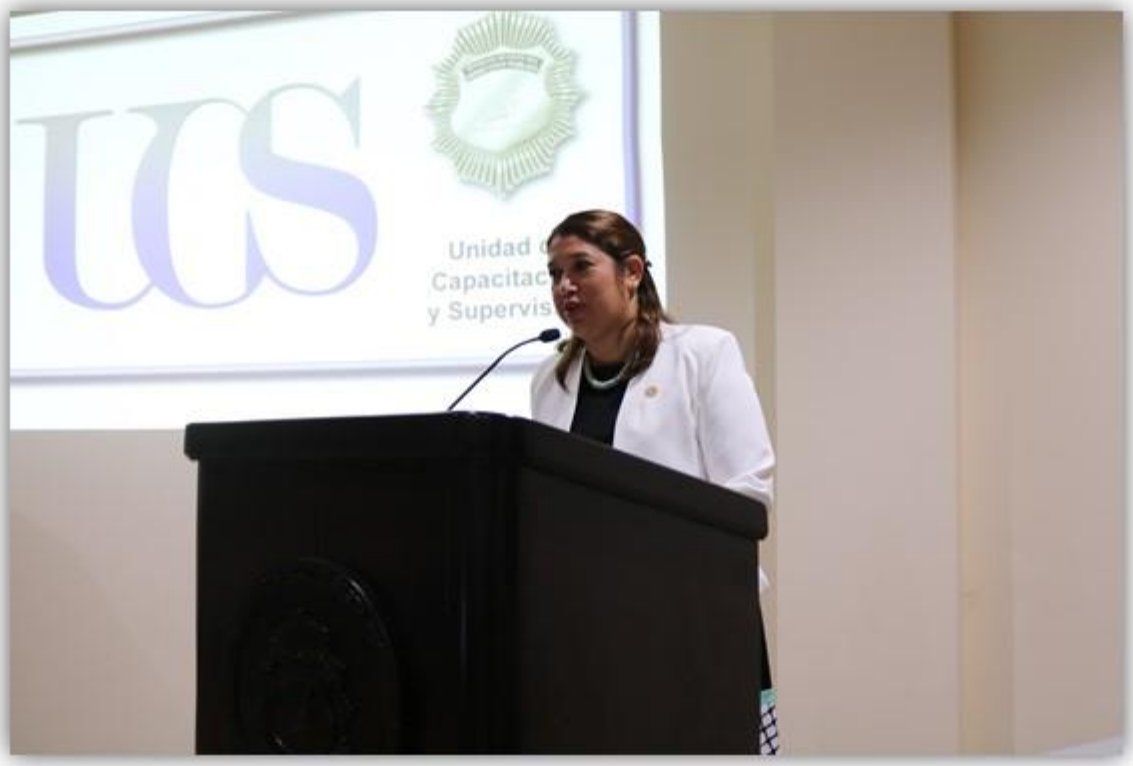


17 de mayo del 2019. Un equipo de fiscales y fiscalas participa en la Misión Consultiva donde se realizará un análisis de la legislación costarricense, en relación con el Convenio de Ciberdelincuencia.
Al trabajo se suma letrados de la Sala III, el Organismo de Investigación Judicial (OIJ), el Instituto Costarricense de Electricidad, el Ministerio de Ciencia (ICE), Tecnología y Telecomunicaciones

(MICITT), Asamblea Legislativa, la Procuraduría General de la República (PGR) y la Agencia de Protección de Datos de los Habitantes.

El acto inaugural se llevó a cabo ayer, en la Unidad de Capacitación y Supervisión (UCS) del Ministerio Público, con la participación de Walter Espinoza Espinoza, director del OIJ; Mayra Campos Zúñiga, jefa de la UCS; Birgit Vleugels, agregada de cooperación de la Unión Europea en Costa Rica; Elvio Salomon, oficial del Proyecto GLACY+(Acción Global sobre Cibercrimen, por sus siglas en inglés) y Luis Salazar Solís, jerarca del MICITT.

“Con esto buscamos el fortalecimiento de las competencias, habilidades y conocimientos, para que las investigaciones de ciberdelincuencia sean planificadas, supervisadas y ejecutadas con un personal entrenado y especializado. Solo comprendiendo el impacto de la tecnología, las telecomunicaciones en la vida cotidiana y en las conductas criminales, el órgano fiscal podrá enfrentar de manera adecuada la tarea encomendada por la Ley”, expuso Campos Zúñiga.



Por su parte, el director del OIJ mencionó que es importante realizar este tipo de actividades, donde se puede analizar la legislación de nuestro país y que, además, se puede escuchar ideas de los expertos internacionales y que de los funcionarios

y funcionarias aporten su conocimiento, para crear un producto que sea útil para todos.

“Necesitamos que una estrategia global, para que los ataques cibernéticos sean más fáciles de detectar y de investigar. Tenemos que trabajar juntos como países y como regiones, para ganar esta batalla”, señaló Vleugels.

Según mencionó Elvio Salomon, realizar esta Misión Consultiva es de mucha importancia para poder luchar contra la ciberdelincuencia y, para el Proyecto GLACY+, la Unión Europea destinó 10 millones de euros, para realizar actividades en distintos países.

Al finalizar la Misión Consultiva, expertos del Consejo de Europa brindarán recomendaciones y emitirán algunas observaciones sobre posibles modificaciones que se pueden realizar, en temas de legislación y sobre la atención que se debería de dar en este tipo de casos.

Oficina de Prensa
Ministerio Público

Ministerio Público de Costa Rica
@FiscaliaCR
Ministerio Público de Costa Rica
2248 3172
prensamp@poder-judicial.go.cr