Parte 1 - Cibercrimen y Evidencia Digital ITU. **Angie Daniela Ruiz Alfonso**

¿Por qué es importante la Ciberseguridad para el país?

R: La Ciberseguridad es importante en el país para combatir, erradicar e investigar los delitos en el ciberespacio, debido a que mientras las tecnologías de la información avanzan, las habilidades de los delincuentes también, ante estos actos ilícitos se deben establecer acciones a seguir a nivel jurídico, técnico e institucional, y se deben establecer marcos de cooperación internacional teniendo en cuenta que en el ciberespacio no existen las fronteras geográficas, debido a que la colaboración mutua entre países refuerza esta lucha y permite ser mucho más eficaces en temas penales.

Fuentes: Modulo 1 – CiberCrimen y Modulo 2 – Combatiendo el CiberCrimen.

Investigue e identifique las diferencias y similitudes entre Ciberseguridad y Seguridad Informática.

R: La Ciberseguridad protege y defiende el uso del ciberespacio de ciber ataques, al igual que protege los activos de información digital de las organizaciones y a los usuarios contra los riesgos de seguridad informática. Para la Real Academia Española, ciberespacio significa "ámbito virtual creado por medios informáticos".

Mientras que la Seguridad Informática protege los elementos computacionales, conectados o no a una red, y que puedan generar impactos negativos ante ataques y amenazas informáticas, mediante medidas y controles.

Ambas son el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas que buscan y se aplican a la protección de la información que se encuentre procesada, almacenada y transportada por sistemas de información interconectados (tecnologías de la información y comunicación).

Ambas se basan en cumplir con la triada de la CID (Confiabilidad, Integridad y Disponibilidad).

Ambas pueden llegar a ser ofensivas y/o defensivas.

Fuentes: Modulo 1 – CiberCrimen, definiciones del ISO 27001:2013 y definiciones del NIST.

Describa, en detalle, un ejemplo de ciberdelito suscitado en su país en el presente año.

R: La Fiscalía General de la Nación (FGN) recibió desde el 2019 varias denuncias de delitos informáticos que eran similares, personas que habían sido abordadas en vía pública por personas que se hacían pasar por asesores comerciales de una entidad financiera, los cuales se robaban sus datos personales y biométricos por medio de ofrecimiento de créditos.

Con estos datos robados los delincuentes procedían a abrir cuentas de ahorro y obtenían créditos a nombre de las víctimas, para luego retirar el dinero de cajeros electrónicos o por medio de compras virtuales, sin tener en cuenta que enviaban dichos productos comprados a las direcciones de colaboradores de la misma organización.

Finalmente, el grupo de Delitos Informáticos del CTI, haciendo uso de interceptaciones telefónicas, vigilancias y seguimientos logró la plena identificación de los implicados y procedió con 12 judicializaciones.

El grupo delincuencial demoniado 'Las Asesoras' según la FGN sería responsable de delitos informáticos en Caquetá, Putumayo, Huila, Tolima y otros departamentos del país. Al parecer el grupo es liderado por Derly Viviana Muñoz Jiménez la cual se hacía pasar por una asesora externa de una entidad financiera, quien engañaba a las víctimas y lograba obtener dinero a través de transferencias y/o compras en internet, habiendo engañado así a más de 50 personas con una defraudación por 362 millones de pesos.

Fuente: https://www.fiscalia.gov.co/colombia/seccionales/con-12-judicializaciones-fue-impactada-la-organizacion-delincuencia-las-asesoras/

¿Existe un marco legal para combatir el cibercrimen en su país?

R: Sí, se tiene una normatividad sobre delitos informáticos en Colombia, el Congreso de la Republica modificó el Código Penal, creando un nuevo bien jurídico tutelado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, y se conoce como la Ley 1273 de 2009.

Detalla el marco legal ante:

- Los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.
- De los atentados informáticos y otras infracciones

Definiendo artículos en caso de:

- Acceso abusivo a un sistema informático.
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Daño Informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos.
- Agravación

Y resaltando las circunstancias de agravación punitiva, donde las penas imponibles de acuerdo con los artículos se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Fuentes: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html y https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Describa un ejemplo de un acto de ciberterrorismo (el ejemplo puede ser de cualquier país del mundo)

R: El fiscal federal interino Clint Johnson anunció que un hombre de Tulsa llamado John Jacobs Ahrens, de 58 años, se declaró culpable ante un tribunal federal por los cargos de amenazar y querer herir al presidente de los Estados Unidos, señaló ser responsable de enviar correos electrónicos amenazantes al canal 6 de KOTV dirigidos al presidente Joseph Biden y miembros anónimos del Congreso y sus familias, ocurrido entre mayo y junio del presente año, pero la sentencia será hasta el 22 de diciembre de 2021.

Un productor ejecutivo de Newson6 alertó sobre los correos electrónicos amenazantes de John Ahrens al Centro Nacional de Operaciones de Amenazas del FBI y este dio cumplimiento a la ley, debido a que cualquier amenaza en línea hecha contra el presidente y los miembros del Congreso se debe llevar ante un tribunal federal. El adulto mayor fue arrestado en su residencia de Tulsa el 18 de junio de 2021 por agentes del FBI y la Oficina de Investigaciones del Estado de Oklahoma y una tarea para los oficiales de la Fuerza de Tarea Conjunta contra el Terrorismo del FBI.

En los mensajes enviados el adulto mayor exigía dinero y que en caso de no hacerlo, mataría al presidente, a los miembros del Congreso y a sus familias. Algunos mensajes:

El 10 de mayo de 2021 envió un mensaje que decía: “Vaya a mi página de Facebook y lea lo que envié a los hombres del Congreso de los Estados Unidos. Tienen menos de 48 horas para entregar mi dinero o sus hijos empezarán a morir en todo el país. Voy a matar a sus hijos usando la misma ley que usó el gobierno para obligar a nuestras familias a seguir el Sendero de las Lágrimas ".

En un mensaje del 17 de junio, escribió: "Tiene hasta el lunes por la mañana a las 8:00 a. M. En punto para entregar un cheque al estado de Oklahoma, la nación Muscogee y mi familia de acuerdo con un acuerdo firmado según lo establecido en el Tratado de 1866".

Otros mensajes incluyeron “Estados Unidos verá cómo le volarán la cabeza a un presidente en funciones justo en frente de ellos” y “… sus familias comenzarán a morir. Después de que termine, volveré aquí una vez más y les diré que entreguen mi dinero ".

Fuente: https://www.justice.gov/usao-ndok/pr/tulsa-man-pleads-guilty-sending-emails-newson6-threatening-president-biden