PRIMER IGF NACIONAL DE HONDURAS

Informe Final

21 DE MARZO DE 2019

UNIVERSIDAD TÉCOLOGICA DE HONDURAS | UTH

www.igf.uth.hn

INDICE

- Artículos de las Conferencias
- Web del Evento
- Información de contacto de la iniciativa nacional de IGF Honduras
- Recomendaciones y Propuestas de las Mesas de Trabajo
- Conclusiones
- Anexos

INTRODUCCIÓN

En la 4ta Revolución Industrial, donde el avance tecnológico de todos los medios electrónicos que obligan tener una conectividad entre sí, el avance de Internet se puede decir que es imparable, de la misma forma las redes sociales y todo lo relacionado con el ciberespacio.

La informática ha tenido un crecimiento de forma magna en la última década provocando cambios en esta sociedad moderna, donde se ha generado vínculos de comunicación con la implementación del Internet de las cosas IoT (Internet of Things) y el Internet Industrial de las Cosas IIoT (Internet Industrial of Things), información digital, y libre expresión, acortando distancias y creando beneficios comerciales, atrayendo cambios culturales globalizados.

El uso del término Gobernanza en Internet implica traer a colación las distintas partes interesadas como mesas de trabajo o también llamadas en su término en inglés “Stakeholders” de las cuales ven la necesidad de crear espacios políticos y económicos para implementar una mejor política o ley sobre el manejo de las mismas y sus implicaciones.

En ella se discute el que y del cómo se debe gestionar el control de Internet, del cómo se debe gobernar un entorno digital, como proteger la privacidad en línea, cuales son las responsabilidades de la empresas privadas, la libertad de expresión, el control a la intimidad, el buen manejo de las redes, etc.

Hay que tener en cuenta que los participantes de esta versión del IGF Honduras 2019, que participarán en estas mesas de trabajo serán:

- Sector Sociedad Civil.
- Sector Gobierno.
- Sector Academia.
- Sector Fuerzas Militares.
- Sector Privado y Público.

Teniendo estos sectores se pretende abarcar cualquier interrogante para poder implementar una Internet de Confianza, con los enfoques necesarios y de cuidado para el mejor funcionamiento en el país o en el sector.

PRIMERA PARTE – DESARROLLO DEL EVENTO

- **COMITÉ ORGANIZADOR**

El comité organizador fue conformado por representantes de la Universidad Tecnológica de Honduras- UTH, quienes fueron los organizadores y patrocinadores principales del evento, representados por el director de Ingenierías el Doctor **Denis Jesús Aguilar**, Vicerrector Doctor Diego Chacón, en representación y apoyo a la universidad el Doctor **Claudio Lucena** (Brasil) cumplió también su representación como veedor del evento, Doctora **Nazly Borrero** (Colombia) como co-organizador y creación del evento y la Licenciada **Sandy Palma**.

- **PATROCINADORES**

  - UTH – Universidad Tecnológica de Honduras.
  - ISOC (Internet Society) Capitulo Honduras.
  - RDS (Red de Desarrollo Sostenible) – Punto .HN.
  - Ser Cargo Express.
  - UTH Florida.
  - Cofisa Honduras.
  - Marca Honduras.
  - GK7.
  - Startup Honduras.
  - ASI Network.
  - COLADCA.

- **COORDINACIÓN**

Personal Directivo y logístico de la Universidad Tecnológica de Honduras Sede San Pedro Sula.

- **PUBLICIDAD Y DIFUSIÓN**

La publicidad y difusión fue a cargo de la Universidad Tecnológica de Honduras Sede San Pedro Sula, por medio de la página web de la Universidad, Pagina web del evento, redes sociales como Facebook y Twitter.

www.igfhonduras.com.hn

#IGFHonduras2019

- **Expectativa**

Generar la importancia y conciencia en la gobernanza del internet y de crear nuevas políticas nacionales para el buen uso de la misma tanto público como en el sector privado. Teniendo en cuenta todas las aplicaciones y manejo de las herramientas del Internet y lo que conlleva, también teniendo en cuenta el control que pueda esta tener en los distintos sectores como son el sector público - gobierno e infraestructuras críticas, sector privado como es el sector bancario, sector académico, sociedad civil y fuerzas armadas (ejército, policial, naval y aéreo).

- **AGENDA**

DÍA 1 - MIÉRCOLES, 20 DE MARZO DE 2019

08:00 08:20	–	Registro de Participantes
08:20 08:50	–	**Ceremonia de Apertura** **Entonación del Himno Nacional** **Evento Artístico** **Mesa Principal** Lic. Roger Danilo Valladares Varela, presidente de la UTH; Máster Roger Enrique Valladares, vicepresidente de la UTH; Dr. Javier Mejía, Rector General de la UTH; Máster José Mora, vice rector Académico de la UTH; Dr. Diego Chacón, vice rector Relaciones Exteriores de la UTH; Dr. Denis Jesús Aguilar, director de la Facultad de Ingeniería de la UTH; Ing. Héctor Leonel Ayala Alvarenga, Secretario de Gobernación, Justicia y Descentralización de Honduras; Señor Emilio Silvestri Ministro de Turismo de Honduras / Señor Guillermo Orellana Viceministro de Turismo de Honduras; Dra. Nazly Borrero - Especialista de Colombia y el Dr. Claudio Lucena - Especialista de Brasil **Palabras Alusivas** - Palabras del Ing. Héctor Leonel Ayala Alvarenga – Secretario de Gobernación, Justicia y Descentralización de Honduras - Palabras del Sr. Roger Danilo Valladares Varela, presidente de la UTH
08:50 09:20	–	**La Ciberseguridad y la Protección de Datos** Sandy Palma (Honduras)
09:20 09:50	–	**Fronteras Invisibles de los Ciberacosos en Niños, Niñas y Adolescentes y su Tipificación en Latinoamérica** Nazly Borrero (Colombia)
09:50 10:20	–	Toma de Fotografía Oficial (Todos los Participantes)

10:20 10:30	–	Coffee Break
10:30 11:00	–	**Automación y el Futuro Del Trabajo: Elementos de una Ruta Estratégica para la Educación en Ambientes Digitales** Claudio Lucena (Brasil)
11:00 11:30	–	**La Transformación Digital en el Sector Industrial y sus Impactos en la Sociedad de la Información** Daniel Monastersky (Argentina)
11:30 12:00	–	**Los Delitos Informáticos en Honduras, Los Operadores de Justicia y Medios Probatorios** Juan Aguilar Godoy (Honduras)
12:00 13:00	–	Almuerzo
13:00 14:00	–	PANEL NO. 1: **RETOS PARA EL PRESENTE Y FUTURO EN MATERIA DE CIBERSEGURIDAD EN LATINOAMERICA:** Sandy Palma, Nazly Borrero, Juan Aguilar Godoy, Claudio Lucena y Daniel Monastersky **Moderador**: Eduardo José Tome Peralta de ISOC Honduras
14:00 15:00	–	Mesas de Trabajo
15:00 15:10	–	Coffee Break
15:10 15:50	–	Presentación Resultados De Las Mesas De Trabajo
15:50 16:00	–	Palabras De Cierre Del Primer Día

AGENDA
Día 2 - jueves, 21 de marzo de 2019

08:00 – 08:30	Registro de Participantes
08:30 – 09:10	**Conferencia Nacional – PENDIENTE DE CONFIRMAR** Javier Mejía (Honduras)
09:10 – 09:50	**Análisis Sistemático de los Ciberataques, para fortalecer las Defensas de los Servicios** María Angélica Castillo (Perú)
09:50 – 10:00	Coffee Break
10:00 – 10:40	**Gestión de Riesgos en la "nueva" Era Digital** Arístides Contreras (Colombia)
10:40 – 11:20	**Diseño de un SOC como Estrategia De Seguridad** Niurka Hernández (Venezuela)
11:20 – 12:00	**Ciberseguridad y Ciberdefensa: Estructura Críticas** Gustavo Guzmán (México)
12:00 – 13:00	Almuerzo
13:00 – 14:00	PANEL NO. 2: **AVANCES EN CIBERSEGURIDAD Y CIBERDEFENSA EN LATINOAMERICA:** Javier Mejía, María Angélica Castillo, Arístides Contreras, Niurka Hernández y Gustavo Guzmán **Moderador**: Dr. Claudio Lucena
14:00 – 15:00	Mesas de Trabajo
15:00 – 15:30	Presentación Resultados De Las Mesas De Trabajo
15:30 – 15:40	Coffee Break

15:40 – 15:50	Entrega de Reconocimientos a Conferencistas y Panelistas y Foto Oficial de Estos
15:50 – 16:00	Palabras De Clausura Del IGF Honduras 2019

- **PERFIL CONFERENCISTA, PANELISTAS Y MODERADORES**

Daniel Monastersky

Doctor en protección de datos personales, delitos informáticos, robo de identidad y reputación online; Fundador de Ciberseguridad LATAM, medio especializado en la temática. Actualmente es el Asesor Legal del Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires (BACSIRT); Executive Certifícate en Gestión y Estrategias de la Ciberseguridad por la Universidad Internacional de Florida (FIU), Estados Unidos.; Miembro de The International Association of Privacy Professionals (IAPP). ; Miembro del Antiphishing Working Group (APWG); Miembro del Consejo Asesor en el Foro Mundial de Ciberseguridad (GFCE); Es Director de la Diplomatura en Gestión y Estrategias de Ciberseguridad de la Universidad CEMA; Seguridad Informática de la Jefatura de Gabinete de Ministros de la Argentina; Presidente de la ONG Ideas que Transforman.

Nazly Borrero

Máster en Derecho Informático y Nuevas Tecnologías. Actualmente es CEO de la compañía IT Service and Beratung SAS, con Presencia en Colombia y Argentina Ingeniera Informática, igualmente cuenta con estudios en las especializaciones y diplomados en Gerencia Estratégica, Auditoria Informática ISO 27001 Seguridad de la Información, e ISO 9001 Control y Calidad, Perito Informático externo; Speaker y organizadora de varios congresos internacionales, en temas de Ciberseguridad y Ciberacosos; Investigadora de Drogas Auditivas y sus efectos; Autora de varios artículos técnicos publicados en universidades de la región, y de los libros: A un click de enredarse; No te enredes y clickea mejor; Fronteras invisibles de la ciberseguridad; A un Click de Enredarse Recargado y Clickea y Procede Mejor.

Niurka Hernández

Especialista en Gerencia, mención Redes y Telecomunicaciones; Licenciada de Administración, ISACA, CRISC; Certificación; Técnico En Informática Ciclo de Webinar ISOC Cybersecurity SIG, 2017 / 2018; Octava Escuela del Sur de Gobernanza de Internet. EEUU Washington DC, mayo del 2018; Ciclo conferencias de Tendencias Tecnológicas y Ciberseguridad, República Dominicana 2018/2017; Modulo Cómo constituir un CERT Nacional y sus Aspectos Básicos, en el Curso Protección de las Infraestructuras Críticas (de la Información) (CIIP), del centro de Estudios Avanzados en Banda Ancha para el Desarrollo (ceabad), Costa Rica2017/2018; IV Simposio internacional de ciberdefensa, ciberseguridad, ciberinteligencia, retos y amenazas.

Gustavo Guzmán

Académico mexicano y especialista en el área de Gobierno de TI y Ciberseguridad; Asesor y consultor para el sector público y privado en el desarrollo de proyectos y soluciones integrales e innovadoras en materia de Gobierno Electrónico, Protección de Datos, Participación Ciudadana, Seguridad

Sandy Palma

Especialista en Acceso a la Información Pública; Actualmente ejerce el cargo Jefe de la Unidad de Transparencia y Acceso a la Información Pública de la Secretaría de Gobernación, Justicia y Descentralización, siendo funciones primordiales: garantiza el acceso a la información pública que genera / custodia nuestra institución; actualización del Portal de Transparencia Institucional; redacción de los informes institucionales sobre el cumplimiento de LTAIP; emisión de los procesos correspondiente para garantizar la protección de la información que contiene los datos personas, información confidencial y reservada en custodia de nuestra Secretaría. Auditor de ISO 9000.

María Angélica Castillo

Ingeniera Informática, Magister en Ingeniería de Sistemas, estudios de Master en Ciberseguridad. Con especializaciones en Ingeniería Software, Gestión de Proyectos TI, Auditoría de TI, Ciberseguridad (España, Israel, USA, Panamá y Perú), CISO Seguridad de la Información, Certificación ISO/IEC 27032.

Nacional y Ciberseguridad; Representante activo de la academia mexicana, del Instituto Politécnico Nacional y miembro activo de diversas organizaciones a nivel nacional e internacional en temas relacionados a la Gobernanza de Internet y la Ciberseguridad.

Actual Jefa de Oficina de Tecnologías de la Información del Ministerio de Relaciones Exteriores Perú. Con más de 20 años de experiencia en el ámbito de tecnologías de la información, telecomunicaciones, estrategia digital y ciberseguridad. Autora de publicaciones en inteligencia artificial, algoritmos metaheurísticos y GRASP reactive.

Eduardo Tome Peralta

2016-2018: Secretario Capitulo – Internet Society Capitulo Honduras (Miembro Fundador); 2018-2020: Vicepresidente – Internet Society Capitulo Honduras; Miembro – Youth SIG (Observatorio de la Juventud); Coordinador Grupo Trabajo Políticas – LACTLD (2019); Reunión Consultiva de Expertos en Materia de Derecho de Asociación en el Entorno Digital – Ciudad de México – ICNL (Centro Internacional de Derecho No Lucrativo) (2019; LACNIC 29– Fellow (Ciudad de Panamá); Taller Legal y de Politicas – LACTLD (Ciudad de Panamá); ICANN 62 – Policy Meeting (Ciudad de Panamá); Youth LACIGF 3 (Buenos Aires); Talle de Capítulos – Internet Society- 2018 (Fellow)– Campaña Redes Comunitarias

Claudio Lucena

Profesor y ex Decano de la Facultad de Derecho de la Universidad Estadual da Paraíba Brasil, investigador de la Agencia Gubernamental Portuguesa Fundación para la Ciencia y la Tecnología, afiliado al Research Center for the Future of Law de la Universidad e Católica Portuguesa. Miembro del Grupo de Investigación en Inteligencia Artificial y Inclusión del ITS-Rio. Investigador Visitante en la Universidad de Haifa, en Israel, y en la Facultad de Derecho de la Universidad e de Georgetown, en Washington. D.C. LLM en Derecho Internacional y Europeo de Vrije Universiteit Brussel y Licenciado en Ciencias de la Computación por la Universidad e Federal Campina Grande, Brasil. Es Fellow de ICANN, del Foro

(Buenos Aires); LACIGF 11 - Buenos Aires; 2018 Internet Society IGF Ambassadors Fellow (Paris)

Arístides Contreras
Presidente Ejecutivo de la Comunidad COLADCA, Comunidad Latinoamericana de Consultores y Asesores en Gestión de Riesgos y Seguridad, es Profesional Certificado en Gestión de Riesgos, Seguridad y Prevención de Pérdidas, Consultor y docente con Resolución emitida por la Superintendencia de Vigilancia y Seguridad Privada de Colombia.

Latinoamericano de Gobernanza de Internet y de la Escuela Sur de Gobernanza de Internet (SSIG). Observador acreditado en el Foro de Gobernanza de Internet en Ginebra y miembro de la Comunidad de Expertos Octopus Cybercrime del Consejo de Europa, de los Capítulos Brasil y Portugal de Internet Society.

Juan Aguilar Godoy
Comisionado de policía profesional de las ciencias jurídicas con orientación penal y de las ciencias policiales, especialista en límites y fronteras, egresado de la maestría de seguridad humana, con conocimientos amplios en delitos informáticos adquiridos en Colombia, España, Alemania, estados unidos, cuba, México, República Dominicana. conferencia e-Goberment, Oracle, (gobierno electrónico) México D.F.; seminario sobre “manejo de incidentes de seguridad cibernética y firmas electrónicas”, Can José Costa Rica; seminario sobre “creación avanzada de csirt”, San José costa rica; curso de “delitos de alta tecnología y terrorismo”, San Lorenzo del Escorial, España; curso de delitos informáticos, Bogotá, Colombia; taller de creación de CSIRT (equipo de respuesta ante incidencias de seguridad cibernética) EE.UU. Washington D.C.; diplomado de ciberseguridad y ciberdefensa, Universidad

de Defensa Nacional, Honduras; curso de “manejo y administración de evidencia digital”, impartido por la Policía de Kentucky, junio de 2018, Escuela de Investigación Criminal, Comayagua, Honduras.; curso de “desarrollo de capacidades de investigación cibernética” impartido por la Policía de Corea, Universidad Nacional de la Policía, noviembre de 2018, Tegucigalpa M.D.C. Honduras.

COBERTURA

- Para el evento se realizó vía Streaming por medio de un canal dedicado otorgado por ISOC Chapter Honduras y .hn.
- Se realizó un Facebook Live durante los dos días en su transmisión.
- En diferido el Canal Nacional TeleProgreso realizó un especial sobre el evento con el tema de la Conferencista Nazly Borrero Vasquez.

Asistentes en Línea 524 conexiones a nivel Latinoamericano. (Información entregada por ISOC Chapter Honduras).

PRENSA

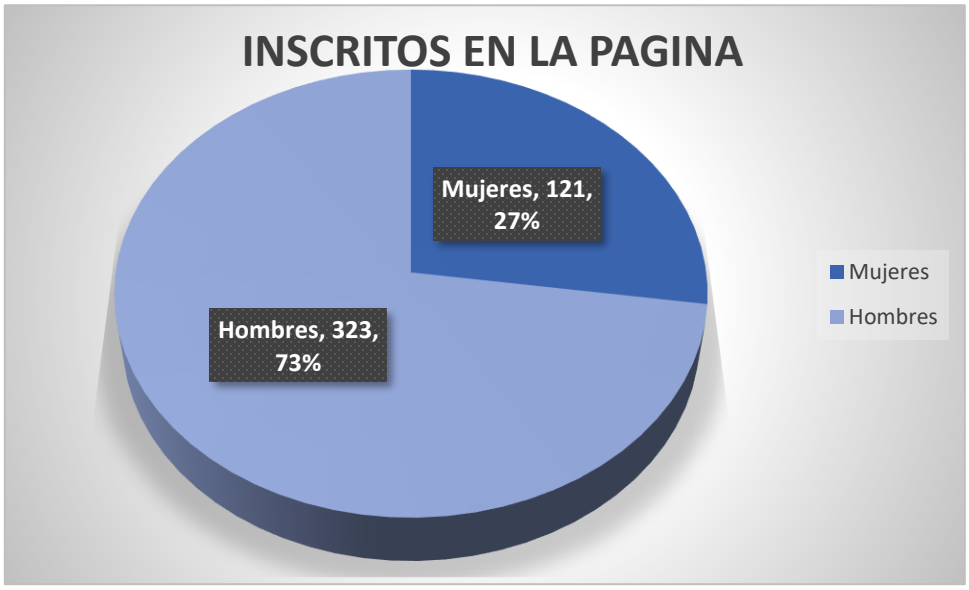
La cobertura en cuanto a prensa la realizaron:

- Periódico El País de Honduras - Publicada en la ciudad San Pedro Sula.
- Periódico La Prensa de Honduras – Publicada en la ciudad San Pedro Sula.
- Canal TeleProgreso – Canal Nacional de Honduras.

ESTADISTICAS

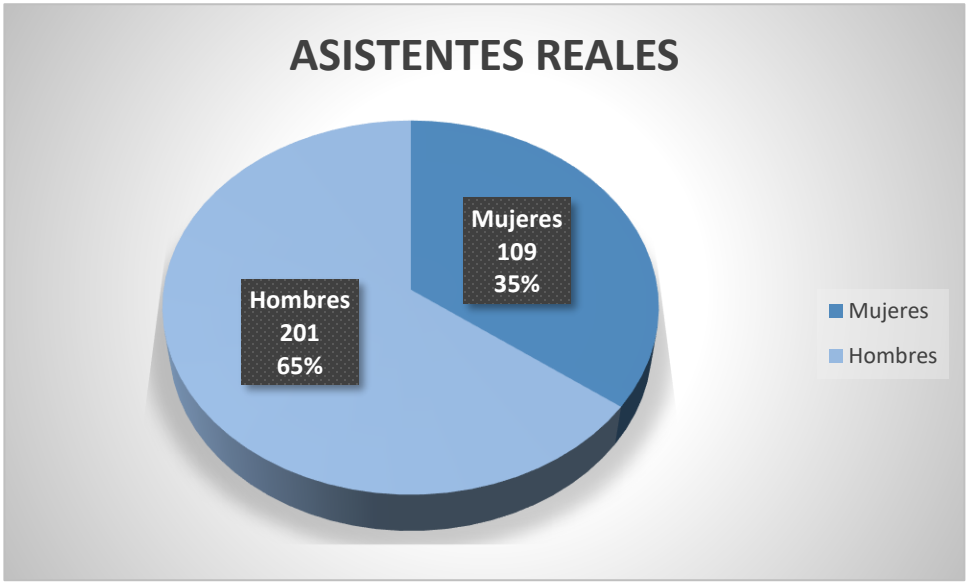
INSCRITOS EN LA PÁGINA

Asistentes	Cantidad
Mujeres	121
Hombres	323
Total	445



ASISTENTES AL EVENTO DE FORMA PRESENCIAL

Asistentes	Cantidad
Mujeres	109
Hombres	201
Total	310



De las personas registradas **12** son de **Guatemala.**

Asistentes en Línea 524 conexiones a nivel Latinoamericano. (Información entregada por ISOC Chapter Honduras).

FINANZAS

PRESUPUESTO DE IGF HONDURAS 2019		
Actividad	**Presupuestado**	**Real**
Alimentacion conferencistas/asistentes	L. 90.000,00	L. 197.618,00
Boletos Aereos mexico	L. 10.760,00	L. 10.760,00
Boletos Aereos Peru	L. 27.345,00	L. 27.345,00
Boletos Aereos Republica Dominicana	L. 23.511,00	L. 23.511,00
Boletos Aereos Colombia	L. 13.495,00	L. 13.495,00
Boletos Aereos Colombia	L. 13.410,00	L. 13.410,00
Boletos Aereos Argentina	L. 31.260,00	L. 31.260,00
Boletos Aereos Argentina	L. 31.260,00	L. 31.260,00
Claudio Lucena	L. 52.540,00	L. 52.540,00
Hotel (6 personas) por 6 dias	L. 76.907,36	L. 117.172,80
Diplomas, Tarjetas, Afiches,Cuadernos publicidad	L. 112.990,35	L. 172.284,38
Camisetas	L. 24.035,00	L. 31.464,00
Placas de reconocimiento		L. 7.244,50
Capitolio alquiler de mesas/ sala lounge		L. 4.370,00
Total	**L. 507.513,71**	**L. 733.734,68**
Equivalente $ Americanos		**$ 29,948.35**

- **GALERÍA FOTOGRÁFICA**

- Desarrollo del Evento

Primer Día

- **Inauguración e inicio de Ponencias**


ASISTENTE

- **CONFERENCIAS**


CONFERENCISTA

Foro

- **MESAS DE TRABAJO**


UTH
Salida

SEGUNDO DÍA

- **CONFERENCIAS**


CONFERENCISTA

- **FORO**

- **MESAS DE TRABAJO**

- **CLAUSURA**


UTH


KASPERSKY
Suscripción Mensual
Kaspersky Endpoint Security for Business
HONDURAS.TRAVEL
APRENDE, PRÁCTICA Y CERTIFICATE

SEGUNDA PARTE – MEMORIAS CONFERENCIAS Y CONCLUSIONES

FRONTERAS INVISIBLES DE LOS CIBERACOSOS EN NNA (NIÑOS, NIÑAS Y ADOLESCENTES) Y SU TIPIFICACIÓN EN AMÉRICA LATINA

Ing. Nazly Borrero Vásquez
Colombia

Resumen:
El uso de las Tecnologías de la Información y de la Comunicación – TIC, se ha venido incorporando en nuestra vida cotidiana y esto conlleva a que haya un constante intercambio de información y comunicación, conllevando a nuevos riesgos y amenazas afectando la seguridad en los sistemas de información pública y privada y que ha hecho que algunas organizaciones realicen una contante concientización de ellas mismas y a todos los ciudadanos. Citando leyes, decretos y exigencias para poder neutralizar el flagelo de la ciberdelincuencia; ha sido de muy buena aceptación para la ciudadanía ya que se ha demostrado resistencia en estas, pero por otro lado la sociedad no acepta las penas leves que versan estas normativas.
La Ciberseguridad y la Seguridad de la Información le exige a todas las empresas tanto públicas como privadas exigen un constante proceso de mejora continua y sistematizada para buscar minimizar la exposición de información determinando los posibles puntos que se puedan comprometer la integridad, disponibilidad y confidencialidad que estos gestionan, estableciendo criterios que permiten potenciar la seguridad.

Pero un enfoque real de la Seguridad de la Información nos enfocamos en algo muy necesaria en la gobernanza en el buen uso de las redes sociales que hoy en día están dentro de las necesidades del hombre, ya que sin ella no sabes con quien estas interactuando, como también verificar si esa persona es real, como saber quiénes son los más afectados, como poder litigar frente a estos modus operandi cuando no se tiene de una tipificación objetiva en el código penal, a esto como valor agregado como hacen otros países para realizar una buena cadena de custodia y para este tipo de "delitos" y no afectarla para un juicio, cual es la importancia de la protección de los datos personales desde el tiempo escolar hasta las empresas públicas y privadas.
Las leyes no son para censurar, o eliminar información es para concientizar, educar y llevar una mejor autonomía.

Palabras Claves:

- **Ciberseguridad**: Según ISACA (*Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información)*, se define la Ciberseguridad como "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".[1]

- **Habeas Data**: Es la facultad que tienen todas las personas de conocer, actualizar, rectificar y suprimir las informaciones recogidas en bancos de datos y en archivos de entidades públicas y privadas, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales, teniendo en cuenta las leyes y constitución política del país.

- **Normas ISO**: Las normas ISO son documentos que especifican requerimientos que pueden ser empleados en organizaciones para garantizar que los productos y/o servicios ofrecidos por dichas organizaciones cumplen con su objetivo.[2]

- **Tipificación**: En el código penal establece con exactitud y precisión qué actos son realmente un delito. Esto implica que un delito está tipificado y, por lo tanto, definido.[3]

- **NNA**: Niños, Niñas y Adolescentes.

- **Convenio de Budapest**: Convenio que establece los principios de un acuerdo internacional sobre seguridad cibernética y la sanción de delitos cibernéticos.

[1] http://www.audea.com/es/diferencias-ciberseguridad-seguridad-la-informacion/

[2] https://www.isotools.org/normas/

[3] https://www.definicionabc.com/general/tipificar.php

INTRODUCCIÓN:

En el inicio de la cuarta revolución industrial, vemos como está avanzando a pasos agigantados y cada vez más rápido; haciéndonos sensibles e inseguros en nuestro entorno. Donde estos cambios tecnológicos a los cuales no estamos preparados y en el que nuestra información sea vulnerada y de fácil acceso.
Con el pasar de los años se ha incrementado la fabricación de dispositivos con acceso a la red externa de una forma sencilla e inmediata, gracias a estos avances tecnológicos se ha logrado agilizar procesos, como también se ha logrado incluir una cantidad de usuarios del común con la que no se contaba hace un tiempo; descuidando el tema de la seguridad de la información. Conllevando a la creación de nuevos delincuentes cibernéticos conocidos como “Crackers”, los cuales se han encargado de poner en riesgo la privacidad del comercio electrónico, de tratamiento y almacenamiento de datos de empresas y usuarios, ya que nos volvemos dependientes de los dispositivos tecnológicos como equipos de cómputo, tablet, celulares, etc. generando un incremento de riesgos al momento de conectarse con el exterior.
Y es aquí donde el tratamiento de la información y las comunicaciones se fue aprovechando para cometer delitos cibernéticos como el Ransomware, Phishing, Malware, Trojanos, y ciberacosos como son el Child Grooming, Ciberstalking, en donde están dentro de la denominación de Ciberbullying, ya que es iniciada por esta caracterización; por nombrar algunos de los ciberdelitos que hoy en día son el común denominador causada por esta revolución.

CONTENIDO*:*

La Ciberseguridad en Latinoamérica es un tema que poco a poco se está construyendo, aunque ha sido un poco lenta ya que se cuenta con muy pocas políticas establecidas, donde vemos que solo hay más atención en otras vulnerabilidades que en esta nueva revolución tecnológica la cual se conoce como la nueva guerra de la década.

Donde esta guerra sólo la ganan los que estén tecnológicamente preparados y es ahí donde nos preguntamos. ¿Cómo actúan? ¿A quienes atacan? ¿Quiénes son?, Y si realmente estamos dispuestos para esto, ya que cada día la tecnología avanza

como la velocidad de la luz, en el que vemos que las capacidades de almacenamiento están cada vez más grandes y que nos demuestra que los canales de la ciberseguridad son vulnerables, dejando las personas con la capacidad nula de inventar nuevos protocolos para cubrir la información de tantos ataques cibernéticos y otras amenazas, de las cuales grandes empresas han sido vulneradas en su seguridad, a pesar de contar con blindaje de última tecnología para evitar el ingreso de estas.

En Colombia, según la Unión Internacional de Telecomunicaciones (UIT), notificó el 30 de noviembre de 2016[4], los resultados del índice mundial de Ciberseguridad mostrando a Colombia en el 9 puesto de Latinoamérica destacando países como Uruguay, Brasil, Estados Unidos y Canadá, como también se debe tener en cuenta que Colombia ocupa el puesto 9 a nivel mundial, mostrándose fuerte en sus medidas de jurídicas con leyes de orden penal, teniendo en cuenta los delitos contra la intimidad, privacidad, informáticos como tal, dando así excelentes resultados en cuanto al manejo de la ciberseguridad, y el manejo de la protección de datos personales tanto financieros como los personales, utilizados por las empresas a nivel nacional.

Teniendo en cuenta la normativización jurídica no podemos dejar de lado la tipificación legal de los acosos cibernéticos, como son el Ciberbullying, Child Grooming, Sexting, Happy Slapping, Ciberstalking, Gossip, sin dejar atrás los Juegos de reto que se han puesto de moda tanto en las redes sociales como en la mensajería instantánea, afectando cada día a todos los cibernautas menores de edad. Entonces de aquí surge otra pregunta, ¿Cómo estamos en la seguridad de los ciberacosos en Latinoamérica frente a otros países? Pues estas también son otro tipo de amenazas silenciosas, peligrosas y frecuentes de fronteras invisibles, ya que con estas se han desenlazado nuevos campos como son los Cibersuicidio, teniendo en cuenta más en Centro América y Sudamérica.

Referencias Bibliográficas.

- https://www.audea.com/es/diferencias-ciberseguridad-seguridad-la-informacion/

[4] https://ingenieria.bogota.unal.edu.co/noticias/item/1041-ranking-global-de-la-uit-situa-a-colombia-9-del-mundo-en-manejo-de-ciberseguridad

- https://www.isotools.org/normas/
- https://www.definicionabc.com/general/tipificar.php
- https://ingenieria.bogota.unal.edu.co/noticias/item/1041-ranking-global-de-la-uit-situa-a-colombia-9-del-mundo-en-manejo-de-ciberseguridad

LA REPUTACIÓN ONLINE Y SU RELEVANCIA EN LA ERA DIGITAL

Dr. Daniel Monastersky
Argentina

Resumen- Gobierno, empresas, instituciones y particulares requieren tomar medidas para poder ofrecer respuestas detalladas acerca de qué podemos hacer, tanto a nivel individual como colectivo, para velar por nuestra seguridad, la de nuestras comunidades y responsabilizarnos del nuevo mundo hacia el cual nos precipitamos. Debemos replantearnos la forma en la que utilizamos nuestros dispositivos y la vinculación que tenemos con la tecnología en general.

Palabras Clave- ciberseguridad, ciberdaño, reputación online, ciberadicciones

INTRODUCCIÓN

La tecnología ha logrado ocupar un lugar preponderante en la vida de los ciudadanos. Ese crecimiento exponencial que ha tenido no guarda en absoluto relación con cuestiones que requieren atención por parte de gobierno, organizaciones y empresas. Para evitar consecuencias no deseadas en la sociedad es fundamental contar con programas de concientización que puedan brindar herramientas y consejos tendientes a minimizar el impacto de un uso no responsable de las TICS. El uso impune de redes sociales y plataformas digitales, consistente en calumniar e injuriar a diestra y siniestra sin medir las consecuencias, tiene un correlato con la impunidad que hasta ahora los tribunales en general han resuelto en gran parte de los países.

REPUTACIÓN ONLINE Y SUS CONSECUENCIAS

La doctrina históricamente sostiene que uno de los fines de la pena es mantener la vigencia de la norma y que, mediante la sanción ante su incumplimiento, se reafirma el valor social de los bienes jurídicos lesionados que, por ser estos penalmente protegidos, se consideran fundamentales. Es así que no castigando la afectación del honor la justicia contribuye a que el mismo bien se siga afectando, se erosiona de esta manera la conciencia social del valor del bien y del respeto por la norma y el derecho.

El honor no es lo único que se ve afectado. La reputación es la opinión que los terceros tienen respecto de una persona. En la era de Internet, esta se construye a partir de lo que los individuos piensan en virtud de la información que existe sobre ellos en la red. ***Uno es quien Google dice que es***, de ahí radica la importancia del contenido que se exterioriza y difunde a través de las plataformas digitales. Incluso una mala reputación online genera un sinnúmero de daños que no solamente

abarcan la percepción de los demás sobre uno, sino también una afectación económica y laboral.

Es conocido que casi la totalidad de las empresas que buscan candidatos, googlean a los mismos. Una reputación online negativa es peor que una primera mala imagen, y como esta, te niega una segunda oportunidad.

La viralización que se consigue a través de internet maximiza el daño, lo convierte en un perjuicio con alcance global, es decir, cualquier persona se encuentre en el país que se encuentre podrá asociar aberrantes delitos con el de una víctima inocente.

El ciberdaño como vemos causa perjuicios a las personas a nivel físico, psicológico y reputacional. Aunque mucho se habla sobre el impacto del cibercrimen en la economía, estas consecuencias que recaen sobre los individuos no están siendo magnificadas en su totalidad.

Internacionalmente se ha consagrado el derecho al honor y a la dignidad de la persona como uno de los derechos fundamentales del hombre, entonces, desde esa óptica ¿bajo qué criterios podemos dejar que se avasallen los mismos con impunidad?

La jurisprudencia es clara en los criterios a considerar en situaciones análogas que ocurren a través de medios tradicionales y prensa escrita. Es decir, en dichos casos se evalúa si se ha individualizado de forma clara a la persona a la cual se le atribuye un delito, si se ha enunciado de forma afirmativa el hecho que se endilga y si se han citado fuentes de las cuales se ha obtenido esa información.

Vivir en una democracia implica poder expresar lo que uno quiere pero también hacerse cargo de lo que uno dice. De ningún modo puede acusarse de restringir la libertad de expresión a quien ven vulnerado su derecho al honor, pues estos derechos son autónomos y en un estado de derecho moderno no se puede permitir que se sacrifique a un individuo en pos del resto, que se menoscaben los derechos de un ser humano en pos del interés público.

El honor, es el plexo de autoestima personal y ética de un sujeto, referidos a sus comportamientos sociales; plexo que, atacado por el desvalor de una acción ofensiva y puntual, puede originar la réplica defensiva con consecuencias jurídicas e integraciones reparadoras.

CONCLUSIONES

Es fundamental que se creen los mecanismos necesarios para que la sociedad toda cuente con la información necesaria para repensar, analizar y tener identidad propia, creando estructuras gubernamentales que trabajen mancomunadamente en el acceso a una educación digital desde una edad temprana. Eso se debe complementar con un plexo normativo actualizado que tenga en cuenta las nuevas modalidades delictivas que la sociedad actual requiere.

LOS DELITOS INFORMÁTICOS EN HONDURAS, LOS OPERADORES DE JUSTICIA Y LOS MEDIOS PROBATORIOS.

Lic. Comisionado Juan Manuel Aguilar G.
Honduras

Resumen- *Considerando que nuestra sociedad a menudo se ve afectada por diferentes fenómenos jurídico - sociales siendo uno de estos los Delitos Informáticos y la falta de Legislación aplicable a los mismos, lo que genera impunidad en la aplicación de la Ley, ya que los delitos son tratados y encasillados de manera no convencional, ejerciendo la acción penal analógica, aun y cuando el derecho Penal no existe la analogía.*

El derecho positivo hondureño trata de dar una respuesta concreta ya que sus instituciones jurídicas han sabido perdurar a lo largo de los años, asimilando nuevas técnicas y nuevas costumbres; pero no cabe la menor duda que vacila ante el fenómeno cambiante y emérgete de las Tecnologías de la Información y las Comunicaciones (TIC), el cual ha sacado del esquema la norma legal vigente, no pudiendo la misma llevar el paso tecnológico de los medios informáticos, quedándose rezagada a la aplicación de normas procesales y penales a las nuevas tendencias delictuales, por ende estos actos o conductas no se encuentran contenidas dentro de los parámetros establecidos dentro de la legislación penal vigente, es decir no existe el principio de legalidad que las regule, el cual establece que no hay pena sin ley.

Las Instituciones encargadas en Honduras por velar por la aplicación y cumplimiento de la ley no se encuentran preparados para hacerle frente a los Delitos Informáticos, Los Operadores de Justicia suelen adaptarse con lentitud a las nuevas tendencias, mientras que los grupos delictivos organizados tienden a adaptarse rápidamente y a aprovechar los adelantos tecnológicos debido a los inmensos beneficios que producen sus actividades ilícitas. Los medios de prueba que se presentan ante el Órgano Jurisdiccional del Estado no presentan integridad y autenticidad, o los peritos contaminaron la escena del suceso y en algunos casos los indicios.

Palabras Clave- Ciberdelincuencia, Ciberseguridad, Delitos Informáticos, normativa legal, medios probatorios, Operadores de Justicia, Peritajes Informáticos.

***INTRODUCCIÓN*.**

La presente ponencia pretende describir y analizar la vulnerabilidad de la sociedad hondureña en relación a las tendencias delictuales modernas, su adopción por grupos del crimen organizado y delincuencia común, los que realizan acciones con la impunidad que la escasa preparación profesional y científica de los operadores de justicia les proporcionan, aunado a esto la falta aplicación de técnicas, procedimientos y políticas destinadas a darle un tratamiento a estas actuaciones de naturaleza criminosa.

En la actualidad los nuevos sistemas de info- telemáticos no sólo se utilizan como herramientas de soporte a las actividades humanas, sino como un medio eficiente para obtener y conseguir información. Estas nuevas tecnologías se transforman en un medio de conexión, en tecnologías cuya esencia se resume en la creación, almacenamiento y transmisión de data y video que puede alterar los comportamientos de los usuarios de los mismos. Esto permite procesar y encontrar a los usuarios de la red de redes, una cantidad innumerable de información relacionada con el conocimiento humano, con lo científico, lo técnico, lo profesional y hasta personal. Es dable asegurar que en la informática no existen límites previsibles, incrementado ello, con el transcurso de los años, haciendo cada vez más difícil e imperceptible la investigación de estos hechos ya sea por los avances cada vez mayores y la brecha que existe entre los entes encargados de hacer cumplir la ley y los infractores de la misma.

Es una realidad, que, en la actualidad, la humanidad guarda más información en soportes informáticos, que en papel. En Internet encontramos más información que toda la contenida desde que el ser humano pudo darse a entender de diferentes formas, ya sea en petroglifos, con jeroglíficos, o con la utilización del papel, hoy en día el uso de escritura digital no sustituye a la contenida en soporte físico como el papel, pero la supera ampliamente, y día con día va ganando más territorio, un ejemplo de ello lo constituye la cantidad de pericias forenses informáticas que las que se realizan, utilizando medios tecnológicos para su evacuación, dejando en el pasado los soportes documentales contenidos en papel. Este constante crecimiento del número de litigios relacionados con los delitos de naturaleza informática, en los cuales el ciberespacio desconoce las barreras humanas denominadas fronteras, por lo cual estas acciones delictuales requieren de PERITAJES INFORMÁTICOS, en donde la constante, es la globalización mundial de estos sistemas, en los cuales se producen fenómenos atípicos (No convencionales en algunos países) que trata de resolver el Derecho Internacional, en los que el autor realiza la acción delictiva en un país, la misma surte efecto en otro Estado y el fruto de esta acción ilícita es gozada por un ciudadano de

nacionalidad distinta a los anteriores y que reside en una nación diferente a las señalas, por lo cual nos preguntamos:

- ¿Qué Estado conocerá del hecho?
- ¿En dónde se realizó la acción criminosa?
- ¿Es un hecho delictivo de acuerdo a las normativas legales de cada país?
- ¿En qué país cumplirán condena?
- ¿Quién tiene la Jurisdicción y la Competencia para conocer este delito?

De la problemática planteada, lo más alarmante, no son los adelantos de los ciberdelincuentes, sino el desconocimiento de las técnicas propias de una pericia, empezando en la escena del suceso donde los Operadores de Justicia cometemos los peores errores en nombre del tratamiento del delito, de la misma forma se actúa cuando se evacuan los medios probatorios, por lo cual es de imperante necesidad hacer desde el levantamiento y custodia de los indicios, hasta la presentación de las pruebas, un trabajo eminentemente científico y profesional.

Es fundamental hacernos un auto evaluación y contestarnos con sinceridad estas preguntas:

- ¿Cuál es el nivel del Sistema Penal hondureño para hacerle frente a las nuevas tendencias delictuales denominadas Delitos informáticos?

- ¿Cuál es el nivel científico-profesional de los operadores de Justicia en el manejo de los indicios encontrados en la escena del suceso, o presentados ante el órgano jurisdiccional del Estado como medio probatorio, con el objeto de incorporarlo al proceso y llegar a la verdad de los hechos?

Los objetivos que se pretende establecer en relación al caso hondureño son los siguientes, se pretende analizar el nuevo Código Penal hondureño, en el cual se aborda de manera diferente los delito cometidos por medios telemáticos, por otro lado el rol de los operadores de justicia en el tratamiento de las nuevas tendencias delictuales denominadas Ciberdelitos o delitos informáticos, señalando las falencias de la institucionales encargadas de su tratamiento, en especial en la escena del suceso o como medios probatorios. De la misma forma se dará una mirada somera a los tratados internacionales de los cuales Honduras es parte, destinados a proteger a la ciudadanía de los delitos informáticos.

En nuestro país se cometen delitos informáticos, los cuales generan daños que están afectando a todas las instituciones en especial a la banca y el comercio, pero

más grande aun, es la impunidad que estos hechos proporcionan a sus autores, los cuales evaden desde cualquier perspectiva el sistema legal hondureño ya que el mismo se encuentra en una flagrante desventaja en relación a los nuevos adelantos tecnológicos, con los cuales cuentan estos ciberdelincuentes y que día a día se ensancha esa brecha existente.

Los adelantos tecnológicos se dan a pasos gigantescos, pero las reformas procesales, penales y policiales se caracterizan por su galopante lentitud, aunado a este problema la falta de una infraestructura forense-info - telemática de los operadores de justicia quienes llevan años y años de retraso técnico, que vuelven altamente vulnerable el sistema Jurídico hondureño.

El conocimiento en los delitos informáticos nos llevará a conocer la naturaleza de los mismos y la manera de cómo tratar este nuevo flagelo, el desarrollo tecnológico científico alcanzado por las mentes criminales y la fácil adopción de tecnología debilita y pone en desventaja a los operadores de justicia, quienes se quedan rezagados en las nuevas tendencias informáticas, las cuales día a día van generando cambio y transformando este mundo globalizado en un lugar vulnerable, en el cual los cibercriminales desarrollan sus conocimientos en detrimento de la ciudadanía, estos menoscaban las raíces morales de las sociedad hasta el punto de corromper a ciertos sectores de la misma.

En Honduras las personas naturales y jurídicas que son requeridas judicialmente por la supuesta comisión de un hecho criminoso en el cual se valió para su ejecución de tecnología informática, son dejadas en su mayoría, en libertad por no encontrarse los méritos necesarios o por la falta de pericia de los funcionarios que realizaron el tratamiento científico de los indicios que liguen a los imputados con la acción criminal o simplemente porque este acto no es constitutivo de delito en nuestro país.

Las nuevas tendencias integracionistas y mundiales definen a los operadores de justicia como garantes de los derechos sociales, económicos y culturales de la sociedad, entes estos que deben estar preparados para enfrentar estos cambios criminosos, por lo tanto deben de estar en constante preparación, con el objeto ayudar a mejorar la impartición de justicia, es difícil aceptarlo pero hay que hablar con la verdad, se han hecho avances significativos para darle tratamiento a estas nuevas formas delictuales, en especial la Policía Nacional, la cual ya cuenta con Laboratorios y equipos de punta que dan un verdadero valor científico a pericia forense informática, pero hace falta mucho en especial en el área de capacitación de todos los que conformamos las partes procesales, siendo ineludible que la legislación este acorde al nuevo actuar social, por lo cual es con la entrada en

vigencia del nuevo Código Penal, se contará con la normativa legal mejorará el tratamiento de estas conductas. [1]

REGULACIONES INTERNACIONALES DE LAS CUALES HONDURAS FORMA PARTE.

Dentro de las regulaciones que Honduras es signataria y sobre las cuales se han realizado acuerdos internacionales para ser incorporados al derecho positivo encontramos las siguientes:

- Declaración Universal de los Derechos Humanos, Adoptada y proclamada por la Resolución de la Asamblea General 217 A (iii) del 10 de diciembre de 1948.
- Convenio con la Organización Mundial de Propiedad de la Intelectual (OMPI) ,15 de noviembre de 1983, Ginebra, Suiza.
- Declaración y Programa de Acción del I Congreso Mundial contra la Explotación Sexual Contra Niños y Niñas, 1996.
- Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de Niños, Prostitución Infantil, el Turismo Sexual y la Utilización de Niños y Niñas en la Pornografía, 2002.
- La Convención contra la Delincuencia Organizada Transnacional, 2002.

NORMAS PENALES NO CONVENCIONALES EN HONDURAS. (ATIPICIDAD)

Un aspecto prioritario a resolver es la problemática existente en lo relativa a estos delitos, los cuales son generados por la ausencia de uno de los elementos del tipo penal cuando se trata de subsumir la conducta ilícita. Las infracciones ostensiblemente antijurídicas que recaen sobre ciertos bienes informáticos como el caso del Software, delitos contra el patrimonio económico especialmente: el Hurto, la Estafa y el Daño informático, aunque toca el ineludible tema de la falsedad informática, de inusitadas repercusiones en lo atinente a documento electrónico, accesos no autorizados a sistemas de procesamiento de datos, violación a la intimidad entre otros. [2]

Actualmente se requieren serias modificaciones y en otros casos nuevas normas

para disminuir en cierta forma la incertidumbre jurídica en que se encuentran sumergidas las nuevas disposiciones penales en materia de delito informático, pese a algunos avances, como la tipificación de delitos como la pornografía sexual infantil y derechos de autor.

Cada vez más, se hace necesario el respaldo legal como la mejor y más adecuada forma de reprimir y castigar estos delitos, esto si tomamos en cuenta la fecha en que entro en vigencia nuestro Código (sep. 1983), en resumen, los tipos penales ahí existentes, no tomaban en cuenta los novísimos adelantos de la informática y la telemática por tanto les hacía inútiles por no decirlo menos, para dar seguridad jurídica ante el posible asedio de la criminalidad informática.

Como ya lo hemos manifestado, en nuestro país los operadores de justicia son los encargados de darle tratamiento a los Delios, pero estos tienen una limitante en relación a los Delitos Informáticos, los que no se encuentran legislados, por lo cual y en virtud del Principio de Legalidad, las acciones cometidas por los ciberdelincuentes no son constitutivas de delito y se amparan en la gran sombra de impunidad que genera la falta de conceptos penales que definan y diferencien sus acciones criminosas. Los hechos punibles, que realizan tienen ciertas características de similitud con los tipificados en su normativa legal, pero los medios utilizados las encasillan en otra naturaleza delictual propia de delitos que han mutado y aprovechan los avances tecnológicos para escapar al reconocimiento legal como hechos delictuales.

Como un ejemplo a estos actos criminosos podemos encontrar la acción ilícita conocida como clonación de tarjetas de crédito, la cual se debe tomar como fraude electrónico ya que la misma conlleva un sinnúmero de acciones criminosas en un solo delito, como sería la obtención fraudulenta de data encriptado, acceso a las bases de datos, falsificación de documentos y robo entre otros, pero actualmente se está tomando esta acción como una mera estafa a las entidades bancarias, por lo que el inculpado es tratado de manera distinta a la verdadera dimensión del delito cometido, ya que en realidad pone a la luz pública la vulnerabilidad de los sistemas bancarios del país y las normas como el Estado trata esta acción delictiva.

En este ejemplo los Operadores de Justicia, en este caso las agencias de cumplimiento de la Ley desde el momento mismo de la detención, no conocen ante que delitos se encuentran y realizan las diligencias propias de una estafa, manipulando y contaminando los indicios por su falta de pericia, lo que puede provocar desde el inicio de la investigación nulidades por desconocimiento propio de los avances tecnológicos, posteriormente el caso es pasado a sede fiscal, donde el acusador del Estado se encasilla en las normas penales vigentes al infractor,

este es llevado a sede Judicial en donde el acusado es tratado por el delito de estafa y condenado por el mismo, desconociendo todos y cada uno de los operadores de justicia la cadena de acontecimientos que generaron la clonación de una tarjeta y que paso por distintas fases y momentos violentando diferentes normas hasta la comisión del delito, más aun el daño causado no se refleja en la acción delictual sino en el daño social y credibilidad de los entes financieros que son vulnerados, ya que la seguridad de los ahorros de una persona constituyen la piedra angular de las instituciones bancarias, quienes prefieren no denunciar estas actividades, ya que la reputación de su institución se encuentra en predicado por lo cual la impunidad de este actuar criminal se fortalece con el silencio de las víctimas, aunado por la falta de normativa legal y su aplicación por los operadores de justicia.

TIPIFICACIONES LEGALES EN HONDURAS EN RELACIÓN A DELITOS INFORMÁTICOS.

En su generalidad las conductas delictuales relacionadas a los Delitos Informáticos son encasilladas o tipificadas en nuestro país en los siguientes tipos penales.

- ***DAÑOS. (CÓDIGO PENAL)***

ARTICULO 254. Se impondrá reclusión de tres (3) a cinco (5) años a quien destruya, inutilice, haga desaparecer o de cualquier modo, deteriore cosas muebles o inmuebles o animales de ajena pertenencia, siempre que el hecho no constituya un delito de los previstos en el capítulo siguiente.

La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos, contenidos en redes, soportes o sistemas informáticos.
Será sancionado con reclusión de tres (3) a seis (6) años.

- ***ESTAFAS Y OTROS FRAUDES.***

ARTICULO 240. Comete el delito de estafa quien, con nombre supuesto, falsos títulos, influencia o calidad simulada, abuso de confianza, fingiéndose dueño de bienes, créditos, empresas o negociación o valiéndose de cualquier artificio, astucia o engaño, indujere a otro en error, defraudándolo en provecho propio o ajeno.

- ***DELITO FINANCIERO Y SUS PENAS.***

Artículo 394-A. Delito financiero.
Comete delito financiero la persona natural o jurídica a través de su representante legal, que por acción u omisión incurra en alguna de las tipificaciones delictivas establecidas en este capítulo.
Para los fines de este capítulo se denominará a la Comisión Nacional de Bancos y Seguros, como la comisión, y cuando se refiera a las Instituciones, se entenderán comprendidas todas aquellas supervisadas por la comisión de conformidad con el artículo seis (6) de la Ley de la Comisión.

Artículo 394-D. Operaciones financieras ilícitas.
Quien utilizando cualquier medio, en beneficio propio o de un tercero, se apodere, haga uso indebido u ocasioné la transferencia ilícita de dineros, valores, bienes u otros derechos de una institución supervisada, autorizada, a cualquier persona natural o jurídica, será sancionado con reclusión de tres (3) a seis (6) años cuando el monto del beneficio no exceda de diez mil (L. 10, 000.00) lempiras, y seis (6) a doce (12) años cuando exceda de dicho monto.

Artículo 394-E. Destrucción, ocultamiento, falsificación de información financiera para obtener un crédito.

Quien destruya, oculte o falsifique libros de contabilidad, libros sociales, documentos legales, certificaciones, constancias, Identidad personal, datos, registros, estados financieros, documentos cuyo soporte sea magnético o electrónico u otra información de una persona natural o jurídica, con el propósito de obtener, mantener o extender una facilidad crediticia o de capital de una institución supervisada.

Será sancionado con reclusión de tres (3) a seis (6) años cuando el monto del beneficio obtenido no exceda de diez mil (lps. 10, 000.00) Lempiras y se seis (6) a doce (12) años cuando exceda de dicho monto.

Artículo 394-F. Ocultamiento de irregularidades en la actividad financiera.
Quien destruya, altere, oculte o falsifique libros de contabilidad, libros sociales, documentos legales, certificaciones, constancias, registros en general, estados financieros, documento cuyo soporte sea Magnético o Electrónico u otra información o archivo de una institución supervisada, con el Propósito de encubrir, distorsionar o modificar maliciosamente operaciones activas o pasivas, obligaciones directas o contingentes, la iliquidez, la insolvencia u otras situaciones Fácticas que deban ser objeto de registro contable u otro tipo de registro, Será

sancionado con reclusión de seis (6) a doce (12) años.

Artículo 394-I. Utilización indebida de sistemas de procesamiento de datos.
Quien acceda ilegalmente a los sistemas de procesamientos de datos de las instituciones supervisadas, para alterar, borrar, dañar o sustraer registros, archivos u otra información de la institución o de sus clientes en beneficio propio o ajeno, será sancionado con reclusión de tres (3) a seis (6) años cuando el monto de lo defraudado no exceda de diez mil (L 10, 000.00) lempiras y de seis (6) a doce (12) años cuando exceda de dicho monto.

En las mismas penas incurrirán quienes bajo cualquier procedimiento Ingrese o utilice indebidamente la base de datos de una institución supervisada para sustraer dinero mediante transferencias electrónicas de una cuenta a otra en la misma o diferente institución. Y quien utilice tarjeta de crédito o de débito de otra persona para hacer pagos de cualquier naturaleza, fingiéndose titular de la misma.

OPERADORES DE JUSTICIA QUE DAN TRATAMIENTO A LOS DELITOS INFORMÁTICOS

A. *Corte Suprema de Justicia.*

B. *Policía Nacional.*
- Dirección de Inteligencia Policial.
- Dirección Policial de Investigaciones.
  - Unidad de Delitos Informáticos. (Laboratorio)
  - Unidad Video Forense. (Laboratorio)
- Unidad de Menores.
- Interpol.

C. *Ministerio Público.*

Se han realizado grandes avances, pero estas instituciones cuentan con estas limitantes:

- Identificar, Preservar y Analizar los indicios.
- Recursos inadecuados o inexistentes.
- Se convierte en una tarea compleja la “replicar” ambientes
- Solo se cuenta con dos laboratorios para el análisis de indicios a nivel nacional.
- Falta de una metodología clara en la cadena de custodia de indicios y su tratamiento.

- Escasa preparación Sistemas Operativos, Ruteadores, Web, Aplicaciones, Bases de datos, etc.
- Falta de Integridad de la Cadena de Custodia
- Esfuerzos dirigidos a “tapar el hueco” en lugar de probar culpabilidad de responsables (procurar pruebas)

ALGUNAS DEFINICIONES CONCEPTUALES INFORMÁTICAS.

A. *Qué es la pericia forense.*
Es toda aquella realizada por una persona o equipo de personas con competencias certificadas en el tema objeto de peritaje, encaminada a obtener criterios certeros e indubitados útiles para los fines de la actividad procesal ante el órgano jurisdiccional del Estado. (Pertenece, Usados, Adecuado para el perito de Peritos)

B. *Que es la pericia informática.*
Es el análisis de los equipos informáticos o dispositivos de almacenamiento de datos, (discos duros externos, CD-DVD, memorias USB) intervenidos por los Operadores de Justicia y a disposición de la Autoridad Judicial, para la investigación del delito objeto de la denuncia o proceso judicial.

C. *Que es la pericia digital.*
Es la aplicación de métodos científicos para REUNIR, PROCESAR e INTERPRETAR, la evidencia digital para una presentación ante una Corte. (Reunir, Procesar, Interpretar)

D. *Examen forense.*
Es el proceso forense, que tiene como propósito el obtener data, de dispositivos de las TIC sin modificación alguna, la cual podrá ser utilizada para responder en algún tipo de incidente en un marco legal y que puede ser replicada por tercera persona (Pericia Paralela)

E. *Seguridad de la información.*
Son todas aquellas actividades de seguridad relacionadas con la información que manejan las personas, seguridad física, cumplimiento o concientización.

F. *Ciberseguridad.*
La capacidad de proteger la integridad, confidencial, disponibilidad de la Información procesada, almacenada, o transmitida por los sistemas TIC, así como la autenticidad de sus componentes y la trazabilidad de sus acciones. [3]

G. *Ciberespacio.*
Es el conjunto de medios físicos y lógicos que conforman las infraestructuras de os sistemas de comunicaciones e informáticos, junto con los usuarios que interactúan con estos sistemas.

H. *Ciberdefensa.*
Es la capacidad de proteger la prestación y gestión de los servicios de TIC en respuesta tanto a potenciales como efectivas acciones maliciosas, originadas en el Ciberespacio.

CONCLUSIONES.

- Es de vital importancia la entrada en vigencia del nuevo Código Penal hondureño, en el cual se establecen nuevas figuras para el tratamiento de los Delitos Informáticos.

- La capacitación y tecnificación de los Operadores de Justicia, evitará que se cometan errores o procedimiento con posibles vicios en la realización de peritajes forenses informáticos.

REFERENCIAS.

[1] N. CALLEGARI, delitos informáticos y legislación, Facultad de Derecho y Ciencias Políticas, Editorial Universidad Pontificia Bolivariana, Caracas Venezuela, Año 1985.

[2] Republica de Honduras, *código penal,* Casa Blanca Tegucigalpa, 2006.

[3] Bermejo, Higuera, Javier, Primer Diploma en Ciberseguridad y Ciberdefensa, In-nova, Universidad de Defensa, Tegucigalpa, Honduras, mayo 2018.

UN ANÁLISIS SISTÉMICO DE LOS CIBERATAQUES, PARA FORTALECER LAS DEFENSAS DE LOS SERVICIOS TI

Mst. María Angélica Castillo
Perú

Resumen
La transformación digital está cambiando de manera acelerada a las organizaciones para mejorar su desempeño, a través del uso masivo de la tecnología digital, este cambio se viene produciendo y responde a una modificación en el mercado y a la demanda de los consumidores de los productos o servicios.
Dicho cambio se viene dando con el desarrollo de nuevas herramientas tecnológicas e integrando sistemas automatizados en muchos casos basados en la nube. Por lo que debe dotarse de software y hardware, así como, implementar diversas medidas que mitigue las vulnerabilidades de los sistemas digitales e infraestructura tecnológica, y de esta manera fortalecer la defensa de los servicios tecnológicos.
Las organizaciones se enfrentan de manera constante a escenarios de amenazas cambiante y por ello a replantear la estrategia de ciberseguridad, por lo que se requiere una estrategia holística de seguridad, para proteger los ataques dirigidos intencionadamente, así como los errores humanos.

Palabras Clave: Ciberataques, seguridad informática, seguridad de la información, ciberseguridad, análisis sistémico, transformación digital.

INTRODUCCIÓN

Actualmente el mundo viene revolucionado en sus procesos y transacciones comerciales, los cuales para su óptimo funcionamiento tienen soporte en la digitalización a través de las tecnologías de la información, este crecimiento de la transformación digital, nos está llevando a cambios de nuestros hábitos y comportamientos, de modo tal que los servicios al ciudadano son cada vez más requeridos mediante el uso de las tecnologías y este cambio tan creciente, nos hace muy dependiente del ciberespacio y en consecuencia de los nuevos riesgos y amenazas que cada vez son mayores, siendo este espacio el más atractivo para los ciberdelincuentes. Con el fin de mitigar los riesgos, se debe considerar un proceso continuo de aseguramiento de las tecnologías de información, estableciendo mecanismos que garanticen la confidencialidad, la integridad y la disponibilidad de la información de estos servicios.

CONTENIDO

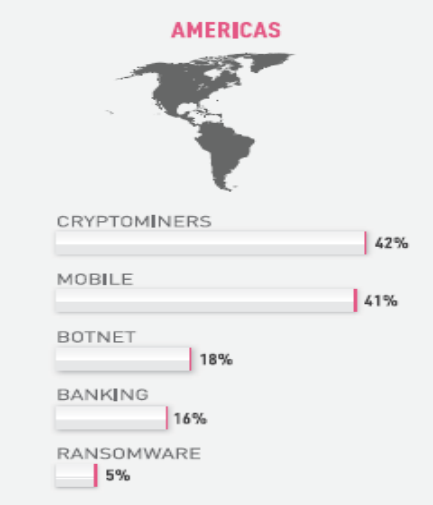
CIBERSEGURIDAD

Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica los servicios que prestan y la información que manejan

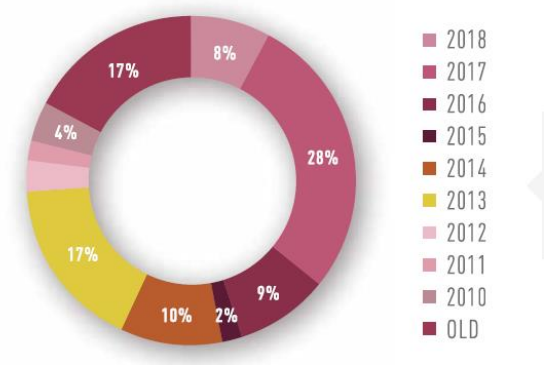
ESTADÍSTICAS DE CIBERATAQUES

- De acuerdo al estudio de ESET Security Report Latinoamérica 2018.
  El 2018 en Latinoamérica se incrementó en un 57% las variantes del Ransomware en comparación a un año antes, y en el 2017 creció en 60% los ataques en variantes de Ransomware, en comparación al 2016. Esto debido a que las organizaciones están atentas a las principales fallas dentro de su infraestructura, en función de prevenir incidentes a futuro, como el ocurrido en mayo de 2017, cuando un ataque de Ransomware aprovechó una vulnerabilidad de Windows y se propagó masivamente, afectando a más 230 mil equipos en 150 países.
- De acuerdo al estudio de ESET Security Report Latinoamérica 2018.
  En el 2018 la explotación de vulnerabilidades en Latinoamérica ha crecido en un 55%.
- De acuerdo a la fuente: 2018 IT Professionals Security Report Survey
  El 76% de las organizaciones mundiales han experimentado un ataque de phishing en el último año.
- De acuerdo a la fuente: Check Point ThreatCloud.
  Más del 20% de las organizaciones mundiales se ven afectadas por Cryptojacking Malware todas las semanas.
- De acuerdo a la fuente: Check Point ThreatCloud
  El 40% de las organizaciones mundiales fueron impactadas. por Cryptominers el año pasado.
- De acuerdo a la fuente: 2018 IT Professionals Security Report Survey
  El 49% de las organizaciones mundiales han experimentado un ataque DDoS en el último año.
- Categorías de ciberataques en América de acuerdo a estudios globales de Check Point.
  Una gran transformación puede observarse como es la tendencia de los nuevos ataques. el impacto del ransomware en las organizaciones en todo el mundo se redujo de un 30% en su punto máximo en el 2017 y menos de un 4% en el 2018. Este cambio puede deberse al resultado de la migración a la encriptación, a las

medidas adoptadas por las organizaciones para implementar acciones de ciberseguridad, también el minado ilegal de criptomonedas es una técnica para que el ciberdelincuente obtenga beneficios.



- De acuerdo con los sensores de ataque globales de Check Point, en el año 2018, el 92% de los ataques observaron vulnerabilidades apalancadas registradas en el 2017 y años anteriores. Más del 40% de los ataques utilizaron vulnerabilidades que tienen al menos cinco años.
- % de ataques que aprovecharon una nueva vulnerabilidad descubierta en el mismo año que el ataque observado.



Fuente: sensores de ataque globales de Check Point 2018.

ATAQUES MALICIOSOS (INTERNOS Y EXTERNOS)

- Los ataques cibernéticos y violaciones de seguridad suceden a cada minuto.
- Algunas son pequeñas y otras más grandes.

- Algunas logran su cometido y otras no.

MODO DE ATAQUES

Ataques Pasivos:

- Acceden a la información del sistema.
- Análisis de tráfico.
- Captura de datos.
- Liberan contenido de un mensaje.

Ataques Activos:

- Producen cambios en la información
- Denegación de servicios.
- Modificación de mensajes
- Escuchas telefónicas (Chuponeos)
- Intentos de ingresar a cuentas ajenas.
- Enmascaramiento.

ATAQUES MÁS COMUNES A LOS SERVICIOS TI.

Ataque de Denegación de servicios (DDoS)

- Una cantidad considerable de sistemas atacan a un objetivo único, provocando la denegación de servicio.
- Sobrecarga de mensajes entrantes en un sistema objetivo fuerza su cierre, denegando el servicio a los usuarios legítimos
- Provoca pérdida de la conectividad de la red por el consumo del ancho de banda de la red del sistema atacado.

¿Cómo proteger del Defacement?

- Instalar firewall
- Reforzar contraseñas seguras
- Servidores actualizados, plugins
- Revisar código html, incrustación de código malicioso.
- Realizar auditorías periódicamente de los sitios
- Tener un plan de recuperación ante este tipo de incidentes para su detección temprana

Defacement
Desfiguración. Deformación o cambio producido de manera intencionada en una página web por un atacante que haya obtenido algún tipo de acceso.

Ataque Por Injection
Sqli (Structured Query Language Injection) es una técnica para modificar una cadena de consulta de base de datos mediante la inyección de código en la consulta.
El SQLI explota una posible vulnerabilidad donde las consultas se pueden ejecutar con los datos validados.

Fuerza Bruta
- Intenta “romper” todas las combinaciones posibles de nombre de usuario y contraseña en una página web.
- Estos ataques buscan contraseñas débiles para ser descifradas y tener acceso de forma fácil.
- Hacer que las contraseñas sean bastante seguras, para que el atacante se canse antes de descifrarla

Ingeniería Social
Engañar o sorprender a las personas y/o usuarios para extraer información confidencial

Phishing
- Es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas, datos de tarjetas de crédito, números de cuentas bancarias, etc.
- Un 30% de los usuarios abren los mensajes de phishing y un 12% cliquea en la URL “sin pensar”.

¿Cómo proteger del phishing?
- Mantenga buenos hábitos y no responda a enlaces en correos electrónicos no solicitados
- No abra adjuntos de correos electrónicos no solicitados.
- Proteja sus contraseñas y no las revele a nadie.
- No proporcione información confidencial a nadie por teléfono, en persona o a través del correo electrónico.
- Compruebe la URL del sitio (dirección web). En muchos casos de phishing, la dirección web puede parecer legítima, pero la URL puede estar mal escrita o el

dominio puede ser diferente (.com cuando debería ser .gob).

- Mantenga actualizado su navegador y aplique los parches de seguridad.
- No hay una forma mejor de reconocer, eliminar y evitar el phishing que utilizar una herramienta de antivirus y antiphishing.

Spammer

Envío de miles de mensajes de correos electrónicos no solicitado, provocando una sobre carga en los servidores de correo y colapso en los buzones.

¿Cómo evitar los spams?

- Filtrado de correo no deseado. Antispam.
- Listas negras públicas
- Análisis de cabeceras
- Si no conoce destino, borre mensaje.
- No responder los spams.
- No dar clic en los enlaces de correos spams.
- Use copias ocultas, para no mostrar direcciones de otros destinatarios

Man in the middle

- MitM, un atacante supervisa (generalmente mediante un rastreador de puertos) una comunicación entre dos partes y falsifica los intercambios para hacerse pasar por una de ellas.
- “hombre en el medio”, es un tipo de amenaza que se aprovecha de un intermediario. El atacante en este caso, tiene la habilidad de desviar o controlar las comunicaciones entre dos partes.

¿Cómo proteger del man in the meddle?

- Autenticación de dos factores, autenticación fuerte
- Usa siempre HTTPS
- Certificados SSL
- Usar última versión de navegadores de internet
- Accesos Cifrados
- Usar una red VPN

Malware y gusanos

- Código malicioso, susceptible de causar daños en la red.
- Se propaga con gran facilidad y velocidad mediante el correo electrónico.
- Tipo de software que tiene como objetivo infiltrarse o dañar

una computadora o sistema de información sin el consentimiento de su propietario

¿Cómo protegerse del malware, virus, gusanos?

- Software anti malware
- Instalar un antivirus y un firewall
- Precaución al ejecutar software procedente de Internet

Ransomware

Restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción. Los ataques más peligrosos los han causado Ransomware como WannaCry, Petya, Cerber, Cryptolocker y Locky.

SEGURIDAD PERIMETRAL

Es un método de defensa de red, un conjunto de sistemas de detección electrónica diseñado para proteger perímetros internos y externos.

Es una estrategia para proteger los recursos de una institución u organización conectada a la red.

Condiciona la credibilidad de una organización en Internet.

Objetivos de la Seguridad Perimetral

- Redirigir y proteger el tráfico de los sistemas y servicios informáticos dentro de la intranet, red interna.
- Permitir sólo ciertos tipos de tráfico o entre ciertos nodos.
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos.
- Proporcionar puntos confiables de interconexión con el exterior.

Arquitectura sin seguridad

- Inexistencia de filtrado de tráfico de entrada y de salida
- Inexistencia de elementos de monitorización.
- Red plana sin segmentar.
- Publicación de servicios internos sin seguridad.
- Inexistencia de verificación de malware o spam en el correo electrónico
- Carencia de permisos al acceder por cliente remoto para acceder a los servicios

Elementos que proveen seguridad al perímetro

Antivirus, antispam

- Sistemas intermedios que filtran contenido malicioso en canales de entrada a la red.
- Detección de malware en pasarelas web y servidores de correo.

Firewall o Corta fuego

- Establece políticas de seguridad entre la red privada y el Internet.
- Determina cuál de los servicios de red pueden ser accedidos desde y hacia el exterior de la red privada
- Controlar las aplicaciones que acceden a un puerto
- Controlar las aplicaciones que acceden a Internet
- No puede ofrecer protección alguna una vez que el agresor lo traspasa.

Filosofía del firewall:

- Política permisiva (lista negra): se acepta todo menos lo que se deniega explícitamente.
- Política restrictiva (lista blanca): se deniega todo menos lo que se acepta explícitamente. Más difícil de mantener, más segura, la que deba usarse.

Redes virtuales privadas (VPN)

Es comúnmente utilizada para conectar usuarios remotos, sucursales u oficinas con su intranet (punto a punto). Encapsula y cifra todo el tráfico en una nueva red virtual.

- Autentificación y autorización: mediante gestión de usuarios y roles y permisos.
- Integridad: con el uso de funciones hash.
- Confidencialidad: la información debe ser cifrada.
- No repudio: los datos transmiten firmados.

DMZ o Zona desmilitarizada

Las DMZ se crean con firewall. En una Tecnología diseñada para filtrar tráfico tanto de entrada como de salida

El objetivo es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa.

Sistema de detección y prevención de Intrusos (IDS/IDPS)

Dispositivo que monitorea y genera alarmas si se producen alertas de seguridad. Detecta accesos no autorizados a un servidor, PC o a una red. Pueden ser ataques realizados por usuarios malintencionados con conocimientos básicos de seguridad.

Los IDPS bloquean el ataque evitando que tenga efecto.

- Identifica posibles ataques.
- Registro de eventos, búsqueda de nuevos patrones de ataque
- Bloquea el ataque. Bloquea la conexión
- Reporta

Tipos de IDS

HIDS: Host IDS, monitoriza cambios en el sistema operativo y aplicaciones.
NIDS: Network Intrusion Detection System Network IDS, monitoriza el tráfico de la red.
NNIDS Network Node Intrusion Detection System Destinado a vigilar el tráfico destinado a un Host.

Métodos de detección

- Firmas, comprobar en una base de datos, si hay coincidencias generar alarmas
- Crear Patrones de comportamiento.

Anti DDOS (Distributed Denial of Service), ataque de denegación de servicio distribuido
Estos ataques usan varios equipos para realizar un ataque coordinado contra una máquina.

- Ataque a un sistema o red, provoca que un servicio o recurso sea inaccesible a usuarios legítimos.
- Provoca pérdida de la conectividad con la red, por el consumo del ancho de banda de la red de la víctima.
- Genera saturación de los puertos con múltiples flujos de información, hace que el servidor se sobrecargue y no pueda seguir prestando su servicio.
- Es la técnica de ciberataque más usual y eficaz por su sencillez tecnológica.
- Consume recursos informáticos como ancho de banda, espacio de disco, o tiempo de procesador.

UTM Gestión unificada de amenazas
Equipo "appliance" que integran en un único dispositivo un conjunto de soluciones de seguridad perimetral.

- Firewall
- Antivirus/
- antispam
- VPN

- IDPS
- Control de navegación web
- Control del uso de mensajería instantánea
- gestión de múltiples conexiones

Arquitectura con seguridad perimetral

- Instalación de antispam y antivirus.
- Instalación de Firewall
- Clientes remotos usan VPN.
- DMZ y Red Interna
- Instalación de IDPS en las tres interfaces.
- Wi-Fi Seguro
- HTTPS: comunicaciones cifradas a través de SSL.
- Autenticación multi-factor y tokens de seguridad
- Seguridad de la navegación web
- Encriptación de voz y data
- Hackeo Ético
- Switch gestionados
- Análisis de vulnerabilidad en código fuente
- WAF (Web Application Firewall) protege servidores de aplicaciones web, evita ataques:
- Cross-site scripting: inclusión de código script malicioso en el cliente que consulta el servidor web.
- SQL injection: introducir un código SQL que vulnere la Base de Datos del servidor.
- Denial-of-service: servidor de aplicación sea incapaz de servir peticiones correctas de usuarios.

REFERENCIAS

L. Rodriguez G. and R. Carnota, “América Latina y el Caribe: Inicios, desarrollos y rupturas”, *Telefónica Fundación*, Madrid España 2015.

C. Valdivia M., *“Sistemas informáticos y redes locales”,*1rad ed., Madrid España, 2014.

E. Ruiz L., *“Nuevas tendencias en los sistemas de información”* Edit. Centro de estudios Ramón Areces, Madrid España, 2017.

F. Miró L., J. Agustina S., José. Medina S., L. Summers, “Crimen, oportunidad y vida diaria”, Centro Crimina para el estudio y prevención de la delincuencia, Madrid España.

G. Díaz O., I. Alzórriz A., E. Sancrostóbal R., M. Alonso C., “Procesos y herramientas para la seguridad de redes”, UNED, Marzo 2014
A. Tanenbaum, “Redes de computadoras”, Pearson Prentice hall, cuarta edición, 2003.
W. Halton, B. Weaver, J. Ahmed A., S. Rao K., M. A. Imran. “Penetration Testing: A survival Guide”, Packt Publishing Ltd. Birmingham, UK, Noviembre 2016.
M. Whitman, H. Mattord, D. Mackey, A. Green, “Guide to network security”, Course Technology, 2013.
H. Bothra, “Hacking be a hacker wjth ethics”, Khanna book publishing Co, Darya Ganj, New Delhi, 2016.
Eset Security report, Latinoamerica 2018, Eset Enjoy safer technology.
Cyber attack trend analysis, key insights to gear up for in 2019, Check point research, 2019 securyty report.
A. Liska, T. Gallo “Ransomware”Defending against digital extortion, O’Reilly, United States of America, 2017.

CIBERSEGURIDAD Y CIBERDEFENSA: RETOS Y OPORTUNIDADES

Dr. Gustavo Guzmán
México

Resumen*- La revolución tecnológica en las últimas décadas ha tenido un impacto importante no sólo en la forma en la que nos comunicamos, sino también las forma de operar y gobernar de los Estados Nación. Dicha revolución ha puesto en las agendas del más alto nivel conceptos clave como la ciberseguridad y ciberdefensa visualizándolos como factores primordiales para garantizar el desarrollo económico, político y social de estos Estados Nación.*

INTRODUCCIÓN

El presente trabajo presenta un análisis del debate sobre la ciberseguridad y la ciberdefensa considerando principalmente los retos y oportunidades para alcanzar una resiliencia cibernética global. A lo largo del análisis realizaremos un breve acercamiento a conceptos clave que nos permiten entender la dupla de la ciberseguridad y la ciberdefensa, tales como: *Ecosistema Digital*, *Seguridad Multidimensional*, *Resiliencia Cibernética y Capacidades Cibernéticas*; para con ello poder edificar un referente que nos facilite visualizar los retos y oportunidades que enfrentan los Estados Nación, los gobiernos, las empresas y la población en general en la esfera del ciberespacio.

DESARROLLO

Los retos a nivel global son cada vez mayores y el ámbito del ciberespacio no es la excepción. Las amenazas cibernéticas en la actualidad son globales, por lo que definitivamente se requiere desarrollar soluciones globales que minimicen el impacto de estas amenazas que día con día crecen en sofisticación e impacto. Estas acciones globales, sin duda alguna deben ser orquestadas de manera contundente y armónica entre todas las partes interesas, desde los gobiernos y organismos multinacionales hasta los sectores industriales y poblaciones alrededor del mundo.

Ante tales desafíos, resulta significativo revalorar el sentido y utilidad de las estrategias, políticas y acciones de los Estados Nación y gobiernos para abordar el tema de la seguridad en el espacio; considerando como uno de los primeros pasos la identificación de los retos y oportunidades que se aproximan a velocidad estridente.

Por lo anterior y tomando en cuenta la complejidad de la ciberseguridad, es imperativo desarrollar una solución en términos de una respuesta factible y creíble; entendiendo en todo momento que resultan innumerables las variables que convergen e interactúan en la esfera del ciberespacio, sin dejar de ser situaciones

y causas heterogéneas, que afectan o fluyen cotidianamente hacia las agendas públicas en busca de atención y solución.

En la actualidad es común escuchar términos como ciberseguridad y ciberdefensa muchas veces sin distinguir uso, límites o alcances entre un término u otro. Por ello resulta indispensable abordar algunos conceptos que nos facilitaran entender el rol que juegan el binomio de la ciberseguridad y la ciberdefensa para los Estados Nación.

a) Ecosistema Digital

El desarrollo científico y tecnológico en el mundo ha sido factor clave para que las tecnologías de la información y de las telecomunicaciones sean un detonador para la convergencia tecnológica a nivel global y regional. En consecuencia las interacciones entre el sector público, privado, industrial, bancario, energético, de salud, entre otros, ha evolucionado con ellos al grado de alcanzar un nivel alto de conectividad e interacción en un espacio digital - cibernético- por medio de las tecnologías antes mencionadas. Dicho espacio es conocido hoy en día como ecosistema digital, y ha impacto gran parte de los principales sectores económicos, políticos y sociales alrededor del mundo.

Este nuevo ecosistema no sólo se encuentra inmerso en infraestructuras de cómputo y telecomunicaciones (eesta infraestructura puede incluir desde un equipo de cómputo, routers, swiches, repetidores, servidores, redes de telefonía, redes de datos, almacenamiento en la nube, ID´s, IP´s, etc.), dispositivos electrónicos, servicios digitales, aplicaciones y usuarios digitales que interactúan a través de Internet. Sino que además la evolución tecnológica ha traído a la mesa tecnologías más sofisticadas como: el *Internet de las Cosas*, la *Inteligencia Artificial*, el *Big Data*, entre otros.

Lo anterior, es un fenómeno generalizado alrededor del mundo, por ello hoy en día se habla de una cuarta revolución industrial, de la industria 4.0 y de ecosistemas digitales. No obstante, este desarrollo tecnológico y digital no se encuentra exento de nuevos riesgos y amenazas. En este contexto, el ciberespacio es de especial interés para delincuentes y terroristas que pueden aprovecharse del anonimato que ofrece el internet y de la falta de homogeneidad en las legislaciones nacionales e internacionales, para actuar con cierto grado de impunidad [1].

Por lo anterior, es impostergable que los Estados Nación tomen acciones de defensa que permitan proteger a la población, sus recursos, territorio, organizaciones, instituciones, y entidades de los riesgos y amenazas en el

ciberespacio; acciones que incluyan prioritariamente el resguardo y defensa de sus activos e infraestructuras críticas.

b) Seguridad Multidimensional

Es pertinente recordar que el concepto de seguridad para los Estados Nación es constantemente abordado desde un enfoque de seguridad nacional, lo que resulta entendible debido que guarda estrecha relación con la soberanía, el control y dominio por parte del Estado; mismos que promueven la estabilidad Política, Económica y Social necesaria para alcanzar el bienestar general y desarrollo sostenible, no obstante este concepto también se ha transformado para dar paso a uno más amplio que reconozca los retos y desafíos del siglo XXI.

Los cambios vertiginosos a escala global que han transformado y estructurado al mundo actual, han llegado acompañados de riesgos y amenazas -desconocidas o relativamente nuevas hasta hace poco tiempo- para las sociedades y gobiernos. De tal forma, cuestiones como el desplazamiento masivo e incontrolado de personas, el crimen organizado, el terrorismo, pobreza alimentaria, escases de recursos naturales, entre otros, son temas recurrentes en las agendas de los gobiernos y organismos internacionales y regionales.

Las situaciones antes mencionadas -incluyendo la ciberseguridad- representan problemas de alto impacto e incrementan la complejidad de gobernar para los Estados Nación, amenazando la seguridad y el bienestar de sus sociedades, obligando a reformular la concepción de seguridad, dando paso a un enfoque más amplio denominado seguridad multidimensional.

En correspondencia, el enfoque de seguridad multidimensional fue planteado por la Organización de Estados Americanos (OEA) en el año 2002, durante el trigésimo segundo período ordinario de sesiones de su Asamblea General realizada en Bridgetown, Barbados, del 2 al 4 de junio de 2002, considerando que:

“*las amenazas, preocupaciones y otros desafíos a la seguridad en el Hemisferio son de naturaleza diversa y alcance multidimensional y que el concepto y enfoque tradicionales deben ampliarse para abarcar amenazas nuevas y no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales.*”

Reconociendo así, la relevancia de hacer frente a las llamadas nuevas amenazas, concibiendo la seguridad con un enfoque multidimensional, que incorpora las amenazas existentes, tradicionales y las nuevas, sin hacer a un lado las preocupaciones, retos y desafíos ineludibles para garantizar y preservar la seguridad de la región y de cada Estado Nación. [2] Y que contribuye de acuerdo

con la OEA a la consolidación de la paz, al desarrollo integral y a la justicia social, basada en valores democráticos, respetando, promoviendo y defendiendo los derechos humanos, la solidaridad, cooperación y respeto a la soberanía nacional [3].

En este orden de ideas, es posible entender la seguridad multidimensional como la ausencia de peligros relacionados con el desarrollo social, económico, tecnológico, energético, demográfico y ambiental que se puedan incidir negativamente sobre los intereses y objetivos nacionales, así como comprometer la estabilidad y el desarrollo de un Estado-Nación.

c) Resiliencia Cibernética

Hasta este punto, ha sido posible concebir la importancia de que los Estados Nación cuiden y proteger las operaciones cibernéticas de su población, instituciones, organizaciones, empresas, etc. no obstante el siguiente paso en la carrera de la ciberseguridad es la resiliencia cibernética, entendida como aquella capacidad de recuperarse ante un ataque cibernético.

Principalmente considerando que los ataques cibernéticos son una amenaza actual y progresiva, que día a día son más efectivos y rentables por su sofisticación operativa y técnica. Dejando a su paso agravios y perjuicios en contra de personas, organizaciones, instituciones o Estados Nación. Por ello nadie que interactúe o participe en el ecosistema digital se encuentra exento de sufrir un ataque de este tipo.

Es pertinente recordar, que para los Estados Nación, un factor vital es cuidar y defender sus Infraestructuras Críticas (IC), siendo las siguientes algunas de ellas:

1) Plantas Nucleares, Redes de Energía, Presas, etc.
2) Redes de transporte terrestre, marítimo, aéreo
3) Redes de comunicación y telecomunicaciones
4) Sector productivo y de alimentos
5) Comercio Mundial
6) Banca y sector financiero
7) Centros médicos y hospitales

d) Capacidades Cibernéticas

Con el exponencial desarrollo tecnológico y el constante incremento del ecosistema digital alrededor del mundo, los Estados Nación han prestado especial interés en el uso y desarrollo de capacidades cibernéticas y de defensa, en específico las Capacidades Cibernéticas Ofensivas, conocidas como OCC (por sus siglas en

inglés Offensive Cyber Capabilities) y reconocidas como capacidades que permiten ingresar a un sistema o red informática con fines perversos.

Gran parte de los Estados Nación alrededor del mundo consideran el ciberespacio como un nuevo dominio operacional de guerra, adicional a la tierra, el aire, el espacio y el mar [4]; incluso la OTAN ha reconocido el ciberespacio como otro dominio militar [5].

En este sentido, países como Bélgica, Colombia, Alemania, Finlandia, India, Emiratos Árabes Unidos y Vietnam han expresado abiertamente su interés en el desarrollo de las OCC con miras a una posible guerra cibernética.

Por otra parte, países como Estados Unidos, China, Rusia, Israel, Reino Unido, Irán y Corea del Norte prevalecen en la línea de fortalecer el desarrollo de sus OCC, mismas que se han ido fortaleciendo desde hace años.

Habiendo expuesto el interés de los Estados Nación por el desarrollo de las capacidades cibernéticas y la importancia de estas para la seguridad del ciberespacio se aprecia a las OCC como herramientas para los Estados Nación, identificando el potencial de estas para cambiar el poder militar. De tal forma, se ha demostrado que las OCC pueden afectar significativamente la manera en que los países usan su poder militar de diversas maneras, sin embargo estas no necesariamente tienen que exponerse públicamente [6].

Sin embargo, es pertinente señalar que hasta la fecha la información sobre la planeación, desarrollo y ejecución de las OCC de los Estados Nación aún es insuficiente.

La implementación y el uso de OCC generalmente se extiende en múltiples etapas, identificando comúnmente cuatro para operaciones avanzadas: 1) reconocimiento, 2) intrusión, 3) escalada de privilegios y 4) entrega de la carga útil [7].

Desde una perspectiva similar, es claro que las OCC son capacidades que pueden tener fines preventivos y reactivos, y que hasta el momento no se tiene regulaciones o controles que monitoreen a los Estados Nación respecto a su uso y desarrollo. No obstante, contrario a las armas nucleares y arsenal bélico el uso y desarrollo de las capacidades cibernéticas tiene un nivel de riesgo menor. Por lo anterior, se ha observado que el crecimiento del mercado del sector privado para OCC genera nuevas oportunidades para que los gobiernos y Estados Nación desarrollen, implementen y usen estas capacidades. [8]

CONCLUSIONES

La seguridad en el ciberespacio, es uno de los muchos problemas y dificultades a los que los Estados Nación deben hacer frente siempre con miras de impulsar políticas públicas que garanticen el desarrollo y el bienestar de sus sociedades, considerando que las políticas deben diseñarse no solamente a partir de los entornos internos, sino también contemplar los cambios a escala internacional, considerando que en los gobiernos las organizaciones públicas son entes multidimensionales que trabajan en redes de colaboración; y que “las relaciones cotidianas entre sociedad y estado toman la forma de problemas y soluciones, demandas y ofertas, conflictos y arbitrajes, necesidades y satisfactores” [9].

Así mismo resulta transcendental expresar que la ciberdefensa y el desarrollo de capacidades cibernéticas desempeñan una función significativa para alcanzar las llamada resiliencia cibernética. El incremento de las capacidades cibernéticas para salvaguardar la información y la protección de las infraestructuras críticas resulta esencial para la seguridad y el bienestar de cualquier Estado Nación.

El tema de la inseguridad en el ciberespacio, debe alcanzar el carácter de agendum, debido a que como hemos visto la ciberseguridad no es un tema menor, sobre todo cuando implica información estratégica de los gobiernos; ya que la explotación de esta información puede afectar significativamente sectores estratégicos de los gobiernos como: el sector económico, político, energético, jurídico, de salud, entre otros, llegando en algunas ocasiones hasta colapsarlos [10].

En el mismo sentido, el tiempo resulta un factor clave a la hora de incrementar la ciberseguridad y la protección de las infraestructuras críticas ya que el rápido desarrollo de las tecnologías en ocasiones llega a exceder la capacidad de respuesta de las instituciones y dependencias públicas y privadas que hacen frente a los ataques cibernéticos.

Los ataques cibernéticos son cada vez más sofisticados y con mayor impacto, estos no se pueden evitar pero si podemos desarrollar capacidades para prepararnos y defendernos de ellos.

Los Estados Nación requieren de un marco jurídico y regulatorio, desarrollo de capacidades técnicas y científicas y una cultura de seguridad de la información.

No sólo los ataques y amenazas cibernéticas crecen, el déficit de profesionales y expertos cibernéticos sigue creciendo a pesar de los esfuerzos que hacen alrededor del mundo. De ahí la importancia de comenzar a desarrollar profesionales que atiendan y colaboren en las diversas áreas de la ciberseguridad, áreas como la

Criminalística avanzada, Peritaje Informático, Operación de CSIRT-CERT´s, Informática Forense, Análisis de tráfico, Monitoreo de redes e infraestructura, Blindaje de comunicaciones y sistemas, Criptografía, Ingeniería Inversa, Pentesting, entre otros. Lo anterior sin dejar de lado lo valioso que resulta el desarrollo de programas académicos que profesionalicen a las nuevas generaciones para hacer frente a los grandes retos y oportunidades que se avecinan en el terreno del ciberespacio.

REFERENCIAS

[1] Rego, Miguel, *"Un llamado a la acción para proteger a ciudadanos sector privado y gobierno"*, Organización de Estados Americanos, White Paper Series, Edición 1, Pág. 7, 2018.

[2] Centro de Altos Estudios Nacionales, *"Conceptos de Seguridad y Defensa de los Países Iberoamericanos"*, Colegio de Defensa del Uruguay, Uruguay, 2013.

[3] Organización de los Estados Americanos, *"Conferencia Especial sobre Seguridad*, *Declaración sobre seguridad en las Américas",* Ciudad de México, 2003.

[4] McGuffin y Mitchell, *"On domains: Cyber and the practice of warfare*". International Journal. 69:3, Págs. 394-412, 2014.

[5] OTAN, *"NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit"*, Recuperado de: https://ccdcoe.org/nato-recognises-cyberspace-domain-operationswarsaw-summit.html, 2016.

[6] Smeets Max y Lin Herbert, *"Offensive Cyber Capabilities: To What Ends*", 10th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinnn. Pág. 13, 2018.

[7] Smeets Max y Lin Herbert, *"Offensive Cyber Capabilities: To What Ends"*. 2018 10th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinnn. Pág. 5, 2018.

[8] Smeets Max y Lin Herbert, *"Offensive Cyber Capabilities: To What Ends"*, 2018 10th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinnn. Pág. 14, 2018.

[9] Rittel, Horsy y Melvin M. Webber, *“Dilemas de una teoría general de la planeación”,* en Luis F. Aguilar Villanueva (ed.), Problemas públicos y agenda de gobierno, México, Miguel Ángel Porrúa, pp. 157-185, 1993.

[10] Warner, Michael, *“Cybersecurity: A Pre-history”*, Intelligence and National Security, pp. 781-799; y Rudner, Martin, “Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge”, International Journal of Intelligence and CounterIntelligence, 26, 3, pp. 453-481, 2013.

WEB DEL EVENTO

www.igfhonduras.com.hn

#IGFHonduras2019

Instagram
Facebook
Twitter

- Información de contacto de la iniciativa nacional de IGF Honduras

Denis Jesús Aguilar	denisaguilar +504 99948956
Nazly Borrero Vasquez	nazlyborrerov@gmail.com +57 3108979178
Claudio Lucena	+51 919349674
Sandy Palma	+504 89639159

RECOMENDACIONES Y PROPUESTAS DE LAS MESAS DE TRABAJO.

- La actualización de la resolución 119/2005, normas para regular las tecnologías y comunicación del sistema bancario.
- Generar puntos políticas macros pero que no sean tan regular las tecnologías y comunicación del sistema bancario.
- Capacitar a los altos mandos para que entiendan la importancia de invertir en tecnología y capacitaciones para prever ciberataques creando una cultura de seguridad de la información.
- Sostenibilidad en los proyectos enfocados a la ciberseguridad en instituciones públicas.
- Observar y conocer experiencias de países más avanzados en temas de ciberseguridad para conocer cuáles fueron sus limitaciones y como lograron superarlos.
- Implementar estándares ISO, TIER, COBIT y auditoria para prevención y cumplir las políticas internacionales de manera eficiente.
- El estado de Honduras debe suscribirse a convenios y tratados internacionales y cumplir sus estándares internacionales. (Convenio de Budapest)
- Crear comisión para revisar y presentar las debilidades y necesidades adicionales de la información, 160-2016.(Ley de acceso a la información).
- Capacitación en todos los niveles sobre ciberseguridad.
- Creación de colegio de ingenieros informáticos, en sistemas, en computación.
- Educar a los legisladores sobre los temas en cuestión antes de aprobar dicha ley.
- Hacer énfasis en crear una tipificación de los delitos informáticos y no encasillarlos en uno o dos.
- Identificar que es un delito informático y que no lo es. Creación de una ley que retome los principios base de la ciberseguridad desde cero, y garantizar la auditoria social y transparencia del mismo estado.
- Hacer una sistematización o documentación de toda la normativa que ya haya sido aprobado sobre el espacio digital.
- Incorporar en la ley de protección de datos la prohibición de transferir la información personal de un usuario desde una empresa a otra, aunque estas pertenezcan a una misma corporación.
- Garantizar la neutralidad de la red y la libertad de expresión y todos los derechos humanos cuando se creen leyes sobre el ciberespacio.

NECESIDAD MÁS IMPORTANTE DEL SECTOR GOBIERNO CON RESPECTO A LA CIBERSEGURIDAD

1. Normas y políticas orientadas en la seguridad de información.
2. Creación de una ley que regule el tema.
3. Política nacional con respecto a la ciberseguridad.
4. Concientización y capacitación que maneja el área de tecnología.
5. Priorizar la educación de TI.
6. Órganos de capacitación.
7. Firma electrónica.
8. Concientización en ciberseguridad.
9. Voluntad política y presupuesto en el tema.
10. Crear centro de seguridad informática, centro de repuesta.
11. Protección de datos en el sector público y privado.
12. Comprar licencias originales.
13. Regular el uso indebido del internet.
14. La ausencia de verdaderos capacitadores en el uso de Internet.
15. Tener propio canal de datos y capacitación del uso de seguridad.
16. La necesidad en el manejo de información una vez que se comparte.
17. Necesidad en seguridad.

CATEGORÍAS UNIFICADAS SOCIEDAD CIVIL, SOCIEDAD ACADEMIA, SOCIEDAD EMPRESA PRIVADA Y FUERZAS ARMADAS:

1. Normas y políticas
2. Inversión en capacitación y órganos competentes
3. Soluciones o centros de seguridad
4. Voluntad política en el apoyo
5. Crear campañas de concientización, campañas de capacitación, realizar jornadas, foros
6. Buscar talento humano, o más bien formar talentos en ciberseguridad, incluyendo hombres y mujeres, romper paradigmas sobre hackers.
7. Generar una aceptación abierta a través de las encuestas sobre el tema a la población.
8. Crear una oficina de ciberseguridad dirigida por la sociedad civil, la empresa privada y el gobierno.

- El mundo físico lo que ha hecho es migrar al mundo virtual.
- Todo es mejorable, con trabajo en equipo y experiencia de otros países.
- Conflictos al momento que la policía tiene información en exceso de las personas. (Necesario para la protección de cada uno de ellos).
- Aspecto de seguridad, la importancia que tiene.
- Política de protección de datos. Las fuerzas armadas deberían de ir considerando, debido que tienen las mismas funciones.
- Cultura de la Ciberseguridad.

  4 puntos principales:

  1. La parte de realizar el diagnostico.
  2. La estrategia o política pública en materia.
  3. Promulgación de la nueva legislación penal relacionada con los delitos informáticos.
  4. Invitar un organismo internacional para dar acompañamiento.

- Consejo de Seguridad es una estrategia de ciberseguridad.
- Se debe de llevar a cabo un buen proceso para que no haya conflicto al derecho humano y control jurisdiccional. (Punto 2)
- Mientras se van dando las estrategias, se van resolviendo.
- Desde el punto de vista de la seguridad es importante mantener oculta información de lo que se hace en el estado.
- Retomar las experiencias malas que han surgido en otros países. Así ver que nos serviría y que deberíamos de cambiar. (Lecciones aprendidas).

CONCLUSIONES

- Gran aceptación de todas las sociedades participantes por el aporte y unión para la mejora de una buena gobernanza.
- Se quedan propuestas y necesidades para que el gobierno Hondureño las tenga en cuenta para las mejoras anuales con el próximo IGF Honduras 2020.
- Se realizara seguimiento por parte de cada uno de los responsables que asistió como líderes de cada sociedad miembro a la que represento en el IGF.
- El próximo informe queda abierto a realizar previo al próximo IGF Honduras 2020 de la mejora en las distintas sociedades.
- Se establece que la UTH (Universidad Tecnológica de Honduras) como sede organizador oficial para la realización del evento en el país, tanto por su infraestructura, y acceso a la institución en cualquier de la sedes del país.
- El comité organizador del IGF Honduras queda establecido y queda firme por 3 años consecutivos.

Organización Evento "IGF Honduras 2019"
Acta Nº. I

A los 22 (Veintidos) día del mes de Noviembre del año 2018, siendo las 14 horas del dia, en las instalaciones de la Universidad Tecnológica de Honduras, en Reunión requerida, se reúnen las siguientes personas:

Denis Jesús Aguilar – Director de Ingenierías de la UTH

Nazly Borrero Vasquez – Co- Organizador IGF Honduras – Externo de Colombia

Diego Chacón – Director de Relaciones Internacionales de la UTH

Se crea reunión para escuchar propuesta por parte de la Ingeniera Nazly Borrero Vasquez, a solicitud y por la necesidad de crear un mejor gobierno en el Internet y en vista de que nadie ha hecho propuesta se le informa a los miembros de la UTH de realizar un IGF (Internet Gobernance Forum) Sus siglas en Ingles, para así dar inicio a una nueva era digital en el país de Honduras.

ORDEN DEL DIA:

1. Apertura de la reunión.
2. Presentar propuesta a la UTH sobre el evento.
3. Estudio Financiero para la creación del evento.
4. Propuestas de fecha y conferencistas.
5. Estudio para aceptación.

1°. Verificación de quórum. En la apertura de la reunión, se convoca al director de la facultad de Ingeniería y el director de relaciones internacionales de la Universidad Tecnológica de Honduras.

2°. Presentar propuesta a la UTH sobre el evento. se da iniciativa del proyecto para la organización del evento del Foro de la Gobernanza para el

Internet en Honduras con una de las organizaciones más grande del país como es la Universidad Tecnológica de Honduras por sus siglas UTH, y del impacto positivo que puede crear al invitar a todas las sociedades pertenecientes e involucradas en el mejoramiento de un internet mas confiable.

3º. Estudio Financiero para la creación del evento. Se le informa a la Universidad que puede ser una de las patrocinadoras del evento, mas la invitación a la sociedad gobierno y otras entidades de orden privado a realizar este evento y su impacto social en el futuro.

4°. Propuestas de fecha del evento y conferencistas. Se propone que para la realización del evento sea para el mes de marzo, dado que nos da el tiempo para iniciar las propuestas de patrocinios y de conferencistas.
Se le informa de igual manera los conferencistas idóneos para este primer evento y veedor con experiencia de IGF en Europa como el Dr. Claudio Lucena y que se contemplen a conferencistas de talla internacional desde México, Argentina, Colombia, Perú, y Republica Dominicana y sin dejar a representantes Hondureños.
Se propone también crear talleres gratuitos previos al evento a Fuerzas Armadas, Gobierno, Empresas Privadas, Periodistas, Universidades y Colegios para familiarizarlos con el evento.

5°. Estudio de Aceptación. Los doctores Denis y Diego quedan al tanto en primera instancia aceptando la propuesta más la escalan a próxima reunión de forma telefónica.

_____ _____

Nazly Borrero Vásquez Denis Jesús Aguilar

_____

Diego Chacón

Organización Evento "IGF Honduras 2019"
Acta Nº. II

A los 12 (Doce) días del mes de Diciembre del año 2018, siendo las 10 horas del día, por Video Conferencia:

Los señores:

Denis Jesús Aguilar – Director de Ingenierías de la UTH

Nazly Borrero Vasquez – Co- Organizador IGF Honduras – Externo de Colombia

Se ve la necesidad de crear la reunión de orden extraordinario para informar que si se realizara el evento en el mes de marzo (última semana) del Internet Gobernance Forum Honduras 2019

ORDEN DEL DIA:

1. Verificación del quorum.
2. Instrucciones para los pasos a seguir en la organización del evento.
3. Tareas a realizar.
4. Personas a involucrar.

1°. Verificación de quórum. En la apertura de la reunión, se realiza la video conferencia con la Ingeniera Nazly Borrero, por parte del Doctor Denis Jesús Aguilar como representante de la Universidad Tecnológica de Honduras.

2°. Instrucciones para los pasos a seguir en la organización del evento. Por parte de la Ingeniera Nazly Borrero, se da inicio a que debe realizar una inscripción en la plataforma del IGF hacia los NRi para dar inicio al evento, convocar a posibles patrocinadores y revisión de Curriculums Vitae de los posibles conferencistas y moderadores al evento, se debe dar información también a la sociedad civil ISOS Chapter Honduras para su participación en el evento.
En ella se define que la sede del evento será en la Universidad Tecnológica de Honduras con sede San Pedro Sula.

También el Doctor Aguilar confirma la participación de la creación de talleres y una gira académica para fomentar la educación de la gobernanza a nivel nacional y así confirmar asistencia para el evento.

3º. Tareas a Realizar.

- El Doctor Denis, queda como responsable para buscar los patrocinios de otros entes para el evento.
- La ingeniera Nazly Borrero, se compromete a estudiar los CV de los conferencistas y realizar los llamados pertinentes para sus invitaciones y traslados al país.
- El Doctor Aguilar se responsabiliza en la compra y reservas de boletos aéreos, hoteles y demás traslados a nivel nacional.

4°. Personas a Involucrar. Se propone involucrar más personal para la optimización de la organización del evento, definiéndose así:

- Ruth Arita: Relacionista Pública de la UTH, se encargara de la relación UTH y sector empresa privada. (Invitada a la organización del evento temporal)
- Sandy Karina Palma: Licenciada que trabaja en el sector gobierno desde la capital de Tegucigalpa, quien es la encargada de invitar y capacitar al Sector Gobierno y Fuerzas Armadas. (Co Organizadora del evento permanente e inscrita al NRi del IGF).
- Diego Chacón: Director de Relaciones Internacionales de la UTH, se encarga de invitar a otros países a la participación como asistentes al IGF. (Invitado a la organización del evento temporal).
- Claudio Lucena: Veedor de la organización del evento.
- Nazly Borrero: Veedora de la organización del evento y Co organizadora de las capacitaciones previas al IGF a todos los sectores.

Se levanta la video llamada sin más requerimientos.

_____	_____
Nazly Borrero Vásquez	Denis Jesús Aguilar

Organización Evento "IGF Honduras 2019"
Acta Nº. III

A los 16 (Diez y Seis) días del mes de Enero del año 2019, siendo las 10 horas del día, por Video Conferencia:

Los señores:

Denis Jesús Aguilar – Director de Ingenierías de la UTH

Nazly Borrero Vasquez – Co- Organizador IGF Honduras – Externo de Colombia

Se ve la necesidad de crear la reunión de orden extraordinario para informar cómo va el proceso de la organización del evento Internet Gobernance Forum Honduras 2019

ORDEN DEL DIA:

1. Verificación del quorum.
2. Proceso de Seguimiento de la Organización del Evento.
3. Invitaciones al exterior y de empresas de Honduras.

1°. Verificación de quórum. En la apertura de la reunión, se realiza la video conferencia con la Ingeniera Nazly Borrero, por parte del Doctor Denis Jesús Aguilar como representante de la Universidad Tecnológica de Honduras.

2°. Proceso de Seguimiento de la Organización del Evento. Por parte del Doctor Aguilar, se confirma las fechas de la organización del evento y los avances de la búsqueda de patrocinadores ha sido optima con buena aceptación y afirmación del sector gobierno, empresa privada y sociedad civil. Por parte de la Ingeniera Borrero, se confirma la aceptación de los conferencistas Gustavo Guzmán, Arístides Contreras, Sandy Palma, Angélica

Castillo, Daniel Monastersky, Niurka Hernández, Juan Manuel Aguilar y Nazly Borrero; dando inicio a la compra de los boletos aéreos y reservas de hoteles.

3º. Invitaciones al exterior y de empresas de Honduras. El Doctor Aguilar, la Licenciada Ruth y el Doctor Chacón, confirman la entrega de invitaciones a patrocinadores, empresas y universidades para la asistencia al evento en el mes de marzo los días 20 y 21 del año 2019.

Se levanta la video llamada sin más requerimientos.

_____	_____
Nazly Borrero Vásquez	Denis Jesús Aguilar

Informe elaborado por:

- **Licenciada Sandy Karina Palma**
- **Ingeniera Nazly Borrero Vasquez**

Revisado por:

- **Doctor Denis Jesús Aguilar**