# UNIVERSIDAD CENTROAMERICANA DE CIENCIAS EMPRESARIALES (UCEM)

Curso de Maestría en" Relaciones Internacionales con mención en Política Exterior, Comercio Internacional y Cooperación Externa"

TRABAJO DE INVESTIGACIÓN DIRIGIDA:

"ANÁLISIS SOBRE LA SEGURIDAD CIBERNÉTICA EN NICARAGUA Y LOS CENTROS DE RESPUESTA A INCIDENTES DE SEGURIDAD CIBERNÉTICA (CSIRT)"


DOCENTE:

- Rector Dr. Alvaro Banchs Fabregat

ALUMNO:

- Marco Antonio Cárcamo Narváez




Managua, Nicaragua
2010

## CONTENIDO

## 1.1.- INTRODUCCIÓN

La información ha desempeñado un papel fundamental a través de la historia y la posibilidad de compartirla mediante la comunicación continúa asombrando a la humanidad. El intercambio de información determina la conducta del ser humano, al punto que lingüistas y biólogos sostienen que el almacenaje de información por medio de diversas técnicas, como el arte, el lenguaje o las herramientas, fue la fuerza impulsora que llevó a los seres humanos a convertirse en la especie dominante del planeta.
Los principales analistas coinciden. El ciberespacio se va a convertir en uno de los principales campos de batalla. Grandes cantidades económicas fluyen por internet -el 77% de las empresas europeas trabajan con los bancos a través de internet-, y ni siquiera los organismos a priori más seguros como la OTAN o el Pentágono están a salvo de los 'ciberataques'.

Los gobiernos de todo el mundo están cada vez más preocupados por la 'ciberseguridad', un problema que no afecta sólo a los usuarios particulares de Internet. Debido al importante desarrollo tecnológico, la seguridad nacional de muchos estados puede estar en peligro y los esfuerzos por salvaguardar la infraestructura digital han aumentado de manera importante.

La Internet, se ha convertido en una infraestructura crítica que debe protegerse. Continúa expandiéndose y existe un continuo movimiento hacia las configuraciones distribuidas y heterogéneas de cliente-servidor. Cada día dependemos más de Internet; desafortunadamente, en este entorno dinámico, distribuido e interconectado, los ataques cibernéticos ocurren rápidamente y pueden expandirse por todo el mundo en cuestión de minutos, independientemente de las fronteras, la geografía o las jurisdicciones nacionales. Como resultado, existe una creciente necesidad de poder comunicar, coordinar, analizar y responder a estos ataques en todos los países.

La seguridad informática, se convierte cada vez más en un factor critico para la estabilidad y el bienestar de todas las organizaciones que se conectan a Internet y del país en general. Nuestras infraestructuras criticas de información y las operaciones gubernamentales y comerciales que dependen de Internet están en peligro. Compartimos la responsabilidad de mejorar la seguridad de Internet y coordinar una respuesta internacional efectiva a los incidentes y eventos de seguridad cibernética.

## 1.2.- OBJETIVO DEL PRESENTE TRABAJO

El presente trabajo pretende dar una visión general de las principales amenazas y vulnerabilidades relacionadas con la seguridad cibernética, así como presentar la estrategia en materia de seguridad cibernética desarrollada por el CICTE como parte de la estrategia multidimensional de la OEA.

## 2.1.- CONCEPTOS

**Seguridad Informática (S.I.):** es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.
La decisión de aplicarlos es responsabilidad de cada usuario.
Las consecuencias de no hacerlo ... también.

**Seguridad Cibernética Nacional:** Es el arte de asegurar la existencia y continuidad de la sociedad de la información de una nación, protegiendo, en el ciberespacio, sus activos de información e infraestructura crítica.

**AMENAZA:**

Posible peligro del sistema. Puede ser una persona (cracker), un programa (virus). Existen diversos tipos de amenazas:
Intercepción, Modificación, Interrupción, Generación.

**VULNERABILIDAD:**

Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.
Tipos de vulnerabilidades:

1. Vulnerabilidad Física
2. Vulnerabilidad Natural
3. Vulnerabilidad del Hardware y del Software
4. Vulnerabilidad de los Medios o Dispositivos
5. Vulnerabilidad de las Comunicaciones
6. Vulnerabilidad Humana

**Desvío de flujos:**
Perturbar una comunicación entre 2 equipos para recuperarla o para bloquearla.

**Invasión, piratería, destrucción:**
Acceso ilegal a los datos de los computadores.

**Spoofing:**
Substituir su computador al sitio que quiere visitar el usuario.

## 2.1.- CONCEPTOS

**Seguridad Informática (S.I.):** es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.
La decisión de aplicarlos es responsabilidad de cada usuario.
Las consecuencias de no hacerlo ... también.

**Seguridad Cibernética Nacional:** Es el arte de asegurar la existencia y continuidad de la sociedad de la información de una nación, protegiendo, en el ciberespacio, sus activos de información e infraestructura crítica.

**AMENAZA:**

Posible peligro del sistema. Puede ser una persona (cracker), un programa (virus). Existen diversos tipos de amenazas:
Intercepción, Modificación, Interrupción, Generación.

**VULNERABILIDAD:**

Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.
Tipos de vulnerabilidades:

1. Vulnerabilidad Física
2. Vulnerabilidad Natural
3. Vulnerabilidad del Hardware y del Software
4. Vulnerabilidad de los Medios o Dispositivos
5. Vulnerabilidad de las Comunicaciones
6. Vulnerabilidad Humana

**Desvío de flujos:**
Perturbar una comunicación entre 2 equipos para recuperarla o para bloquearla.

**Invasión, piratería, destrucción:**
Acceso ilegal a los datos de los computadores.

**Spoofing:**
Substituir su computador al sitio que quiere visitar el usuario.


Gráfico 1.- Amenaza, vulnerabilidad y riesgo.

**Defecto del OS o aplicativo, backdoors (puertas traseras):**
Utilización de bug o puntos de control en los productos para controlar, perturbar o explorar (computadores o equipos de red).

**Deny Of Service (DOS):**
Ataque masivo sobre un equipo para bloquear su funcionamiento por saturación.

**Social Engineering (ingeniera social):**
Contactar un usuario y utilizar conocimientos sobre la organización de la empresa y los empleados para aprender su contraseña e informaciones confidenciales.

**Bluejacking** es el envçio de mensajes sin permiso a traves de dispositivos con Bluetooth como celulares, PDAs, portátiles y algunos PCs, enviando una vCard, una Nota o un Contacto que usualmente contiene un mensaje el campo del nombre a otro dispositivo Bluetooth a través del protocolo OBEX. Bluetooth tiene un rango muy limitado, usualmente alrededor de 10 metros en algunos celulares, pero en portátiles puede superar los 100 metros con algunos transmisores potentes.

**Malware** (del inglés malicious software), también llamado badware, software malicioso o software malintencionado es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El

- (estos porcentajes son significativamente mayores para los adultos jóvenes en línea) a como se puede observar en el siguiente gráfico.

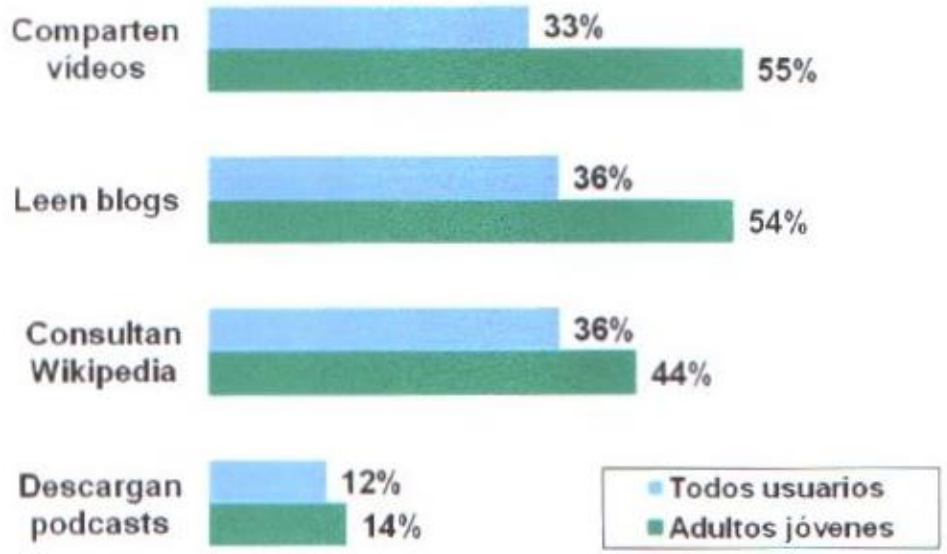


Gráfico 3. Uso de Internet por adultos jóvenes.

Fuente: PEW/Internet. Presentación ante la University of North Florida, *Homo Connectus: The impact of technology on people's everyday lives*, 5 de noviembre de 2007.

Crece el número de aparatos digitales

***En el estudio del PEW Internet Project se observa un aumento en el número de* teléfonos celulares, aparatos de TV, reproductores de DVD, iPods, videograbadoras personales, etc.**

- 88% de los estudiantes tienen teléfonos celulares
- 81% tienen cámaras digitales
- 63% tienen reproductores de MP3
- 55% tienen cámaras de vídeo digitales
- 55% tienen computadoras portátiles
- 27% tienen agendas electrónicas o Blackberries
- 77% utilizan juegos en línea

En la tabla 1, se reflejan datos interesantes sobre la cantidad de aparatos digitales al año 2006, la cual ha aumentado considerablemente durante los años 2007 y 2008, teniendo una ligera contracción en el 2009 e iniciando un alza durante el año 2010.

- (estos porcentajes son significativamente mayores para los adultos jóvenes en línea) a como se puede observar en el siguiente gráfico.

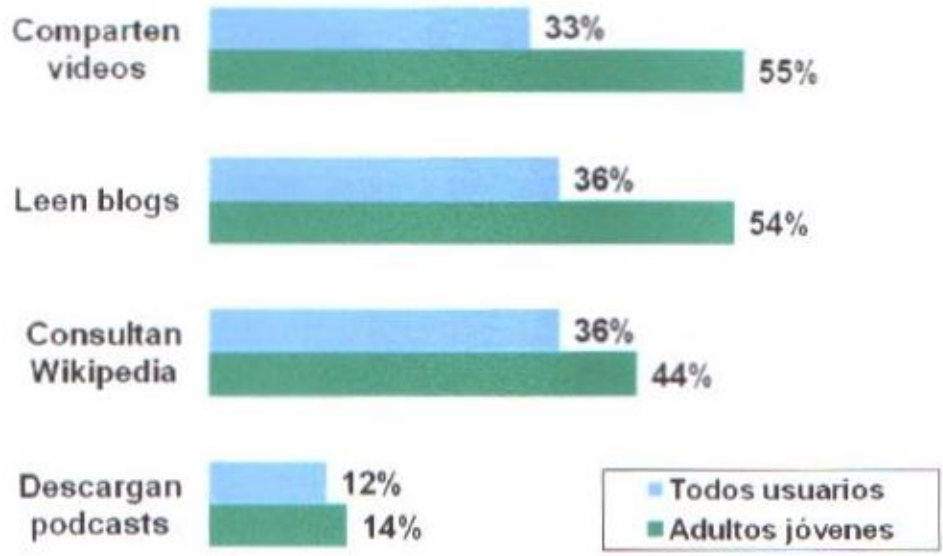


Gráfico 3. Uso de Internet por adultos jóvenes.

Fuente: PEW/Internet. Presentación ante la University of North Florida, *Homo Connectus: The impact of technology on people's everyday lives*, 5 de noviembre de 2007.

Crece el número de aparatos digitales

***En el estudio del PEW Internet Project se observa un aumento en el número de* teléfonos celulares, aparatos de TV, reproductores de DVD, iPods, videograbadoras personales, etc.**

- 88% de los estudiantes tienen teléfonos celulares
- 81% tienen cámaras digitales
- 63% tienen reproductores de MP3
- 55% tienen cámaras de vídeo digitales
- 55% tienen computadoras portátiles
- 27% tienen agendas electrónicas o Blackberries
- 77% utilizan juegos en línea

En la tabla 1, se reflejan datos interesantes sobre la cantidad de aparatos digitales al año 2006, la cual ha aumentado considerablemente durante los años 2007 y 2008, teniendo una ligera contracción en el 2009 e iniciando un alza durante el año 2010.

La sociedad de la información ha tenido un rápido crecimiento a como se puede reflejar en los siguientes indicadores (ver gráfico 4,- . Crecimiento de la Sociedad de la Información 1991-2007):

1.- Las líneas telefónicas principales han aumentado desde 1991 de 546 millones de usuarios hasta 1276 millones en el año 2007.
2.- Los usuarios de Internet han aumentado desde 1991 de 4.4 millones de usuarios hasta 1396 millones en el año 2007, con lo que se logra que la cantidad de usuarios de internet supere la cantidad de líneas telefónicas principales.
3.- Las líneas telefónicas móviles han aumentado desde 1991 de 16 millones de usuarios hasta 3356 millones en el año 2007. Se calcula que durante el 2009 ya superó los 4,000 millones de suscriptores móviles.

Tabla 1.- Aparatos digitales

| DEVICE | MILLIONS IN 2006 |
|---|---|
| Digital Cameras | 400 |
| Camera Phones | 600 |
| PCs | 900 |
| Audio Players | 550 |
| Mobile Subscribers | 1,600 |
| LCD/Plasma TVs | 70 |

Fuente: Internet Innovation Alliance, *"Broadband Fact Book"*, julio de 2007

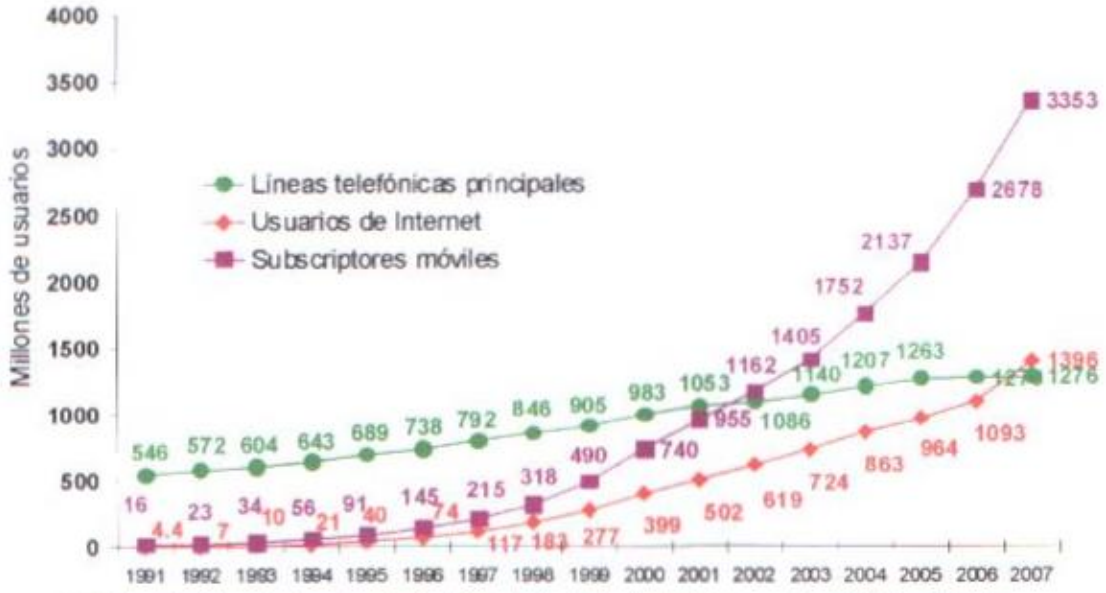


Gráfico 4. Crecimiento de la Sociedad de la Información 1991-2007
Fuente: ITU
Notas: Datos de usuarios de Internet 1991-2005 (ITU), 2006 estimado (Internet World Statistics)

## DATOS TIC PARA NICARAGUA (DATOS OFICIALES SEGÚN TELCOR)

En Nicaragua el nivel de penetración de la tecnología aún es bajo, sin embargo, es bueno mencionar que las tecnologías de punta, en especial la 3G y Wi Max han sido primero implementadas en Nicaragua antes que el resto de países del área centroamericana.

Tabla 2.- Datos TIC para Nicaragua.
Fuente: Sitio oficial de Telcor. www.telcor.gob.ni
ICT Statistics 2008

| | |
|---|---|
| Population | 5667325 |
| GDP (US) | 6349370225 |
| Fixed telephone lines per 100 inhab. | 5.51 |
| Mobile cellular subscriptions per 100 inhab. | 54.84 |
| Computers per 100 inhab. (2005) | 4.03 |
| Internet users per 100 inhab. | 3.26 |
| Broadband Internet subscribers per 100 inhab. | 0.64 |
| Radio sets per 100 inhab. (1998) | 27.70 |
| TV sets per 100 inhab. (2005) | 13.02 |
| % population covered by mobile signal (2005) | 70.00 |

## 2.3.- SEGURIDAD CIBERNÉTICA: AMENAZAS Y RIESGOS VIRTUALES

Hasta no hace mucho (2006) los principales riesgos para la ciberseguridad de los países y gobiernos eran la propagación masiva de virus y gusanos en sus sistemas.
Sin embargo, se están produciendo en los últimos años unos cambios de tendencias significativos, que provocan una percepción de menores 'ataques a Internet':

- Cambios en la motivación de los atacantes, antes se buscaba prestigio y satisfacción personal, ahora, principalmente dinero
- Focalización de los ataques, de ataques a escala global a ataques dirigidos,
- Mayor complejidad y sigilo en los ataques, que supone una complejidad mayor para la investigación/detección de nuevos ataques,

Motivación

- Progresiva profesionalización y maduración del mercado del cibercrimen
- Se buscan principalmente resultados económicos rápidos,
- Bandas financiadas por otros negocios ilícitos ('hackers pagados por delincuentes')
- Aumento de la especialización y diferenciación de los mercados: creadores de virus, vendedores de servicios de hacking, BotNets, NICs anónimos, ISPs 'colaboradores' (fast-flux domain hosting),

Otras motivaciones 'menores'.

- Espionaje industrial y económico
- Servicios de Inteligencia de otras naciones
- Espionaje industrial
- Terrorismo
- Islamismo radical (e-yihad)
- Activismo político

**Nuevos objetivos: Gobierno**

- Ataques crecientes de phising a las agencias y sistemas tributarios; mismos esquemas que ataques de phising bancario
- Son los primeros '.gov' en recibir ataques de phising, pero no los últimos.
- Mantienen relaciones de pago/cobro con ciudadanos
- Son organismos 'confiables'
- Desarrollo de troyanos específicos para robo de información confidencial en dominios gubernamentales
- Ataques de ingeniería social; ataques físicos y lógicos combinados

Mayor complejidad y sigilo

- 'La plataforma rusa': NICs, ISPs, Botnets, como prestadores de servicios para el cibercrimen:
- Garantizando el anonimato,
- Ofreciendo grandes recursos y servicios

- Plataformas emergentes: China, con un mercado en desarrollo de producción de malware e infraestructuras para el cybercrimen.

Se debe entender como ***ciberterrorismo*** el empleo generalizado de las tecnologías de la información (TI), por parte de grupos terroristas ó afines, para la consecución de sus objetivos; utilizando Internet (sistemas informáticos y contenidos) como ***instrumento de comisión del delito*** ó como ***acción del delito***. Se debe desmitificar pero no subestimar la ***amenaza Emergente*** que supone Internet.

Actuales Tendencias del Crimen Cibernético:
- ✓ Fraude y Robo
- ✓ Involucramiento de la mafia en crímenes financieros.
- ✓ Extorsión cibernética
- ✓ Arbitraje jurisdiccional.
- ✓ Lavado de dinero.
- ✓ Crimen Organizado
- ✓ Relaciones de piratas cibernéticos con el crimen organizado.
- ✓ El crimen organizado utiliza la Internet con fines de comunicación codificada.-

Algunos tipos de ataques a los Sistemas de Información:
- ✓ Acceso no autorizado
- ✓ Alteración de los sistemas de Información
- ✓ Ejecución de Software Malicioso que modifiquen o destruyan datos (robo de identidad).
- ✓ Intercepción de las comunicaciones
- ✓ Falsificación Maliciosa
- ✓ Fraudes ciber financieros
- ✓ Pedofilia
- ✓ Fraude electrónico - Phishing
- ✓ Ataques a redes Wi -Fi
- ✓ Denegación de Servicio a Mail Server,
- ✓ Espionaje Industrial
- ✓ Sabotaje informático

La primera vez que apareció un gusano importante en la infraestructura global de TI fue a finales de los años ochenta. El gusano, llamado Morris2, se propagó rápidamente y logró infectar numerosos sistemas de TI de todo el mundo.

**Algunos datos del 'CSI Computer Crime & Security Survey 2008'**

- Los incidentes más costosos de seguridad son aquellos relacionados con el fraude financiero...
- Con una media de costes reportados de 500,000 USD
- Los incidentes de virus siguen ocurriendo frecuentemente...

- Ocurriendo en al menos el 50% de las organizaciones,
- La segunda causa de incidentes es el abuso del personal interno, ocurriendo en un 44% de los casos, seguido del robo de dispositivos móviles.
- Al menos una de diez organizaciones reporta que han tenido problemas de seguridad con el servicio de nombres (DNS)

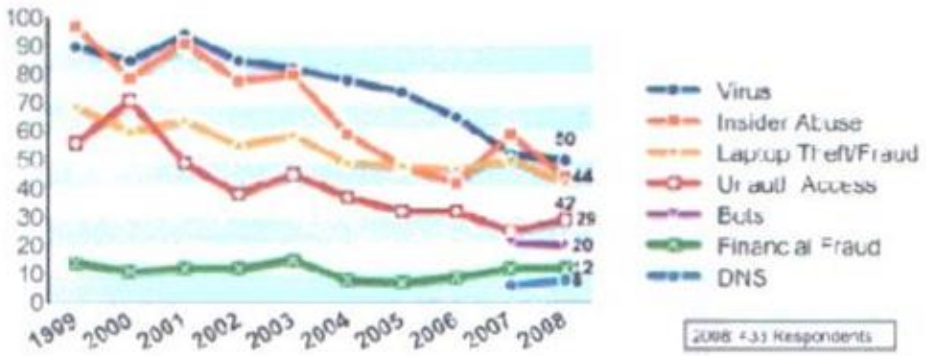


Gráfico 5.- Tipos de incidentes
Fuente: Presentaciones del Taller Hemisférico conjunto de la OEA en el Desarrollo de un Marco Nacional para Seguridad Cibernética 16 al 20 de noviembre de 2009 Río de Janeiro, Brasil.

**Ataques a objetivos de gobierno**

•Hackers" boicotearon difusión de resultado electoral en Colombia
La empresa subcontratada para transmitir los datos de las legislativas por internet detectó "accesos inexplicables" a la Web.
Fuente: AFP - BOGOTA - 09:48 - 17/03/2010

**Corea del Sur / USA, Julio 2009**

•Direcciones de IP usadas para distribuir virus de computadoras que causaron una ola de interrupciones en portales de internet tanto en Estados Unidos como en Corea del Sur.

**Georgia, Agosto 2008**

• Ataque a los sitios del gobierno en el marco de un conflicto armado

• **Lituania, Julio 2008**

• 300 Websites

• **USA, Junio de 2007**

• Redes del Pentágono

• **Estonia, Abril de 2007**

• Ataques de DDoS y defacement masivos contra sitios de gobierno e infraestructura de internet.

• **Alemania, Mayo 2007**

• Sistemas informáticos de la Canciller Alemana y tres Ministerios

• **India 2007 y 2008**

• Ataques de fuentes rusas al National Informatics Centre

• Sitios de gobierno como www.cabsec.gov.in

Ghostnet y ECHELON

A finales del 2009, informáticos canadienses descubrieron Ghostnet, una importante red de espionaje china que se utilizó para espiar ordenadores de la OTAN y de numerosas embajadas.
Gracias a Ghostnet fue posible navegar por el sistema operativo, obtener documentos y activar la webcam y micrófonos para escuchar conversaciones. Se trata de una red similar -aunque menor- a la norteamericana ECHELON, capaz de analizar más de 3.000 millones de conversaciones diarias.

CIA espía la Red
La revista WIRED, reveló que In-Q-Tel, una empresa inversionista de la (CIA), vigila cada día más de medio millón de sitios en internet, revisando más de un millón de conversaciones, foros y spots en diferentes blogs, foros en linea, Flickr, YouTube, Twitter y Amazon.

**Cyber-riesgos globales: la próxima ola**
Estudios recientes revelan tres grandes aspectos claves:
• Crecientes riesgos a la seguridad nacional: El espionaje web es cada vez más avanzado, moviéndose desde la 'curiosidad' a las operaciones bien financiadas y organizadas, no solo con un fin financiero, sino político.
• Incremento de los riesgos a los servicios on-line, afectando a individuos y la industria, debido a la sofisticación de los ataques.
• Mercado emergente de herramientas y vulnerabilidades software, que son usadas para realizar ataques y espionajes a gobiernos e infraestructuras criticas; no existe una clara frontera entre la venta legal e ilegal de vulnerabilidades.
Las actividades cyber criminales han pasado de ser realizada por 'geeks' a organizaciones criminales organizadas, que ahora son 'high-tech'

**Riesgos a los servicios on-line**
Los servicios on-line se han convertido en uno de los objetivos principales de los cyber-criminales
• Los ciber-criminales continúan refinando sus formas para los ataques, siendo en el 2008 los principales:
– Nuevas y sofisticadas formas de ataques
– Ataques contra nuevas tecnologías, como VoIP (vishing – phishing via VoIP & phreaking – hacking de las redes telefónicas para hacer llamadas de larga distancia), y ataques a redes P2P
– Ataques que tienen como objetivo las redes sociales,
– Ataques contra servicios on-line, especialmente servicios on-line bancarios y de gobierno
• Hay un nuevo nivel de complejidad en el malware nunca visto antes. Son más difíciles de detectar y erradicar (uso técnicas criptográficas, automodificación, etc). Por ejemplo, Nuwar tambien conocido como 'Zhelatin' and 'Storm' worm', etc: aparecen nuevas variantes todos los días
• Uso de PCs en redes Bot (Botnets) para perpetrar estos ataques y distribuir malware.

**El crimen tecnológico: Una economía en auge**

Existe un mercado creciente para las amenazas Zero-day y las herramientas para el cibercrimen.

• Con tantos PC infectados (se calcula que alrededor del 5% de los computadores del mundo son Zombies), el mercado para suplir botnets se ha endurecido. El costo de alquiler de una plataforma de Bots para spam cuesta entre $ 0,03 – 0,07 por Bot por semana.

• Con un presupuesto de entre $ 25 a $ 1500 se puede comprar un troyano para robar tarjetas de crédito personalizado. El malware está siendo desarrollado para atacar compañías y agencias específicas.

• Ya no son necesarias habilidades en informática para participar en el cibercrimen. Actualmente los programadores de malware no necesitan cometer crímenes ellos mismos. Ahora se desarrollan herramientas con soporte técnico y actualizaciones para aprovecharse de vulnerabilidades (MPACK, Pinch)

• Existe un mercado negro establecido para datos robados (tarjetas de crédito, e-mails, cuentas de skype, etc), los costos de una tarjeta de crédito robada empiezan en $ 5.

**Tendencias próximas**

Las tendencias indican un crecimiento en los paraísos del cibercrimen, resaltándose la importancia de los acuerdos de cooperación internacional

• Es una realidad inevitable que algunos países se conviertan en paraísos para ciber criminales donde la presión internacional no tendrá mucho efecto.

• Se prevé que en los próximos años los gobiemos realicen acciones decididas contra los individuos, grupos o compañías que presten estos servicios (Ej. RBN) y las organizaciones intermediarias (ISPs y proveedores de software) para tomar medidas que protejan al público contra el malware, el hacking y la ingeniería social.

• Es probable la proliferación de códigos de prácticas de la industria que demanden medidas de seguridad, respaldados por esquemas de aseguramiento y pólizas de seguros.

La sofisticación de los ataques está en crecimiento y el intruso requiere menos conocimiento para conducir el ataque a como lo demuestra el siguiente gráfico:

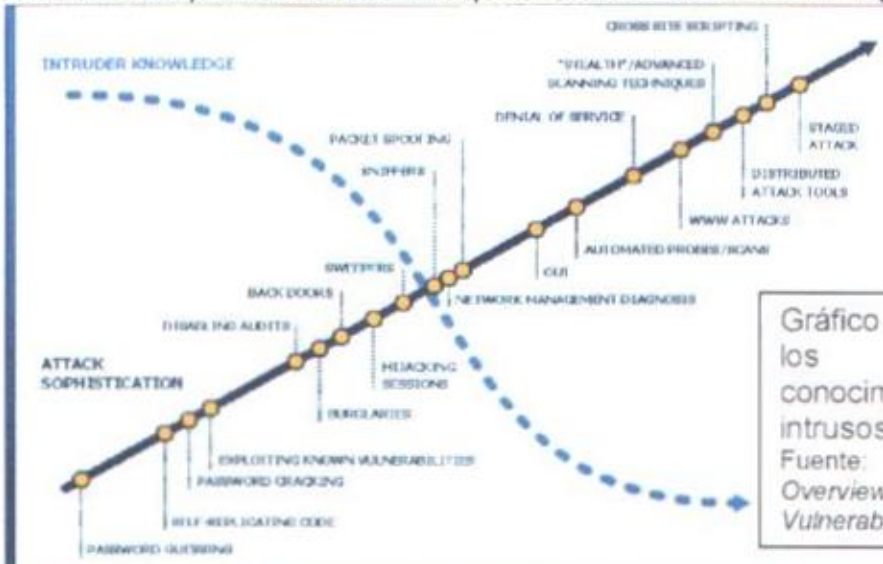


Gráfico 6. Sofisticación de los ataques con conocimientos de los intrusos
Fuente: CERT/CC, *CERT/CC Overview - Incident and Vulnerability Trends*


Gráfico 7.- Vulnerabilidades en crecimiento

El gráfico 7 refleja que los años más críticos para la seguridad cibernética han sido los años 2002 y 2006, teniendo un descenso entre los años 2007 y 2008. Durante el año 2009 se dieron una serie de incidentes relacionados con aspectos financieros, sobre todo en suplantación de identidades, pero muchos bancos no los reportan ya que esto mina su credibilidad.

El gráfico 8, nos ilustra sobre el nivel de amenaza el cual es igual a:
la capacidad X intenciones + la importancia X nivel estratégico.
Actualmente hasta los estados son amenazados por ataques de otros estados como fue el caso de Estonia y Georgia.

Nivel de amenaza = capacidad x Intenciones + importancia x Nivel estratégico


Gráfico 8, Nivel de amenaza vs Capacidades
Fuente: *"Taller Avanzado sobre Manejo de un Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT) Nacional", Febrero 16 al 20, 2009,San José – Costa Rica. Presentación del equipo participante por Brasil.*

## 2.4.- ACTIVIDADES ILICITAS ENFRENTADAS EN NICARAGUA

- Ataque al sitio Web del Consejo Supremo Electoral (CSE).
- 4 Planificaciones de Atentados vía e-mail en contra de personalidades del país.
- 6 Casos de Pornografía Infantil, 2 de ellos en Coordinación con la Guardia Civil de España (12 Detenidos 4 Nacionales y 8 Extranjeros).
- 12 Casos de Extorsiones y Amenazas vía e-mail.
- Un Fraude Electrónico que dejo 5,700 personas afectadas (Agave Azul), dos detenidos y cuatro Mexicanos Prófugos.

# CAPÍTULO III.- CONSECUENCIA DE LA TECNOLOGIA CONTRA LA SEGURIDAD Y LA DEFENSA NACIONAL EN LAS EXPRESIONES DEL PODER.

## 3.1.- LA EXPRESIÓN ECONÓMICA.

Esta expresión es una de las más vulnerables, principalmente a los ataques cibernéticos, por la cantidad de información, operaciones, servicios bancarios, depósitos de los clientes del sistema, el espionaje industrial, robo de base de datos, robo de números de tarjetas de crédito, a los cuales pueden tener acceso, conociendo sus respectivos códigos, por esa razón, existe el 70% de los asaltos a los clientes de las Instituciones bancarias en algunos países especialmente en Centroamérica por personal de los mismos bancos para fines delincuenciales. Asimismo se debe considerar las diferentes herramientas que ya mencionamos en el Capitulo 3, especialmente el espionaje corporativo que hace mucho daño en la actualidad, existen casos en las instituciones bancarias de los países del hemisferio, por el robo de información de algunos proyectos financieros que son utilizados por otras Instituciones, lo que no se publica en los medios de comunicación por evitar que los clientes conozcan sus vulnerabilidades y se tenga un temor generalizado de efectuar sus respectivos depósitos. Lo que puede afectar el desarrollo interno de los diferentes países que componen el hemisferio y por la posible falta de credibilidad de los inversionistas extranjeros y las transnacionales, que pueden afectar el logro de los objetivos nacionales establecidos en las Cartas Magnas especialmente de los países de Latinoamérica. Podemos hablar entonces de una amenaza proveniente de la cibernética y ya no sólo de una amenaza interna o externa, con el agravante de no poderla enmarcar en ninguna de las dos, por las características del espacio tan grande de la red. La facilidad que tienen las organizaciones terroristas, crimen organizado, narcotraficantes, para acceder a la tecnología de punta es muy alta, por lo que las posibilidades de acceder a la información confidencial que manejan los bancos sobres sus clientes se les facilita, los Hacker, los Cracker, los piratas informáticos, el espionaje corporativo, las bombas lógicas, son verdaderos peligros para las instituciones financieras y para las transnacionales, las empresas nacionales etc. Algunos países del hemisferio por el contrario, como las Islas Caimán o Islas Canarias que además tienen otro ingrediente como lo es el secreto bancario, reciben muchas veces recursos producto del lavado de dinero, por la misma flexibilidad que tienen para recibir fondos, misma situación que presentan los bancos Suizos. Estos son factores que afectan directamente el desarrollo principalmente de los países latinoamericanos, que en muchas ocasiones no cuentan con las herramientas necesarias para proteger la información que poseen de las empresas y las personas naturales que tienen sus depósitos bancarios.
En 1998, casi todas las 500 empresas que figuran en la famosa lista de la revista Fortune habían sido penetradas en alguna ocasión por delincuentes informáticos. El FBI estima que este tipo de delitos moviliza 10,000 millones de dólares anuales, y que solo el 17% de las compañías agredidas, estafadas o chantajeadas electrónicamente efectúan las respectivas denuncias.

Otro factor que no es menos dañino es la piratería comercial principalmente a la industria cinematográfica y musical, esto aparentemente puede afectar a las grandes transnacionales de Hollywood en los Estados Unidos o a Sony Music, sin

## 3.1.- LA EXPRESIÓN ECONÓMICA.

Esta expresión es una de las más vulnerables, principalmente a los ataques cibernéticos, por la cantidad de información, operaciones, servicios bancarios, depósitos de los clientes del sistema, el espionaje industrial, robo de base de datos, robo de números de tarjetas de crédito, a los cuales pueden tener acceso, conociendo sus respectivos códigos, por esa razón, existe el 70% de los asaltos a los clientes de las Instituciones bancarias en algunos países especialmente en Centroamérica por personal de los mismos bancos para fines delincuenciales. Asimismo se debe considerar las diferentes herramientas que ya mencionamos en el Capitulo 3, especialmente el espionaje corporativo que hace mucho daño en la actualidad, existen casos en las instituciones bancarias de los países del hemisferio, por el robo de información de algunos proyectos financieros que son utilizados por otras Instituciones, lo que no se publica en los medios de comunicación por evitar que los clientes conozcan sus vulnerabilidades y se tenga un temor generalizado de efectuar sus respectivos depósitos. Lo que puede afectar el desarrollo interno de los diferentes países que componen el hemisferio y por la posible falta de credibilidad de los inversionistas extranjeros y las transnacionales, que pueden afectar el logro de los objetivos nacionales establecidos en las Cartas Magnas especialmente de los países de Latinoamérica. Podemos hablar entonces de una amenaza proveniente de la cibernética y ya no sólo de una amenaza interna o externa, con el agravante de no poderla enmarcar en ninguna de las dos, por las características del espacio tan grande de la red. La facilidad que tienen las organizaciones terroristas, crimen organizado, narcotraficantes, para acceder a la tecnología de punta es muy alta, por lo que las posibilidades de acceder a la información confidencial que manejan los bancos sobres sus clientes se les facilita, los Hacker, los Cracker, los piratas informáticos, el espionaje corporativo, las bombas lógicas, son verdaderos peligros para las instituciones financieras y para las transnacionales, las empresas nacionales etc.
Algunos países del hemisferio por el contrario, como las Islas Caimán o Islas Canarias que además tienen otro ingrediente como lo es el secreto bancario, reciben muchas veces recursos producto del lavado de dinero, por la misma flexibilidad que tienen para recibir fondos, misma situación que presentan los bancos Suizos. Estos son factores que afectan directamente el desarrollo principalmente de los países latinoamericanos, que en muchas ocasiones no cuentan con las herramientas necesarias para proteger la información que poseen de las empresas y las personas naturales que tienen sus depósitos bancarios.
En 1998, casi todas las 500 empresas que figuran en la famosa lista de la revista Fortune habían sido penetradas en alguna ocasión por delincuentes informáticos. El FBI estima que este tipo de delitos moviliza 10,000 millones de dólares anuales, y que solo el 17% de las compañías agredidas, estafadas o chantajeadas electrónicamente efectúan las respectivas denuncias.

Otro factor que no es menos dañino es la piratería comercial principalmente a la industria cinematográfica y musical, esto aparentemente puede afectar a las grandes transnacionales de Hollywood en los Estados Unidos o a Sony Music, sin

información obtenida en muchas ocasiones producto de la obtención de información de los mismos integrantes de un partido político, toda la información obtenida puede ser efectuada con medios electrónicos, como lo decíamos antes los celulares, las agendas electrónicas, los Jump Drive, las cámaras digitales, han hecho que las grabadoras o las antiguas cámaras fotográficas pasen a un segundo plano y ahora la información se pase en tiempo real.

Las consecuencias políticas de las nuevas amenazas podrían conllevar a un debilitamiento del estado de derecho, a la vulnerabilidad y falta de credibilidad de las instituciones democráticas, a la ingobernabilidad, la degradación del clima de seguridad ciudadana y en general a la inestabilidad política, económica y social.

Los riesgos implícitos de la nueva situación hemisférica apuntan fundamentalmente a producir desestabilización en la gobernabilidad y estabilidad política de los estados, a la vez que una creciente sensación de inseguridad en las personas, por cuanto las "nuevas amenazas a la seguridad", entre las que destacan las migraciones ilegales masivas; el narcotráfico, terrorismo, tráfico ilícito de armas, cibercrimen, la corrupción y sus vinculaciones con la delincuencia transnacional organizada; las enfermedades pandémicas; las catástrofes y desastres naturales y el transporte de sustancias peligrosas, tienen consecuencias y alcances que escapan al control individual de los Estados.

Frente a ello, la cooperación interestatal es imprescindible para el desarrollo de instrumentos jurídicos apropiados a las nuevas amenazas a la seguridad hemisférica, el esfuerzo regional es necesario para hacer frente a estos peligros que afectan a todo el hemisferio. Sin embargo se puede observar muchos vacíos legales que favorecen a los diferentes actores fuera de la ley que se han mencionado. Lo que en muchos países han tenido reacciones hasta del mismo ejecutivo, como es el caso de Ecuador, donde existía una iniciativa de ley para readecuar el poder judicial a las nuevas amenazas, que al final terminaron con el gobierno del ex presidente Lucio Gutiérrez.

## 3.3.- LA EXPRESIÓN PSICOSOCIAL.

En ésta expresión la amenaza más grande es la inseguridad pública, lo cual se convierte en amenaza cuando rebasa la capacidad de las instituciones responsables. Así mismo el incremento del tráfico y consumo de drogas, la escalada de hechos delictivos; especialmente el secuestro, perturban en el presente, la tranquilidad pública y crean un clima de desconfianza e inseguridad, lo cual obstaculiza el logro de los Objetivos Nacionales. Por lo que al conjugarse la informática y las comunicaciones en la tecnología encontramos una serie de medios que son de especial interés para el crimen organizado y que amenazan la estabilidad de la empresa privada y de la población en general.

Las coordinaciones que se hacen por los medios existentes en estas dos áreas están relacionadas con las áreas de la delincuencia, donde entran flagelos tales como el narcotráfico y los secuestros, existe mucha facilidad para que delincuentes bien equipados obtengan información clasificada del patrimonio de una empresa o una persona cuyos bienes provoque secuestros o robos.

Las coordinaciones que hacen los delincuentes desde la prisión donde se encuentran es clara, muchas acciones delincuenciales se han ejecutado por cabecillas capturados, en algunos países de Centroamérica por ejemplo los grupos conocidos como "maras"(El salvador), reciben instrucciones para recaudar dinero de manera ilícita, para el mantenimiento de estos grupos, pago de sobornos y pago de sicarios para asesinar hasta los mismo agentes penitenciarios, por los cabecillas capturados. Cuando las instituciones de seguridad pública obtienen los resultados de las investigaciones efectuadas, la mayoría de los resultados son los siguientes:

a.- Empleo de teléfonos celulares y satelitales.

b.- Utilización del Internet para seleccionar los procedimientos a utilizar en las acciones delincuenciales.

c.- Hasta la utilización de uno de los medios de comunicación más antiguos como el mensajero.

Como consecuencia de este tipo de acciones debidamente comprobadas, se han tenido que efectuar una serie de medidas adicionales en los penales o reclusorios a fin e evitar el acceso a los medios electrónicos antes mencionados, este tipo de regulaciones han tenido como consecuencias amotinamientos como en Guatemala, Honduras y El Salvador en Centroamérica.

## 3.4.- LA EXPRESIÓN MILITAR.

En el ámbito militar las amenazas pueden desarrollarse con la obtención de información sobre las posibles alianzas con países vecinos ante un posible conflicto externo que amenace la soberanía y la integridad territorial de un Estado. Ante las situaciones planteadas respecto a las capacidades limitadas de países subdesarrollados para proteger la información que se maneja en dependencias como: los Ministerios de Defensa, los Estados Mayores o las diferentes Unidades con el manejo de información clasificada, donde la contrainteligencia es una herramienta eficiente para la protección de documentos, instalaciones físicas y de comunicaciones. La mayoría de las instituciones armadas constantemente investigan a su personal y hace pruebas poligráficas, este tipo de procedimientos los realizan desde los Estados Unidos hasta los países suramericanos, por ser una autoprotección a la información confidencial que manejan. Sin embargo cuando apreciamos las acciones realizadas por Al Qaeda el 11 de Septiembre del 2001, nos damos cuenta que la obtención de inteligencia para detectar este tipo de operaciones requiere de un trabajo conjunto.

Cuando tocamos la defensa nacional las amenazas son más claras, sin embargo las herramientas actuales proporcionan la ventaja de poder enviar por correo electrónico diferentes tipos de documentos confidenciales de un país a otro, con accesorios como los teléfonos celulares de última generación que han evolucionado en los últimos 10 años de manera constante, con costos muy económicos y fáciles de adquirir, las agendas electrónicas y las cámaras fotográficas digitales, las cuales no se necesitan ni sacar de las instalaciones,

basta con sacar la memoria que miden como máximo una pulgada y un grosor de 2 milímetros, los Jump Drive que pueden tener una capacidad de 500 Mbytes y tienen también un tamaño muy fácil de ocultar. Aunque es un tema muy delicado siempre los orígenes están basados principalmente en la parte económica, la compra de voluntades del mismo personal que trabaja en las dependencias más sensitivas. Por eso cobra vigencia como se menciona anteriormente la contrainteligencia, la protección de los documentos con las contraseñas, son las soluciones más apropiadas para proteger la información valiosa que se maneja por ejemplo de operaciones militares como lo es en el caso de Colombia, donde en la reciente visita efectuada por el Colegio Interamericano de Defensa, se pudo apreciar la cantidad de medidas de seguridad y el compartimentaje de la información que se maneja, para evitar que personal ajeno a la instituciones militares la obtenga y detecte la planificación de las operaciones militares a futuro y en desarrollo.

Sin embargo, es importante mencionar que existen mecanismos como las conferencias y reuniones de los Altos Mandos de las Fuerzas Armadas de toda América, que ayudan a fortalecer la confianza mutua entre las instituciones armadas del continente y ayudan a determinar problemas que puedan ser afrontados en forma conjunta y coordinada, en virtud de que dichos problemas pudieran tener incidencias para la paz y la seguridad de los países y subregiones del hemisferio. Aspectos como la Seguridad Hemisférica, la Confianza Mutua, la Transparencia y la Defensa y Desarrollo Regional son ejemplos de los importantes temas que se discuten en estos foros y que proporcionan nuevas experiencias para las instituciones militares y de seguridad pública, para afrontar de una manera más eficiente las crecientes amenazas a la seguridad y la defensa nacional.

# CAPÍTULO IV.- CSIRT. INICIATIVAS Y EXPERIENCIAS.

## 4.1.- QUÉ ES UN CSIRT

El término CSIRT significa Computer Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad Informática), y ha sido acuñado respondiendo simultáneamente a diferentes abreviaturas usadas para denotar a nivel mundial este tipo de equipos:

- CSIRT (Computer Security Incident Response Team / Equipo de Respuesta a Incidentes de Seguridad Informática): Término usado en Europa.
- CERT o CERT/CC (Computer Emergency Response Team / Coordination Center, equipo de respuesta a emergencias informáticas / Centro de coordinación): Término registrado en los Estados Unidos de América por el CERT Coordination Center (CERT/CC).
- IRT (Incident Response Team / Equipo de respuesta a incidentes).
- CIRT (Computer Incident Response Team / Equipo de respuesta a incidentes informáticos).
- SERT (Security Emergency Response Team / Equipo de respuesta a emergencias de seguridad).

Un CSIRT es un equipo de expertos en seguridad informática que pretenden responder a los incidentes de seguridad relacionados con la tecnología de la información y a recuperarse después de sufrir uno de estos incidentes. Para minimizar los riesgos también se ofrecen servicios preventivos y educativos relacionados con vulnerabilidades de software, hardware o comunicaciones y se informa a la comunidad sobre los potenciales riesgos que toman ventaja de las deficiencias de la seguridad.

## 4.2.- ANTECEDENTES

Durante la segunda mitad de los años ochenta se vio la red Arpanet salir de la fase de I&D y convertirse en una realidad práctica bajo el impulso del mundo universitario y desarrollada por el DoD (el Departamento de Defensa estadounidense). La eficacia y la constante mejora de los distintos servicios, entre los cuales se cuenta el correo electrónico, rápidamente hicieron que esta red sea indispensable para numerosos sitios.

En noviembre de 1988, un estudiante de la Universidad de Cornell lanzó en esta red un programa que se propagaba y se replicaba solo. Este programa, conocido con el nombre de "gusano de Internet", aprovechaba distintos fallos de seguridad del sistema Unix (el sistema operativo de la mayoría de los ordenadores conectados en la red). Aunque no fue programado con malas intenciones, este primer virus informático, se propagó rápidamente obstruyendo al mismo tiempo las máquinas infectadas por múltiples copias del gusano. En ese entonces, la red constaba de aproximadamente 60.000 ordenadores. Con sólo el 3 o 4 % de las máquinas contaminadas, la red estuvo totalmente indisponible durante varios días, hasta que se tomaron medidas cautelares (incluyendo la desconexión de numerosas máquinas de la red).

Para eliminar este "gusano de Internet", se creó un equipo de análisis ad hoc con expertos del MIT, de Berkley, Purdue. Se reconstituyó y analizó el código del virus, lo cual permitió, por una parte, identificar y corregir los fallos del sistema operativo, y por otra parte, desarrollar y difundir mecanismos de erradicación. Después de este incidente, el director de obras de Arpanet, la DARPA (Defense Advanced Research Projects Agency), decidió instalar una estructura permanente, el CERT Coordination Center (CERT/CC) parecido al equipo reunido para resolver el incidente.

Este incidente actuó como una alarma e impulsó la necesidad de cooperación y coordinación multinacional para enfrentarse este tipo de casos. En este sentido, la DARPA (Defence Advanced Research Projects Agency / Agencia de Investigación de Proyectos Avanzados de Defensa) creó el primer CSIRT: El CERT Coordination Center (CERT/CC[1]), ubicado en la Universidad Carnegie Mellon, en Pittsburgh (Pensilvania, USA).

Poco después el modelo se adoptó en Europa, y en 1992 el proveedor académico holandés SURFnet puso en marcha el primer CSIRT de Europa, llamado SURFnet-CERT[2]. El número de CSIRTs continuó creciendo, cada uno con su propio propósito, financiación, divulgación y área de influencia. La interacción entre estos equipos experimentó dificultades debido a las diferencias en lengua, zona horaria y estándares o convenciones internacionales. Siguieron otros muchos equipos, y en la actualidad existen más de 100 equipos reconocidos alrededor del mundo. Con el tiempo, los CERT ampliaron sus capacidades y pasaron de ser una fuerza de reacción a prestadores de servicios de seguridad completos que incluyen servicios preventivos como alertas, avisos de seguridad, formación y servicios de gestión de la seguridad. Pronto el término "CERT" se consideró insuficiente, y a finales de los años noventa se acuñó el término "CSIRT". En la actualidad, ambos términos (CERT y CSIRT) se usan como sinónimos.

Internet comenzó su vertiginoso crecimiento y muchas compañías comenzaron a confiar en Internet sus transacciones diarias. Así mismo, los CSIRTs continuaron creciendo alrededor del globo, soportando gobiernos enteros u organizaciones multinacionales.

Desde ese entonces, Internet ha seguido creciendo hasta llegar a ser la red que se conoce actualmente, con una multiplicación rápida de las máquinas conectadas (varios millones) y de las fuentes de agresión.

---

[1] CERT-CC. Tomado de: http://www.cert.org. U.A: 2008/09/26. Publicado por: Software Engineering Institute - Carnegie Mellon University. Autor: No determinado

[2] SURFnet-CERT. Tomado de: http://www.surfnet.nl/en/Pages/default.aspx. U.A: 2008/09/26. Publicado por: SURFnet network. Autor: No determinado

| Nombre del Documento | Resumen | Enlace | Fuente |
|---|---|---|---|
| Method | | | Version 1.0.pdf |
| State of the Practice of Computer Security Incident Response Teams | Teoría General en temas de CSIRT | http://www.cert.org/ | State of the Practice of Computer Security Incident Response Teams.pdf |
| The Real Secrets of Incident Management | Teoría General en temas de CSIRT | http://www.cert.org/ | The Real Secrets of Incident Management.pdf |
| The Real Secrets of Incident Management | Teoría General en temas de CSIRT | http://www.cert.org/ | The Real Secrets of Incident Management.MP3 |
| Incident Response SHight | Teoría General en temas de CSIRT | http://www.rediris.es/cert/links/csirt.es.html | Incident_Response_SHight.pdf |
| Improving CSIRT Communication Through Standardized and Secured Information Exchange | Teoría General en temas de CSIRT | http://www.tesink.org/thesis.pdf | Thesis.pdf |
| Limits to Effectiveness in Computer Security Incident Response Teams | Teoría General en temas de CSIRT | https://www.cert.org/archive/pdf/Limits-to-CSIRT-Effectiveness.pdf | Limits-to-CSIRT-Effectiveness.pdf |
| eCSIRT.net Deliverable Common Language Specification & Guideline to Application of the Common Language part (i) | Teoría General en temas de CSIRT | http://www.ecsirt.net/cec/service/documents/wp2-common-language.pdf | wp2-common-language.pdf |
| eCSIRT.net Deliverable1 Guideline to Application of the Common Language part (ii) | Teoría General en temas de CSIRT | http://www.ecsirt.net/cec/service/documents/wp2-and-3-guideline.pdf | wp2-and-3-guideline.pdf |
| Seguridad Informática para Administradores de | Teoría General en temas de CSIRT | http://www.arcert.gov.ar/ncursos/material/Seg-adm-6p.pdf | Seg-adm-6p.pdf |

| Nombre del Documento | Resumen | Enlace | Fuente |
|---|---|---|---|
| Redes y Servidores | | | |
| Seguridad Informática para Administradores de Redes y Servidores | Teoría General en temas de CSIRT | http://www.arcert.gov.ar/cursos/seguridad_adm/Seguridad%20para%20Administradores.pdf | Seguridad%20para%20Administradores.pdf |
| Helping prevent information security risks in the transition to integrated operations | Teoría General en temas de CSIRT | http://www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_029-037.pdf | Page_029-037.pdf |
| State of the Practice of Computer Security Incident Response Teams (CSIRTs) | Teoría General en temas de CSIRT | http://www.rediris.es/cert/links/csirt.es.html | 03tr001 - State of the Practice of Computer Security Incident Response Teams.pdf |
| Expectations for Computer Security Incident Response | Teoría General en temas de CSIRT | http://www.ietf.org/rfc/rfc2350.txt | Expectations for Computer Security Incident Response.doc |
| Site Security Handbook | Teoría General en temas de CSIRT | http://www.ietf.org/rfc/rfc2196.txt | Site Security Handbook.doc |
| Guidelines for Evidence Collection and Archiving | Teoría General en temas de CSIRT | http://www.ietf.org/rfc/rfc3227.txt | Guidelines for Evidence Collection and Archiving.doc |
| Why do I need a CSIRT? | Teoría General en temas de CSIRT | http://www.terena.org/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf | jaroszewski-assistance-csirt.pdf |
| Description of the different kinds of CSIRT environments | Teoría General en temas de CSIRT | http://www.enisa.europa.eu/cert_guide/pages/05_01_04.htm | Description of the different kinds of CSIRT environments.docs |
| Informe del relator del séptimo período ordinario de sesiones del Comité Interamericano Contra el Terrorismo | Antecedentes de los CSIRT | http://scm.oas.org/pdfs/2007/CICTE00188E.pdf | CICTE00188E.pdf |
| Adopción de una | Antecedentes de | http://dgpt.sct.gob.mx/filead | doc_472-04.doc |

| Nombre del Documento | Resumen | Enlace | Fuente |
|---|---|---|---|
| estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética | los CSIRT | min/ccp1/redes/doc._472-04.doc | |
| Puesta en marcha del CSIRT y Gestión de Seguridad de la Información de ANTEL | Antecedentes de los CSIRT | http://jiap.org.uy/jiap/JIAP2007/Presentaciones%20Jiap%202007/ANTEL.pdf | Antel.pdf |
| FIRST - Forum for Incident Response and Security Teams | Experiencias en el Mundo | http://www.first.org/ | Página Web |
| ENISA - European Network and Information Security Agency | Experiencias en el Mundo | http://www.enisa.europa.eu/cert_guide/downloads/CSIRT_setting_up_guide_ENISA-ES.pdf | Página Web |
| APCERT (Asia Pacific Computer Emergency Response Team) | Experiencias en el Mundo | http://www.apcert.org/ | Página Web |
| CERT Coordination Center de la Universidad Carnegie Mellon | Experiencias en el Mundo | http://www.cert.org/ | Página Web |
| Alemania - CERT-Bund | Experiencias en el Mundo | http://www.bsi.bund.de/certbund/ | Página Web |
| Arabia Saudita - CERT-SA (Computer Emergency Response Team - Saudi Arabia) | Experiencias en el Mundo | http://www.cert.gov.sa/ | Página Web |

| Nombre del Documento | Resumen | Enlace | Fuente |
|---|---|---|---|
| Argentina - ArCERT (Computer Emergency Response Team of the Argentine Public) | Experiencias en el Mundo | http://www.arcert.gov.ar/ | Página Web |
| Australia - AusCERT (Australia Computer Emergency Response Team) | Experiencias en el Mundo | http://www.auscert.org.au/ | Página Web |
| Austria - CERT.at (Computer Emergency Response Team Austria) | Experiencias en el Mundo | www.cert.at | Página Web |
| Brasil - CERT.br (Computer Emergency Response Team Brazil) | Experiencias en el Mundo | http://www.cert.br | Página Web |
| Canadá - PSEPC (Public Safety Emergency Preparedness Canada) | Experiencias en el Mundo | http://www.psepc-sppcc.gc.ca/prg/em/ccirc/index-en.asp | Página Web |
| Chile – CSIRT-GOV | Experiencias en el Mundo | http://www.csirt.gov.cl/ | Página Web |
| Chile – CLCERT | Experiencias en el Mundo | http://www.clcert.cl | Página Web |
| China - CNCERT/CC (National Computer Network Emergency Response Technical Team) | Experiencias en el Mundo | http://www.cert.org.cn/english_web/ | Página Web |
| Corea del Sur - KrCERT/CC (CERT Coordination Center Korea) | Experiencias en el Mundo | http://www.krcert.or.kr/ | Página Web |
| Dinamarca – DK.CERT (Danish Computer | Experiencias en el Mundo | https://www.cert.dk/ | Página Web |

| Nombre del Documento | Resumen | Enlace | Fuente |
|---|---|---|---|
| Argentina - ArCERT (Computer Emergency Response Team of the Argentine Public) | Experiencias en el Mundo | http://www.arcert.gov.ar/ | Página Web |
| Australia - AusCERT (Australia Computer Emergency Response Team) | Experiencias en el Mundo | http://www.auscert.org.au/ | Página Web |
| Austria - CERT.at (Computer Emergency Response Team Austria) | Experiencias en el Mundo | www.cert.at | Página Web |
| Brasil - CERT.br (Computer Emergency Response Team Brazil) | Experiencias en el Mundo | http://www.cert.br | Página Web |
| Canadá - PSEPC (Public Safety Emergency Preparedness Canada) | Experiencias en el Mundo | http://www.psepc-sppcc.gc.ca/prg/em/ccirc/index-en.asp | Página Web |
| Chile – CSIRT-GOV | Experiencias en el Mundo | http://www.csirt.gov.cl/ | Página Web |
| Chile – CLCERT | Experiencias en el Mundo | http://www.clcert.cl | Página Web |
| China - CNCERT/CC (National Computer Network Emergency Response Technical Team) | Experiencias en el Mundo | http://www.cert.org.cn/english_web/ | Página Web |
| Corea del Sur - KrCERT/CC (CERT Coordination Center Korea) | Experiencias en el Mundo | http://www.krcert.or.kr/ | Página Web |
| Dinamarca – DK.CERT (Danish Computer | Experiencias en el Mundo | https://www.cert.dk/ | Página Web |

| Nombre del Documento | Resumen | Enlace | Fuente |
|---|---|---|---|
| Emergency Response Team) | | | |
| Emiratos Árabes Unidos – aeCERT (The United Arab Emirates Computer Emergency Response Team) | Experiencias en el Mundo | http://www.aecert.ae/ | Página Web |
| España - ESCERT (Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas) | Experiencias en el Mundo | http://escert.upc.edu/index.php/web/es/index.html | Página Web |
| España – IRIS-CERT (Universidades) | Experiencias en el Mundo | http://www.rediris.es/cert/ | Página Web |
| España - CCN-CERT (Cryptology National Center - Computer Security Incident Response Team) | Experiencias en el Mundo | https://www.ccn-cert.cni.es/ | Página Web |
| España - INTECO-CERT (Centro de Respuestas a Incidentes en TI para PYMES y Ciudadanos) | Experiencias en el Mundo | http://www.inteco.es/rssRead/Seguridad/INTECOCERT | Página Web |
| Estados Unidos - US-CERT (United States - Computer Emergency Readiness Team) | Experiencias en el Mundo | http://www.us-cert.gov | Página Web |
| Estonia – CERT-EE | Experiencias en el Mundo | http://www.ria.ee/?id=28201 | Página Web |
| Filipinas - PH-CERT (Philippines Computer Emergency Response Team) | Experiencias en el Mundo | http://www.phcert.org/ | Página Web |
| Francia-CERTA (Centre d'Expertise Gouvernemental de | Experiencias en el Mundo | http://www.certa.ssi.gouv.fr/ | Página Web |

| Nombre del Documento | Resumen | Enlace | Fuente |
|---|---|---|---|
| Réponse et de Traitement des Attaques informatiques) | | | |
| Hong Kong - HKCERT (Hong Kong Computer Emergency Response Coordination Centre) | Experiencias en el Mundo | http://www.hkcert.org/ | Página Web |
| Hungría - CERT-Hungria | Experiencias en el Mundo | http://www.cert-hungary.hu/ | Página Web |
| India - CERT-In | Experiencias en el Mundo | http://www.cert-in.org.in/ | Página Web |
| Japan - JPCERT/CC (JP CERT Coordination Center) | Experiencias en el Mundo | http://www.jpcert.or.jp/ | Página Web |
| México – UNAM-CERT | Experiencias en el Mundo | http://www.cert.org.mx/index.html | Página Web |
| Nueva Zelandia – CCIP (Centre for Critical Infrastructure Protection) | Experiencias en el Mundo | http://www.ccip.govt.nz/ | Página Web |
| Holanda - GOVCERT.NL | Experiencias en el Mundo | http://www.govcert.nl/ | Página Web |
| Polonia - CERT Polska (Computer Emergency Response Team Polska) | Experiencias en el Mundo | http://www.cert.pl/ | Página Web |
| Qatar - Q-CERT (Qatar CERT) | Experiencias en el Mundo | http://www.qcert.org | Página Web |
| Reino Unido – GovCertUK | Experiencias en el Mundo | www.govcertuk.gov.uk | Página Web |
| | Experiencias en el Mundo | www.cpni.gov.uk | Página Web |
| Singapur – SingCERT (Singapore CERT) | Experiencias en el Mundo | http://www.singcert.org.sg/ | Página Web |
| Sri Lanka – SLCERT | Experiencias en el Mundo | http://www.cert.lk/ | Página Web |

| Nombre del Documento | Resumen | Enlace | Fuente |
|---|---|---|---|
| Túnez - CERT-TCC (Computer Emergency Response Team - Tunisian Coordination Center) | Experiencias en el Mundo | http://www.ansi.tn/en/about_cert-tcc.htm | Página Web |
| Venezuela CERT.ve (VenCERT - Centro de Respuestas ante Incidentes Telemáticos del Sector Público) | Experiencias en el Mundo | http://www.cert.gov.ve/ | Página Web |
| Comité Interamericano Contra el Terrorismo de la OEA (CICTE) | Experiencias en el Mundo | http://www.cicte.oas.org/Rev/ES/Events/Cyber_Events/CSIRT%20training%20course_Colombia.asp | ENISA - work_programme_2006.pdf |
| CSIRT COLOMBIA | Experiencias en Colombia | http://www.udistrital.edu.co/comunidad/grupos/arquisoft/colcsirt/?q=colcsirt | CSIRT COLOMBIA.doc |
| Developing an Effective Incident Cost Analysis Mechanism | Aspectos Financieros de un CSIRT | http://www.securityfocus.com/infocus/1592 | Developing an Effective Incident Cost Analysis Mechanism.doc |
| Incident Cost Analysis and Modeling Project | Aspectos Financieros de un CSIRT | http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMPReport1.pdf | ICAMPReport1.pdf |
| Incident Cost Analysis and Modeling Project I-CAMP II | Aspectos Financieros de un CSIRT | http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMPReport2.pdf | ICAMPReport2.pdf |
| Defining Incident Management Processes for CSIRTs | Procesos de un CSIRT | http://www.cert.org/ | 04tr015 - Defining Incident Management Processes for CSIRTs.pdf |
| Benchmarking CSIRT work Processes | Procesos de un CSIRT | http://www.hig.no/index.php/content/download/3302/70468/file/Kj%C3%A6rem%20-%20Benchmarking%20CSIRT%20work%20processes.pdf | KjÃ¦rem - Benchmarking CSIRT work processes.pdf |
| How to Design a | Procesos de un | http://www.securityfocus.com | How to Design a |

| Nombre del Documento | Resumen | Enlace | Fuente |
|---|---|---|---|
| Useful Incident Response Policy | CSIRT | /infocus/1467 | Useful Incident Response Policy.doc |
| Effectiveness of Proactive CSIRT Services | Productos y Servicios de un CSIRT | http://www.first.org/conference/2006/papers/kossakowski-klaus-papers.pdf | kossakowski-klaus-papers.pdf |
| Recommended Internet Service Provider Security Services and Procedures | Productos y Servicios de un CSIRT | http://www.ietf.org/rfc/rfc3013.txt | Recommended Internet Service Provider Security Services and Procedures.doc |
| CSIRT Services List | Productos y Servicios de un CSIRT | http://www.cert.org/ | CSIRT-services-list.pdf |
| ENISA - Possible services that a CSIRT can deliver | Productos y Servicios de un CSIRT | http://www.enisa.europa.eu/cert_guide/pages/05_02.htm | ENISA - Possible services that a CSIRT can deliver.doc |
| Organizational Models for Computer Security Incident Response Teams (CSIRTs) | Estructura de un CSIRT | http://www.rediris.es/cert/links/csirt.es.html | 03hb001 - Organizational Models for Computer Security Incident Response Teams (CSIRTs) |
| Organizational Models for Computer Security Incident Response Teams | Estructura de un CSIRT | http://www.sei.cmu.edu/publications/documents/03.reports/03hb001/03hb001chap07.html | Organizational Models for Computer Security Incident Response Teams.doc |
| Staffing Your Computer Security Incident Response Team | Estructura de un CSIRT | http://www.cert.org/ | Staffing Your Computer Security Incident Response Team.doc |
| CERT-FI First 12 months | Modelo de Negocio de un CSIRT | http://www.terena.org/activities/tf-csirt/meeting8/huopio-certfi.pdf | huopio-certfi.pdf |
| A step-by-step approach on how to set up a CSIRT | Modelo de Negocio de un CSIRT | http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_csirt_setting_up_guide.pdf | enisa_csirt_setting_up_guide.pdf |
| Steps for Creating National CSIRTs | Modelo de Negocio de un CSIRT | http://www.cert.org/archive/pdf/NationalCSIRTs.pdf | NationalCSIRTs.pdf |
| Action List for Developing a CSIRT | Modelo de Negocio de un CSIRT | http://www.cert.org/ | Action List for Developing a CSIRT.pdf |
| ENISA - Cómo | Modelo de | http://www.enisa.europa.eu/c | CSIRT_setting_up_gui |

| ore del mento | Resumen | Enlace | Fuente |
|---|---|---|---|
| un CSIRT a paso | Negocio de un CSIRT | ert_guide/downloads/CSIRT _setting_up_guide_ENISA-ES.pdf | de_ENISA-ES.pdf |

## 4.5.- ANÁLISIS DEL ESTADO DE LA SEGURIDAD DE LA INFRAESTRUCTURA INFORMÁTICA DE LOS EUA

En junio del 2009 se dio a conocer el documento llamado "Cyberspace Policy Review", un análisis del estado de la seguridad de la infraestructura informática de los EUA y que fue entregado al Presidente de aquella nación; plantea también el plan de acción a seguir.

Aunque algunos han criticado el documento por ser muy general, se trata de delinear la estrategia a seguir, es la intención presidencial de preocuparse por la seguridad, o como dijo Obama "*our digital infrastructure, the networks and computers we depend on everyday, will be treated as they should be - as a strategic national asset*".

El documento presenta dos cuestiones fundamentales:

a).- La seguridad es prioritaria: se le da a la seguridad de la información el lugar que se merece y es muy importante que un Presidente se dé cuenta de esto, es la alta dirección manifestando su prioritario interés por la infraestructura informática de una nación. No hay nada más reconfortante que saber que los altos mandos entienden la sensibilidad de lo que está en juego, que entienden el valor de la información que se maneja en redes y sistemas. No hay necesidad de convencerlos, ya lo están.

b).- En segundo lugar, se manifiesta una necesidad de invertir en investigaciones académicas orientadas a encontrar nuevas tecnologías y metodologías de seguridad; la gran importancia que tiene el llamado "*research*", aquel que no es una simple recopilación de datos, sino la que es innovadora y propone nuevos temas en el campo de la seguridad.

Los puntos importantes del documento en cuestión:

- Reconoce la importancia de las tecnologías de información en la vida de la nación, empresas e individuos.
- Se reconoce que la infraestructura digital de los EUA no es tan segura.
- Reconocen que ya se tienen pérdidas económicas debido a crímenes en la red y también se establece el hecho de que ya se ha perdido información militar.
- El gobierno de los EUA no está bien organizado para enfrentar estas amenazas.
- Se deben de desarrollar políticas, procesos e integrar personas y tecnologías para mitigar los riesgos.
- Cooperación pública y privada: la infraestructura depende de ambos; no se entiende el apoyo a la seguridad gubernamental sin el apoyo al sector privado; ambos deben de jalar parejo.

- Diálogo nacional para concientizar al público en general sobre estas amenazas.
- Apoyo a la investigación para crear nuevas tecnologías y enfrentar mejor la falta de seguridad en las infraestructuras.

## 4.6.- EN RESUMEN, TIPOS DE CSIRT´s

A modo de resumen de la revisión documental acerca de las iniciativas y experiencias de CSIRT nacionales e internacionales se identifica una tipificación de los CSIRT acorde con sus estructuras, objetivos y funciones.

CSIRTs PÚBLICOS

El carácter público de los CSIRT suelen ser los responsables por la seguridad de la información para las entidades gubernamentales, enfocándose en servir como punto único y de coordinación para el manejo de incidentes de la información relacionados con las infraestructuras críticas nacionales. Así mismo, son responsables por la definición de estándares y buenas prácticas e impulsan la formación y difusión del conocimiento en temas de seguridad de la información. Se identifican dos tipos de estructuras: Unidades públicas independientes o unidades de negocio dependientes de entidades existentes.

- Unidades públicas independientes: Tiene su área de influencia limitada al país y a las entidades públicas, pero cuentan con plena autoridad para impulsar medidas y tomar acciones preventivas a lo largo de los sectores económicos y administrativos. Dentro de los beneficios de contar con un CSIRT dentro de la *estructura del gobierno se pueden considerar* el permitir identificar un punto único *de contacto central, así como la capacidad de tener un equipo capaz de instrumentar y conducir una rápida respuesta para contener un incidente de* seguridad de la información que pueda poner en riesgo la infraestructura crítica nacional.
- *Unidades de negocio dependientes de entidades existentes.* Estas dependencias suelen estar asociadas a las áreas de inteligencia, sector de las comunicaciones, la ciencia y tecnología, directamente vinculadas a gabinetes de gobierno o a las entidades policiales o militares. Suelen tener autoridad compartida con otras instancias para el manejo del incidente informático.

CSIRTs PRIVADOS

- Organismos consultivos sin ánimo de lucro: Despliegan gran parte de sus servicios y actividades a favor de sus miembros inscritos, quienes pagan una suma por la afiliación para el mantenimiento de la estructura del CSIRT. Tiene un papel consultivo y no tiene ninguna autoridad para ordenar o realizar tareas por parte de sus miembros o el área de influencia. Son fuentes generalizadas de buenas prácticas, documentos técnicas compartidos con la comunidad y creación

de estándares de mercado. De igual forma, promueven foros para la creación y difusión de conocimiento técnico.

- Organismo con ánimo de lucro: Identificados como proveedores, el mercado ofrece los servicios de los CSIRT a través de varias alternativas:
  - Centros de Análisis, que se concentran en la agrupación y análisis de datos desde varias fuentes para determinar las tendencias y patrones en la actividad de incidentes.
  - Equipos de Proveedores, que manejen informes de vulnerabilidades en sus productos de software o hardware.
  - Proveedores de Respuesta a Incidentes, que ofrecen servicios de manejo de incidentes para otras organizaciones.

No tienen ningún tipo de autoridad para la mitigación o tratamiento en los incidentes informáticos.

- Iniciativas Académicas: Bajo este esquema universitario, se generan equipos con énfasis en la investigación y el análisis de la seguridad informática. Se elaboran publicaciones, foros y talleres, cursos de capacitación y boletines periódicos.

CSIRTs INTERNOS

Estos equipos sólo responden a las necesidades de las organizaciones privadas a las que pertenecen, imparte instrucciones, políticas y reglas de aplicación. Su principal actividad es la gestión de incidentes en sus propias entidades.

CSIRTs DE COORDINACIÓN

Estas organizaciones coordinan y facilitan el manejo de incidentes de seguridad de la información con el apoyo de todas las entidades relacionadas con el tema a nivel nacional y a través de varios CSIRTs nacionales e internacionales.

ESQUEMA ASOCIATIVO ENTRE EL SECTOR PÚBLICO Y EL PRIVADO

Esta alianza se organiza con el fin de proteger la infraestructura de internet del pais, ante ataques que pongan en juego su seguridad de la información, beneficiándose del patrocinio económico del sector privado.

## 5.1.- EL CICTE

El CICTE se rige en el desempeño de sus responsabilidades y funciones conforme a lo dispuesto por la Carta de la OEA, su Estatuto y su Reglamento, por las decisiones de la Asamblea General y por sus propias decisiones.

En este marco, el CICTE orienta sus labores basándose en las convenciones interamericanas e internacionales sobre la materia, en particular la Convención Interamericana contra el Terrorismo, los principios y objetivos de las declaraciones, resoluciones y planes de trabajo aprobados por el CICTE y en la resolución 1373 (2001) del Consejo de Seguridad de las Naciones Unidas.

## 5.2.- ANTECEDENTES Y SU NATURALEZA JURÍDICA

Los antecedentes del CICTE son:

- Declaración de Principios de la 1° Cumbre de Las Americas celebrada en Miami en 1994, donde se expresa la voluntad de los jefes de Estado y de Gobierno de combatir, en forma conjunta los actos terroristas en el hemisferio, a través de todos los medios legales.
- Conferencia Especializada Interamericana sobre Terrorismo, desarrollada en Lima, Perú del 23 al 26 de abril de 1996 donde se aprobó la Declaración y el Plan de Acción de Lima para prevenir, combatir y eliminar el terrorismo.
- "Medidas para Eliminar el Terrorismo Internacional" adoptada por la Asamblea General de las Naciones Unidas (ONU) el 17 de diciembre de 1996
- Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas, abierto a la firma a partir del 12 de enero de 1998, en la sede de las Naciones Unidas.

EL CICTE fue creado por la Asamblea General de la Organización de Estados Americanos (OEA) que se reunió en la ciudad de Guatemala en Julio de 1999. La decisión de ponerlo en marcha fue el resultado del consenso de todos los representantes de los gobiernos del continente americano para enfrentar el TERRORISMO TRANSNACIONAL.

El Consenso tuvo como resultado la creación de nuevas herramientas que permitieran la cooperación entre las naciones del continente americano.

Desde su origen, el CICTE fue concebido como una red; una amplia coalición de estados nacionales americanos decididos a construir un nuevo tipo de organización capaz de dar las respuestas que el combate contra el TERRORISMO requiere.

Sus misiones fueron definidas en el documento de su fundación. En esos textos se habla claramente de una tarea principal: crear una red continental que

conectara a los elementos de las fuerzas de seguridad de los estados miembros con incumbencia directa en la lucha contra el TERRORISMO.

El COMITÉ INTERAMERICANO CONTRA EL TERRORISMO (CICTE), en su cuarto período ordinario de sesiones, celebrado en Montevideo-Uruguay DEL 18 AL 30 DE Enero 2004, adoptó la declaración de Montevideo (CICTE/DEC. 1/04 rev. 3), en la que se declara su compromiso de IDENTIFICAR Y COMBATIR LAS AMENAZAS TERRORISTAS EMERGENTES, INDEPENDIENTEMENTE DE SU ORIGEN O MOTIVACION, TALES COMO AMENAZAS A LA SEGURIDAD CIBERNÉTICA, ante lo cual se da origen al Programa de Seguridad Cibernética.

El programa de atención del CICTE a la Seguridad Cibernética, tiene como objetivo fortalecer las capacidades de los Estados Miembros para cumplir eficazmente con los requerimientos de la Estrategia Integral Interamericana para combatir amenazas a la seguridad cibernética [AG/RES. 2004 (XXXIV-O/04)]. Apoyar el establecimiento de los EQUIPOS DE RESPUESTA A INCIDENTES DE SEGURIDAD CIBERNETICA (CSIRT) y la creación de una Red Hemisférica de CSIRT's (Ver ANEXO 1). El CICTE coordina actividades con el grupo de trabajo en crímenes cibernéticos de la reunión de Ministros de Justicia de las Américas (REMJA) y el Comité Interamericano de Telecomunicaciones (CITEL) de la OEA.

## 5.3.- LA NATURALEZA, PRINCIPIOS Y PROPÓSITOS

**Artículo 1 del Estatuto del CICTE.** El Comité Interamericano contra el Terrorismo (en adelante, "el CICTE") es una entidad de la Organización de los Estados Americanos (OEA) establecida por la Asamblea General, de acuerdo con el artículo 53 de la Carta de la OEA.
El CICTE tiene como propósito principal promover y desarrollar la cooperación entre los Estados Miembros para prevenir, combatir y eliminar el terrorismo, de acuerdo con los principios de la Carta de la OEA, y con la Convención Interamericana contra el Terrorismo, y con pleno respeto a la soberanía de los países, al estado de derecho y al derecho internacional, incluidos el derecho internacional humanitario, el derecho internacional de los derechos humanos y el derecho internacional de los refugiados.
El CICTE goza de autonomía técnica en el ejercicio de sus funciones, dentro de los límites impuestos por la Carta de la OEA, por su propio Estatuto y su Reglamento, así como por los mandatos adoptados por la Asamblea General.
El CICTE ejerce sus funciones en el marco de la Declaración de Lima para Prevenir, Combatir y Eliminar el Terrorismo (en adelante, "Declaración de Lima"); el Plan de Acción de Lima sobre Cooperación Hemisférica para Prevenir, Combatir y Eliminar el Terrorismo (en adelante, "Plan de Acción de Lima"); el Compromiso de Mar del Plata; y las demás declaraciones adoptadas en el marco del CICTE.

conectara a los elementos de las fuerzas de seguridad de los estados miembros con incumbencia directa en la lucha contra el TERRORISMO.

El COMITÉ INTERAMERICANO CONTRA EL TERRORISMO (CICTE), en su cuarto periodo ordinario de sesiones, celebrado en Montevideo-Uruguay DEL 18 AL 30 DE Enero 2004, adoptó la declaración de Montevideo (CICTE/DEC. 1/04 rev. 3), en la que se declara su compromiso de IDENTIFICAR Y COMBATIR LAS AMENAZAS TERRORISTAS EMERGENTES, INDEPENDIENTEMENTE DE SU ORIGEN O MOTIVACION, TALES COMO AMENAZAS A LA SEGURIDAD CIBERNÉTICA, ante lo cual se da origen al Programa de Seguridad Cibernética.

El programa de atención del CICTE a la Seguridad Cibernética, tiene como objetivo fortalecer las capacidades de los Estados Miembros para cumplir eficazmente con los requerimientos de la Estrategia Integral Interamericana para combatir amenazas a la seguridad cibernética [AG/RES. 2004 (XXXIV-O/04)]. Apoyar el establecimiento de los EQUIPOS DE RESPUESTA A INCIDENTES DE SEGURIDAD CIBERNETICA (CSIRT) y la creación de una Red Hemisférica de CSIRT's (Ver ANEXO 1). El CICTE coordina actividades con el grupo de trabajo en crímenes cibernéticos de la reunión de Ministros de Justicia de las Américas (REMJA) y el Comité Interamericano de Telecomunicaciones (CITEL) de la OEA.

## 5.3.- LA NATURALEZA, PRINCIPIOS Y PROPÓSITOS

**Artículo 1 del Estatuto del CICTE.** El Comité Interamericano contra el Terrorismo (en adelante, "el CICTE") es una entidad de la Organización de los Estados Americanos (OEA) establecida por la Asamblea General, de acuerdo con el artículo 53 de la Carta de la OEA.

El CICTE tiene como propósito principal promover y desarrollar la cooperación entre los Estados Miembros para prevenir, combatir y eliminar el terrorismo, de acuerdo con los principios de la Carta de la OEA, y con la Convención Interamericana contra el Terrorismo, y con pleno respeto a la soberanía de los países, al estado de derecho y al derecho internacional, incluidos el derecho internacional humanitario, el derecho internacional de los derechos humanos y el derecho internacional de los refugiados.

El CICTE goza de autonomía técnica en el ejercicio de sus funciones, dentro de los límites impuestos por la Carta de la OEA, por su propio Estatuto y su Reglamento, así como por los mandatos adoptados por la Asamblea General.

El CICTE ejerce sus funciones en el marco de la Declaración de Lima para Prevenir, Combatir y Eliminar el Terrorismo (en adelante, "Declaración de Lima"); el Plan de Acción de Lima sobre Cooperación Hemisférica para Prevenir, Combatir y Eliminar el Terrorismo (en adelante, "Plan de Acción de Lima"); el Compromiso de Mar del Plata; y las demás declaraciones adoptadas en el marco del CICTE.

## 5.4.- FINES

El CICTE tiene como misión primordial "... la coordinación de los esfuerzos destinados a proteger los ciudadanos de los países miembros del flagelo del terrorismo. Funcionando a través del intercambio de información entre los principales líderes, los peritos en la materia y los encargados de tomar las decisiones trabajan juntos para fortalecer la solidaridad y seguridad hemisféricas".

La Asamblea General de la OEA estableció el CICTE, los objetivos del CICTE comprendidos en el Compromiso de Plata son:

- Mejorar el intercambio de información por las actividades nacionales competentes, incluyendo el establecimiento de una base de datos interamericana sobre cuestiones relacionadas con el terrorismo.
- Formular una propuesta para ayudar a los Estados miembro a formular una legislación a apropiada contra el terrorismo en todos los Estados.
- Recopilar los tratados y acuerdos bilaterales subregionales y multilaterales suscritos por los Estados miembros y promover la adhesión universal a las convenciones internacionales contra el terrorismo.
- Aumentar la cooperación en las fronteras y las medidas de seguridad relacionadas con la documentación de viajes.

## 5.5.- ESTRUCTURA ORGÁNICA

El CICTE consta de seis programas que conforman su estructura orgánica en un mismo nivel de importancia:

1 - CONTROLES FRONTERIZOS
- Seguridad en la Aviación
- Seguridad en Puertos
- Seguridad de Documentos y Prevención de Fraudes
- Inmigración y Aduanas

2 – LEGISLACION CONTRA EL TERRORISMO

3 – EJERCICIO DE SIMULACIÓN CONTRA EL TERRORISMO

4 – FINANCIAMIENTO DEL TERRORISMO

5 – POLÍTICAS DE DESAROLLO Y COORDINACIÓN

6 – PROTECCIÓN DE INFRAESTRUCTURAS
- Turismo e Instalaciones Recreativas
- Seguridad Cibernética

## 5.6.-PROGRAMA DE PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA - ASPECTO DE SEGURIDAD CIBERNÉTICA.

- OBJETIVO DEL PROGRAMA DE SEGURIDAD CIBERNÉTICA

Ayudar en la creación de capacidades en los Estados Miembros para cumplir con eficacia con los requisitos de CSIRT en la Estrategia Comprensiva Interamericana de OEA para combatir amenazas a la Seguridad Cibernética, (AG/RES. 2004 (XXXIV-O/04)). Esto incluye el soporte del establecimiento de CSIRTS nacionales y la creación de una Red Hemisférica.

- ESTRATEGIAS (RECOMENDACIONES DEL CICTE EN CÍBER SEGURIDAD)

  - Establecer CSIRT en cada uno de los Estados Miembros;
  - Fortalecer los CSIRT del hemisferio;
  - Ubicar puntos nacionales de contactos en cada un de los Estados Miembros;
  - Ubicar servicios considerados más esenciales;
  - Detectar y diagnosticar problemas;
  - Establecer protocolos y procedimentos para el intercambio de información;
  - Diseminar rapidamente información sobre ataques en la region;
  - Proveer alertas regionales sobre vulnerabilidades en los sistemas;
  - Proveer alertas regionales sobre actividades sospechosas y desarollar cooperación necesária para analizar y diagnosticar dichas actividades;
  - Proveer información sobre acciones para remediar o mitigar ataques o amenazas;
  - Reducir la duplicación en el análisis, desarollada por cada CSIRT;
  - Fortalecer la cooperación técnica y entrenamiento para establecer CSIRT;
  - Utilizar mecanismos subregionales existentes;
  - Incentivar la cooperación interregional.

## 5.7.- ESTRATEGIA MULTIDIMENSIONAL DE LA OEA EN ASPECTOS DE SEGURIDAD.

De acuerdo al mandato de la OEA respecto a la Protección de Infraestructura Crítica y Ciberseguridad se creó la unidad multidimensional de seguridad cibernética en la cual el Comité Interamericano contra el Terrorismo (CICTE), Comisión Interamericana de Telecomunicaciones (CITEL), y Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de la Américas

## 5.6.-PROGRAMA DE PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA - ASPECTO DE SEGURIDAD CIBERNÉTICA.

- OBJETIVO DEL PROGRAMA DE SEGURIDAD CIBERNÉTICA

Ayudar en la creación de capacidades en los Estados Miembros para cumplir con eficacia con los requisitos de CSIRT en la Estrategia Comprensiva Interamericana de OEA para combatir amenazas a la Seguridad Cibernética, (AG/RES. 2004 (XXXIV-O/04)). Esto incluye el soporte del establecimiento de CSIRTS nacionales y la creación de una Red Hemisférica.

- ESTRATEGIAS (RECOMENDACIONES DEL CICTE EN CÍBER SEGURIDAD)

  - Establecer CSIRT en cada uno de los Estados Miembros;
  - Fortalecer los CSIRT del hemisferio;
  - Ubicar puntos nacionales de contactos en cada un de los Estados Miembros;
  - Ubicar servicios considerados más esenciales;
  - Detectar y diagnosticar problemas;
  - Establecer protocolos y procedimentos para el intercambio de información;
  - Diseminar rapidamente información sobre ataques en la region;
  - Proveer alertas regionales sobre vulnerabilidades en los sistemas;
  - Proveer alertas regionales sobre actividades sospechosas y desarollar cooperación necesária para analizar y diagnosticar dichas actividades;
  - Proveer información sobre acciones para remediar o mitigar ataques o amenazas;
  - Reducir la duplicación en el análisis, desarollada por cada CSIRT;
  - Fortalecer la cooperación técnica y entrenamiento para establecer CSIRT;
  - Utilizar mecanismos subregionales existentes;
  - Incentivar la cooperación interregional.

## 5.7.- ESTRATEGIA MULTIDIMENSIONAL DE LA OEA EN ASPECTOS DE SEGURIDAD.

De acuerdo al mandato de la OEA respecto a la Protección de Infraestructura Critica y Ciberseguridad se creó la unidad multidimensional de seguridad cibernética en la cual el Comité Interamericano contra el Terrorismo (CICTE), Comisión Interamericana de Telecomunicaciones (CITEL), y Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de la Américas

(REMJA) representan cada una un pilar de la estrategia Inter-americana sobre Ciberseguridad.

Los esfuerzos multidisciplinarios de estos cuerpos soportan el crecimiento, desarrollo y protección de Internet y los sistemas de información involucrados así como la protección de los usuarios de estas redes de comunicación.
El objetivo: Crear y brindar soporte a una cultura sobre ciberseguridad.

• Actividades en proceso:

– Coordinación y cooperación entre las Secretarías del CICTE, CITEL Y REMJA y grupos de expertos de diferentes gobiernos en Cybercrimen

– Fortalecimiento de la coordinación entre las autoridades nacionales y entidades, incluidos los CSIRT´s, relacionados en temas de ciberseguridad.


*AG/RES. 2004 (XXXIV-O/04)
ADOPCIÓN DE UNA ESTRATEGIA INTERAMERICANA INTEGRAL DE SEGURIDAD CIBERNÉTICA: UN ENFOQUE MULTIDIMENSIONAL Y MULTIDISCIPLINARIO PARA LA CREACIÓN DE UNA CULTURA DE SEGURIDAD CIBERNÉTICA"

Gráfico 9.- Estrategia Multidimensional de la OEA en temas de Seguridad Cibernética.
Fuente: Sitio oficial del CICTE. Ver www.cicte.oas.org


Gráfico 10. Equipos de respuesta a incidentes de seguridad cibernética CSIRT, auspiciados por el CICTE-
Fuente: Sitio oficial del CICTE. www.cicte.oas.org

# CAPÍTULO VI .- 5 PASOS BÁSICOS PARA LA CREACIÓN DE UN CSIRT

## 6.1.- PASO 1: EDUCACIÓN DE LOS INTERESADOS DIRECTOS SOBRE LA CREACIÓN DE UN EQUIPO NACIONAL

Etapa de concientización en la que los que necesitan participar y promover o "abogar" por la creación y el desarrollo de una capacidad nacional de respuesta a incidentes aprenden lo que se necesita para establecer un CSIRT: las decisiones que deben tomarse, la función que debe desempeñar el CSIRT (por ejemplo, como punto focal nacional para la denuncia y respuesta de incidentes) y las cuestiones claves que deben enfrentarse (administración y personal, desarrollo de comunicaciones confiables y coordinación, procesos efectivos, etc.).
Además de aprovechar la capacitación públicamente disponible sobre cuestiones de creación de un CSIRT, deberán organizarse reuniones y paneles para discutir o plantear cuestiones especificas relacionadas con el establecimiento de un CSIRT nacional y sus beneficios. Estas reuniones y discusiones tendrán, entre otros, los siguientes propósitos:

- entender los motivos comerciales subyacentes a esta necesidad de contar con un equipo nacional (requisitos normativos aplicables, infraestructuras críticas que deben protegerse, tipos de incidentes o ataques que ocurren y que afectan los intereses nacionales, etc.),
- entender lo que se necesita para crear capacidades de respuesta a incidentes en el plano nacional (por ejemplo, identificar los requisitos legales y normativos, determinar el área de cobertura, movilizar y contratar personal para el equipo, definir los recursos e infraestructura necesarios, obtener financiación, crear alianzas, establecer lineamientos y políticas de seguridad),
- identificar a las personas que participarán en las discusiones para crear un equipo nacional, las que participarán en el desarrollo y promoción del CSIRT y las que deberán comprometerse en los procesos de planeamiento e implementación. Estas personas pueden incluir representantes de organismos gubernamentales, infraestructuras críticas, organizaciones de seguridad nacional, organizaciones militares, asociaciones industriales u organizaciones comerciales, CSIRT locales u organizacionales o equipos de seguridad, proveedores de tecnología, proveedores de productos de seguridad, expertos confiables, enlaces políticos o de aplicación de la ley, gerentes comerciales, personal de informática y telecomunicaciones, etc.,
- aprender cuáles son los recursos claves e infraestructuras críticas que existen dentro de la nación,
- identificar los tipos de canales de comunicación que deberán definirse, no solo para la coordinación durante el proceso de desarrollo, sino con posterioridad, para la comunicación entre los participantes del área de cobertura del CSIRT,
- considerar los tipos de misión, metas, objetivos y expectativas de alto nivel que podría establecer un equipo nacional,
- determinar las leyes, regulaciones y otras políticas especificas que afectarán el desarrollo del CSIRT nacional (límites, nivel de autoridad,

protección de la información o cuestiones de cumplimiento que determinarán su funcionamiento),
• investigar e identificar estrategias de financiación que puedan utilizarse para desarrollar, planificar, implementar y operar la capacidad de respuesta,
• discutir los planes de respuesta básicos e interdependencias según se apliquen a una variedad de sectores (gobierno, empresas, finanzas, educación, etc.),
• entender el conjunto potencial de servicios fundamentales que podría brindar un CSIRT a su área de cobertura, revisar e investigar las estrategias que otros países utilizan para crear sus equipos nacionales e identificar prácticas óptimas o lineamientos que puedan aplicarse a este esfuerzo de desarrollo.

## 6.2.- PASO 2: PLANEAMIENTO DEL CSIRT

Aprovechando el conocimiento y la información obtenidos en la etapa 1, el siguiente paso consiste en diseñar y planificar el CSIRT nacional. Las cuestiones revisadas y discutidas durante esta etapa incluirán: articular la necesidad de contar con un equipo y sus posibles beneficios, identificar su área de cobertura, los servicios y el apoyo (o "función") que prestará el CSIRT nacional, y determinar el costo estimado de crear y operar el equipo, un marco temporal para ponerlo en práctica, y las personas que estarán encargadas del progreso del plan hasta la implementación y operación del CSIRT.

## 6.3.- PASO 3: IMPLEMENTACIÓN DEL CSIRT

Durante esta etapa, el equipo utiliza la información obtenida en las dos etapas previas para crear y poner en práctica el CSIRT nacional.

Los pasos básicos son los siguientes:

• obtener los fondos de las fuentes identificadas durante la etapa de planificación (es decir, conseguir que los fondos estén disponibles),
• anunciar públicamente la creación del CSIRT nacional y los lugares en que se puede obtener más información (acerca del equipo, motivos por los que se creó la capacidad, progreso, requisitos de denuncias, etc.),
• formalizar los mecanismos de coordinación y comunicación con grupos de interés y otros contactos adecuados (identificando el proceso para establecer puntos de contacto, requisitos formales de confidencialidad o acuerdos de intercambio de información, estándares de codificación o lineamientos para la difusión de información y procedimientos correspondientes, etc.),
• implementar sistemas de información segura e infraestructuras de redes para operar el CSIRT nacional (por ejemplo, servidores seguros,

aplicaciones, computadoras, equipos de telecomunicaciones y otros recursos de apoyo de infraestructura).

## 6.4.-PASO 4: OPERACIÓN DEL CSIRT

En esta etapa, el CSIRT nacional tiene una capacidad básica de manejo de incidentes y el equipo recibe activamente denuncias de incidentes y coordina respuestas. Es operacional. Las tareas identificadas en las etapas de planeamiento e implementación adquieren forma y sustancia. La visión del CSIRT nacional tiene un marco que define la misión, las metas y los objetivos, la estructura, la autoridad, la financiación, los recursos y la infraestructura para apoyar y sostener al equipo. Se han desarrollado y puesto en práctica políticas y procedimientos, incluidos métodos para desarrollar y mantener relaciones confiables con socios, procesos para establecer canales de comunicación protegidos, planes para coordinar funciones de respuesta y análisis, métodos para desarrollar estrategias de mitigación y difusión de información a las correspondientes áreas de cobertura.
Los grupos de interés clave (CSIRT y expertos confiables) reconocen el equipo y los servicios y el apoyo brindado.

## 6.5.- PASO 5: COLABORACIÓN

A medida que el CSIRT nacional continúa sus operaciones y perfeccionamiento, también madura y desarrolla relaciones confiables con grupos de interés clave, socios y otros CSIRT. Este equipo maduro ha existido por cierto período de tiempo y tiene amplia experiencia en manejo y administración de incidentes. Es un socio confiable en la comunidad global de CSIRT.

# CAPÍTULO VII.- ANÁLISIS CONCLUSIVO

## 7.1.- ANALISIS CONCLUSIVO GENERAL

1.- Se considera que el empleo de los medios electrónicos especialmente en el área de la informática y de las comunicaciones no solamente amenazan el campo militar, sino también los campos psicosocial, económico y político, lo que pone vulnerables a los países del hemisferio a los ataques del ciberterrorismo, por la falta de medios para contrarrestarlos.

2.- La política de defensa en los países del hemisferio, anteriormente no había sido considerada con la responsabilidad que actualmente se está haciendo, lo que no permitía establecer los conceptos de seguridad y defensa nacional, que sirvieran para obtener los argumentos de cara a la obtención de un mejor presupuesto para las carteras de la defensa nacional, actualmente los diferentes Estados han publicando o están en proceso de hacerlo, sus libros blancos de la defensa nacional, para concretar este esfuerzo, lo que fortalece la confianza mutua.

3.- En lo que respecta al desarrollo tecnológico existe una marcada brecha entre los Estados Unidos y Canadá, con el resto del hemisferio, producto de las grandes diferencias en las economías de estos países, la gran mayoría del hemisferio son países en vías de desarrollo, que no tienen dentro de sus prioridades, el desarrollo tecnológico, salvo ligeras excepciones como: Brasil, Chile, Argentina, Colombia y Ecuador, que hacen esfuerzos por superar estas deficiencias.

4.- El hemisferio casi en su totalidad requiere del fortalecimiento del poder u órgano judicial, para poder enfrentar las amenazas emergentes, proporcionando a las Fuerzas Armadas, la Seguridad Pública y los Organismos de Inteligencia de Estado, las leyes que respalden el accionar de las mismas, con su respaldo en la carta magna o leyes auxiliares de los diferentes países que lo componen.

5.- La globalización está incidiendo positivamente cuando se habla de los adelantos tecnológicos, por su aporte a los diferentes esfuerzos de integración y negativamente en lo que se refiere a las nuevas amenazas que utilizan la tecnología, para ejecutar acciones de terrorismo, crimen organizado, narcotráfico y delincuencia común, lo que obliga a las diferentes instituciones de los Estados a coadyuvar esfuerzos regionales para contrarrestar este flagelo.

6.- Actualmente las instituciones no están siendo fortalecidas con la adquisición de tecnología vigente. Por tener presupuestos que en su gran mayoría en un 80 ó 90%, sirven solamente para cubrir el pago de salarios, lo que limita en gran medida las capacidades de contrarrestar las vulnerabilidades, ni adquirir tecnología de punta, por lo que las instituciones deben establecer planes a largo plazo para adquisición de estos medios, como producto de un buen diagnóstico.

7.- La seguridad cibernética no había sido tocada por los países del hemisferio como una amenaza, sin embargo en la Conferencia Especial de Seguridad Hemisférica realizada en México, en octubre de 2003, inició la concepción de un nuevo concepto de seguridad, definiendo el enfoque "multidimensional", que dará un nuevo impulso en la búsqueda de soluciones a ésta vulnerabilidad.

8.- Es necesario reconocer que la Política de Defensa Nacional, es importante para los países que componen el Hemisferio, porque tienen como fundamento los Objetivos Nacionales y los principios estipulados en las respectivas Cartas

## 7.1.- ANALISIS CONCLUSIVO GENERAL

1.- Se considera que el empleo de los medios electrónicos especialmente en el área de la informática y de las comunicaciones no solamente amenazan el campo militar, sino también los campos psicosocial, económico y político, lo que pone vulnerables a los países del hemisferio a los ataques del ciberterrorismo, por la falta de medios para contrarrestarlos.

2.- La política de defensa en los países del hemisferio, anteriormente no había sido considerada con la responsabilidad que actualmente se está haciendo, lo que no permitía establecer los conceptos de seguridad y defensa nacional, que sirvieran para obtener los argumentos de cara a la obtención de un mejor presupuesto para las carteras de la defensa nacional, actualmente los diferentes Estados han publicando o están en proceso de hacerlo, sus libros blancos de la defensa nacional, para concretar este esfuerzo, lo que fortalece la confianza mutua.

3.- En lo que respecta al desarrollo tecnológico existe una marcada brecha entre los Estados Unidos y Canadá, con el resto del hemisferio, producto de las grandes diferencias en las economías de estos países, la gran mayoría del hemisferio son países en vías de desarrollo, que no tienen dentro de sus prioridades, el desarrollo tecnológico, salvo ligeras excepciones como: Brasil, Chile, Argentina, Colombia y Ecuador, que hacen esfuerzos por superar estas deficiencias.

4.- El hemisferio casi en su totalidad requiere del fortalecimiento del poder u órgano judicial, para poder enfrentar las amenazas emergentes, proporcionando a las Fuerzas Armadas, la Seguridad Pública y los Organismos de Inteligencia de Estado, las leyes que respalden el accionar de las mismas, con su respaldo en la carta magna o leyes auxiliares de los diferentes países que lo componen.

5.- La globalización está incidiendo positivamente cuando se habla de los adelantos tecnológicos, por su aporte a los diferentes esfuerzos de integración y negativamente en lo que se refiere a las nuevas amenazas que utilizan la tecnología, para ejecutar acciones de terrorismo, crimen organizado, narcotráfico y delincuencia común, lo que obliga a las diferentes instituciones de los Estados a coadyuvar esfuerzos regionales para contrarrestar este flagelo.

6.- Actualmente las instituciones no están siendo fortalecidas con la adquisición de tecnología vigente. Por tener presupuestos que en su gran mayoría en un 80 ó 90%, sirven solamente para cubrir el pago de salarios, lo que limita en gran medida las capacidades de contrarrestar las vulnerabilidades, ni adquirir tecnología de punta, por lo que las instituciones deben establecer planes a largo plazo para adquisición de estos medios, como producto de un buen diagnóstico.

7.- La seguridad cibernética no había sido tocada por los países del hemisferio como una amenaza, sin embargo en la Conferencia Especial de Seguridad Hemisférica realizada en México, en octubre de 2003, inició la concepción de un nuevo concepto de seguridad, definiendo el enfoque "multidimensional", que dará un nuevo impulso en la búsqueda de soluciones a ésta vulnerabilidad.

8.- Es necesario reconocer que la Política de Defensa Nacional, es importante para los países que componen el Hemisferio, porque tienen como fundamento los Objetivos Nacionales y los principios estipulados en las respectivas Cartas

agnas, lo cual tiene relación con la posición de los Estados en su Política terior, basadas en la búsqueda de la solución pacifica de las controversias.

- Los adelantos tecnológicos en la aérea de la informática están dando pie a que stituyan las tradicionales agresiones militares, por las agresiones cibernéticas, lo al complicará y exacerbará las vulnerabilidades que se deben prevenir y mbatir. Por lo que la inversión en la tecnologia es una necesidad en los paises l Hemisferio.

.- Los pocos paises que están desarrollando proyectos tecnológicos como gentina, Brasil, Colombia, Chile y Ecuador, tienen como agravante la pendencia de otros países para desarrollar su tecnología especialmente en lo e se refiere a recursos humanos y materiales. Por lo que la inversión será ayor tanto por la especialización del personal como por la adquisición de la ateria prima.

.- Los adelantos tecnológicos pueden proporcionar capacidad de disuasión en el emisferio especialmente cuando se tienen recursos para ello, por ejemplo la pacidad de producir hidrocarburos, la capacidad nuclear, la tecnología etalúrgica, la modificación o construcción de medios aéreos o navales, equipos guerra electrónica y la capacidad de producción de munición. Lo que puede pporcionar una ventaja significativa o de igualdad entre los países que lo tengan.

.- Las Bombas Lógicas, los Caballos Troyanos, los Gusanos Electrónicos, los rus, los Hacker y otras herramientas de la guerra de la información son ahora el senal en un nuevo cálculo geopolítico con que los enemigos pueden desafiar a superpotencia que no puede enfrentarse con armas convencionales. Lo que s puede llevar a establecer la premisa de que a mayor tecnología puede existir mayor terrorismo.

.- Los diferentes paises del Hemisferio tienen mucha dependencia de la cnología que proporcionan las transnacionales, en el área de informática y las municaciones, el monopolio es una limitante para que estos Estados puedan sarrollar sus propios sistemas. Lo que puede ser resuelto en parte con los cursos económicos necesarios o con proyectos a largo plazo, enmarcados en ses.

.- La guerra de la información presenta desafios muy grandes para los ganismos de inteligencia de estado, por el gran flujo de información que se tiene por ejemplo de la Internet que sobrepasa la capacidad para procesarla y tener un producto útil en la prevención de actos terroristas. Lo que obliga a tas instituciones a modernizarse e integrarse para disminuir su impacto.

.- Los planes de desarrollo de los países del hemisferio son de suma portancia para poder mejorar la capacidad de desarrollo tecnológico,

.- Se puede determinar cómo las crecientes amenazas a la seguridad y la fensa nacional son originadas principalmente por los medios electrónicos, con pacidad para la obtención de información sin ni siquiera ser percibidos por los ganismos de inteligencia.

.- Las leyes contra los diferentes delitos en muchos países del hemisferio son uy débiles y en muchas ocasiones, lejos de afectar a los delincuentes comunes, rcotraficantes o crimen organizado, los beneficia, por eso es que países como lombia tienen que apoyarse en la extradición en el caso de los narcotraficantes

# BIBLIOGRAFIA

## REFERENCIAS BIBLIOGRAFICAS:


Presentaciones del Taller Hemisférico conjunto de la OEA en el Desarrollo de un Marco Nacional para Seguridad Cibernética 16 al 20 de noviembre de 2009 Río de Janeiro, Brasil.

Presentaciones del Taller Avanzado en Seguridad Cibernética, Fecha: Marzo, 2009, Lugar: San José, Costa Rica.

Presentaciones del Curso subregional de Concientización en Seguridad Cibernética, Creación y Manejo de CSIRTs (Computer Security Incident Response Teams – CSIRT, por sus siglas en inglés) Fecha: del 7 al 11 de abril, 2008, Lugar: Antigua, Guatemala

Panel No 2 de seguridad nacional, políticas de defensa y fuerzas armadas, de la OEA 20 de Mayo de 2002 (www.libroblancoecuador.org/panel2p.pdf).
Publicación Electrónica del USIS, Vol. 3, No. 4, noviembre de 1998, (www.**usis**.com/).
www.washingtonpost.com/wp-dyn/articles/A38110-2003Feb6.html.
Articulo "Estados Unidos teme un ataque Ciberterrorista" 20/09/2002, cibernauta.com/ciberactual/...?articulo=3274.php.
*Creating a Computer Security Incident Response Team: A Process for Getting Started* http://www.cert.org/csirts/Creating-A-CSIRT.html

# ANEXO 1.- PROYECTO DE RESOLUCIÓN. ADOPCIÓN DE UNA ESTRATEGIA INTERAMERICANA INTEGRAL PARA COMBATIR LAS AMENAZAS A LA SEGURIDAD CIBERNÉTICA: UN ENFOQUE MULTIDIMENSIONAL Y MULTIDISCIPLINARIO PARA LA CREACIÓN DE UNA CULTURA DE SEGURIDAD CIBERNÉTICA

CONSEJO PERMANENTE DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

COMISIÓN DE SEGURIDAD HEMISFÉRICA

OEA/Ser.G
CP/CSH-635/04 rev. 2
13 mayo 2004
Original: inglés

**PROYECTO DE RESOLUCIÓN**

**ADOPCIÓN DE UNA ESTRATEGIA INTERAMERICANA INTEGRAL PARA COMBATIR LAS AMENAZAS A LA SEGURIDAD CIBERNÉTICA:**

**UN ENFOQUE MULTIDIMENSIONAL Y MULTIDISCIPLINARIO PARA**

**LA CREACIÓN DE UNA CULTURA DE SEGURIDAD CIBERNÉTICA**

**(Aprobado por la Comisión en su reunión celebrada el día 11 de mayo de 2004)**

LA ASAMBLEA GENERAL,

VISTO el informe anual del Consejo Permanente a la Asamblea General, en particular la sección sobre los temas encomendados a la Comisión de Seguridad Hemisférica, y específicamente las recomendaciones sobre una Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética;

RECORDANDO su resolución AG/RES. 1939 (XXXIII-O/03), "Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética";

TENIENDO PRESENTE que el Comité Interamericano contra el Terrorismo (CICTE), en su cuarto periodo ordinario de sesiones, celebrado en Montevideo, Uruguay, del 28 al 30 de enero de 2004, adoptó la Declaración de Montevideo (CICTE/DEC. 1/04 rev. 3), en la que declara su compromiso de identificar y combatir las amenazas terroristas emergentes, independientemente de sus origen o motivación, tales como las amenazas a la seguridad cibernética;

OBSERVANDO CON SATISFACCIÓN:

Que la Conferencia de la OEA sobre Seguridad Cibernética, celebrada en Buenos Aires, Argentina, del 28 al 29 de julio de 2003, en cumplimiento de la resolución AG/RES. 1939 (XXXIII-O/03), demostró la gravedad de las amenazas en el ámbito de seguridad cibernética a los sistemas de información esenciales, las estructuras de información esenciales y las economías en todo el mundo y subrayó que una acción eficaz para abordar este problema debe contar con cooperación intersectorial y coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales;

Que el CICTE, en su cuarto periodo ordinario de sesiones, celebrado en Montevideo, Uruguay, del 28 al 30 de enero de 2004, consideró el documento "Marco para el establecimiento de unaa Red Interamericana CSIRT de vigilancia y alerta" (CICTE/INF.4/04) y decidió celebrar una reunión de expertos gubernamentales en materia de seguridad cibernética en marzo de 2004 en Ottawa, Canadá, a fin de preparar sus recomendaciones para el proyecto de Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, en cumplimiento de la resolución AG/RES. 1939 (XXXIII-O/03); y

Las recomendaciones formuladas por el CICTE (CICTE/REGVAC/doc.2/04), la CITEL (CPP.I-TEL/doc.427/04 rev. 2) y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMAJ) y su Grupo de Expertos Gubernamentales en Materia de Delito Cibernético (CIBER-III/doc.4/03);

ACOGIENDO CON BENEPLÁCITO el proyecto de Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para crear una cultura de seguridad cibernética, recomendado a la Asamblea General por el Consejo Permanente como un esfuerzo conjunto de los Estados Miembros y sus expertos con los conocimientos técnicos especializados del CICTE, la CITEL y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA (CP/doc.../04);

RECONOCIENDO:

La urgente necesidad de incrementar la seguridad de las redes y sistemas de información comúnmente denominados Internet, a fin de abordar las vulnerabilidades y proteger a los usuarios, la seguridad nacional y las infraestructuras esenciales frente a las graves y perjudiciales amenazas que representan aquellos que podrían llevar a cabo ataques en el espacio cibernético con fines maliciosos o delictivos;

La necesidad de crear una red interamericana de alerta y vigilancia para diseminar rápidamente información sobre seguridad cibernética y responder a crisis, incidentes y amenazas a la seguridad de las computadoras y recuperarse de los mismos;

La necesidad de desarrollar redes y sistemas de Internet dignos de confianza y fiables, mejorando de ese modo la confianza del usuario en dichas redes y sistemas;

REITERANDO la importancia de desarrollar una estrategia global para la protección de la infraestructura de información que adopte un enfoque integral, internacional y multidisciplinario;

CONSIDERANDO:

Las resoluciones 55/63 y 56/121 de la Asamblea General de las Naciones Unidas sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, la resolución 57/239 relativa a la creación de una cultura mundial de seguridad cibernética y la resolución 58/199 sobre la creación de una cultura mundial de seguridad cibernética y la protección de las infraestructuras de información esenciales; y

Que en su XII Reunión, el Comité Directivo Permanente de la Comisión Interamericana de Telecomunicaciones (COM/CITEL), señaló que la "creación de una cultura de ciberseguridad para proteger la infraestructura de las telecomunicaciones aumentando la conciencia entre todos los participantes de las Américas en las redes y sistemas de información relacionados con el riesgo de dichos sistemas y desarrollando las medidas necesarias para hacer frente a los riesgos de seguridad respondiendo rápidamente a los ciber-incidentes" es parte de los mandatos de la CITEL,

RESUELVE:

1. Adoptar el proyecto de Estrategia Interamericana Integral de Seguridad Cibernética que se adjunta.

2. Instar a los Estados Miembros a implementar dicha Estrategia.

3. Instar a los Estados Miembros a establecer o identificar grupos nacionales de "vigilancia y alerta", también conocidos como "Equipos de Respuesta a Incidentes de Seguridad en Computadoras" (CSIRT).

4. Dar renovado énfasis a la importancia de lograr sistemas seguros de información de Internet en todo el Hemisferio

5. Solicitar al Consejo Permanente que, por medio de la Comisión de Seguridad Hemisférica, siga abordando esta cuestión y continúe facilitando las medidas de coordinación para implementar dicha Estrategia, en particular los esfuerzos de los expertos gubernamentales, el Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Expertos en Materia de Delito Cibernético de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA) y otros órganos pertinentes de la OEA.

6. Instar a los Estados Miembros y a los órganos, organismos y entidades de la OEA a que coordinen sus esfuerzos para incrementar la seguridad cibernética.

7. Solicitar a las Secretarías del CICTE y la CITEL y al Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA que asistan a los Estados Miembros, cuando lo soliciten, en la implementación de las respectivas partes de la Estrategia y presenten un informe conjunto al Consejo Permanente, por medio de la Comisión de Seguridad Hemisférica, sobre el cumplimiento de esta resolución, antes del trigésimo quinto período ordinario de sesiones de la Asamblea General.

8. Respaldar la celebración de la segunda Reunión de Practicantes Gubernamentales en Materia de Seguridad Cibernética que convocará el CICTE para el seguimiento oportuno de las recomendaciones sobre el Establecimiento de la Red Interamericana de Alerta y Vigilancia, que figuran en el documento CICTE/REGVAC/doc.2/04 y que forman parte de la Estrategia.

9. Estipular que esa Reunión de Practicantes Gubernamentales en Materia de Seguridad Cibernética se celebre con los recursos asignados en el programa-presupuesto de la Organización y otros recursos, y solicitar que la Secretaría General y la Secretaría del CICTE proporcionen el apoyo administrativo y técnico necesario para esta reunión.

10. Instar a los Estados Miembros a implementar, según corresponda, las recomendaciones de la Reunión Inicial del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA (REMJA-V/doc.5/04) y las recomendaciones relativas a seguridad cibernética de la Quinta Reunión de la REMJA (REMJA-V/doc.7/04 rev. 4) como medio de crear un marco para promulgar leyes que protejan los sistemas de información, impidan el uso de computadoras para facilitar actividades ilícitas y sancionen el delito cibernético.

11. Solicitar al Consejo Permanente que informe a la Asamblea General en su trigésimo quinto período ordinario de sesiones sobre la implementación de esta resolución.

## ANEXO 2.- PROPUESTA DE CREACIÓN DE UN CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD CIBERNÉTICA EN NICARAGUA (CSIRT.Ni)

El equipo para la elaboración de propuesta:

- Sub Comisionado Luis Guevara, PN
- Lic Lucía Herrera , E de N
- Ing. Marco Cárcamo MINREX

### 1.- NATURALEZA

1. El **CSIRT** Nacional se regirá de acuerdo a las Leyes, reglamentos y normativas de Nicaragua , así como normativas internacionales que existen, considerando los acuerdos y resoluciones referidas de la Seguridad Cibernética aprobadas y ratificadas por nuestro país ante la Organización de Estados Americanos de la Región (OEA) así como con otros organismos de carácter regional con los cuales Nicaragua establezca acuerdos de colaboración.
2. El CSIRT Nacional será integrado por diferentes entidades gubernamentales, empresas privadas y entidades educativas. Constituye la organización encargada del manejo de Incidentes de Seguridad Informática (Análisis, repuesta, soporte).

### 2.- VISIÓN

Coordinar los esfuerzos de carácter nacional en materia de Seguridad Cibernética constituyéndose en el punto de enlace de los CSIRT de las entidades del gobierno que poseen infraestructura crítica, empresa Privada, ISP y las entidades Educativas, estableciendo la comunicación en tiempo real, así mismo, contribuir al fortalecimiento jurídico con la promoción de la aprobación de leyes que conduzcan a la prevención del crimen cibernético y mayor seguridad del ciberespacio.

### 3.- MISIÓN

- El Equipo de Repuestas a incidentes de Seguridad Informática (CSIRT.NI) permitirá proveer de los servicios necesarios para manejar e implementar una estrategia de Defensa Nacional, fortalecer las capacidades nacionales en materia de Seguridad Cibernética para garantizar la seguridad de los Sistemas de Información y Comunicación priorizando aquellos que constituyan infraestructura crítica así como objetivos estratégicos del país, reducir los riegos y ser menos vulnerables ante los eventuales problemas de seguridad cibernética y las amenazas emergentes de la misma.

## 4.- SERVICIOS QUE BRINDARÁ EL CSIRT.Ni

Para el CSIRT, la adecuada selección de servicios se convierte en una decisión relevante para su definición, fortalecimiento, sostenimiento y continuidad. A continuación, se presenta una recopilación de los principales tipos de servicios que podría llegar a ofrecer el CSIRT partiendo de la experiencia de otros CSIRT a nivel mundial. De manera general, los posibles servicios se agrupan así:

Tabla 4.- Servicios CSIRT Nacional

| SERVICIOS REACTIVOS | SERVICIOS PROACTIVOS | SERVICIOS PREVENTIVOS |
|---|---|---|
| Alertas y advertencias | Anuncios | Análisis de riesgo |
| Gestión de incidentes | Observación de la tecnología | Planificación de continuidad del negocio y recuperación de desastres |
| Análisis de incidentes | Auditorías o evaluaciones de seguridad | Consultoría de seguridad |
| Respuesta al incidente en el lugar | Configuración y mantenimiento de las herramientas, aplicaciones, infraestructuras y servicios de seguridad | Concientización |
| Soporte de respuesta a incidentes | Desarrollo de herramientas de seguridad | Educación/capacitación |
| Coordinación de respuesta a incidentes | Servicios de Detección de Intrusión | Evaluación y/o Certificación de Productos |
| Gestión de vulnerabilidades | Divulgación de información relacionada con seguridad | |
| Análisis de vulnerabilidades | | |
| Respuesta a vulnerabilidades | | |
| Coordinación de respuesta a vulnerabilidades | | |
| Gestión de "artifacts"[1] | | |
| Análisis de "artifacts" | | |
| Respuesta a "artifacts" | | |
| Coordinación de la respuesta a "artifacts" | | |

Es importante anotar que a pesar que todos los servicios ofrecidos serán responsabilidad y experticia del CSIRT, su labor principal será la de coordinación de todas las acciones y entidades involucradas en el manejo de incidentes de la información a nivel nacional y el desarrollo de estas actividades será objeto de tercerización, buscando el beneficio de las mejores experiencias y conocimientos a nivel nacional e internacional. En este sentido, ejercerá las funciones de coordinador de otros CSIRT nacionales o internacionales, las entidades públicas y privadas involucradas en los incidentes de seguridad de la información, los proveedores de servicios relacionados con la seguridad de la información, los proveedores de hardware y software y la academia. En particular con los entes policivos, su responsabilidad llegará hasta la entrega de los casos y sus insumos correspondientes para su posterior judicialización. A continuación, se detalla cada uno de los servicios que puede brindar con el apoyo de las entidades coordinadas.

## SERVICIOS PREVENTIVOS

Aquellos servicios que proveen asistencia y atención para ayudar a preparar, proteger y asegurar un componente de sistema en anticipación a futuros ataques, problemas o eventos. Llevar a cabo este tipo de servicios reducirá directamente el número de incidentes en el futuro.

- Comunicados: Este servicio busca informar de manera proactiva a sus clientes, nuevas vulnerabilidades o herramientas de intrusión recientemente detectadas. Estos comunicados tales como: alertas de intrusos, advertencias de vulnerabilidad y avisos sobre seguridad, permiten proteger sistemas y redes de nuevos problemas antes de que éstos se presenten.
- Análisis de riesgos: Este servicio busca diagnosticar y evaluar los posibles riesgos sobre los activos críticos relacionados con la información, para mejorar así o determinar las estrategias de protección y respuesta.
- Observatorio de la tecnología: Busca que a través del análisis al entorno de su injerencia, el CSIRT observe y haga seguimiento a nuevos desarrollos técnicos, actividades de intrusos y tendencias en identificación de futuras amenazas. Lo cual podrá incluir las disposiciones jurídicas y legislativas, las amenazas sociales o políticas y las nuevas tecnologías. Todo lo anterior se deberá desarrollar mediante diferentes actividades tales como: lectura de listas de correo de seguridad, sitios web de seguridad y noticias y artículos periodísticos de carácter científico, tecnológico, político y público, con lo cual se logrará una buena retroalimentación en información relacionada con la seguridad de los sistemas y las redes de los clientes. Adicionalmente y con el objeto de obtener y validar la información e interpretación exacta, se deberán buscar alianzas o conexiones con otros CSIRT o partes consideradas autoridades en este ámbito. El producto de este servicio podrá materializarse a través de comunicados, directrices o unas recomendaciones centradas en las cuestiones de seguridad a medio o largo plazo.
- Planificación de la continuidad de los negocios y la recuperación tras un desastre: Teniendo en cuenta que cada vez serán más los incidentes potenciales que provoquen una degradación grave de las operaciones comerciales, se ofrece este servicio que permite aprovechar el conocimiento y experiencia del CSIRT,

para la planificación de la continuidad de negocio y la recuperación tras un desastre en los eventos relacionados con los ataques y las amenazas a la seguridad de la información.

- Evaluaciones de la seguridad: Estudio y evaluación de la infraestructura de seguridad de una organización, basados en los requisitos establecidos por ésta o por otras normas nacionales o internacionales aplicables. Existen varios tipos entre las que se destacan:
- Revisión de las infraestructuras: Con el fin de asegurar las políticas de mejores prácticas y las configuraciones estándar de la organización o de la industria, se revisan manualmente todos los dispositivos informáticos que intervengan o prevengan un incidente informático, entre los que se destacan de manera general el hardware, software, enrutadores, cortafuegos, servidores, etc.
- Revisión de las mejores prácticas: Con el objeto de determinar si las prácticas de seguridad se adaptan a la política establecidas y definida por la organización u otras normas establecidas, se realizaran entrevistas con los empleados y con los administradores del sistema y de la red.
- Escaneo: Uso de detectores de vulnerabilidades o de virus para averiguar qué sistemas y redes son vulnerables.
- Pruebas de penetración: Con esta evaluación o auditoria se busca comprobar la seguridad de un sitio a través de un ataque deliberado a sus sistemas y redes.
- Auditorías de la seguridad: Las auditorias de seguridad pueden ser técnicas, que se centran en los riesgos existentes en los sistemas de información de la organización y en la calidad técnica de las medidas de protección introducidas, y no técnicas o procedimentales, que estudian el cumplimiento efectivo de la Política de Seguridad de la organización y de sus procedimientos.
- Alertas y advertencias: Servicio que difunde información, por medio de la cual se describe el ataque de un intruso, vulnerabilidades de seguridad, alertas de intrusos, virus informáticos o hoaxes[3], etc. Este a su vez recomienda, acciones a corto plazo para la atención o solución a problemas consecuentes.
- Configuración y mantenimiento de herramientas, aplicaciones, infraestructuras y servicios de seguridad: Este servicio, tiene como objeto principal la identificación y orientación para configurar y mantener de un modo seguro las herramientas, las aplicaciones y la infraestructura informática general que usan los clientes atendidos por el CSIRT. El alcance a este servicio será cualquier cuestión o problema que surja con las configuraciones o con el uso de herramientas y aplicaciones que el CSIRT considere podría dejar a un sistema, vulnerable a un ataque. Dentro de este servicio, se podrá actualizar la configuración y realizar el mantenimiento de herramientas y servicios de seguridad, como los sistemas de detección de intrusos, el escaneo de la red o el control de los sistemas, filtros, cortafuegos, redes privadas virtuales (VPN) y mecanismos de autenticación. Incluso se podrá configurar los servidores, los ordenadores personales y portátiles,

---

3 Mensajes de correo electrónico engañosos que se distribuyen en cadena.

los asistentes digitales personales (PDA) y otros dispositivos inalámbricos de acuerdo con las políticas de seguridad, así como encargarse de su propio mantenimiento.

- Desarrollo de herramientas de seguridad: Este servicio ofrece desarrollar herramientas específicas para necesidades particulares o generales de sus clientes o propias del CSIRT. Como por ejemplo, desarrollo de actualizaciones correctivas de seguridad para el software utilizado por el grupo de clientes o la distribución de software protegido que se pueda utilizar para reconstruir ordenadores comprometidos. Así mismo se podrá desarrollar herramientas o secuencias de comandos que amplíen la funcionalidad de las herramientas de seguridad existentes, tales como un nuevo plug-in para una vulnerabilidad o escáner de red, secuencias de comandos que faciliten el uso de la tecnología de encripción o mecanismos de distribución automática de actualizaciones correctivas.
- Difusión de información relacionada con la seguridad: Servicio que proporciona de manera fácil y completa, información útil para mejorar la seguridad. Dicha información puede incluir:
  - Directrices de comunicación e información de contacto del CSIRT
  - Ficheros de alertas, advertencias y otros comunicados
  - Estadísticas y tendencias actuales de los incidentes de seguridad de la información.
  - Recolección, análisis y publicación de estadísticas de seguridad de la información para el país por medio de redes de investigación abiertas.
  - Asesoramiento general sobre seguridad de la información
  - Documentación acerca de las mejores prácticas actuales
  - Políticas, procedimientos y listas de comprobación
  - Desarrollo de actualizaciones correctivas y difusión de información
  - Enlaces con proveedores
  - Otras informaciones que puedan mejorar las prácticas generales de seguridad.

Esta información podrá proceder de fuentes externas tales como otros CSIRT, proveedores, y expertos en seguridad.

## SERVICIOS REACTIVOS

Aquellos servicios que se provocan o se desencadenan por un evento o requerimiento. Este tipo de servicios, son un componente clave para un trabajo de atención de incidentes.

- Tratamiento de incidentes: Servicio que abarca la recepción, evaluación, priorización y respuesta a peticiones y comunicaciones, así mismo al análisis de incidentes y acontecimientos. Las actividades de respuestas pueden ser entre otras las siguientes:
  - Actuaciones para proteger sistemas y redes afectadas o amenazadas por la actividad de intrusos.
  - Aportación de soluciones y estrategias de mitigación a partir de avisos o alertas.

- Reconstrucción de sistemas.
- Filtrado del tráfico de la red.
- Búsqueda de actividad de intrusos en otras partes de la red.
- Corrección o reparación de sistemas.
- Desarrollo de otras estrategias de respuesta o provisionales.

• Análisis de Incidentes: Este servicio busca definir el alcance del daño e incidentes causados, su naturaleza, así como también la estrategia definitiva o temporal de respuesta. Este análisis es un examen general de la información disponible y de las pruebas o instancias relacionadas con un incidente o evento. Existen muchos niveles de análisis de incidentes y numerosos subservicios, que dependen del servicio mismo, objetivos y procesos del CSIRT. A continuación se detallan dos sub servicios.

- Recopilación de pruebas forenses: Acción que incluye la recolección, la conservación, la documentación y análisis de las pruebas procedentes de un sistema informático comprometido, para determinar cambios en el sistema y ayudar a reconstruir los eventos que han desembocado en el compromiso. Las actividades de recopilación de pruebas forenses incluyen, entre otras cosas, la realización de una copia bit a bit del disco duro de los sistemas afectados, la búsqueda de cambios en el sistema, tales como nuevos programas, archivos, servicios y usuarios, el examen de los procesos en ejecución y los puertos abiertos, y la búsqueda de troyanos y juegos de herramientas. Es usual que las personas que tengan a cargo este tipo de responsabilidades, declaren como testigos periciales en actos judiciales.
- Seguimiento o rastreo: Busca rastrear los orígenes de un intruso o identificar sistemas a los que éste haya tenido acceso. Con este servicio además de incluir la identificación del intruso, se podrá en los sistemas afectados y redes relacionadas, incluir el seguimiento al acceso del intruso.

• Coordinación de la respuesta a incidentes: Servicio que busca coordinar tareas de respuesta entre las partes implicadas en el incidente. Dentro de estos se incluye, la víctima del ataque, los sitios relacionados con el ataque y cualquier otro sitio necesario de asistencia para el análisis del ataque. Este se hace extensivo inclusive, aquellas áreas de soporte (IT) de la víctima, tales como proveedores de servicio de internet, administradores de sistema y la red, así como también a otros CSIRT. La recolección de información sobre contactos, la notificación a los sitios de su implicación potencial (como víctimas o como orígenes de un ataque), la recolección de datos estadísticos sobre el número de sitios implicados y tareas dirigidas a facilitar el intercambio y el análisis de la información, así como el reporte del incidente a departamentos internos o externos, serán entre otras las tareas de coordinación que pueden abarcar este servicio. Este no incluye una respuesta a los incidentes directa e in situ.

• Apoyo respuesta a incidentes: Servicio proporcionado a través de orientación remota, para que el personal in situ realice por si mismo las tareas de recuperación. La función del CSIRT será la de orientar y ayudar al grupo víctima del ataque, a recuperarse del incidente, pero lo hará por medios telefónicos, correo electrónico fax o documentación. Dentro del servicio se podrá incluir, entre

otros, la interpretación de los datos recogidos, la entrega de información sobre contactos o la orientación en cuanto a estrategias de mitigación y recuperación.

- Coordinación del Manejo de evidencias: Con fines policivos, se coordina la labor de recopilación y manejo de evidencias en casos de incidentes de la información, con el fin de garantizar el debido proceso en el manejo de evidencias digitales (Servicios Forenses).
- Respuesta a incidentes in situ: Asistencia directa, que busca ayudar a los clientes del grupo atendido a recuperarse de un incidente. El CSIRT se encargara de analizar físicamente los sistemas afectados, repararlos y recuperarlos, en especial en aquellos casos que no exista un equipo local respondiendo al incidente. Para sospecha de incidente, el servicio incluye todas las actividades necesarias para su corrección o mitigación.

## GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Son servicios establecidos y muy conocidos, diseñados para mejorar la seguridad general de una organización. Estos servicios están diseñados para tener en cuenta los comentarios recibidos y las lecciones aprendidas basándose en los conocimientos adquiridos al responder a incidentes, vulnerabilidades y ataques. Lo anterior hace que se oferten productos que permitan a terceros ayudar a mejorar toda la seguridad de una organización, identificar riesgos, amenazas y debilidades del sistema. Son servicios generalmente no técnicos pero preventivos en naturaleza, contribuyendo indirectamente a la reducción en el número de incidentes.

- Consultoría sobre seguridad: Este servicio busca asesorar y orientar, a los grupos de clientes atendidos en las mejores prácticas de seguridad. Por lo cual el CSIRT participará en las recomendaciones o identificación de requisitos de compra, instalación o protección de nuevos sistemas, aplicaciones de software, dispositivos de red entre otros. Así mismo se ofrece asistencia y orientación en la definición de políticas de seguridad.
- Publicaciones: Se busca elaborar y distribuir folletos que expliquen de manera simple, las diferentes amenazas, acciones preventivas y correctivas para el tratamiento de riesgos informáticos. Estas publicaciones podrán tener adjuntos Discos Compactos de libre uso doméstico de herramientas de seguridad y de control parental[4].
- Sensibilización: Buscando que los grupos de clientes atendidos y/o potenciales, desarrollen sus labores cotidianas de manera más segura, así como también de mejorar el grado de entendimiento de las temáticas relacionadas con seguridad, se ofrece un servicio que intenta reducir el número de ataques con éxito y aumentar la probabilidad de que se detecten y comuniquen ataques. Lo anterior, por medio de la sensibilización de incidentes de seguridad de la

---

4 Programas (software) que tienen la capacidad de bloquear, restringir o filtrar el acceso a determinada información ofensiva para los niños o personas susceptibles.

información a través de artículos y desarrollando pósteres, boletines, sitios web u otros recursos informativos que explican las mejores prácticas en seguridad y consejos sobre las precauciones que conviene tomar. Durante este proceso de sensibilización también se incluye reuniones o seminarios de actualización.

- Prensa: Participar en emisiones periódicas en los principales medios nacionales, creando así un posicionamiento del CSIRT.
- Educación / Formación: Este servicio busca capacitar tanto a primer respondiente en las entidades, como a los grupos de clientes atendidos y/o potenciales, entre otros temas en la comunicación de incidentes, métodos de respuesta adecuados, herramientas de respuesta a incidentes, métodos de prevención de incidentes y otras temáticas necesarias para protegerse de incidentes de seguridad de la información, detectarlos, comunicarlos y responder a ellos. El servicio podrá ofrecerse a través de seminarios, talleres, cursos y/o tutoriales. Incluso podrá crearse diplomados especializados en seguridad. Teniendo en cuenta la importancia de la seguridad de la información dentro de cualquier organización, su amplio campo de acción laboral y el incremento a la demanda de personal capacitado, se pueden crear y ofrecer con colaboración de la academia programas de capacitación. Estos servicios se enfocarán y desarrollarán teniendo en cuenta las necesidades propias de cada uno de los sectores públicos y privados, sin embargo este servicio será cobrado únicamente al sector privado.
- Formación Comunitaria: Este servicio podría enfocarse y ofrecerse a la sociedad en general y específicamente a la familia a través de entidades estatales que lo promuevan. El objeto principal será la de explicar de manera didáctica en especial a los niños, los riesgos y reglas básicas de la protección, en diferentes temas que afecten su vida cotidiana. Este servicio busca inculcar a edades tempranas una cultura de protección y mitigación de cualquier tipo de riesgo, incluidos los informáticos. Lo anterior podrá ser ofrecido a través de concursos, historietas, obras de teatro, juegos pedagógicos, etc.
- Centro de interacción multimedia: Línea de atención a nivel de seguridad, que tendrá como función, facilitar la comunicación entre el CSIRT y los clientes a través de cualquier medio interactivo (Ej, internet, chat, teléfono, SMS, etc), permitiendo que estos últimos contacten o sean contactados para solución de problemas e inquietudes de seguridad de la información. Este servicio será fuente de información que podrá materializarse en estadísticas y diseño de nuevos servicios.
- Estandarización de pliegos de seguridad de la información del sector gobierno: Con el objeto de apoyar la contratación pública, y dar un acompañamiento a las interventorías de seguridad de la información, el CSIRT con su experiencia normalizara parámetros que permitan a las entidades del Gobierno, de acuerdo con sus necesidades de seguridad de la información, realizar contrataciones públicas con estándares mínimos exigibles para cada caso.

información a través de artículos y desarrollando pósteres, boletines, sitios web u otros recursos informativos que explican las mejores prácticas en seguridad y consejos sobre las precauciones que conviene tomar. Durante este proceso de sensibilización también se incluye reuniones o seminarios de actualización.

- Prensa: Participar en emisiones periódicas en los principales medios nacionales, creando así un posicionamiento del CSIRT.
- Educación / Formación: Este servicio busca capacitar tanto a primer respondiente en las entidades, como a los grupos de clientes atendidos y/o potenciales, entre otros temas en la comunicación de incidentes, métodos de respuesta adecuados, herramientas de respuesta a incidentes, métodos de prevención de incidentes y otras temáticas necesarias para protegerse de incidentes de seguridad de la información, detectarlos, comunicarlos y responder a ellos. El servicio podrá ofrecerse a través de seminarios, talleres, cursos y/o tutoriales. Incluso podrá crearse diplomados especializados en seguridad. Teniendo en cuenta la importancia de la seguridad de la información dentro de cualquier organización, su amplio campo de acción laboral y el incremento a la demanda de personal capacitado, se pueden crear y ofrecer con colaboración de la academia programas de capacitación. Estos servicios se enfocarán y desarrollarán teniendo en cuenta las necesidades propias de cada uno de los sectores públicos y privados, sin embargo este servicio será cobrado únicamente al sector privado.
- Formación Comunitaria: Este servicio podría enfocarse y ofrecerse a la sociedad en general y específicamente a la familia a través de entidades estatales que lo promuevan. El objeto principal será la de explicar de manera didáctica en especial a los niños, los riesgos y reglas básicas de la protección, en diferentes temas que afecten su vida cotidiana. Este servicio busca inculcar a edades tempranas una cultura de protección y mitigación de cualquier tipo de riesgo, incluidos los informáticos. Lo anterior podrá ser ofrecido a través de concursos, historietas, obras de teatro, juegos pedagógicos, etc.
- Centro de interacción multimedia: Línea de atención a nivel de seguridad, que tendrá como función, facilitar la comunicación entre el CSIRT y los clientes a través de cualquier medio interactivo (Ej, internet, chat, teléfono, SMS, etc), permitiendo que estos últimos contacten o sean contactados para solución de problemas e inquietudes de seguridad de la información. Este servicio será fuente de información que podrá materializarse en estadísticas y diseño de nuevos servicios.
- Estandarización de pliegos de seguridad de la información del sector gobierno: Con el objeto de apoyar la contratación pública, y dar un acompañamiento a las interventorías de seguridad de la información, el CSIRT con su experiencia normalizara parámetros que permitan a las entidades del Gobierno, de acuerdo con sus necesidades de seguridad de la información, realizar contrataciones públicas con estándares mínimos exigibles para cada caso.

## 5.- ESTRUCTURA PROPUESTA PARA EL CSIRT NACIONAL CSIRT.Ni

La Estructura orgánica y funcional del CSIRT.Ni constará de dos niveles principales y un equipo técnico:

**EL PRIMER NIVEL** : Podria estar integrado por delegados de las entidades del gobierno Ministerio de Relaciones Exteriores, Ejército de Nicaragua, Policia Nacional Administrador de Dominios, y delegado de los ISP .

**Funciones que podria realizar:**

- Se constituye en el Punto de enlace Nacional y establece los convenios de cooperación e intercambio con los demás paises miembros de la Organización de Estados Americanos,
- Coordina a las entidades que tiene representación en el CSIRT Nacional, y los CERTs y propone actividades encaminadas al manejo de vulnerabilidades e Incidentes en la comunidad y, proporcionarles estrategias de mitigación y recomendaciones para la recuperación posterior a un incidente.
- Provee de información adecuada para el manejo de incidentes para tales como recomendaciones, alertas, bases de datos de vulnerabilidades, herramientas, etc. o referencias de los mismos.
- Define políticas que contribuyan a la clasificación y manejo de la información confidencial para el trabajo de Inteligencia de Estado.
- Promueve la creación de CSIRT en las entidades educativas y el sector privado a fin de lograr y establecer una Red de colaboradores en el manejo de incidentes, establecer la cooperación colaboración y el intercambio de la información de Inteligencia de Estado
- Propone la Agenda de trabajo y retoma el consenso de todas las partes que garanticen la integración y participación de las diferentes entidades del Gobierno, Empresa Privada, Entidades Educativas y Proveedores de Servicio de Internet,) en el diseño e implementación de una estrategia que proporcione la Seguridad de los Sistemas de Información en nuestro pais con una proyección de Estado, Defensa y Seguridad Nacional.
- Promueve la creación, desarrollo y fortalecimiento de una cultura sobre las mejores prácticas de seguridad a todos los niveles de usuarios, mediante la realización de Foros, Encuentros, seminarios con el apoyo con la participación de de las diferentes universidades estatales y privadas.
- Contribuiria al fortalecimiento jurídico y con ello la prevención del crimen cibernético y mayor seguridad del ciberespacio.

- Preparación y capacitación de de especialistas en la Seguridad de los Sistemas de Información e infraestructura Critica y manejo y administración del CSIRT. Nacional, la seguridad de Sistemas y la aplicación de herramientas Forenses para la determinación de la comisión del Delito.

Para el desempeño de sus funciones este equipo nacional cuenta con un equipo de apoyo formado por un consejo Ampliado y un equipo técnico.

**SEGUNDO NIVEL:**

**Consejo Ampliado** : Está integrado por Especialistas y dotados para la toma de decisión los cuales son delegados como representes de entidades de los CSIRT formado por sectores Gobierno ,Universidades, Seguridad Nacional, proveedores de Servicio de Internet ISP, Entidades públicas y privadas en sus Entidades educativas (Universidades, escuela Técnicas ),

a) Elaborar Plan para Manejo de Incidentes
b) Analizar los incidentes de seguridad y las tendencias actuales que deberán de denunciarse.
c) Establecer los tipos de Servicios que se brindaran en la Comunidad.
d) Establecimientos de los canales de comunicación e intercambio de información y coordinación para difundir en el área de cobertura del CSIRT Nacional (Correo electrónico, sitios Web, Informes publicados y otros mecanismos)
e) Define los principios éticos por los cuales se regirá el el intercambio de la información
f) Elaborar del cronograma de trabajo (Para coordinar los esfuerzos para la instalación del CSIRT).
g) Clasificar la información confidencial, secreta uso de servicio y pública

**Equipo Técnico** : Está integrado por especialista en Administración de Redes , Especialista en Informática Forense, Analistas , especialista en la aplicación de políticas de Seguridad informática, Análisis de riesgos.


## ESTRUCTURA DEL EQUIPO CSIRT- NACIONAL AMPLIADO

Gráfico 11. Estructura propuesta para el CSIRT.Ni

## 6.- PROPUESTA DE TAREAS A REALIZAR

- Sensibilizar sobre la necesidad de atender la Seguridad de los Sistemas de Información y las comunicaciones como una prioridad con carácter de Seguridad Nacional.
- Proponer la institucionalización del CSIRT- Nicaragua
- La presentación a los tomadores de decisión sobre la importancia y necesidad de conformación del CSIRT Nacional.
- Promover la preparación de especialistas en la Seguridad de los Sistemas de Información e infraestructura Crítica y administración de los CSIRT.
- Establecer cooperación con otros CSIRT´s de la región.

## 7.- RETOS FUTUROS

- • Mayor conectividad, ubicuidad, sistemas embebidos y perímetros difusos.
- • El cumplimiento de las regulaciones dictará las actualizaciones y cambios, se incrementará la complejidad de los sistemas.
- • Se espera un incremento de las demandas civiles como consecuencia de ataques y pérdidas de información.
- • El almacenamiento masivo de datos y sus consecuencias legales. (Redes sociales, perfiles en línea, etc.)
- • Actualmente los cibercriminales no están amenazados por una prosecución efectiva. Es necesario crear el clima de seguridad legal conseguido en otros ámbitos criminales

## XO 3. ARTICULO EL NUEVO DIARIO SOBRE HACKEO A SERVIDORES DE UNAN LEON

EL NUEVO DIARIO

Buscar

CON TODO EL PODER DE LA INFORMACION

Managua, Nicaragua - Domingo 24 de Enero de 2010 - Edición 10578



# Hacker "entran" a universidades

Las universidades no han dejado de ser la mira para grupos de hacker locales, lo mismo que sitios politicos y gubernamentales. Esta semana fue hackeado el sistema de registro académico de la UNAN-León

Victor Ayala G.
vayala@elnuevodiario.com.ni

El pasado jueves 21 de enero fue el dia de la entrega de notas para los bachilleres que optan estudiar en la universidad más antigua de Nicaragua y Centroamérica, la UNAN-León. Aprovechando esa fecha, hacker locales vulneraron el sistema y se hizo que todos los estudiantes de nuevo ingreso pasaran con la nota máxima de 105 puntos. ¡De Ripley!
El hecho ocurrió a tempranas horas del jueves, provocando que administradores del sistema de la UNAN sacaran temporalmente el servidor.

Según el grupo de hacker denominado Team Nicatech que se adjudicó este nuevo ataque, mismos que colocaron la bandera de Nicaragua y una foto del Rio San Juan en el portal web de la Presidencia de Costa Rica, "esta acción se hizo para demostrar la gravedad que siguen estando los sistemas habilitados en las universidades del país".

"La confianza en los sistemas automatizados de la UNAN no existe. ¿Cómo es posible que fallen, (es decir) que pueden fallar a la hora de controlar notas, becas y dinero", dijeron.

Informatica

»Hacker "entran" a universidades

»IPv4 casi a su fin casi a su fin

»Fuente Online

»Terremoto de Haiti muestra el poder de Internet

»Retos de 2009 son fuente de optimismo

»Fuente Online

»Las predicciones TIC para el 2010

»Innovaciones tecnologicas en Centroamérica en 2010

»Fuente Online