ESCUELA DE GRADUADOS

Proyecto Final para Optar por el Titulo de:

Maestría en Comercio Electrónico

Título:

Modelo y Estrategia de Prevención de Delitos en el Comercio Electrónico

Sustentado Por:

Nombre:	**Matrícula:**
Licurgo E. Yunes Pérez	**2013-0711**

Asesor (a):

Sanción Raquel Zorob Ávila

Santo Domingo, República Dominicana
Diciembre, 2014

TABLA DE CONTENIDO

ILUSTRACIONES

TABLAS

DEDICATORIA

Le agradezco a Dios por haberme acompañado y guiado a lo largo de la maestría, por haber sido mi fortaleza en todos los momentos y mantenerme firme hasta al final.

Le doy gracias a mi madre Sonaida Mercedes Pérez Lora, por su apoyo de estímulos y por los valores que me inculcó y la educación que tuve, por haberme dado buenos ejemplos de la vida. A mis hermanas por ser parte importante y de apoyo en mi vida. Yanet y Paola Yunes Pérez, y mis sobrinas y sobrinos, especialmente Yanecita, Estefanía y la Tita, por ser parte de unión en el momento que las he necesitado.

Gracias a mis compañeros de clases por haber compartido conmigo durante todo este tiempo nuevos conocimientos profesionales como los fueron el General Claudio Peguero, Victor Angomas, James Pichardo y Silvestre Perez, quienes siempre nos mantuvimos unidos y luchamos contra las adversidades, a mis compañeros de trabajo por el apoyo siempre dado especialmente a Miguel Angel, Elkin, Carlos Leonardo, Federico y Hugo.

Un agradecimiento muy especial a mis maestros Alexander Almonte, Ivelice Zorob, Carlos Contreras hijo, Jesus Martin, por el apoyo, dedicación y guía en las enseñanzas en todo el trayecto.

Por ultimo agradezco a mis hijos y mi esposa por su apoyo y estímulo de ver finalizar mi maestría, por los momentos que no pude compartir con ellos y siempre tuvieron paciencia, con amor y comprensión. A ellos le dedico la inspiración de llegar más lejos cada día para ser ejemplo en sus vidas.

INTRODUCCIÓN

El comercio electrónico es un modelo de negocio que ha venido en constante crecimiento en nuestro país, ya que es constituido por la integración entre la tecnología y el acto de intercambiar productos o servicios entre empresa y consumidores finales. El desarrollo de los medios de comunicación e internet, en los últimos 20 años, ha dado paso a esta modalidad de negocio.

La ley (126-02) sobre comercio electrónico la cual fue promulgada el 4 de septiembre del 2002 ha sido un gran paso en el desarrollo del comercio electrónico en la República Dominicana. Sin embargo, este desarrollo también involucra grandes riesgos potenciales y peligrosos ante los usuarios y las empresas que ofrecen sus servicios mediante esta gran carretera de la información y comunicación.

El principal objetivo de esta investigación es identificar los riesgos latentes y sus diferentes denominaciones de manera tal que nos permita implementar medidas preventivas y correctivas para protección de los usuarios y empresas.

El entendimiento de los sistemas que involucran, es clave para identificar qué mecanismos de seguridad deberán implementarse, las responsabilidades de las partes y mucho más importante cuales de las normativas deben ajustarse, modificarse o crearse.

Para desarrollar este trabajo y alcanzar los objetivos planteados, se han considerado las siguientes tareas científicas:

1. Búsqueda de información para la determinación del marco contextual en fuentes bibliográficas y de Internet relacionadas con el comercio electrónico, historia, orígenes y modalidades.
2. Estudio de la evolución de los delitos de comercio electrónico, en base a la legislación vigente, con énfasis en la Republica Dominicana.
3. Entrevistas a expertos en materia legal y de seguridad de la información en el país.
4. Elaboración en base a los resultados obtenidos, de un modelo y estrategia de prevención de delitos de comercio electrónico en la Republica Dominicana.

El propósito de la investigación, sobre las bases del objetivo general, es que a través de este análisis y recomendaciones, lograr la creación de conciencia general que a su vez se traduzca en confianza ante este novedoso modelo de negocio. La estructura de la investigación está compuesta por tres capítulos que abarcan desde el origen y la historia del comercio electrónico, con el propósito de conocer el contexto del funcionamiento y riesgos existentes en esta modalidad de negocios. Se analiza el funcionamiento del Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología, DICAT, como institución creada para estos fines. Finalmente se plantea el modelo y la estrategia para la prevención de los delitos del comercio electrónico en la Republica Dominicana. “Cuando se trata de seguridad digital no existe defensa impenetrable”. Robert. D. Austin

CAPITULO I.
EL COMERCIO ELECTRÓNICO Y SUS DELITOS

1.1 Conceptualización en el comercio electrónico

El comercio electrónico es también conocido, en el ámbito tecnológico, por sus siglas en inglés como e-Commerce, se define como toda actividad de compra y venta de productos y servicios, tangibles o intangibles a través de internet y el uso de medios electrónicos, con la opción de incluir las actividades de marketing en las de redes sociales. La Organización Mundial del Comercio (OMC), en su rol como entidad para la normalización del comercio electrónico entre países, mediante acuerdos que aseguren la flexibilidad, previsibilidad y libertad posible, la define como: "*la producción, publicidad, venta y distribución de productos a través de las redes de telecomunicaciones*". (OMC, 2014).

Por otra parte, la Ley Modelo sobre Comercio Electrónico, aprobada por la Asamblea General de la ONU en su 29º período de sesiones, de 28 de mayo a 14 de junio de 1996, en Nueva York, establece que el comercio electrónico comprende todas aquellas transacciones comerciales realizadas por medio del intercambio electrónico de datos y por otros medios de comunicación, en los que se usan medios de comunicación y almacenamiento de información sustitutivos de los que usan papel. (Sanca, 2013).

Hay quienes señalan, que la expresión "comercio electrónico" abarcaría todas "aquellas facetas de la actividad económica cuando éstas se inician, se desenvuelven o se concluyen a través de medios de telecomunicación a distancia. Mientras que para otros

autores sería más adecuado utilizar una definición, considerada como más estricta, de comercio electrónico, como "toda forma de comercio en la cual se utilizan las redes de ordenadores como medio de comunicación entre los diferentes agentes implicados. (Sanca, 2013). Por tanto, se puede definir el comercio electrónico como un conjunto de actividades comerciales de bienes tangibles o intangibles, la cuales siempre se producen por vía electrónica, utilizando Internet para interconectar los diferentes agentes implicados. Dada la interconexión entre los distintos tipos de agentes que intervienen en el comercio electrónico; para cada tipo de entorno, se establece un marco de trabajo con un patrón de comportamiento que rige las relacione entre empresas, fabricantes y distribuidores, así como distribuidores y minoritas, hasta llegar a la modalidad final proveedor - cliente.

1.2 Modalidades del comercio Electrónico

Con la expansión del internet, existen varias modalidades principales del comercio electrónico de acuerdo a los agentes involucrados y el objetivo del negocio. Entre ellos: B2B, 2C, C2B, C2C, P2P.

Ilustración 1. Comercio Electrónico y sus distintas modalidades.

El comercio electrónico entre empresas B2B (Business to Business):

Este tipo de comercio electrónico se refiere a la compra y venta de productos o servicios entre empresas. Actualmente esta modalidad es la que genera el mayor volumen de transacciones, debido a que hoy día las empresas demandan altos niveles de interdependencia entre sí, generando una cadena de relaciones comerciales que incluye a fabricantes, distribuidores, mayoristas y minoristas.

Esta modalidad utiliza el modelo EDI (*Electronic Data Interchange*) que se refiere al intercambio electrónico de datos estructurados entre sistemas de información, y es la modalidad que tiene mayor tiempo de establecida.

El comercio electrónico Empresa-Consumidor (Business to Consumer B2C):

Esta modalidad consiste en la compra y venta de productos o de servicios a través de medios electrónicos en tiendas virtuales en Internet, normalmente a través de catálogos con una gran cantidad de galerías de imágenes, procesados en un software de carrito de compras, llegando a expandirse exponencialmente con el desarrollo de la Word Wide Web (WWW), y el uso de los motores de búsquedas.

El comercio electrónico Consumidor-Empresa (Consumer to Business C2B):

Esta modalidad de negocio electrónico se origina por el usuario final o consumidor o grupos de consumidores que utilizan la red para conseguir mejores condiciones de ventas con las empresas. El mayor ejemplo se encuentra en páginas donde usuarios ofrecen casas para alquiler o venta, y las compañías de bienes raíces combaten por dichas ofertas.

El comercio electrónico entre Consumidores (Consumer to Consumer C2C):

Este modalidad de negocio electrónico se caracteriza por transacciones privadas entre consumidores que pueden tener lugar mediante el intercambio de correos electrónicos o el uso de tecnologías de punto a punto o P2P (Peer to Peer), mediante sitios web que ofrecen ofertas especiales, permitiendo a los usuarios realizar pedidos online.

Al analizar las distintas modalidades del comercio electrónico existentes en la actualidad, cabe resaltar que existe un modelo para cada necesidad y las fronteras para realizarlo son casi nulas, siendo el único reto generar la percepción de seguridad y confianza entre el cliente y el proveedor, a través de los medios de pagos electrónicos, y la consiguiente entrega o recepción del bien o servicio solicitado.

Por consiguiente, de toda actividad de comercio electrónico se derivan dos objetivos estratégicos; uno tangible; que es el producto o servicio que se espera recibir a cambio de una remuneración, y otro intangible; que resulta de las experiencias exitosas de compras, que generan compras recurrentes y recomendación del servicio para captar nuevos clientes.

Incursionar en el logro de estos objetivos supone una gran oportunidad de crecimiento para las empresas, pero también acarrea un gran reto para lograr la diferenciación en el servicio y la seguridad desde el punto de vista del cliente.

1.3 Ventajas y Desventajas del Comercio Electrónico para la Empresa y el Cliente

En todo negocio o empresa se tienen ventajas y desventajas, y en el comercio electrónico pasa lo mismo. A continuación se enumeran las ventajas para la empresa y el cliente que se pueden encontrar la siguiente tabla.

Ventajas para la Empresa	Ventajas para el Cliente
Ámbito geográfico ilimitado y potencialización del mercado.	Elección dentro de un mercado global.
Disponibilidad 24/7- 365 días.	Acceso a la información en cualquier momento.
Reducción del personal y costo de inventario, así como del presupuesto en publicidad.	Abaratamiento del precio.
Mejor relación Cliente-Negocio.	Cadena de distribución reducida.
Agilidad en las operaciones.	Pedido de forma inmediata.
Mejor servicio y captura de cliente.	Acceso a más información y mejor servicio pre y pos venta.
Personalización de la oferta.	Personalización de la demanda.

Tabla 1. Ventajas del comercio electrónicos para clientes y empresas.

Desventajas del comercio electrónico

✓ **Privacidad y seguridad**. La mayoría de los usuarios no tienen la suficiente confianza para utilizar su tarjeta de crédito como medio de pago para concretar una compra en los portales web de comercio electrónico. Esto debido a los diversos tipos de ataques e incidentes en los que se han visto envuelta empresas de renombre que han incursionado en este esquema de negocios.

✓ **Desconocimiento de la empresa.** Existe un gran riesgo en el comercio electrónico al no conocer la empresa que vende, ni el país de origen de la misma, y por consguiente la constitución legal de las mismas.

✓ **Seguridad en la Forma de Pago.** Aunque el comercio electrónico avanza de forma acelerada, todavía no hay una transmisión de datos segura ciento por ciento, por esta razón se han desarrollado avances entorno al desarrollo de un medio de pago electrónico, para disminuir las amenazas constantes que existen y resguardar la informaciones bancarias sensibles envueltas en dichas transacciones.

1.4 Origen y tendencias del comercio electrónico en la Republica Dominicana

A finales de la década del siglos XIX empresas comerciales como Montgomery y Sears iniciaron las venta de catálogos de productos por televisión en los Estados Unidos, aún sin la comodidad de un medio de pago electrónico, lo cual propulsó el uso de la tarjeta de créditos, y ya para el 1970 comenzó a ejecutarse el comercio electrónico basado en la trasferencia de fondo monetarios, alcanzando en los 80's una modalidad que utilizaba el teléfono para confirmar los datos.

Hasta el 1995 fue cuando los integrantes del Grupo G7/G8 crearon las iniciativas de un mercado global para PyMEs, con el propósito de acelerar el uso de comercio electrónico a nivel mundial, que incidió en el uso de la Internet en República Dominicana para realizar transacciones comerciales.

En el año 1991, se otorgó la administración del Top Level Domain ".DO" a la Pontificia Universidad Católica Madre y Maestra por las autoridades de la Internet Assigned Numbers Authority (IANA), organización responsable de la coordinación global del Sistema de Nombres de Dominios, el direccionamiento IP y otros recursos de protocolos de Internet.

Para llevar a cabo estas funciones se creó el NIC-DO que es la oficina de Información y registro encargada de la administración del Country Code Top Level Domain .DO, cuya función es proporcionar un servicio de alto nivel en beneficio de la comunidad local y global de Internet.

1.4.1 Inicios del internet y el portal en la Republica Dominicana

La historia del surgimiento de la internet en la República Dominicana, se remonta al año 1995, cuando All America Cables and Radio (AACR), inauguró el primer nodo de internet en tierra dominicana, dando paso al servicio comercial de internet. Destacándose también la participación de Tricom, primera empresa en instalar un nodo de Internet local para ofrecer el servicio dial-up. Varios meses después el sistema de conexión a internet ya contaba con más de 100 usuarios y con un enlace internacional con Puerto Rico, a una velocidad de 64Kbps, logrando que nuestro país iniciara conexión con todo el mundo. Esto dio paso a que empresas proveedoras de servicios telefónicos como: Viva (Centennial y AACR), Orange, CODETEL (Verizon y Claro), Tricom, iniciaran una gran competencia soportadas con campañas de marketing ofreciendo el mejor el mejor servicio de conexión a internet, lo que permitió que nuestro país se convirtiera en unos de los mejores comunicados en esa época.

El avance en las telecomunicaciones y el acceso a internet abrió un abanico de oportunidades para las Pymes, que estalló en una creciente explotación del Internet, básicamente en el uso del correo electrónico y el registro de dominios .com.do para publicitar empresas y captar nuevos clientes de forma más eficiente.

El primer portal que realizó comercio electrónico en la Republica Dominicana fue la EAN internacional, la cual publicó su página en julio del 1995 orientada en el comercio B2B, después de haber sido fundada en el 1977 como una asociación sin fines de lucros, con el objetivo desarrollar una cadena de logística para la administración de los abastecimientos en el ámbito global.

Ilustración 2. Página web http://www.eanrd.org.do en el 2004 (Archive.org, 2006)

En el 2005 EAN International se fusionó con la empresa Americana UCC (Uniform Code Council) y pasó a ser GS1 (Global Standard, Global Solution, Global System), con presencia en más de 100 países. (GS1 Dominicana, 2010)

Ilustración 3. Estado actual de la página web www.GS1rd.org.do (GS1 Dominicana, 2014)

Luego de la primera página web en julio del 1995, las grandes instituciones y empresa comenzaron a registrar sus portales, según se observa a continuación:

Nombre de Dominio	Tipo	Fecha Registro
PRESIDENCIA.GOV.DO	Gubernamental	1/9/1995
BANCENTRAL.GOV.DO	Gubernamental	1/9/1995
JCE.ORG.DO	Gubernamental	1/9/1995
PROCOMUNIDAD.ORG.DO	Gubernamental	1/9/1995
CODETEL.COM.DO	B2C	16/9/1995
GRUPOM.COM.DO	B2C	16/9/1995
BHD.COM.DO	B2C	16/9/1995
BPD.COM.DO	B2C	16/9/1995
BRUGAL.COM.DO	B2C	16/9/1995
CCAMPO.COM.DO	B2C	16/9/1995
CDNRADIO.COM.DO	Informativa	16/9/1995
FERSAN.COM.DO	B2C	16/9/1995
LISTIN.COM.DO	Informativa	16/9/1995
SISTEC.COM.DO	B2B	16/9/1995
SID.COM.DO	B2C	16/9/1995
TRICOM.COM.DO	B2C	16/9/1995
VESUVIO.COM.DO	B2C	16/9/1995
UNIBE.EDU.DO	Educativa	16/9/1995
CENAPEC.EDU.DO	Educativa	16/9/1995
INTEC.EDU.DO	Educativa	16/9/1995
VINICOLA.COM.DO	B2C	16/9/1995

Tabla 2. Primeras páginas web creadas en el NIC.DO, en el 1995. (Collado Vilorio, 2014)

1.5 Evolución del Comercio Electrónico en la República Dominicana

Durante el período 2007 - 2011 el registro de dominios .do creció 74.38% en solo 5 años, lo que produjo un aumento en cuanto al uso del comercio electrónico en la Republica Dominicana. Teniendo en cuenta que el departamento Nic.do fue creado en el año 1991 y los proveedores de servicios de internet llegaron en el año 1995.

Dominio	**2007**	**2008**	**2009**	**2010**	**2011**
com.do	7,946	8,005	8,644	10,030	9,820
net.do	639	574	469	485	485
org.do	641	598	596	663	645
web.do	169	153	132	130	128
edu.do	240	237	258	294	294
art.do	154	152	116	109	109
gov.do	382	398	381	424	430
gob.do	119	171	211	286	293
mil.do	31	23	24	31	30
sld.do	17	20	21	22	22
.do	0	0	0	5,733	5,771
Total	**10,338**	**10,331**	**10,852**	**18,207**	**18,027**

Tabla 3. Estadística de los dominios creados entre los años 2007 al 2011 en NIC.DO (PUCMM, 2014)

Actualmente el 53% de los dominios asignado por el Nic.do son de (.com.do), seguido del (.do) con un 35%.

Dominio	Tipo	Cantidad	%
.com.do	Comerciales	11,822	53%
.do	Regional	7,715	35%
.org.do	Sin fines de lucro	671	3%
.gob.do	Gubernamentales	506	2%
.net.do	Proveedores de servicios	420	2%
.edu.do	Educación	416	2%
.gov.do	Gubernamentales	370	2%
.web.do	Servicios web	90	0%
.art.do	Artes	68	0%
.mil.do	Militares	49	0%
.sid.do	Salud	15	0%
	Total	22,142	100%

Tabla 4. Estadísticas de los dominios activos en NIC.DO a la fecha 30/11/2014. (Collado Vilorio, 2014)

Ranking de los portales web con más visitas desde la Republica Dominicana según la encuestadora Alexa.

Rank	Página Web	Tipo
1	Facebook.com	Social
2	Google.com.do	Buscador
3	Youtube.com	Entretenimiento
4	Google.com	Buscador
5	Amazon.com	B2C
6	Live.com	Correo
7	Yahoo.com	Buscador
8	Wikipedia.org	Enciclopedia
9	Ebay.com	B2C
10	Blogspot.com	Informativo
11	Adcash.com	B2C
12	Twitter.com	Social
13	Ask.com	Informativa
14	Alibaba.com	B2C
15	Msn.com	Comerciar
16	Bpd.com.do	B2C
17	Listindiario.com	Informativo
18	Instagram.com	Social
19	Xvideos.com	Entretenimiento
20	Corotos.com.do	B2C
21	Diariolibre.com	Informativo
22	Gob.do	Gubernamental
23	Aliexpress.com	B2C
24	Google.es	Buscador
25	Vodoumedia.com	Software
26	Bhdleon.com.do	B2B
27	Noticiassin.com	Informativo
28	Taringa.net	Entretenimiento
29	Wordpress.com	Entretenimiento
30	Onclickads.net	B2C
31	Remolacha.net	Informativa

32	Elcaribe.com.do	Informativa
33	Paypal.com	B2C
34	Hoy.com.do	Informativa
35	Ilividnewtab.com	Informativa
36	Go.com	Entretenimiento
37	Badoo.com	Social
38	Slideshare.net	Educativa
39	Banreservas.com.do	B2C
40	Acento.com.do	Informativo
41	Espn.go.com	Deportiva
42	Youradexchange.com	Software
43	Adf.ly	Software
44	Super-carros.com	C2C
45	Microsoft.com	Software
46	Entertainment-factory.com	Entretenimiento
47	Lapulga.com.do	C2C
48	Uasd.edu.do	Educativa
49	Xnxx.com	Sexual
50	Emarket.do	C2C
51	Playerme.org	Entretenimiento
52	Outbrain.com	B2C
53	Linkedin.com	Social
54	Rt.com	Informativa
55	Softonic.com	Software
56	Netflix.com	B2C
57	Usagc.org	Educativa
58	Imdb.com	Entretenimiento
59	Alofokemusic.net	Entretenimiento
60	Pinterest.com	Social
61	Blogger.com	Entretenimiento
62	Apple.com	B2C
63	Elnacional.com.do	Informativa
64	Elnuevodiario.com.do	Informativa
65	Uapa.edu.do	Educativa
66	Mercadolibre.com.do	C2C

67	Monografias.com	Informativa
68	Claro.com.do	B2C
69	Wordreference.com	Educativa
70	Lidom.com	Deportiva
71	Iminent.com	Software
72	Dgii.gov.do	A2C
73	Eldia.com.do	Informativa
74	Cnn.com	Informativa
75	Yaske.to	Entretenimiento

Tabla 5. Las 75 Páginas de internet más visitadas desde Rep. Dom. (Alexa Internet, Inc, 2014)

El cuadro anterior nos permite identificar que los portales web de comercio electrónico internacional más visitados desde la Republica Dominicana son: **Amazon y Ebay.**

También se puede apreciar que los principales 10 portales web de comercio electrónico de dominios locales y/o presencia local, más visitados desde la Republica Dominicana son:

1	**Bpd.com.do (Banco Popular)**
2	Coroto.com.do
3	Bhdleon.com.do (Banco Leon)
4	Banreservas.com.do
5	Super-carros.com
6	Lapulga.com.do
7	Emarket.do
8	Mercadolibre.com.do
9	Claro.com.do
10	Dgii.gov.do

Tabla 6. Las 10 páginas dominicanas más visitadas desde Rep. Dom. (Alexa Internet, Inc, 2014)

1.6 Evolución de los delitos en el comercio electrónico en República Dominicana

Después que la República Dominicana quedó interconectada a través del internet en el año 1995, sus usuarios eliminaron las fronteras de la comunicación, trayendo como consecuencia que se transformara el comercio en todos los sentidos, haciéndolo más accesible a todos los ciudadanos por medio de un clic, pero con ello también se abrió un abanico de oportunidades para los usuarios locales y extranjeros con más experiencia, que explotaban las vulnerabilidades inherentes de las primeras implementaciones de los servicios web, y en el transcurso del tiempo generó una subcultura de cibernautas que transformaron el delito tradicional de un patrón físico a uno virtual.

Al observar el crecimiento del delito informático durante el período 2005 al 2006, según las estadísticas locales de las investigaciones realizadas por los organismos competentes, entiéndase: Policía Nacional, DNI, DNCD, entre otras, donde se reflejaba la carencia de una ley que las soportara y no dejara impune los actores de dichos delitos, por la falta de legislación oportuna que los sancionara, en fecha 23 de abril del 2007, que se promulgó la ley 53-07 sobre crímenes y delitos de alta tecnología, con la cual se comenzó a tener una estadística según la tipificación del caso, como se muestra en la siguiente gráfica:

ESTADISTICA DE LOS CASOS RESUELTOS 2005-2006 (DICAT)			
TIPOS DE DELITOS	**TOTAL 2005**	**TOTAL 2006**	**TOTAL GENERAL**
DIFAMACION Y BLOQUEO DE PAGINA WEB	2	0	2
HACKING	1	0	1
FRAUDES ELECTRONICOS A BANCAS DE LOTERIA	12	1	13
FRAUDES ELECTRONICOS A EMPRESAS	0	1	1
TERMINACION DE LLAMADAS ILEGAL	0	1	1
ACCESO ILICITO Y SABOTAJE	0	1	1
PEDOFILIA	0	1	1
TOTAL DE CASOS	15	5	20
ANALISIS REALIZADOS	**TOTAL 2005**		
ANALISIS A IMAGEN DE VIDEO	1		
EXPERTICIA A CPU	2		
EXPERTICIA A LAPTOP	1		
RASTREO DE DIRECCION DE E-MAIL	1		
EXPERTICIA A DISCO DURO DE CPU	1		
TOTAL DE CASOS	6		

Tabla 7. Estadísticas de casos resueltos por el DICAT, antes de la promulgación de la ley (DICAT, 2006)

Observando el presente cuadro estadístico, podemos apreciar que un 65% de los casos reportados, eran casos que había afectado al sector de ventas de jugadas de lotería en bancas de apuestas, y los mismos consistían en atrasar el reloj de la computadora con la intención de jugar un ticket ganador con los números del sorteo del día en que se efectuó el delito, es evidente que ciertamente no se reportaron muchos casos a la Policía Nacional, para ser investigados en esta materia, por las siguientes razones.

- ✓ La ciudadanía no estaba enterada que había un departamento que tenía la capacidad para investigar esos casos.
- ✓ El acceso al internet en ese período de fecha 2005-2006, era muy pobre.
- ✓ No existía una ley que tipificara los delitos de alta tecnología.

Perfil Corporativo del Departamento de Investigaciones y Crímenes y Delitos de Alta Tecnología, DICAT

El DICAT se crea en noviembre de 2004 motivado por el incremento de los delitos electrónicos tanto a nivel mundial como nacional, así como también para facilitar que las fuerzas del orden estén preparadas acorde a las nuevas formas y métodos de los delitos.

De igual manera fomentar una integración de las fuerzas del orden con los esquemas internacionales en materia de ciberdelincuencia.

Misión del DICAT

Coordinar y realizar investigaciones relacionadas con la criminalidad de las nuevas tecnologías y las comunicaciones, así como apoyar a los demás departamentos investigativos en la recuperación y análisis de evidencia digital en casos de crímenes y delitos tradicionales.

Funciones:

- Investigar todas las denuncias de crímenes o delitos considerados de alta tecnología.
- Responder con capacidad investigativa a las amenazas y ataques a la infraestructura nacional.
- Desarrollar análisis estratégicos de amenazas informáticas.
- Desarrollar inteligencia en internet.

Estructura:

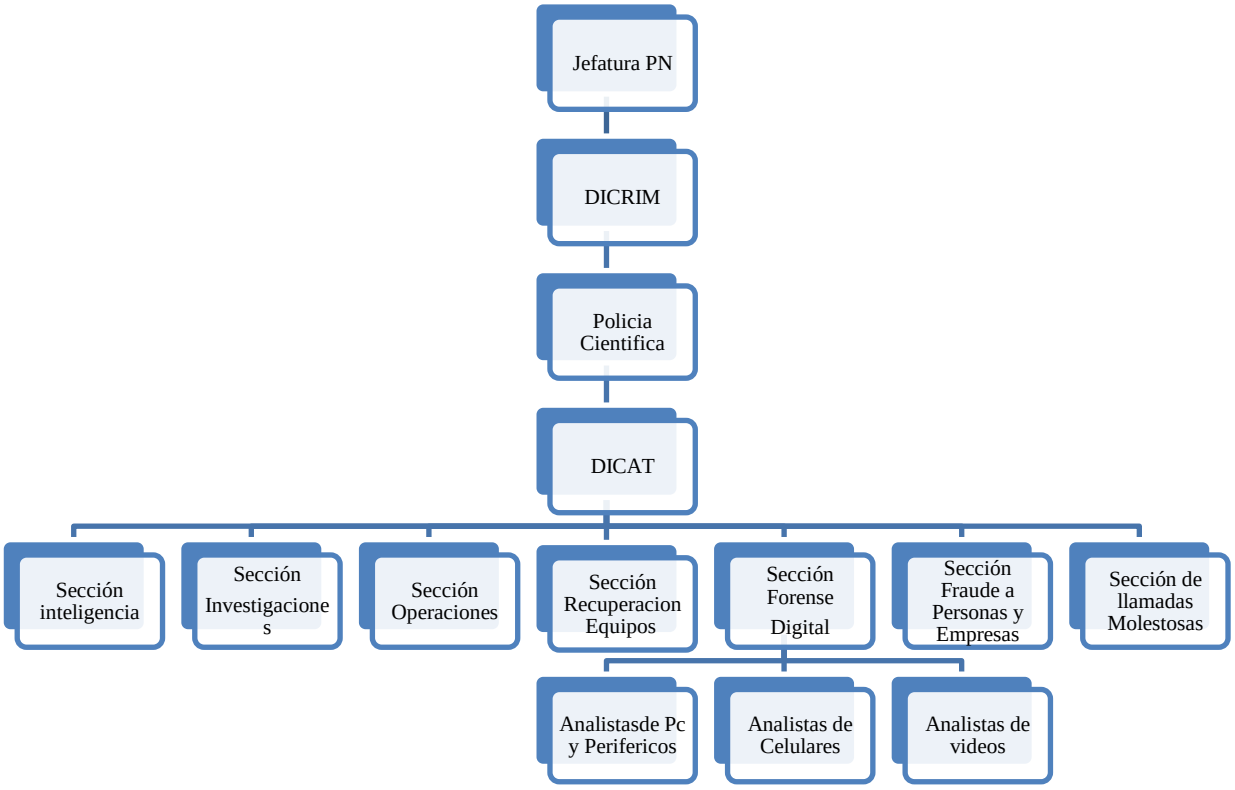

Ilustración 4. Estructura del Departamento

Marco regulatorio de los crímenes y delitos tipificados en la Ley 53-07

En fecha 23 de abril del 2007, fue promulgada la Ley 53-07, producto de que los crímenes y delitos relacionados a las tecnologías de la información y comunicación no estaban previstos en la legislación penal dominicana, por lo que los autores de tales acciones no podían ser sancionados sin la creación de una legislación previa, y en consecuencia, resultaba necesario su tipificación, y la adopción de mecanismos suficientes para su lucha efectiva, facilitando la cooperación entre el Estado y el sector privado para la detección, investigación y sanción a nivel nacional de estos nuevos tipos de delitos y más que las tecnologías de la información y de la comunicación han

experimentado un desarrollo impresionante, con lo que se brindan un nuevo soporte para la comisión de delitos tradicionales y crean nuevas modalidades de infracciones y hechos no incriminados, los cuales afecta a los intereses patrimoniales y extra patrimoniales de las personas físicas y morales, así como del Estado y las instituciones que lo representan.

De esta manera la ley está organizada por dos grandes títulos y a su vez en varias secciones y artículos con sus definiciones, literales y numerales, de manera clara, llana y moderna, ya que fue creada por una comisión compuesta por expertos del INDOTEL, Ministerio Publico, Sector Privado y de la Policía Nacional, esta última por ser la pionera en esta materia estando al frente en ese entonces el Coronel de la Policía Nacional, Ing. Claudio Peguero Castillo, hoy General de Brigada, quien llevó la voz cantante en este sentido tanto nacional como internacional, logrando posteriormente que dicha ley fuera homologada con el Convenio de Europa y nuestro país hoy día sea signatario de dicho convenio.

La ley en su artículo primero, especifica que tiene como misión, la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos.

En su artículo segundo, especifica que se aplicará en todo el territorio de la República Dominicana, a toda persona física o moral, nacional o extranjera, que cometa un hecho sancionado por sus disposiciones, en cualquiera de las siguientes circunstancias:

A. Cuando el sujeto activo origina u ordena la acción delictiva dentro del territorio nacional;

B. Cuando el sujeto activo origina u ordena la acción delictiva desde el extranjero, produciendo efectos en el territorio dominicano;

C. Cuando el origen o los efectos de la acción se produzcan en el extranjero, utilizando medios que se encuentran en el territorio nacional; y finalmente,

D. Cuando se caracterice cualquier tipo de complicidad desde el territorio dominicano.

En su artículo tercero, especifica sus principios generales de aplicación los cuales se describen a continuación:

A. Principio de Territorialidad. Esta ley penal se aplicará a las infracciones cometidas en el territorio de la República Dominicana. Sin embargo, la infracción se reputará cometida en el territorio nacional desde que alguno delos crímenes o delitos previstos en la presente ley, se cometa fuera del territorio de la República en las condiciones expresadas en los literales b) y c) del Artículo 2, quedando el sujeto activo, en caso de que no haya sido juzgado mediante sentencia definitiva por el mismo hecho o evadido la persecución penal en tribunales extranjeros, a la disposición de la jurisdicción nacional.

B. **Principio de Razonabilidad y Proporcionalidad**. Las restricciones y prohibiciones deben ser proporcionales a los fines y medios del peligro que se intenta evitar, ponderándose con prudencia las consecuencias sociales de la decisión. Al aplicar las penalidades impuestas por la presente ley, el juez competente deberá considerar la gravedad del hecho cometido y tomar en cuenta que las penas deben tener un efecto social y regenerador, no sólo para el individuo al que se le aplica sino también para la sociedad en su conjunto.

Posteriormente en la segunda sección se describen los artículos con sus definiciones, multas y sanciones, lo que agrupamos en la tabla siguiente.

Ley 53-07					
Articulo	Descripcion	Actual Pena Minima	Pena Maxima	Multa Minima	Multa Maxima
5	Codigos de Acceso	1	3	20	100
Parrafo	Clonacion Dispositivos	1	10	2	500
6	Acceso Ilicito	3m	1	1	200
Parrafo I	Uso de Datos por Acceso Ilicito	1	3	2	400
Parrafo II	Explotacion Ilegitima Acceso Inint	1	3	2	400
7	Acceso Ilicito para Servicios a Terceros	3m	1	3	500
Parrafo	Beneficio de Actividades de un Tercero	3m	6m	2	200
8	Dispositivos Fraudulentos	1	3	20	100
9	Interceptacion de Datos y Señales	1	3	20	100
10	Daño o Alteracion de Datos	3m	1	3	500
Parrafo		1	3	6	500
11	Sabotaje	3m	2	3	500
12	Atentado Contra la Vida de la Persona				
13	Robo Mediante Utilizacion de Alta Tec	2	5	20	500
14	Obtencion Ilicita de Fondos	3	10	100	500
Parrafo	Transferencia Electronica de Fondos	1	5	2	500
15	Estafa	3m	7	10	500
16	Chantaje	1	5	10	200
17	Robo de Identidad	3m	7	2	200
18	De la Falsedad de Documentos y Firmas	1	3	50	200
19	Uso de Equipos para Invasion de Privacidad	6m	2	5	500
20	Comercio Ilicito de Bienes y Servicios	3m	5	5	500
Parrafo	Trafico de Personas o de Drogas				
21	Difamacion	3m	1	5	500
22	Injuria Publica	3m	1	5	500
23	Atentado Sexual	3	10	5	200
24	Pornografia Infantil	2	4	10	500
Parrafo	Adquisicion y Posesion	3m	1	2	200
25	Delitos Propiedad Intelectual y Afines				
26	Delitos de Telecomunicaciones	3m	10	5	200
27	Crimenes y Delitos contra la Nacion	15	30	300	2,000
28	Actos de Terrorismo	20	30	200	1,000

Tabla 8. Extracto de las penas aplicadas a la violación a la ley 53-07.

Aspectos Metodológicos de la Investigación de Delitos.

Sin discusión posible, en la actualidad hay que tener en cuenta que existen los delitos informáticos. Todo parte desde el momento en que se realiza una acción que reúna las características que delimitan el concepto de delito y sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea de hardware o de software. Para ello se ha de tener en cuenta que en el ordenamiento penal dominicano se considera el delito como la acción u omisión típica, antijurídica y culpable, es decir, la conducta prohibida por ley bajo la conminación de una sanción penal preexistente al hecho que la motiva.

Para realización de este análisis, debemos conocer algunos conceptos relevantes, como son la descripción del delito y su tipificación como tal, la incorporación de los diferentes departamentos que interactúan para su evaluación, acción inmediata de los peritos forenses que determinen la magnitud de los mismos, acciones inmediatas que sean regidas por la ley y como se tramitan estos procesos para poder llegar hasta las últimas consecuencias. (Chiovenda, 1940).

Etapas del Proceso

Como en cada proceso de investigación, nuestro proyecto comienza con la identificación de los conceptos que intervienen o se asocian a esta ley. Iniciando con el conocimiento y problemática que dieron origen a dicha ley, la cual pretende adecuar la actual legislación dominicana a la par, con los avances de la tecnología y su uso como instrumentos para la ejecución de penas de estos crímenes.

Entre los puntos más sobresalientes de la ley están la protección integral de los sistemas que utilicen tecnologías de información y su contenido, así como la persecución de los delitos mediante dicha intervención tecnológica. Además, tipificará los crímenes contra la confidencialidad, integridad, disponibilidad de daños y sistema de información. La Ley también contempla el uso de la tecnología asociada a otros crímenes como homicidio, robo, estafa, acceso ilícito, chantaje, falsedad, difamación e injuria, ciber-terrorismo, entre otros. (El Nuevo Diario, 2007)

La Cámara Alta también sancionó en segunda lectura el proyecto de Ley que modifica los artículos 79 de la ley general de Telecomunicaciones y 141 del Código

Tributario, en cuanto a la competencia jurisdiccional para conocer y dirimir los recursos de apelación que sean interpuestos contra las decisiones emanadas de los cuerpos colegiados y homologadas por el órgano regulador previsto en la referida ley de telecomunicaciones, a cargo actualmente de la Suprema Corte de Justicia.

Esta iniciativa fue sometida el 2 de marzo del año en curso por la Suprema Corte y estudiada por la Comisión de Justicia y Derechos Humanos. (Manzueta Espaillat, 2007)

El Instituto Dominicano de las Telecomunicaciones (INDOTEL) entregó al presidente de la Cámara de Diputados, Alfredo Pacheco un anteproyecto de ley sobre Crímenes y Delitos de Alta Tecnología, que contempla drásticas sanciones contra la pornografía infantil, la interceptación e intervención de señales o datos, la estafa, la difamación, la injuria, el robo, la trata de personas y violaciones contra la propiedad intelectual, cuando estos sean cometidos a través de sistemas electrónicos, informáticos, telemáticos y de telecomunicaciones. (Núñez Campusano, 2012)

Diversidad de Delitos

La diversidad de los hechos delictivos de alta tecnología se consideran incluidos en dicha propuesta los denominados delitos electrónicos, informáticos, cibernéticos, telemáticos y de telecomunicaciones. El doctor Rafael Vargas en la reunión que sostuvo con el Señor Alfredo Pacheco, presidente de la Cámara Baja, le solicitó que se eliminará del proyecto de Código Penal los artículos que tratan sobre los delitos electrónicos a los fines de que se deje a una legislación especial por ser una materia tan especializada.

En la entrega del anteproyecto de ley participaron representantes del INDOTEL, de la OPTIC y del sector privado que interviene en el negocio de las telecomunicaciones.

La Ley 53-07, fue producto del trabajo consensuado de una comisión coordinada desde agosto del año 2003 por el INDOTEL, la Policía Nacional, las telefónicas y parte de algunas participaciones de la sociedad civil, la cual tuvieron como misión elaborar un anteproyecto de ley sobre delitos electrónicos, informáticos y de las telecomunicaciones". Destacando que en el anteproyecto de ley se tomara en consideración la regulación de esta materia especial, sus principios constitucionales y legales, y sobre todo la situación nacional e internacional, y las disposiciones legales vigentes en la República Dominicana.

El Ministerio Público

En cuanto al ámbito procesal, señala la ley 53-07, que se incorporan medidas para "la conservación de la prueba y la integridad de la evidencia digital o electrónica contenida en un sistema de información, otorgándole a las autoridades competentes facultades que faciliten y agilicen el proceso investigativo".

El ministerio público, bajo las disposiciones de la ley 53-07, contra Crímenes y Delitos de Alta Tecnología, cuenta con una dependencia especializada en la investigación y persecución de los crímenes y delitos de alta tecnología como lo es el DICAT.

Adicionalmente se creó la Comisión Interinstitucional en contra de los Crímenes y Delitos de Alta Tecnología (CICDAT), la cual está integrada por representantes de la Policía Nacional, la secretaría de las Fuerzas Armadas (FFAA), la Dirección Nacional de Control de Drogas (DNCD), el Departamento Nacional de Investigaciones (DNI), la Procuraduría General de la República (PGR), INDOTEL, la Superintendencia de Bancos (SB), el Consejo Nacional de la Niñez (CONANI) y el Instituto Tecnológico de las Américas (ITLA).

Entre las funciones de esta comisión de la CICDAT, se encuentran la coordinación y cooperación con autoridades policiales, militares, de investigación y judiciales, para mejorar y dar cabal cumplimiento a las disposiciones de la Ley 53-07.

El papel de la Policía Nacional (PN)

Además, establecer la coordinación y cooperación con gobiernos e institucionales nacionales y extranjeras para prevenir y reducir la comisión de actos ilícitos de alta tecnología en la República Dominicana y el resto del mundo, así como promover la adopción y tratados internacionales en esta materia, debiendo velar por la implantación y cumplimiento de los mismos. Uno de los avances más importante de la ley 53-07, fue crear el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), como entidad subordinada a la Dirección Central de Investigaciones Criminales de la Policía Nacional, la cual sería una dependencia especializada".

La comisión que trabajó en la elaboración de esta propuesta legislativa que logró la creación de la ley 53-07, la integraron representantes de instituciones públicas, privadas y de la sociedad civil, como son la Procuraduría General de la República, el DNI, las empresas de telecomunicaciones "All América Cable and Radio, Inc.", Centennial Dominicana, Orange Dominicana, Tricom, Verizon Dominicana, la Fundación Institucionalidad y Justicia, entre otras.

Igualmente, trabajaron en este proyecto distinguidos profesionales del área, entre éstos la ex diputada Ángela Jaqués, Licenciado Manuel Ramón Vásquez Perrota y la firma de abogados Pellerano y Herrera. (INDOTEL, 2005)

Ilustración 5. La comisión que trabajó en la elaboración de esta propuesta legislativa

Departamentos o Instituciones que Intervienen en este Proceso:

Estas Instituciones y/o Departamentos están designado por leyes y normativas y sujetos a reglas ya establecidas en este momento en la constitución de la república.

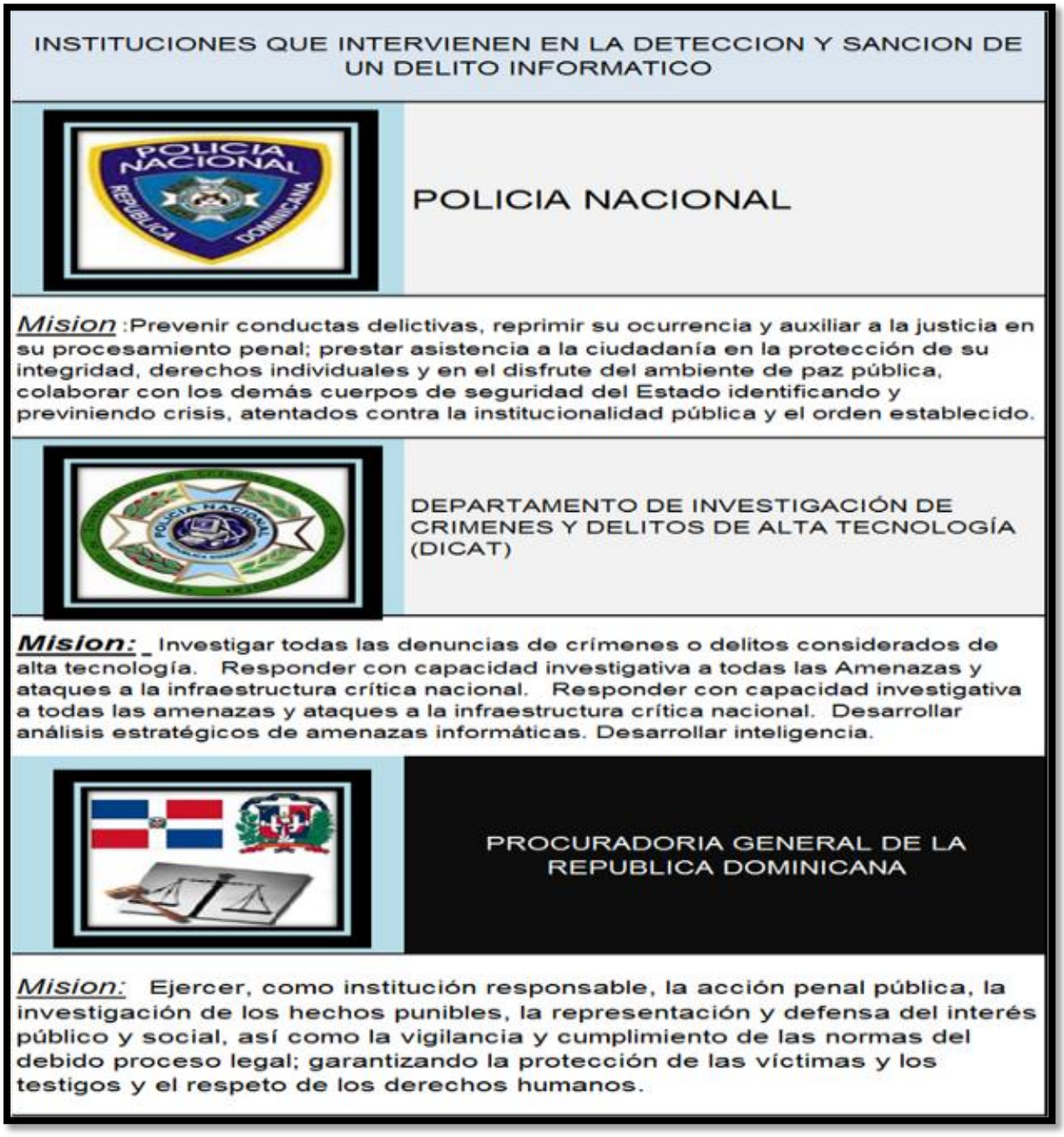

Ilustración 6. Departamentos que intervienen en la detección y Aplicación de la ley sobre delito informático.

Esquema Operativo

1	*Deteccion de la Anomalia: El usuario o empresa ha detectado que existe algun tipo de alteracion o perdida*	
2	*Determinacion del Departamento que recibe al denunciante*	POLICIA NACIONAL REPUBLICA DOMINICANA
3	*Activacion de los peritos Forenses que analizaran las pruebas*	dni electrónico; POLICIA NACIONAL
4	*Activacion de los mecanismos legales para dar seguimiento a los procesos y velar porque se cumpla la ley*	

Ilustración 7. Esquema Operativo en la detección y Aplicación de la ley sobre delito informático

Tipificación de los Delitos informáticos más comunes en la Republica Dominicana, Según el departamento de Delito informático o de alta tecnología DICAT.

Delitos Informaticos Clasificacion por Orden Alfabetico	
1	Acceso ilícito y sabotaje
2	Activaciones fraudulenta de celulares
3	Clonación CD, DVD de audio y película
4	Clonación de cable de MODEM
5	Clonación de tarjetas de cerditos
6	Daños y alteración de datos
7	Difamación y amenaza vía e-mail e Internet
8	Difamación y amenaza vía telefónica
9	Difamación y bloqueo de paginas Web
10	Estafa vía telefónica
11	Fraude electrónicos a personas y empresas
12	Fraudes electrónicos a banca de lotería
13	Hacking
14	Interceptación telefónicas
15	Phishing
16	Piratería se software
17	Robo de e-mail
18	Robo de identidad
19	Sustracción de equipos electrónicos
20	Sustracción de software
21	Terminación de llamas ilegales

Tabla 9. Tipificación de los Delitos Informáticos según el DICAT.

Descripción Gráfica del Delito Informático

Ilustración 8. Descripción gráfica del Delito Informático

Descripción Conceptual de algunos Delitos Informáticos

- **Manipulación de los datos de entrada**. Este delito es también conocido como "sustracción de datos", delito de nueva generación muy común en el ámbito del derecho bancario. Este delito no precisa de conocimientos técnicos de informática y puede utilizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos;

- **Manipulación de programas**. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas para producir resultados diferentes a los originalmente elegidos.

- **Manipulación de datos de salida**. Es el caso de manipulación que usualmente se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. En un comienzo este delito se llevaba a cabo mediante tarjetas bancarias robadas y hoy en día utilizan equipos y programas especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

- **Delito efectuado por manipulación informática**. Aprovecha las repeticiones automáticas de los procesos de cómputo. Es la técnica que se reconoce como Salami en la que cantidades de dinero muy pequeñas se van sacando repetidamente de una cuenta y se transfieren a otra.

- **Delitos contra sistemas, daños o modificaciones de programas o datos computarizados.**
  - ✓ Sabotaje Informático.
  - ✓ Falsificaciones informáticas.
  - ✓ Violación a la intimidad por sustracción o utilización no autorizada de datos personales.
  - ✓ Interceptación de comunicaciones.

- **Robo de servicios**. Estos se refieren al robo de un servicio tecnológico que identificaremos como de bajo nivel.
- **Parasitismo informático**. Se alude a las conductas que tienen por objeto el acceso ilícito a los equipos físicos o a los programas informáticos, para utilizarlos en beneficio del delincuente.
- **Hurto calificado por transacciones electrónicas de fondos**. Es el robo que se comete mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o también cuando se viola el empleo de claves secretas.

Ilustración 9. Descripción gráfica del Delito Informático

Entre los delitos informáticos más comunes están los siguientes

Acceso Ilícito y Sabotaje: El hecho de ingresar o la intención de ingresar sin autorización, o a través del acceso de un tercero, a un sistema de información, permaneciendo o no en él.

Activación Fraudulenta de Celulares: Es cuando se registran la activación de un celular en una compañía proveedora de servicios con datos de un tercero.

A. **Clonación de Tarjeta de Crédito, cable de Modem, CD, DVD de audio y película**: Duplicación o reproducción exacta de una serie electrónica, un número o sistema de identificación de un dispositivo de almacenamientos o un medio de acceso a un servicio.
B. **Difamación y amenaza vía telefónica, e-mail e internet**: Cuando se realiza envíos de mensajes o publicaciones que ponen en peligro la vida de un ser humano.
C. **Estafa vía telefónica**: Es cuando se realiza la acción de engaños empleando de medios electrónicos, informáticos, telemáticos o de telecomunicaciones.
D. **Delito electrónico a persona, empresa y banca de lotería**: Es cuando se realizan una serie de delito realizado por persona cercana a esta, abusando de la confianza de los propietarios, utilizando medios electrónicos.
E. **Hacking**: Esta conducta se refiere al acceso no autorizado que realiza un sujeto activo a un sistema de información atentando contra el sistema de seguridad que este tenga establecido.
F. **Interceptación Telefónica**: Apoderar, utilizar, afectar, detener, desviar, editar o mutilar, de cualquier forma un dato o una transmisión de datos perteneciente a otra

persona física o moral, por su propia cuenta o por encargo de otro, para utilizar de algún modo o para conocer su contenido, a través de un sistema de información o de cualquiera de sus componentes.

G. **Phishing**: Es cuando se realiza una suplantación de identidad de una empresa o persona jurídica con el fin de capturar informaciones que le puedan servir para acceder por cuenta propias.

H. **Robo de Identidad y Correo**: El hecho de una persona valerse de una identidad ajena a la suya, a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con penas de tres meses a siete años de prisión y multa de dos a doscientas veces el salario mínimo.

I. **Spear Phishing**: Es una versión del phishing pero más agresiva, ya que no espera que a la azar a alguien que quiera acceder a la página, sino que se basa en el envió de un correo electrónico suplantando una empresa con el fin de obtener información para utilizarla a su conveniencia.

Estas figuras delictivas son previamente calificadas según el perjuicio causado, el papel que el computador desempeñe en la realización del mismo, el modo de actuar, el tipo penal en que se encuadren y el tipo de actividad que implique según los datos involucrados.

Es de conocimiento de todos que algunas de las referidas acciones ilegales son llevadas a cabo por personas con conocimientos especiales, por lo que es obvio que se produzcan como consecuencia de estos actos perjuicios más graves, que pueden incluso repercutir desfavorablemente contra terceros.

1.7 Situación actual de los delitos en el comercio electrónico en la Republica Dominicana

2007- 2008

De acuerdo a los datos estadísticos en los años posteriores a la creación de la ley de delitos informáticos en RD, podemos analizar a partir de que todos los delitos presentaron un aumento significativo desde el 2007 al 2008.

En 2008 pudimos hacer notar que fue el año detonante de los casos de phishing bancario, producto del aumento del uso de herramientas de Internet Banking.

En 2007 se registró uno de los casos más significativo, en el cual un grupo de personas se dedicaron a la clonación de cajas receptoras de señal de TV por cable, en perjuicio de empresas comercializadoras de TV por cable y sus clientes.

Cuadro Estadístico de Casos Resueltos por el DICAT en el Periodo 2007-2008.				
Tipos de Delitos		Total 2007	Total 2008	Total General
1	Llamadas molestosas y/o amenazantes	28	207	235
2	Phishing	0	192	192
3	Delitos electrónicos a personas e empresas	11	69	80
4	Sustracción de equipos electrónicos	10	58	68
5	Hacking	1	10	11
6	Robo de identidad	0	6	6
7	Acceso ilícito y sabotaje	0	6	6
8	Difamación y bloqueo de página web	1	2	3
TOTAL DE CASOS		51	550	601

Tabla 10. Estadística de los Casos Resueltos por el DICAT en el periodo 2007 – 2008. (DICAT, 2014)

2009-2010

En este periodo podemos observar como aumentante considerablemente los casos de phishing luego de haber presentado una disminución en comparación con el periodo anterior, así como también el aumento de los Delitos a empresas y los hackeos a portales dominicanos.

El caso más relevante de este periodo fue precisamente relacionado al phishing, en el cual una organización criminal integrada por dominicanos realizaba transferencias ilícitas fruto de haber comprometido las credenciales de acceso de varias personas mediante el envío de correos usurpando la identidad de una entidad bancaria nacional, por medio a los cuales solicitaba a los clientes la introducción de sus datos de acceso, los que luego capturaban y utilizaban para realizar las transferencias a terceros en perjuicio de la entidad bancaria y sus clientes.

Cuadro Estadístico de Casos Resueltos por el DICAT en el Periodo 2011-2012.				
Tipos de Delitos		Total 2009	Total 2010	Total General
1	Llamadas molestosas y/o amenazantes	297	247	544
2	Phishing	96	195	291
3	Delitos electrónicos a personas e empresas	78	111	189
4	Sustracción de equipos electrónicos	83	43	126
5	Hacking	25	63	88
6	Estafa vía telefónica	4	41	45
7	Difamación y bloqueo de página web	5	37	42
8	Robo de identidad	18	8	26
9	Clonación de tarjetas (skimming)	22	3	25
10	Acceso ilícito y sabotaje	2	1	3
TOTAL DE CASOS		630	749	1,379

Tabla 11. Estadística de los Casos Resueltos por el DICAT en el periodo 2009 - 2010 (DICAT, 2014)

2011-2012

Al analizar este periodo podeos observar la disminución en el phishing producto de las medidas que tomaron las entidades bancaria con la implementación de tarjeta de código y token, los cuales dificultaban a los atacantes el realizar las transacciones, aunque de igual manera se mantuvieron en gran aumento los envío de correos falsos con fines de phishing. De igual manera de denota un gran aumento en el robo de equipos electrónicos por la delincuencia común, ya sea mediante robo, atraco.

En este periodo se registró un caso que afectó de manera directo el comercio electrónico en su modalidad, C2C, ya que se registró un aumento en los delitos realizados por los portales de clasificados electrónicos, mediante los cuales personas ofrecen artículos y servicios. Una banda criminal se dedicaba a publicar artículos electrónicos de gran valor mediante los portales, para luego estafar a las personas solicitándoles el pago adelantado a los mismos, para luego no enviarlos y desaparecer.

Cuadro Estadístico de Casos Resueltos por el DICAT en el Periodo 2011-2012.				
Tipos de Delitos		Total 2011	Total 2012	Total General
1	Sustracción de equipos electrónicos	224	456	680
2	Llamadas molestosas y/o amenazantes	309	250	559
3	Phishing	114	95	209
4	Estafa vía telefónica	58	59	117
5	clonación de tarjetas (skimming)	3	109	112
6	Delitos electrónicos a personas e empresas	56	36	92
7	Difamación y bloqueo de página web	43	28	71
8	Robo de identidad	32	30	62
9	Hacking	21	29	50
10	Acceso ilícito y sabotaje	4	6	10
TOTAL DE CASOS		864	1,098	1,962

Tabla 12. Estadística de los Casos Resueltos por el DICAT en el periodo 2011 - 2012 (DICAT, 2014)

2013-2014

Al observar detenidamente los datos estadísticos en los informes de investigación del Departamento DICAT en el período 2013-2014, se puede apreciar que los mayores delitos informático que afectan al comercio electrónico son los 5, 6, 10 y 11 de la tabla mostrada a continuación. Estos son phishing, Delito electrónico a empresas, hacking y acceso ilícito y sabotaje.

Cuadro Estadístico de Casos Resueltos por el DICAT en el Periodo 2013-2014.				
Tipos de Delitos		Total 2013	Total 2014	Total General
1	Llamadas molestosas y/o amenazantes	144	133	277
2	Clonación de tarjetas (skimming)	168	51	219
3	Estafa vía telefónica	80	99	179
4	Difamación y robo de identidad en redes sociales	45	65	110
5	Phishing	43	65	108
6	Delitos electrónicos a personas e empresas	48	38	86
7	Robo de identidad	34	39	73
8	Difamación y amenaza vía e-mail	39	18	57
9	Sustracción de equipos electrónicos	14	35	49
10	Hacking	32	6	38
11	Acceso ilícito y sabotaje	4	8	12
12	Pornografía infantil	2	2	4
TOTAL DE CASOS		653	560	1,222

Tabla 13. Estadística de los Casos Resueltos por el DICAT en el periodo 2013-2014. (DICAT, 2014)

En el total de casos de mayor relevancia en el período 2013 fue el desmantelamiento de una poderosa banda de Búlgaros, que venían al país a afectar el comercio electrónico de manera negativa, ya que los mismos infectaban los cajeros automáticos de los principales bancos del país, en las zonas turísticas, situación que provocaba que tantos los turistas como los nacionales que frecuentaban esas zonas, les clonaran sus tarjetas de créditos y luego con

dicha información procedían a consumir y hacer pagos a pedidos de bienes y servicios electrónicos por los distintos portales de renombre que existen en la web. Afectando la credibilidad y la buena imagen de nuestro país como destino turístico, así como también la economía de la banca nacional e internacional.

1.8 Análisis de expertos en materia legal, programación y seguridad tecnológica de la información en la República Dominicana

Se procedió a entrevistar a un experto en material legal, el cual opinó desde el punto de vista económico en beneficio del país, y sobre como las facilidades de pagos por medios electrónicos han contribuido al desarrollo de la presencia del comercio electrónico. La empresas intermediarias de pagos electrónicos nacionales han ofrecido grandes facilidades y flexibilidades a los comercios para que tengan presencia en la web con la capacidad técnica de transaccional sus productos y servicios con el consumidor final electrónicamente, lo que contribuye a que grandes comercios realicen transacciones B2B y el público consumidor también pueda aprovechar estas facilidades en la modalidad B2C, representando este una parte importante del movimiento de la economía nacional ascendente a los 11MM en un semestre del año 2014.

En el ambiente legal, el experto considera que la entidad reguladora de calidad al consumidor tiene como objetivo reforzar la parte protectora en este tipo de transacciones, así como también iniciar con los pasos correspondientes para regular la seguridad de en las transacciones de los portales que ofrecen servicios mediante transacciones electrónicas.

Se procedió a entrevistar a un experto desde punto de vista técnico a nivel de programación, el cual manifestó su opinión positiva en cuanto al beneficio económico y el desarrollo al país, aunque entiende ha sido un poco lento, aunque reconoce que las empresas hoy en día sienten la necesidad de tener presencia en la web, como medio de realizar sus ventas. Manifiesta también que debe existir un método más fácil de validación de identidad para las tarjetas de créditos locales, a través de la participación de los bancos y burós de crédito. Con requisitos y procedimientos claros del manejo de la información confidencial de las tarjetas de crédito. Acompañados de las creaciones de campañas publicitarias para incentivar el uso del internet para las compras locales, enfatizando en la seguridad y facilidad de las transacciones.

También se entrevistó a un experto desde el punto de vista de seguridad tecnológica, el cual nos mostró su opinión más receptiva en cuanto a que los programadores hoy en día, en su mayoría aplican poco las mejores prácticas en el desarrollo de las aplicaciones web y disponen de pocos mecanismos de manera oportuna para indicar una desviación de cambios significativos en las transacciones que se registran, para responder inclusive a ataques del día 0.

Continúa manifestando que se debe establecer una recomendación para todos aquellos portales seguros en nuestro país, con controles para saber cuándo ha existido o un posible intento de compromiso en sus áreas de responsabilidad y de esta manera hacer que el comercio electrónico en nuestro país se torne funcionalmente más seguro.

En las entrevistas hechas a los oficiales investigadores y técnicos de DICAT, manifiestan que en los últimos años se han incrementado los ataques que afecta

directamente al comercio electrónico, como son los casos de portales C2C y B2C en los cuales los usuarios son afectados por metodologías del engaño por parte de los atacantes al solicitar datos sensibles y personales valiéndose de enlaces y paginas falsas, afectando directamente la marca del servicio que simulan ser. Así también se puede resaltar, que aunque los casos de estafas bancarias (phishing) han disminuido en cantidad de ataques, los montos de los ataques aislados de han incrementado considerablemente, lo que advierte a los investigadores que esta modalidad ha evolucionado con el fin de hacerse cada día más orientados a objetivos específicos, sofisticados y lucrativos.

CAPITULO II.
MODELO Y ESTRATEGIA DE PREVENCION DE LOS DELITOS DEL COMERCIO ELECTRONICO EN LA REPUBLICA DOMINICANA

2.1 Condiciones Previas de Mejores Prácticas de Prevención de los Delitos en el Comercio Electrónico

El comercio electrónico ha llegado al punto de ser casi imprescindible en el día a día, ya que la tendencia es que todas las transacciones de intercambio de bienes tangibles e intangibles se realicen electrónicamente. Esto representa una ventaja y una herramienta vital tanto para el consumidor como para el negocio. De igual manera mientras avanza la utilización y desarrollo, la herramienta debe luchar contra los constantes ataques y amenazas por parte de los ciber delincuentes que utilizas los avances del comercio electrónico para realizar delitos que afectan directamente tanto a negocios como a consumidores. Específicamente para robar información sensible con el fin de obtener beneficios lucrativos.

Una de las principales debilidades en los modelos de comercio electrónico es la utilización de ingeniería social, la cual se enfoca en engañar al usuario o consumidor, más que en vulnerar los sistemas de seguridad tecnológicos tradicionales. Es una realidad también que el frecuente uso de herramientas de software pirateadas o manipuladas para evitar el pago de licenciamiento, presenta un riesgo de amenaza, ya que los usuarios de portales de comercio electrónico que manejan información sensible pueden ser

comprometidos, afectando esto directamente al usuario al comprometer los datos de acceso. En las estadísticas actuales proporcionadas por el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología se pueden observar la cantidad de delitos cometidos a portales de banca electrónica y portales de venta de artículos, en los cuales se han afectado clientes de ese tipo de comercios a raíz de sus datos haber sido comprometidos al intentar realizar una transacción en los portales.

Desde el 2007 hasta el 2014 el Departamento de resuelto un total de 776 casos de "Phishing" producto de haber sido afectados luego de que sus datos fueran robados al momento de utilizar un servicio de comercio electrónico o banca en línea.

PHISHING		
AÑO	DENUNCIAS	RESUELTOS
2007	0	0
2008	97	192
2009	364	96
2010	195	195
2011	110	114
2012	94	95
2013	29	43
2014	17	41
Total ∑	906	776

Tabla 14. Estadísticas de casos resueltos por el DICAT, Desde la promulgación de la ley 53-07. (DICAT, 2014)

2.2 Estructura y Elementos de la Estrategia de Prevención

La estrategia de prevención propone un conjunto de acciones necesarias para mitigar y disminuir el riesgo de que los clientes de una empresa que ofrezca bienes o servicios electrónicamente sean afectados por el delito. Estas acciones de complementan de igual manera con herramientas tecnológicas que serían fundamentales para asegurar en mayor proporción los datos e información sensible de los clientes, ya que el delito puede ser exitoso valiéndose tanto de las debilidades del consumidor, como también de la plataforma tecnológica del negocio.

1. Selección de la plataforma de comercio electrónico correcta

Durante la creación y diseño de una página de comercio electrónico, hay muchas plataformas de comercio electrónico que se pueden elegir, estás pueden ser una solución de Web completa o simplemente proporcionar las funcionalidades de comercio en línea a una página web ya existente.

La investigación que se hace en relación con la elección de una plataforma es un paso crucial para asegurar que la página tenga la menor cantidad de vulnerabilidades que se pueden explotar para la realización de un delito. Cuando se está investigando diferentes proveedores de plataformas, se debe buscar más allá de los costos mensuales y las tasas de transacción y analizar en mayor profundidad las características de la plataforma. Es posible que algunas de las plataformas con las mejores tarifas no sean las más convenientes en el ámbito de la protección contra el delito. Por lo que se debe buscar una plataforma que ofrezca apoyo de primera categoría a la gestión de riesgos.

A continuación se presentan 10 plataformas / soluciones que ofrecen mayor control y seguridad de las transacciones en comercio electrónico, estos servicios permiten crear una web de comercio electrónico de manera rápida y segura, con plantillas pre-diseñadas, y varios servicios, como son los de cobro, facturación, seguridad, cumplimiento de las normas internacionales. Junto a estás se presentan imágenes mostrando parte de los servicios que ofrecen al usuario y/o los clientes que utilizan dichos servicios.

- **Shopify** – es una de las favoritas de diseñadores y desarrolladores web, les encanta por sus diseños fáciles de usar y plantillas y gran cantidad de características, además de un carrito de la compra, compatible con dispositivos móviles, para el acceso desde cualquier dispositivo.

Ilustración 10. Algunos diseños de páginas de E-Commerce logradas utilizando el servicio shopify. (Shopify, 2014)

- **Stripe** - Este servicio se encarga de todos los requisitos de PCI-cumplimiento, y permite la liquidez de las operaciones cada siete días en lugar de mensual.

Ilustración 11. Sistema de pagos diseñado por Stripe. (Stripe, 2014)

- **Highwire** - Además de las plantillas fáciles de usar y móvil-listos, este servicio tiene un enfoque multi-canal y vende sus productos en Facebook, Bonanza, y eBay, además de su sitio web.

Ilustración 12. Plantilla para páginas de venta de artículos electrónicos. (inkFrog, Inc., 2014)

- **Volusion** - Además de tener uno de los precios más bajos (un mini plan de $ 9 / mes por un máximo de 25 productos), adicionalmente este servicio tiene la opción de hacer publicidad a los productos contratados.

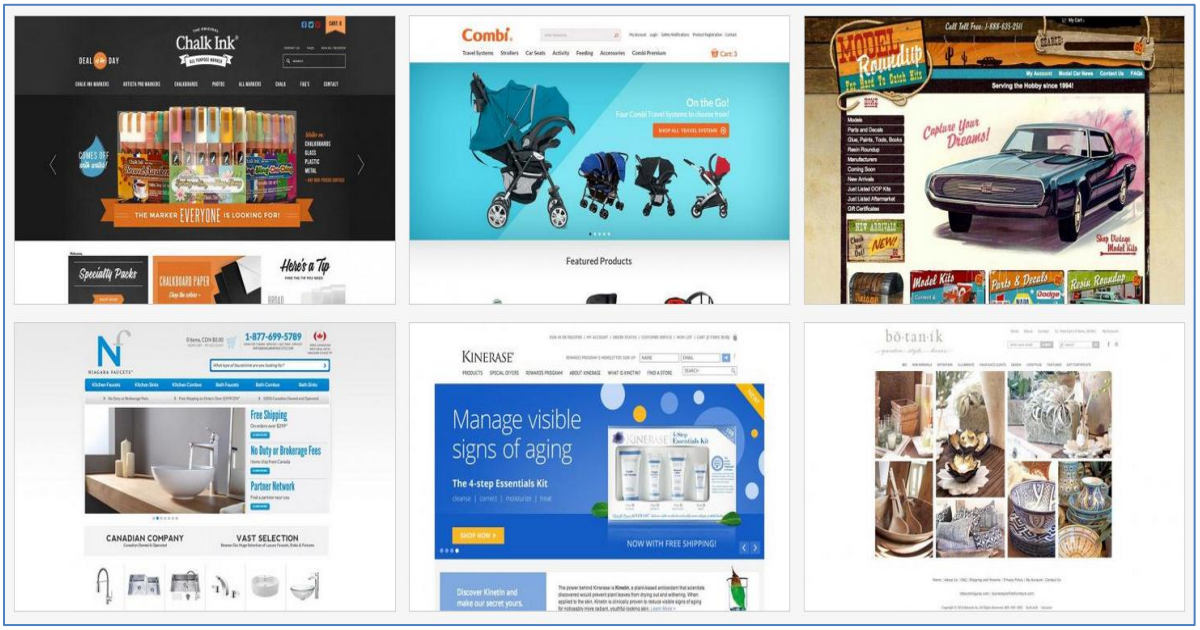

Ilustración 13. Páginas que utilizan los servicios de volusion. (Volusion, Inc, 2014)

- **Payza** - Este servicio es uno de los mejores para el procesamiento de pagos y comercio electrónico internacional, y ofrecen opciones asequibles y convenientes para países emergentes y mercados con pocos servicios.

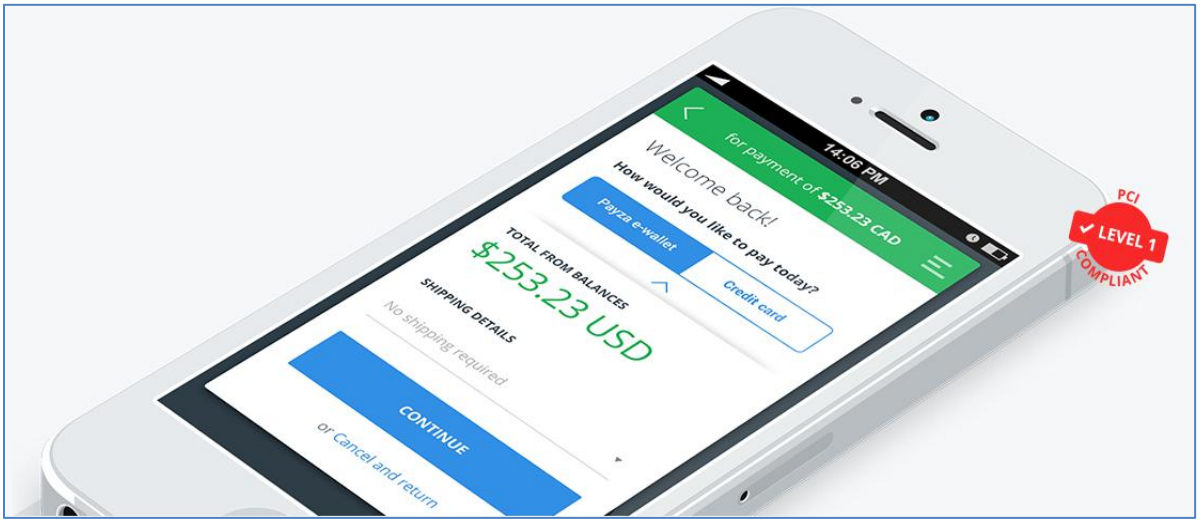

Ilustración 14. Servicio de pagos a través del celular. (Damaras Limited, 2014)

- **Bigcommerce** – tiene una plataforma para comercio móvil, este servicio ofrece una sola página de compra y permite comentarios de los usuarios de los productos. Además, se puede configurar para que el cliente reciba un correo electrónico si este abandona el carrito de compras (para recordarles de la compra potencial).

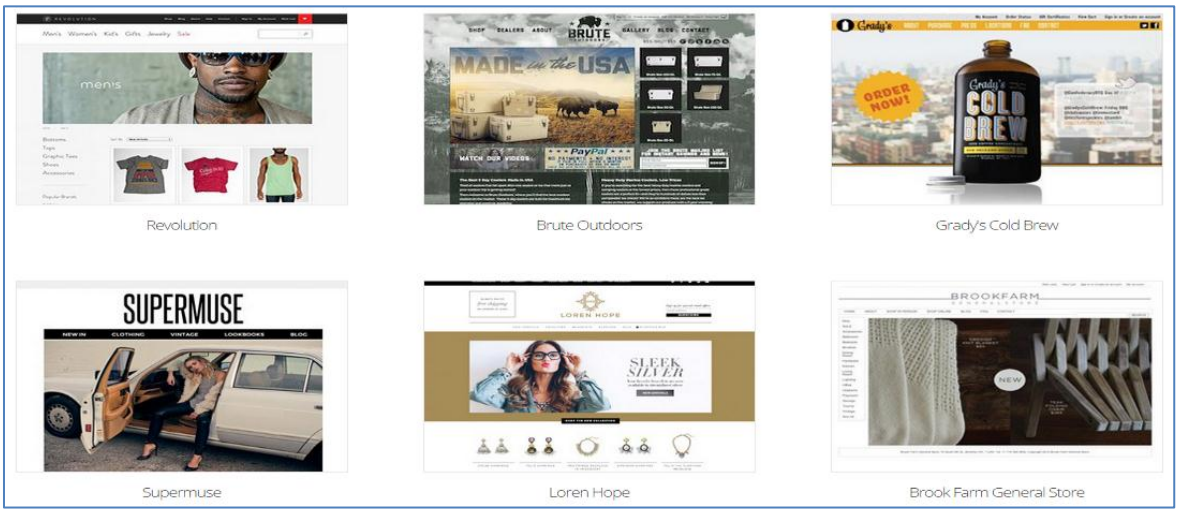

Ilustración 15. Muestra de las páginas de clientes de la compañía Bigcommerce. (Bigcommerce, 2014)

- **Magento** – Es gratuito, este servicio no está vinculado al proveedor ya que es de código abierto, por lo que puede ser modificado para crear una experiencia personalizada para los usuarios y puede alojar el servicio en cualquier lugar.

Ilustración 16. Listado de clientes que utilizan los servicios de la compañía Magento. (Ebay Inc., 2014)

- **osCommerce** - libre y construido por la comunidad de código abierto. Se trata de una página web completa con carrito de compra que se puede instalar en cualquier servidor web. Hay una enorme comunidad de usuarios, así como más de 7.000 complementos de ellos (que se puede descargar y sin costo alguno), además de plantillas gratuitas disponibles.

Ilustración 17. Página de demostración del sistema osCommerce. (osCommerce, 2014)

- **FoxyCart** – con este servicio puede alojar su sitio en cualquier lugar; sin embargo, el carrito de compra y el pago de los productos técnicamente será alojado en la página web de FoxyCart para manejar todos los detalles de seguridad.

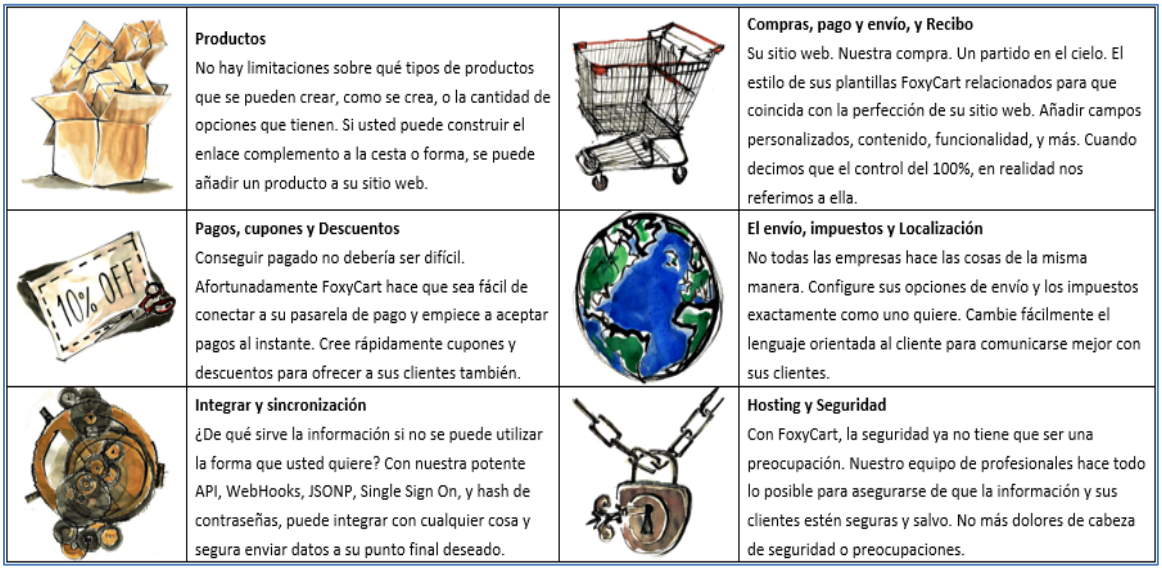

Ilustración 18. Servicios que ofrece FoxyCart. (FoxyCart, LLC, 2014)

- **DPD** - Similar a FoxyCart, este servicio aloja únicamente el carrito de compra y el pago de los productos. DPD se especializa en productos digitales, especialmente para blogs y sitios web que tienen productos para vender. También hay un programa integrado de afiliados que pagar una comisión a los afiliados a cambio de referencias.

Ilustración 19. Modo del servicio que ofrece DPD. (DPD, 2014)

2. Lograr y mantener el cumplimiento de las normas PCI

De acuerdo con la Guía de cumplimiento de las normas de PCI , la Industria Estándar de Seguridad de Datos de Tarjetas de Pago (PCI DSS). Es un conjunto de requisitos que permiten asegurar que todas las empresas que procesan, almacenan o transmiten información de tarjetas de crédito, básicamente cualquier comerciante con una identificación del comerciante (MID) -mantiene un entorno seguro.

PCI está diseñado para proteger de forma proactiva los datos del cliente y se aplica a todas las organizaciones y comerciantes, independientemente del tamaño o el número de transacciones, que aceptan, transmiten o almacenan datos de titulares de tarjetas, y es absolutamente obligatorio. Además el incumplimiento puede resultar en una multa de $ 5.000 a $ 100.000 por mes para el banco adquirente (que a su vez lo transmitirá al comerciante), además de otras sanciones que no se discute abiertamente, pero podría ser perjudicial para las empresas.

Hay cuatro niveles de cumplimiento comerciante basado en el número de transacciones que procesan cada año y si las operaciones son desde una tienda física o por Internet. Cada marca de la tarjeta de pago establece sus requisitos específicos, y estas son las definiciones de nivel de cumplimiento de PCI-Visa:

- **Nivel 1:** Más de 6 millones de transacciones por año
- **Nivel 2:** 1-6 millones de transacciones por año
- **Nivel 3:** 20.000 a 1 millón de transacciones por año
- **Nivel 4:** Menos de 20.000 transacciones por año

Cualquier comerciante que ha sufrido un hackeo que comprometió datos de la cuenta se le podría elevar a un nivel más alto de validación.

El cumplimiento de PCI generalmente implica precauciones básicas de seguridad, como cambiar las contraseñas por defecto de fábrica en todos los equipos de la red y el establecimiento de un cortafuego entre su conexión a Internet y cualquier sistema que almacena números de tarjetas de crédito.

Los comerciantes deben cumplir con la aplicación PCI y el proceso de revisión, que incluye:

- Identificar el Tipo de validación para determinar qué cuestionario de autoevaluación va a utilizar para la empresa.
- Completar el cuestionario de Auto-evaluación de acuerdo a las instrucciones dadas.
- Completar y obtener evidencia de haber pasado un análisis de vulnerabilidades con un Proveedor Aprobado de Escaneo (ASV) PCI SSC, si procede.
- Completar la documentación correspondiente certificando el cumplimiento del cuestionario de autoevaluación.
- Presentar el Cuestionario de Autoevaluación, con la evidencia de su aprobación, y la declaración de cumplimiento, así como cualquier otra documentación solicitada, a su adquirente. O un profesional de la seguridad con credenciales de Asesor de Seguridad Calificado (QSA) llevará a cabo una revisión independiente de sus procesos y sistemas.

Dependiendo del proveedor de la plataforma de comercio electrónico, algunos de estos pasos pueden ser llevados a cabo por el proveedor. PayPal tiene una solución compatible con PCI llamado Payflow Link, que se ocupa de las normas PCI para por el usuario con plantillas de página de pago que se pueden personalizar. Esta solución agiliza el proceso de documentación, aunque todavía tiene que completar el cuestionario y acatar análisis trimestrales de seguridad.

A continuación algunas soluciones de comercio electrónico que cumplen PCI:

- **Shopify** está certificado que cumple con las normas PCI DSS Nivel 1.
- **Etsy** ha sido auditado y certificado que cumple con las normas PCI.
- **Stripe** maneja todos los requisitos de seguridad por el usuario, haciendo uso de SSL (https en lugar de http).
- **Highwire** opera una salida compatible con PCI totalmente segura y maneja todo el SSL por el usuario.

3. Hacer una Revisión de la Seguridad de su Sitio Web

Una vez que se haya elegido la mejor y más segura plataforma de procesamiento de pagos y se encuentra en cumplimiento con los requisitos de PCI, es propicio considerar la adopción de nuevas medidas para garantizar que toda la información personal y financiera de sus clientes, su negocio, su banco, y su compañía de tarjeta de crédito están a salvo y seguro.

- Comprobar si todas las URL de caja se mantienen en "https" durante el proceso de pago.

- Revisar qué sucede cuando dejas las zonas de cajas de su sitio web y regresa a la caja más adelante. ¿El sitio mantiene las URLs «https» donde se necesitan?
- Cambiar las contraseñas al panel de control del servidor web y las bases de datos regularmente.
- Considerar la posibilidad de contratar a un auditor de seguridad para ver si pueden encontrar vulnerabilidades en el sitio web.

Existen programas específicos (sobre todo con las empresas de tarjetas de crédito y las empresas de software de seguridad) que proporcionan una protección adicional contra fraudes y hackeos, en perjuicio de la empresa. A continuación se listan cuatro programas de este tipo:

- Verified by Visa
- VeriSign
- McAfee Secure
- MasterCard Merchant protección contra fraudes

Si utiliza una plataforma de código abierto, estará en mayor riesgo de transacciones fraudulentas, ya que no se incluirán las medidas de seguridad superiores tomadas por los servicios de plataforma de mayor tamaño.

4. Configurar alertas del sistema a la pantalla de Actividades Sospechosas

Dependiendo del software o plataforma de procesamiento que está utilizando, la plataforma puede que le avise automáticamente cuando se produce una actividad sospechosa, como por ejemplo:

- Múltiples pedidos realizados por la misma persona con diferentes tarjetas de crédito.
- Los números de teléfono que no coincidan con el código de área de la dirección de facturación.
- Los derrochadores que piden grandes cantidades de productos, varios de un mismo producto, o pagar extra para enviar rápidamente (posiblemente usando una tarjeta de crédito robada para obtener los productos de forma rápida y revender para un beneficio).
- Ordenes donde el nombre del titular de la tarjeta es diferente del nombre del destinatario, en particular para direcciones en el extranjero (posiblemente porque están enviando un producto a un destino en el que un cliente fraudulento puede recogerlo sin ser rastreado).

Shopify ofrece información sobre AVS devueltos y órdenes CVV2 para que el dueño de la tienda puede hacer su propia decisión informada.

5. Códigos de Tarjeta de Crédito de Seguridad

El código de seguridad de la tarjeta de crédito es de 3 o 4 dígitos impreso en la parte posterior de una tarjeta de crédito. Utilizando el código en un proceso de transacción garantiza que el titular de la tarjeta está en posesión física de una tarjeta válida.

Una vez que se procesa la transacción, el emisor de la tarjeta responde con un código de respuesta confirmando o rechazando la validez del número proporcionado.

Este número se conoce por diferentes nombres para las tarjetas de crédito específicas, de la siguiente manera:

- Visa - CVV2
- MasterCard - CVC2
- Descubra - CID
- American Express - CID (4 dígitos por encima de número de la tarjeta)

Asegúrese de emplear estos códigos de seguridad de tarjetas de crédito para asegurar las transacciones más seguras posibles para la empresa y sus clientes.

6. No Almacenar Datos Confidenciales de Clientes o Datos de Transacciones.

En la mayoría de los casos, las normas PCI prohíben estrictamente a las empresas el almacenamiento de datos de los clientes, en particular a los números de tarjetas de crédito, fechas de caducidad y códigos CVV2. Si por alguna razón usted tiene alguno de estos datos almacenados, deshacerse de él de inmediato, y mantener sólo la cantidad mínima de datos posibles, sólo lo suficiente para reembolsos y devoluciones de cargo.

Sin embargo, si usted tiene un sistema establecido donde tiene que cargar una tarjeta de manera recurrente, se puede almacenar información de tarjetas de crédito, siempre y cuando cumpla con cifrado estándar PCI y las directrices de política de almacenamiento.

Nunca almacene códigos CVV2. En esencia, si no tiene datos para robar, entonces los hackers no tienen razón para robarle.

7. Número de Seguimiento de los Envíos de Pedidos

Los números de seguimiento de las transacciones ayudan a proteger a las empresas del fraude de cargo. El fraude de devolución de cargo, también conocido como el fraude amable, es cuando un cliente solicita la devolución de fondos de un comerciante, que se inicia por la fuerza por el banco emisor. Cuando esto sucede, el comerciante tiene que rendir cuentas a pesar de las medidas adoptadas para verificar la transacción.

Además, los comerciantes por lo general todavía tienen que pagar por todos los gastos de transacción, incluyendo los costos asociados con la eliminación de los fondos fraudulentos de la cuenta bancaria del comerciante.

Una manera en que los clientes realizan fraude de cargo es afirmar que un producto nunca fue entregado y que quieren que su dinero sea devuelto. Pero si utiliza números de seguimiento, se obtiene la confirmación de que el producto fue entregado al cliente. Exigir una firma en la entrega es otra buena manera de prevenir este tipo de delito.

8. Requerir Contraseñas Seguras a los Clientes

Cuando los clientes están abriendo una cuenta con la empresa, Se debe solicitar contraseñas seguras que no sean fáciles para los hackers el acceso. Exigir un número mínimo de caracteres y letras mayúsculas, números y símbolos. Complicando la contraseña lo suficiente como para que los hackers no puedan violar la información del cliente y realizar compras fraudulentas.

9. Educar al Personal sobre los Protocolos de Seguridad y Delito

Si bien existen medidas de seguridad que la empresa debe, también hay formas de que los empleados y usuarios puedan cumplir con las medidas de seguridad para proteger la empresa del delito.

Las contraseñas que los empleados utilizan para acceder a los sistemas de pago y registros comerciales deben regirse por las mismas reglas estrictas como para los clientes. Asegurándose de que saben cómo monitorear las transacciones, para prevenir cualquier ataque innecesario o compras fraudulentas. Ellos necesitan entender no sólo sus procedimientos de gestión de riesgo, sino también la gravedad de los riesgos para que puedan protegerse a sí mismos, la empresa y los clientes contra la piratería y el delito potencial.

10. Crear y Mantener un Archivo de Transacciones y los Intentos Fraudulentos Anteriores

En caso de que el sistema ha sido hackeado o comprometido o si la empresa ha sido víctima de fraude, se debe mantener un registro de todos los datos en un archivo. Se debe de registrar el evento desafortunado para que la empresa y sus empleados puedan aprender, para el futuro y evitar que la situación vuelva a suceder. Se debe utilizar el archivo para comparar con las transacciones futuras, y aprobar o negar dichas transacciones basándose en la experiencia adquirida.

Una gran cantidad de veces que se van a ver patrones de donde se puede aprender. Se pueden notar que los cargos fraudulentos provienen de:

- Determinados países o regiones geográficas.
- Envío direcciones que no coinciden con la dirección de facturación.
- Pedidos inusualmente grandes.

Si es posible, se puede modificar el sistema para poner esas transacciones en espera o para su posterior revisión. Además, la empresa debe asegurarse que sus empleados tengan conocimiento de estos patrones para que puedan detener dichas transacciones preventivamente.

La protección contra el fraude y los demás delitos electrónicos, aunque no es perfecta, es posible cuando se toman las precauciones necesarias. Hay muchos servicios y protocolos que ya están a disposición para ayudar a lograr este objetivo, y también se puede desarrollar protocolos propios internamente para garantizar que todos los aspectos de la empresa están completamente cubierto. (Bishop, 2014)

CAPITULO III.
VALORACIÓN DEL MODELO Y ESTRATEGIA DE PREVENCIÓN DE DELITOS EN EL COMERCIO ELECTRÓNICO EN REPÚBLICA DOMINICANA

3.1 Ejemplificación del modelo y la estrategia en la prevención del delito XXX en el comercio electrónico dominicano

Habiendo hecho una reseña de la problemática local respecto al delito utilizando tecnología relacionado al comercio electrónico en la República Dominicana, sus consecuencias, y crecimiento, así como los avances tecnológicos que han hecho posible su aceptación, tanto por parte de los sectores económicos como por los usuarios finales, entendemos que la estrategia para reducir o mitigar los riesgos en este esquema de negocios, debe seguir dos directrices claras y bien definidas, que apunten por un lado a la concientización del usuario final para la utilización de las plataformas de comercio electrónico de forma segura", y por otro lado; al reforzamiento de los controles y regulaciones por parte de los proveedores que implementen las transacciones de pagos electrónicos, haciendo que ambas directrices tenga un punto de convergencia entorno a la protección contra la violación de datos personales sensibles (**Data Breach**).

Dicha estrategia debería coexistir con la esperada utilización de forma estándar del protocolo IPv6, y el ya muy agotado IPv4, pero todo esfuerzo en este sentido debe ser claramente acuñado por una cultura a nivel regional de aseguramiento, mediante políticas claras que regule los diferentes grupos de interés en este sector, así como también con la

creación de convenios entre países, debido al factor de anterioridad que envuelve todo incidente de tecnologías de la información, y contando además con una evaluación, actualización y cooperación constante de los actores principales, tales como: Instituciones Militares y Policiales de Investigación Criminal, en conjunto con los diferentes Grupos de Respuestas a Incidentes de TI (CSIRT – Computer Security and Incident Response Team) y las Asociaciones Bancarias y Financieras.

Entrando en detalles, desde el punto de vista del usuario, los esfuerzo deben enfocarse en campañas de orientación y concientización, a través de los portales de comercio electrónicos y las políticas de servicio de las asociaciones de bancos e instituciones financieras, por ser estos los proveedores de los medios de pagos actuales y la base para la futura tendencia de medios de pagos electrónicos (*Cryptocurrencies*). Estas acciones deben girar en torno a las precauciones que debe tomar el usuario al momento realizar sus transacciones, siendo específico en puntos como:

A. Que el PC o dispositivo móvil esté a salvo de virus u otros malware,

B. No realizar compras desde un PC o dispositivo móvil que no esté bajo control del usuario,

C. No guardar contraseñas en el navegador,

D. Usar un programa seguro de gestión de contraseñas,

E. Monitorizar periódica o continuamente las transacciones;

En esta última acción pueden intervenir de forma imperativa, tanto el proveedor de medios de pagos electrónicos, como los proveedores de plataformas comercio, incluyendo dichas revisiones en los módulos de seguridad de sus aplicaciones.

Tomando como partida el enfoque de prevención entorno al usuario final en el comercio electrónico, guiados por las directrices enunciadas anteriormente, en conjunto con las mejores prácticas mencionadas en el **Punto 2** de esta investigación, para asegurarnos de los criterios de confidencialidad, integridad y autenticidad de la plataforma usada, pasamos a detallar los puntos de interés con respecto al proveedor y las metodologías que no se deben dejar de implementar para combatir los riesgos inherentes en las transacciones soportadas en la comercialización, a través de internet y sus diversas plataformas. Y para esto hemos definido la cadena de eliminación de los incumplimientos en los cuales usualmente convergen ambos actores: el usuario y el proveedor.

Cadena de Eliminación de los Incumplimientos:

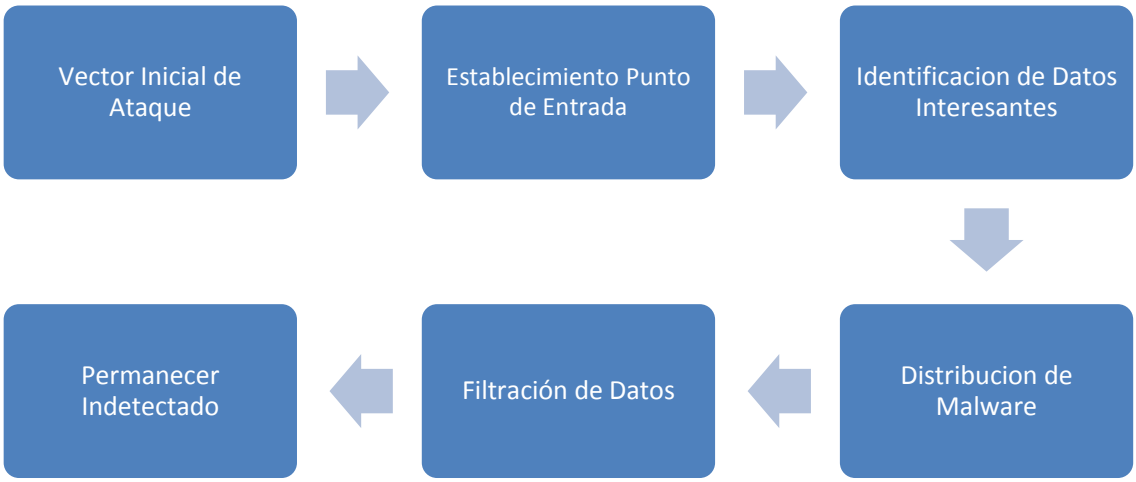

Ilustración 20. Cadena de Ataque de Infiltración. (Sanchez, 2014)

El ataque puede ser interrumpido en cualquier punto de la cadena. Idealmente, una compañía deberá tener controles en cada punto para crear una defensa estratégica profunda. Un modelo "**Cyber Kill Chain**" muestra que un ataque, a través de internet puede incorporar un amplio rango de acciones violentas, desde ***spear phishing*** y espionaje, hasta malware y filtración de datos que puede persistir indetectable por un tiempo indefinido.

Partiendo de este hecho, y siempre teniendo en cuenta la inclusión del protocolo cabera de Internet IPv6, podemos tomar en consideración, en primer lugar el cumplimiento del Estándar PCI - DSS (**Payment Card Industry Data Security Standard**), atendiendo los seis puntos de interés enunciados en el siguiente cuadro, donde se muestran las medidas preventivas, y el foco de control dentro de la cadena de ataque. Tómese en cuenta que, en el comercio electrónico, hay dos actores (usuario y proveedor de servicio), pero ambos convergen en un actor intermediario que anida un servicio para pago electrónico, que en el actual esquema es una tarjeta de crédito o su equivalente, cosa que en un futuro cercado ira girando hacia la tendencia y evolución de los "*Cryptocurrencies*", cosa que puede redefinir o cambiar el concepto de la entidad bancaria, partiendo del hecho de que grandes proveedor verticales tecnológicos como Apple, tienen un ojo puesto en este nicho.

Modelo de Cadena de Eliminación de Brechas y PCI DSS:

PCIDSS v1.1	
Principios	**Requerimientos**
Construir y mantener una red segura	Requerimiento 1: Instalar y mantener un cortafuegos y su configuración para proteger la información de tarjetas
	Requerimiento 2: No emplear parámetros de seguridad y usuarios del sistema por defecto
Proteger los datos de tarjetas	Requerimiento 3: Proteger los datos almacenados de tarjetas
	Requerimiento 4: Cifrar las transmisiones de datos de tarjetas en redes abiertas o públicas
Mantener un programa de gestión de Vulnerabilidades	Requerimiento 5: Usar y actualizar regularmente software antivirus
	Requerimiento 6: Desarrollar y mantener de forma segura sistemas y aplicaciones
Implementar medidas de control de acceso	Requerimiento 7: Restringir acceso a la información de tarjetas según "need-to-know"
	Requerimiento 8: Asignar un único ID a cada persona con acceso a computadores
	Requerimiento 9: Restringir el acceso físico a la información de tarjetas
Monitorizar y testear regularmente las Redes	Requerimiento 10: Auditar y monitorizar todos los accesos a los recursos de red y datos de tarjetas
	Requerimiento 11: Testear de forma regular la seguridad de los sistemas y procesos
Mantener una política de seguridad de la información	Requerimiento 12: Mantener una política que gestione la seguridad de la información

Tabla 15. Requerimientos PCI-DSS para la eliminacion de brechas. (Domínguez Torres, 2007)

Dada la alta incidencia durante los últimos tres años de los delitos electrónicos, se han desarrollado iniciativas para una mayor en la prevención de intrusiones cibernéticas específicas a nivel mundial, y una muestra de ello son ***Las señales de la Dirección Australiana (ASD)***, que en Australia respondió adecuadamente al aumento de la actividad de intrusión observada con las "Estrategias para mitigar los blancos de ataque par a las intrusiones cibernéticas. Esta es una lista de 35 estrategias clasificadas en orden de efectividad que las organizaciones pueden implementar para reducir la probabilidad de éxito de una intrusión cibernética dirigida.

Esta estrategia tiene cuatro pilares bien definidos, que pueden agregar un marco de referencia para mitigar los riesgos que comprometen data importante, tanto a nivel privado como público, según se detalla a continuación:

1) Listado de Aplicaciones Seguras.
2) Parchear las Aplicaciones dentro de 48 horas
3) Parchear el sistema operativo dentro de 48 horas
4) Limitar el número de usuarios con privilegios Administrativos

A continuación se muestra un esquema de cómo podría implementarse este esquema y que objetivos de control puede ser reforzados con esta metodología:

Estrategia de Mitigación	Resistencia del Usuario	Costos	Mantenimiento	Ayuda A detectar Intrusiones	Ayuda a Mitigar Ejecuciones de Código	Ayuda a Mitigar la Propagación de Infecciones	Ayuda a Mitigar la Filtración de Datos
Listado de Aplicaciones Seguras o Confiables. Esto para prevenir la ejecución de programas maliciosos o no aprobados, incluyendo archivos DLL, scripts e instaladores de programas desconocidos.	Media	Alta	Media	Si	Si	Si	Si
Parchear las Aplicaciones dentro de 48 horas. Java, visores de PDF, Flash, navegadores de internet, Suites de Ofimática. Siempre deben de estar actualizadas para evitar vulnerabilidades y riesgos.	Baja	Alta	Alta	No	Si	Posible	No
Parchear el sistema operativo dentro de 48 horas. De ser posible siempre utilice la última versión aplicable del sistema operativo. Y actualice constantemente para evitar vulnerabilidades en el sistema. Evite sistemas operativos sin soporte o actualizaciones.	Baja	Media	Media	No	Si	Posible	No
Limitar el número de usuarios con privilegios Administrativos. También dichos usuarios deben de utilizar una cuenta sin privilegios para las tareas que no necesiten dichos privilegios.	Media	Media	Baja	No	Posible	Si	No

Tabla 16. Metodología de los Cuatro Signos Australianos (ASD) (Department Of Defense, 2014)

Desde el punto de vista de la redes, es importante mantener también una rigurosa monitorización de los recursos y actividades, según detallamos a continuación:

Seguridad de las Redes:

Revisar las configuraciones de firewall y asegúrarse de que sólo se permite que los protocolos puertos, servicios e Internet (IP) se está comunicando con la red interna.
Separar las redes de procesamiento de pagos de otras redes.
Aplicar las listas de control de acceso (ACL) en la configuración del router para limitar el tráfico no autorizado a redes de procesamiento de pagos.
Crear ACL con estrictos sistemas de segmentación de cara al público y los sistemas de bases de datos de tarjetas de pago de la casa.
Implementar herramientas de prevención de fuga de datos / de detección para detectar y ayudar a prevenir la exfiltración de datos.
Implementar herramientas para detectar el tráfico de red anómalo y el comportamiento anómalo de los usuarios legítimos (credenciales comprometidos).

Tabla 17. Requerimientos de Protección de la red contra Malware. (US-CERT, 2014)

En cuando a los accesos administrativos, es importante controlar todo acceso privilegiado, en base a las siguientes directrices:

Accesos Administrativos:

Utilizar autenticación de dos factores (2FA por sus siglas en ingles) cuando se accede a la red de procesamiento de pagos. Aun si utiliza una red privada virtual, es importante que este implementado el sistema 2FA, para ayudar a mitigar los ataques por key-loggers o ataque de robo de credenciales.
Limitar los privilegios administrativos a los usuarios y aplicaciones.
Periodicamente revisar el sistema en busca de usuarios desconocidos o no utilizados.

Tabla 18 . Mejores Practicas en cuanto a Accesos Administrativos. (Sanchez, 2014).

Finalmente, luego de que todos los requerimientos de infraestructura y arquitectura estén dispuestos, y se tenga una metodología implementada o parte de esta, es imprescindible el uso de la encriptación de punto a punto (End to End Encryption), ya que convertirse en el proveedor de un servicio comercio electrónico certificado en PCI, envuelve el uso de tecnología avanzada y una seguridad muy estrecha basada en estándares. De ahí que el uso de este tipo de encriptación, sabiéndolo combinar con el protocolo IPv6 puede ofrecer mayores garantías a los usuarios de tarjetas de crédito e información sensitiva de ser atacados, E2EE (End - To - End Encryption) siempre debe estar en el tope de lista cuando se trata de proteger información en tecnologías emergentes de mercaderistas, y para esto se hace necesario el requerimiento PCI DSS 3.0 que encripta las transmisión de un lector de tarjetas a través de redes públicas.

A pesar de todas las medidas de seguridad y metodologías aplicadas en el proceso de prevenir cualquier incidente de seguridad, se debe desarrollar unas políticas de respuesta a incidentes, acompañada de sus correspondientes procedimientos de respuesta y seguimiento, así como análisis forense para determinar los controles fallidos y mejorarlos, según se aprecia a continuación:

Primeras 24 horas:

☑	**Grabar la fecha y hora** del momento en que fue descubierta la brecha, así como también el momento en que fue alertado el equipo de respuesta y se inició la contramedida.
☑	**Alertar y activar a todos** en el equipo de respuesta, incluyendo a los agentes externos, para iniciar la ejecución del plan de contención.
☑	**Asegurar el área** alrededor de donde ocurrió la brecha de datos para preservar la evidencia.
☑	**Detener cualquier pérdida de datos adicional**. Se deben desconectar de la red las maquinas afectadas, pero no deben de ser apagadas hasta que el equipo forense lo indique.
☑	**Documentar todo** lo concerniente a la brecha: Quien la descubrió, quien la reportó, a quien fue reportada, quien más sabe al respecto, que tipo de brecha ocurrió, que se perdió, como se perdió, que sistemas fueron afectados, que dispositivos están perdidos, etc…
☑	**Entrevistar los que están envueltos** en descubrir la brecha y cualquiera que sepa acerca de esta. Documentar la investigación.
☑	**Revisar los protocolos** relativos a la diseminación de información acerca de la brecha para todos los que están envueltos en las etapas iniciales.
☑	**Sopesar las prioridades y riesgos** basándose en lo conocido acerca de la brecha.
☑	**Buscar una compañía forense** para iniciar una investigación profunda de la brecha.
☑	**Notificar a los agentes de la ley,** si es necesario, después de consultarlo con los asesores legales y la administración.

Tabla 19. Pasos a seguir en las primeras 24 horas al momento de una brecha de información. (Sanchez, 2014)

3.2 Las Mejores Prácticas del Modelo y la Estrategia de Prevención Propuesto

Entre las mejores prácticas para la disminución del delito a través del comercio electrónico, podemos citar un mapa de 20 controles críticos importantes para disminuir la ocurrencia de un ataque en comercio electrónico, según se observa a continuación:

1	Inventario de equipos Autorizados y no Autorizados (Laptops, Smartphones, Etc…)
2	Inventario de Programas Autorizados y no Autorizados (Puertas Traseras)
3	Configuraciones seguras de hardware y software en equipos Móviles, Laptops, Estaciones de Trabajo, Servidores.
4	Evaluación continua de Vulnerabilidades y Soluciones
5	Defensas de malware
6	Aplicación de Software de Seguridad
7	Control de Acceso Inalámbrico
8	Capacidad de Recuperación de Datos
9	Habilidades de Seguridad de Evaluación y Capacitación Adecuada para llenar los vacíos
10	Configuraciones seguras para los dispositivos de red tales como cortafuegos, routers y switches
11	Limitación y Control de los puertos de red, protocolos y servicios
12	El uso controlado de privilegios de administración
13	Límites de Defensa
14	Mantenimiento, Monitoreo y Análisis de registros de auditoría
15	Acceso controlado Basado en la necesidad de conocer
16	Cuenta Seguimiento y Control
17	Protección de Datos
18	Respuesta y Gestión de Incidentes
19	Ingeniería de red segura
20	Pruebas de Penetración y Ejercicios de Ataque

Tabla 20. Mapa de los 20 controles críticos de seguridad cibernética (Council On Cybersecurity, 2014)

Pero todas estas actividades de prevención y descubrimiento de patrones de ataque al comercio electrónico, no sirven de nada si no se desarrolla una cultura de Gobierno, Riesgo y Cumplimiento, pues aun con todo ello se podrían seguir presentando fraudes, por lo que resulta importante conocer y estar actualizados con:

- Técnicas de revisión
- Herramientas de análisis
- Crear comités especiales de evaluación
- Capacitarse constantemente
- Instalar sistemas de monitoreo
- Utilizar la mayor cantidad de normas y estándares
- No guardar información sensible ya utilizada.

CONCLUSIONES

En la actualidad, los esfuerzos para frenar el impacto de los posibles riesgos a los que se expone la creciente utilización del comercio electrónico, está basada principalmente en la selección de la plataforma de comercio electrónica y el mantenimiento del cumplimiento de las normas PCI, además de las mejores prácticas mencionadas en el capítulo anterior, orientadas todas a disminuir las probabilidades de ocurrencia de algún incidente, así como prevenir al usuario educándolo al respecto.

Pero hoy día, con los avances y la abismal tendencia a la convergencia de servicios en medios de comunicación móviles, tales como: celulares inteligentes, tabletas, relojes, entre otros; lo cual añade un abanico de oportunidades de fallas y vulnerabilidades en los nuevos sistemas operativos y los servicios para dichos dispositivos, ya que la Norma PCI no está diseñada para frenar intrusiones, y las demás medidas disuasivas quedan del lado de usuario final, y al margen de sus conocimientos.

De igual manera, para nadie es un secreto que tarde o temprano se dejara de utilizar dinero físico, para pasar a utilizar medios electrónicos de pagos más sofisticados y fáciles de usar para el usuario, tal como lo ocurre hoy día con la tarjeta de crédito, pero de una forma más sencilla y flexible. Es por ello que en la última década grandes proveedores de tecnología han desatado una competencia por dominar este nicho del mercado, tal es el caso de: Google Wallet, CurrentC y Apple Pay que logró en apenas 72 horas de su lanzamiento en el mercado captar 1 millón de tarjetas de créditos, y en apenas su primera

semana ya existen más usuarios que en todos los demás competidores de este tipo de pago en los últimos 3 años, al ser altamente acepto para realizar pagos de forma muy sencilla con solo colocar las huellas de tu dedo en la lectora del teléfono y especificando el monto a pagar.

Estos nuevos avances han hecho que los proveedores de tecnologías móviles como Apple, desarrollen tecnologías como Apple Watch, en la que el usuario no necesite utilizar colocar sus huellas para confirmar la transacción, sino que este monitorea los vasos capilares sobre tu piel para confirmar tu pago.

Todas estas tendencias, hacen que los medios de prevención tradicionales y que actualmente están surtiendo efecto para disminuir el riesgo en toda transacción comercial pasaran rápidamente a quedar en desuso, por el vertiginoso avance de la tecnología en este nicho del comercio electrónico.

RECOMENDACIONES

Nuestra sociedad, tanto a nivel de la geografía nacional, así como regionalmente hablando, y por qué no decir; esta pequeña **"*Aldea Global*"** intenta cada vez más interconectar virtualmente todas las actividades económicas y sociales, a través de la transformación continua de las acciones informales a la interactividad de un universo formal donde los objetos concretos y abstractos tienen una real comunicación omnidireccional, proporciona grandes ventajas sociales, así como oportunidades de elevar las garantías de un mejor nivel de vida y confort, pero con ello también se abre un gran número de nuevos retos para proporcionar seguridad en este creciente entorno virtual, llamado Comercio Electrónico.

Es por ello, esta investigación apunta principalmente a crear conciencia sobre el desarrollo de nuevos estilos de pensamientos no tradicionales, donde la convergencia del saber científico se hace necesario para lograr el salto, en el cual los profesionales de las diversas disciplinas de las tecnologías de la información somos llamados a ser los principales actores, en esta transición de lo informal a lo formal, que ha evolucionado partiendo de un mundo análogo, pasando a la sociedad virtual del internet, hasta la sociedad del e-business, y el actual mercadeo digital que se vive hoy día, con resultados concretos entorno a cuatro pilares de interés: a) El *"Internet de las Cosas"*, b) La creciente dependencia a los dispositivos conectados, c) La resiliencia Vs la seguridad, d) Novedad y complejidad de los riesgos de TI.

Inmersos en estas cuatro razones, y apoyados en los avances de la nueva era del negocio digital se supone la difuminación de los mundos físico y virtual, con claros ejemplos como son: la impresión 3D digital, la moneda digital **(*"Cryptocurrencies"*),** resultando en un marco de negocio autónomo, donde se aprovecharían las tecnologías con capacidades **"humanlike" o "humanreplacing",** lo que hace necesario repensar sobre un nuevo esquema con muchos retos tecnológicos y operativos con una palabra clave "**Alineamiento IPv6**", en razón de la alta dependencia en los **Dispositivos Conectados**, para el **2020** tendremos más de **26 Mil Millones** conectados en la red.

Es conveniente considerar la **Resiliencia versus Seguridad, debido a que** el Internet fue concebido pensando en al **Resiliencia**, no en la **Seguridad**, y hasta ahora, los defensores han ganado la batalla e Internet sigue siendo un medio confiable, pero tal vez estamos frente a una generación de tecnologías disruptivas en las que los atacantes finalmente ganen. (World Economic Forum, 2014)

En este sentido, se recomiendan las directrices para mantener la ciberseguridad, las cuales son:

1. Toma de conciencia de la importancia de la ciberseguridad.
2. Coordinar el trabajo entre las tres líneas de defensa: Auditoría Interna, Administración del Riesgo, y Gobernabilidad.
3. Revisiones continuas.
4. Alineamiento de todos los procesos del negocio con la ciberseguridad.

REFERENCIAS BIBLIOGRÁFICAS

- Alexa Internet, Inc. (05 de 12 de 2014). *Alexa Internet, Inc*. Obtenido de Alexa: http://www.alexa.com/topsites/countries/DO
- Archive.org. (2006). *Wayback.Archive.org*. Obtenido de Wayback.Archive.org: http://wayback.archive.org/web/20060613144029/http://www.eanrd.org.do/main.asp
- Bigcommerce. (2014). *Bigcommerce Pty. Ltd.* Obtenido de Bigcommerce: https://www.bigcommerce.com/
- Bishop, E. (2014). *KISSmetrics*. Obtenido de A BLOG ABOUT ANALYTICS, MARKETING AND TESTING: https://blog.kissmetrics.com/stop-ecommerce-fraud/
- Chiovenda, G. (1940). Instituciones De Derecho Procesal Civil. En G. Chiovenda, *Instituciones De Derecho Procesal Civil* (pág. 265). Madrid: Revista de Derecho Privado.
- Collado Vilorio, C. A. (05 de 12 de 2014). Solicitud de Informacion acerca del Comercio Electronico. (E. Valenzuela, Entrevistador) Obtenido de www.
- Council On Cybersecurity. (2014). *The Critical Security Controls for Effective Cyber Defense.* Obtenido de Sans: https://www.sans.org/critical-security-controls/
- Damaras Limited. (2014). *Damaras Limited*. Obtenido de Payza: http://www.payza.com/
- Department Of Defense. (February de 2014). *Mitigation Strategies 2014.* Obtenido de Australian Signals Directorate: http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf
- DICAT. (2006). Estadistica de los casos resueltos 2005-2006.
- DICAT. (2014). *Estadística de los Casos Resueltos por el DICAT en el periodo 2007 - 2008.*
- DICAT. (2014). *Estadística de los Casos Resueltos por el DICAT en el periodo 2009 - 2010.*
- DICAT. (2014). *Estadística de los Casos Resueltos por el DICAT en el periodo 2011 - 2012.*
- DICAT. (2014). *Estadística de los Casos Resueltos por el DICAT en el periodo 2013-2014.*

- Domínguez Torres, M. Á. (Septiembre de 2007). *http://www.isecauditors.com/*. Obtenido de Internet Security Auditors: http://www.isecauditors.com/sites/default/files/files/SIC-76_PCI-DSS_Como_cumplir.pdf
- DPD. (2014). *Portal Labs*. Obtenido de DPD - Digital Product Delivery: http://getdpd.com/
- Ebay Inc. (2014). *Ebay Inc.* Obtenido de Magento: http://magento.com/
- El Nuevo Diario. (10 de 04 de 2007). *El Nuevo Diario*. Obtenido de El Nuevo Diario: http://www.elnuevodiario.com.do/app/article.aspx?id=53328
- El.Economista. (28 de Mayo de 2012). *Periódico El Economista S.A.* Obtenido de http://eleconomista.com.mx/: http://eleconomista.com.mx/podcast/banca-linea/2012/05/28/conoce-las-ventajas-comercio-electronico
- FoxyCart, LLC. (2014). *FoxyCart, LLC*. Obtenido de FoxyCart!: http://www.foxycart.com/
- GS1 Dominicana. (2010). *GS1 Dominicana*. Obtenido de GS1 Dominicana: http://www.gs1rd.org.do/index.php/gs1-dominicana/historia
- GS1 Dominicana. (2014). *GS1 Dominicana*. Obtenido de GS1 Dominicana: http://www.gs1rd.org.do/
- INDOTEL. (30 de Marzo de 2005). *INDOTEL*. Obtenido de Instituto Dominicano de las Telecomunicaciones: http://www.indotel.gob.do/index.php/cgblog/393/INDOTEL-elabora-anteproyecto-de-ley-sobre-Crimenes-y-Delitos-de-Alta-Tecnologia
- inkFrog, Inc. (2014). *inkFrog, Inc.* Obtenido de Highwire: http://www.highwire.com
- Manzueta Espaillat, V. (11 de 04 de 2007). *presenciahoy*. Obtenido de presenciahoy: http://presenciahoy.blogspot.com/2007/04/aprueban-proyecto-contra-crmenes-y.html
- *Marketing y Comercio Electrónico*. (25 de Junio de 2012). Obtenido de karinsofia14: http://karinsofia14.wordpress.com/
- Núñez Campusano, E. (12 de Mayo de 2012). *Elisa Núñez Campusano*. Obtenido de http://elisanunezcam.blogspot.com/2012/12/derecho-informatico-penal.html
- Organización Mundial del Comercio. (05 de 12 de 2014). *Organización Mundial del Comercio*. Obtenido de Organización Mundial del Comercio: http://www.wto.org/spanish/thewto_s/whatis_s/inbrief_s/inbr00_s.htm

- osCommerce. (2014). *osCommerce*. Obtenido de osCommerce: http://www.oscommerce.com
- PUCMM. (05 de 12 de 2014). *NIC.DO*. Obtenido de NIC.DO: http://nic.do/noticias/NICDOInforma.php3
- Real Decreto Legislativo . (1996).
- Sanca, F. D. (2013). Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español : una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau. En F. D. Sanca, *Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español : una propuesta para su implementación en el ordenamiento jurídico de Guinea-Bissau.*
- Sanchez, J. (2014). *ISACA.* Obtenido de ISACA: http://www.isaca.org/education/conferences/documents/naisrm/241.pdf
- Sánchez, M. (14 de Agosto de 2014). *Prensa Popular SAC*. Obtenido de Gestión: http://gestion.pe/tecnologia/payu-latam-fraude-electronico-inherente-todas-transacciones-financieras-empresas-2105601
- Shopify. (2014). *Shopify*. Obtenido de http://www.Shopify.com
- Stripe. (2014). *Stripe*. Obtenido de Stripe: http://www.stripe.com
- TuAbogadoDefensor. (s.f.). *Tu Abogado Defensor*. Obtenido de http://www.tuabogadodefensor.com/proteccion-comercio-electronico/#
- US-CERT. (31 de July de 2014). *United States Computer Emergency Readiness Team (US-CERT)*. Obtenido de https://www.us-cert.gov: https://www.us-cert.gov/ncas/alerts/TA14-212A
- Volusion, Inc. (2014). *Volusion, Inc*. Obtenido de Volusion: http://www.volusion.com/
- World Economic Forum. (2014). *Global Risks.*

ANEXOS

ESCUELA DE GRADUADOS

Anteproyecto Final para Optar por el Titulo de:

Maestría en Comercio Electrónico

Título:

Modelo y Estrategia de Prevención de Delitos en el Comercio Electrónico

Sustentado Por:

Nombre:	**Matrícula:**
Licurgo E. Yunes Pérez	**2013-0711**

Asesor (a):

Sanción Raquel Zorob Ávila

Santo Domingo, República Dominicana
Diciembre, 2014

TABLA DE CONTENIDO

CAPITULO 1. SELECCIÓN Y DEFINICIÓN DEL TEMA DE INVESTIGACIÓN

Título de la investigación:

Modelo y estrategia de prevención de fraudes en el comercio electrónico de República Dominicana.

Definición del tema de investigación:

Fraude: es una acción que resulta contraria a la verdad y a la rectitud. El fraude se comete en perjuicio contra otra persona o contra una organización (como el Estado o una empresa). (Definicion.de, http://definicion.de/fraude/, s.f.)

Fraude Electrónico: Delito informático, caracterizado por la utilización de un medio de procesamiento electrónico, con el fin de adquirir información confidencial de los usuarios de un sistema. (Castillo, Ortega F, & Vargas J)

Modelo de Prevención: Se refiere al conjunto de parámetros y directrices aplicados prevenir y mitigar una amenaza potencial.

Comercio Electrónico: consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas.

Internet: es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP. (Definicion.de, http://definicion.de/internet/, s.f.)

CAPITULO II. PLANTEAMIENTO DEL PROBLEMA DE LA INVESTIGACION

Desde sus inicios, el cibercrimen no actuaba con fines de daño ni con fines de lucro, sino con intención de desafiar la seguridad de los sistemas y puramente satisfacción de ego. Luego de unos años la misma evolución de los comercios y de la tecnología llevó a los que realizaban estas prácticas a realizar ataques con fines de lucro para beneficio propio o bien de otra organización.

El día de hoy las amenazas han evolucionado de una manera que los ataques se hacen más sofisticados y dirigidos a objetivos específicos atentando directamente a los negocios que ofrecen sus servicios mediante el comercio electrónico.

La práctica del ciberdelito es un negocio que dio paso a una economía clandestina que crece cada día más. Los mismos delitos y fraudes tradicionales que se realizaban en las transacciones físicas y personales, ahora han evolucionado para adaptarse al comercio electrónico.

Durante los últimos años la tecnología ha presentado una penetración importante en República Dominicana disminuyendo cada día más la brecha digital. Este ha dirigido a que los comercios evolucionen junto con la tecnología orientando sus negocios al comercio electrónico. Este avance se traduce en términos de eficiencia en la comercialización, tiempo de respuestas más rápido que las negociaciones de manera física, así como también en términos de costos en la gran mayoría de los casos.

El comercio electrónico de igual forma puede resultar de alto beneficio crear oportunidades en nuevos y mejores servicios a los clientes. Sin embargo, todas estas ventajas vienen de la mano con riesgos potenciales inherentes a la tecnología. Los sistemas electrónicos y la infraestructura que le da soporte al comercio electrónico son susceptibles de situaciones de mal uso, fallas y ataques en muchas de sus formas. Esto afecta directamente en las transacciones B2B, C2B y C2C, incluyendo a todas las partes que participan en ellas.

Los riesgos de ataques cibernéticos constituyen una realidad ineludible en el mundo de la información y los sistemas informáticos. El uso de Internet y las redes sociales como sistema de comunicación, tanto por parte de empresas como de usuarios individuales, esconde peligros difíciles de reconocer a simple vista.

Las empresas que desarrollan su negocio en las redes sociales pueden acceder a un universo de usuarios mucho más amplio a través de estos nuevos canales de difusión y publicidad. Los datos cedidos por estos usuarios son almacenados de manera inmediata, quedando a disposición de los ataques de ciberdelincuentes que venden esta valiosa información o la utilizan para lucro propio.

Las operaciones en el comercio electrónico constituyen transacciones habituales y aceptadas por la mayoría de los usuarios en su día a día, por lo que las empresas deben crear un entorno de seguridad adecuado y proteger los datos que los usuarios les han confiado.

Actualmente en nuestro país están teniendo auge las tiendas online de intercambio entre clientes finales (C2C), como es el caso de eMarket, LaPulga, SuperCarros, SuperCasa, entre otros. Muchas de ellas en ocasiones han sido afectadas por ciberdelicuentes que aprovechan brechas de seguridad para poner en riesgo las operaciones del negocio y los datos de los clientes, así como también clientes mal intencionados que aprovechando la facilidad del anonimato en los canales eléctricos, se valen de técnicas de engaño a alguna de las partes de las transacciones, ya sea proveedor o cliente.

FORMULACION DEL PROBLEMA

¿A qué se debe el aumento considerado del fraude electrónico en la Republica Dominicana durante el año 2014?

SISTEMATIZACION DEL PROBLEMA.

¿Cuáles son las causas del aumento del Fraude Electrónico?

¿Qué consecuencias produce el Fraude Electrónico?

¿Cómo afecta el fraude a los usuarios del Comercio Electrónico?

¿Cómo incide en la Economía el Fraude Electrónico?

CAPITULO III. OBJETIVOS DE LA INVESTIGACIÓN

3.3 Objetivos General:

Analizar la necesidad de una propuesta de prevención de fraudes electrónicos, que mitiguen los riesgos y amenazas del comercio electrónico en los negocios electrónicos en la empresa en la Republica Dominicana, durante el año 2014.

3.4 Objetivos Específicos:

- Caracterizar los delitos electrónicos que inciden en el comercio electrónico. (pasado)

- Elaborar un modelo y estrategia de prevención de fraudes según las áreas de incidencia del comercio electrónico de la Republica Dominicana. (presente)

- Valorar la pertinencia del modelo y la estrategia en la prevención en el fraude del comercio electrónico en la Republica Dominicana.

CAPITULO IV. JUSTIFICACIÓN DE LA INVESTIGACIÓN

4.1 Justificación Teórica

La prevención del ciberdelito ante el comercio electrónico es fundamental para la empresa que ofrezcan sus productos o servicios online, ya que asegura la reputación de su marca y garantiza la fidelización de sus clientes. Dentro de los diferentes tipos de fraudes que se pueden prevenir mediante la implementación de un modelo tales como: Phishing, Malvertising y el Robo de identidad. Para la realización de esta investigación de manera teórica se utilizaran, libros, revistas, artículos, documentos, páginas web, entre otros.

4.2 Justificación Metodológica

Asegurar que la información sensible de los clientes dentro de su plataforma electrónica tenga controles que minimicen el riesgo de las informaciones de sus clientes, para evitar que sean víctimas de una de las modalidades del ciberdelito que en gran porcentaje, escapan de la capacidad técnica implantada por el comercio. Además de las debilidades técnicas que pueda presentar cualquier negocio que provea servicios sobre la plataforma del comercio electrónico, también existen amenazas latentes que se valen de técnicas de engaño directamente a los usuarios de la plataforma. Utilizando las mejores prácticas de seguridad a la hora de implementar seguridad en el comercio electrónico, como son: OWAP, PCI, etc.

4.3 Justificación Práctica

PARA QUE SIRVE…T DE DECISIONES… BENIFICIOS

A través de la investigación que se realice se ofrecerá una propuesta sobre cómo reducir o mitigar los fraudes que afectan el comercio electrónico y así ofrecer a usuarios y a empresas, las mejores prácticas para reducir considerablemente los fraudes que hoy en día afectan a la sociedad dominicana en general que usa dicho servicio como un medio más viable para obtener productos y servicios.

CAPITULO V. MARCO DE REFERENCIA

5.1 Marco Teórico

EL FRAUDE ELECTRONICO.

"Para Patrick Caín, miembro del APWG, los ataques phishing se convirtieron en una de las más peligrosas amenazas que acechan a los internautas. Los mismos consisten en el uso de falsos mensajes de correo electrónico, pop ups (o ventanas emergentes) y sitios web, con el objetivo de conseguir datos financieros de los usuarios, tales como números de cuentas y tarjetas de crédito, contraseñas o PIN". (AEempresarial.com, s.f.)

El phishing es uno de los delitos que más afectan actualmente al comercio electrónico, y uno de los más difíciles de erradicar, ya que no vulnera procesos técnicos, sino que ataca y vulnera directamente a las personas, es decir, que se vale de mecanismos de manipulación y engaño para que los mismos usuarios garanticen su efectividad.

LA CIBERDELINCUENCIA.

La ciberdelincuencia se define con carácter general como cualquier tipo de actividad ilegal en la que se utilice Internet, una red privada o pública o un sistema informático doméstico. Aunque muchas formas de ciberdelincuencia giran en torno a la obtención de información sensible para usos no autorizados, otros ejemplos son la invasión de la intimidad del mayor número posible de usuarios de ordenadores. La ciberdelincuencia comprende cualquier acto criminal que utilice ordenadores y redes. (BullGuard, n.d.)

Otro elemento importante es que la ciberdelincuencia ya no busca satisfacción al tener éxito en los ataques, sino en el beneficio lucrativo de los mismos. El factor principal que movilizar la maquinaria que bombardea el comercio electrónico de trampas de fraude, es el beneficio económico resultante de los mismos.

5.2 Marco conceptual

Comercio Electrónico: Consiste en la compra y venta de productos o de servicios a través de sistemas electrónicos, tales como Internet y otras redes informáticas. (Asociación Española de la Economía Digital, 2012)

Marketing Digital: Es la aplicación de las estrategias de Marketing en los medios digitales apoyándose en las plataformas Tecnológicas y las Redes Sociales con el propósito de expandir sus mercados y aumentar su potencial competitivo. (Editorial Vértice, 2011)

Internet: conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. (Definicion.de, http://definicion.de/internet/, s.f.)

Dominio de Internet: Es una forma de identificación que está asociada a un grupo de computadoras conectadas a Internet. El propósito de los nombres de dominio de Internet y del sistema de nombres de dominio (DNS) es traducir una dirección IP (Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz de un dispositivo habitualmente una computadora dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP.) de cada computadora conectada a ellos a términos fáciles de encontrar. Este tipo de abstracción posibilita que cualquier servicio de red pueda moverse de un lugar a otro en la red. (Okhosting.com, s.f.)

Phishing: El phishing consiste en el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales. El caso más típico de phishing es el envío de correos electrónicos que se hacen pasar por procedentes de una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falseada. (Antivirus.interbusca.com, s.f.)

Malware: es un código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario y robar información. El software se considera malware en función de los efectos que, pensados por el creador, provoque en un computador. El término malware incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables. (Ciencialuz.bligoo.com.mx, s.f.)

Sistemas de Información: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. En este caso refiere a sistemas informáticos que almacenan dicha información. (Significados.com, s.f.)

Malvertising: Programa malicioso que se oculta en publicidades en páginas de terceros para infectar malware.

CAPITULO VI. ASPECTOS METODOLOGICOS

6.1 Propósito de la Investigación: Aplicada

Con el fin de alcanzar los objetivos específicos, la investigación será aplicada sobre las bases del objetivo general, enfocado en desarrollar un modelo de prevención ante el ciberdelito que afecta el comercio electrónico, principalmente orientado al robo de información sensible, sabotaje y estafa, valiéndose de técnicas de seguridad informática, la aplicación de políticas y mejores prácticas de éxito.

6.2 Tipo de Estudio:

6.2.1 Exploratorio

Ya que a través de la problemática planteada se va a buscar alternativas mediante las mejores prácticas conocidas al respecto y documentación que permita conocer de manera profunda la mitigación del problema.

6.2.2 Descriptivo.

Porque a través de las distintas investigaciones realizadas por el Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología de la Policía Nacional, se va a conocer las características de la población que realiza los fraudes, así como las características que afectan los delitos en el comercio electrónico en el país.

Así como se realizaran algunas entrevistas a expertos conocedores del tema para poder demostrar junto con los resultados de las investigaciones realizadas los objetivos planteados en la investigación.

6.2.3 Explicativo.

Se analizaran y explicaran las respuestas de las entrevistas que se realicen, así como los distintos cuadros y gráficos que se obtengan de las investigaciones mensuales obtenidas durante el año 2014.

6.3 Metodología de Investigación

6.3.1 Métodos:

6.3.1.1 Observación. A lo largo de toda la investigación se estará realizando una observación directa participante para poder demostrar los distintos fraudes que se están realizando a través del comercio electrónico.

6.3.1.2 Inducción - Deducción. Debido a que la investigación es tanto teórica como práctica, unas veces se partirá de principios particulares para poder generalizar y otras veces será viceversa, es decir, se parte de una idea general para poder llegar a obtener resultados particulares y específicos.

6.3.1.3 Análisis - Síntesis. A través de los análisis exhaustivo de las investigaciones y de las investigaciones del año 2014 y las entrevistas que se realicen a los expertos se podrán presentar los datos estadísticos que van apoyar la investigación los fraudes electrónicos.

6.4 Técnicas y procedimientos

En cuanto a las fuentes documentales a ser utilizada en el trabajo final, las mismas serán tanto primaras, tales como libros, revistas, documentos, entre otras, como secundarias tales como, enciclopedias, diccionarios, informes de investigación, leyes, ya que ambas son valederas en este tipo de investigación. Respectos a las técnicas que se utilizaran, al ser una investigación retrospectivas se analizaran de manera detalladas, existente en la institución durante el año 2014, así como se realizara una entrevistas a dos expertos con **10 preguntas** abiertas para que puedan explicar detalladamente los objetivos de la investigación sobre el fraude electrónico.

6.5 Tratamiento de la información

La información recopilada en las investigaciones existentes, se codificara, se tabulará y se analizara cada una de ellas. En cuantos a las entrevistas se analizara cada una de las preguntas para comparar las respuestas de las personas entrevistadas.

CAPITULO VII. TABLA DE CONTENIDO.

CAPITULO VIII. REFERENCIAS BIBLIOGRÁFICAS

- Anonimo. (s.f.). *Los Tiempos*. Obtenido de Tendencia: más comercio electrónico y cibercrimen: http://www.lostiempos.com/observador-economico/tendencias-observador-economico/tendencias/20131203/tendencia-mas-comercio-electronico-y-cibercrimen_237150_514773.html
- Asociación Española de la Economía Digital. (2012). *Libro blanco del comercio electrónico : guía práctica del comercio electrónico para Pymes.* Madrid, España: Asociación Española de Economía Digital.
- Editorial Vértice, S. (2011). *Marketing Digital.* Málaga, España: Vértice.
- Fernández, B. (2014). *Ambito*. Obtenido de http://www.ambito.com/diario/noticia.asp?id=736264
- http://www.antivirus.interbusca.com (s.f.). *PHISHING* Obtenido de http://www.antivirus.interbusca.com/glosario/PHISHING.html
- idconline. (2009). idconline. Obtenido de Ciberdelito, mal del comercio electrónico: http://www.idconline.com.mx/juridico/2010/12/09/ciberdelito-mal-del-comercio-electronico
- KPMG. (s.f.). *KPMG*. Obtenido de http://www.uazuay.edu.ec/bibliotecas/e-marketing/E-Commerce%20and%20Cyber%20Crime.pdf
- Maggiore, M. L. (2013). Proyecto Amparo. Obtenido de http://www.proyectoamparo.net/files/ciberdelito_lac_lacnic_amparo_estudios2013_completo_vfinal.pdf

- Marcelo Héctor González, C. (2000). ISACA. Obtenido de Comercio Electrónico: La nueva perspectiva de los negocios: http://www.isaca.org/Journal/Past-Issues/2000/Volume-6/Pages/Comercio-Electronico.aspx
- Mayur Patel, N. P. (s.f.). Rimtengg . Obtenido de http://www.rimtengg.com/iscet/proceedings/pdfs/adv_nw_tech/21.pdf
- Pozerski, J. (2009). astaro. Obtenido de http://www.astaro.com/blog/security-perspectives/cybercrime-and-its-affect-on-e-commerce
- Prandini, P. (2011). sadvisor. Obtenido de http://www.sadvisor.com/downloads/webcrimen.pdf
- PWC. (s.f.). PWC. Obtenido de http://www.pwchk.com/webmedia/doc/634648119386924897_rcs_ecom_cybercrime_feb2012.pdf
- Shaw, F. (2013). Computing. Obtenido de http://www.computing.es/seguridad/opinion/1066318002501/cibercrimen-problema-acuciante-empresas.1.html
- Voigt, K. (s.f.). CNN. Obtenido de http://edition.cnn.com/2009/TECH/12/13/cybercrime.2009.review/index.html#cnnSTCText
- BullGuard. (s.f.). *http://www.bullguard.com/*. (BullGuard) Obtenido de http://www.bullguard.com/es/bullguard-security-center/internet-security/security-tips/cybercrime.aspx
- Castillo, J., Ortega F, S., & Vargas J, D. (s.f.). Fraude Electronico. Obtenido de scribd.com: https://es.scribd.com/doc/5985552/Fraude-Electronico

- Ciencialuz.bligoo.com.mx. (s.f.). *http://ciencialuz.bligoo.com.mx/malware#.VHvKcjHF99M*. Obtenido de http://ciencialuz.bligoo.com.mx/malware#.VHvKcjHF99M: http://ciencialuz.bligoo.com.mx/malware#.VHvKcjHF99M
- Definicion.de. (s.f.). *http://definicion.de/fraude/*. Obtenido de http://definicion.de/fraude/: http://definicion.de/fraude/
- Definicion.de. (s.f.). *http://definicion.de/internet/*. Obtenido de http://definicion.de/internet/: http://definicion.de/internet/
- Editorial Vértice, S. (2011). *Marketing Digital.* Málaga, España: Vértice.
- http://www.antivirus.interbusca.com. (s.f.). *http://www.antivirus.interbusca.com/glosario/PHISHING.html*. Obtenido de http://www.antivirus.interbusca.com/glosario/PHISHING.html: http://www.antivirus.interbusca.com/glosario/PHISHING.html
- http://www.significados.com. (s.f.). *http://www.significados.com/sistema/*. Obtenido de http://www.significados.com/sistema/: http://www.significados.com/sistema/
- Okhosting.com. (s.f.). *http://okhosting.com/dominios-web/que-es-dominio-web-funcion-y-definicion*. Obtenido de http://okhosting.com/dominios-web/que-es-dominio-web-funcion-y-definicion: http://okhosting.com/dominios-web/que-es-dominio-web-funcion-y-definicion