ANÁLISIS DE EMERGENCIAS CIBERNÉTICAS QUE SE PRESENTAN EN LAS CIUDADES DE TUNJA, DUITAMA Y SOGAMOSO CON RESPECTO AL RESTO DEL PAÍS EN LOS ÚLTIMOS 2 AÑOS

DIANA MARÍA ORDUZ BARRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SOGAMOSO
2018

ANÁLISIS DE EMERGENCIAS CIBERNÉTICAS QUE SE PRESENTAN EN LAS CIUDADES DE TUNJA, DUITAMA Y SOGAMOSO CON RESPECTO AL RESTO DEL PAÍS EN LOS ÚLTIMOS 2 AÑOS

DIANA MARÍA ORDUZ BARRERA

Trabajo de monografía para optar al título de
Especialista de Seguridad Informática

Director
CHRISTIAN REYNALDO ANGULO RIVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SOGAMOSO
2018

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

1. FORMULACIÓN DEL PROBLEMA

¿En la ciudad de Tunja, Duitama y Sogamoso se han presentado emergencias cibernéticas y cuentan con estrategias de manejo de estos riesgos al compararlas con situaciones semejantes en el resto del país?

RESUMEN

En la presente monografía se explican los términos y definiciones sobre ciberseguridad y cibercrímen, además de las incidencias que han tenido en el departamento de Boyacá, especialmente en las ciudades de Tunja, Duitama y Sogamoso. De igual modo, se realiza un diagnóstico en estas tres ciudades, interactuando con diferentes entidades de carácter público y privado, interrogándolas sobre la percepción que tienen acerca de un tema tan delicado e importante, que en los últimos tiempos no solo toca a un grupo específico de personas sino a la comunidad o por decirlo mejor a toda una nación, y que por su desconocimiento puede generar pérdidas materiales, económicas y sociales.

También, las maneras de prevenir y promover las diferentes medidas de seguridad que se deben tener en un entorno digital. Al igual que las diferentes leyes que rigen en Colombia para las personas que incurran en delitos informáticos, la forma en la que Colombia ha venido implementando el Estrategia de Gobierno en Línea, y con la cual se pone en el mismo nivel de muchos países, logrando dar bienestar a la nación tecnificando procesos a través de internet para facilitar la vida de las personas y tener a la mano cualquier proceso que anteriormente solo se relacionaba con trámites de mucho tiempo.

2. JUSTIFICACIÓN

Con todos los cambios constantes en el cual el mundo está expuesto y dado que es importante estar a la par con el desarrollo de la tecnología para poder ser competitivos en un mercado global, para ser posible ingresar en un entorno digital es tan necesario conocer los procesos, normas y especificaciones técnicas como también los riesgos a los cuales se está expuesto. Para lograr evitarlos y prevenirlos con un plan de manejo de riesgos y continuidad de un evento en caso de llegar a presentarse. Adicionalmente, no solo se deben tener en cuenta estos aspectos para un campo comercial sino también dentro de una comunidad, lograr la protección del entorno social, familiar, ya que esta es la base de una sociedad, y puede generar pérdidas económicas el desconocimiento de ciertas normas y procesos

De ese modo, el motivo de realizar la investigación radica en el incremento de delitos cibernéticos a nivel nacional, tal como se puede evidenciar en información confidencial suministrada por un investigador de una entidad pública que controla estos aspectos y el falta de conocimiento de la comunidad en denunciar ante la entidad que brindan los mecanismos para crear planes de contingencias que protejan a la sociedad. De esa manera, determinar si estos casos están en aumento, ya que por falta de dichas denuncias se vive en desconocimiento y esto genera que con más frecuencia se expongan a crímenes cibernéticos, así que es de gran importancia establecer por cuáles delitos informáticos puede verse afectada la comunidad para lograr establecer y definir los posibles procesos para contrarrestar estos delitos y verificar las vulnerabilidades a las que se expone la comunidad.

Otro punto de gran importancia son las normas y políticas de ciberseguridad y ciberdefensa que tiene el país para apoyo a los diferentes incidentes que se han presentado en el campo de la tecnología, y se crean diferentes organismos de protección para crear un entorno digital seguro en el cual de acuerdo a todos los adelantos tecnológicos, lo que logra fortalecer un entorno político, económico y social, respetando y dando a conocer las normas, especialmente la Ley 1581 de 2012 de protección de datos personales. Para esto, se toman las tres principales ciudades del departamento de Boyacá: Tunja, Duitama y Sogamoso, con el fin de poder entender y analizar en cada una de acuerdo a su población y desarrollo social, tecnológico y económico, las posibles amenazas y casos presentados en estas ciudades y poder determinar si se puede ofrecer a la comunidad un espacio digital seguro”.

Así, al poder reconocer que las tres principales ciudades del departamento han presentado casos de delitos informáticos, se pueden tomar las medidas necesarias para proteger de futuras amenazas y generar una alerta a las autoridades competentes para que continúen ejerciendo la educación a la comunidad en pro de prevenir esta clase de alertas, puesto que por ser una región tranquila en la cual nunca se han presentado emergencias a gran escala no se está exento de que puedan suceder; incluso sobre algo tan común como delitos financieros , todavía la

población desconoce el tema y no logra dimensionar el riesgo al cual están expuestos.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Analizar las emergencias cibernéticas que se presentan en los municipios de Tunja Duitama y Sogamoso, y realizar un paralelo con el resto del país.

3.2. OBJETIVOS ESPECÍFICOS

- Recopilar información necesaria de toda la documentación que lleve a sustentar la ciberseguridad y los cibercrímenes.

- Identificar planes de control de incidentes cibernéticos que hay en las ciudades de Tunja, Duitama y Sogamoso.

- Definir ¿cuáles son los principales incidentes cibernéticos en las ciudades de Tunja, Duitama y Sogamoso?

- Realizar un diagnóstico a una muestra de la población de estudio relacionadas con incidentes cibernéticos que se presentan en las ciudades de Tunja. Duitama y Sogamoso.

- Realizar un informe que permita evidenciar incidentes informáticos que se presentan en Tunja, Duitama y Sogamoso, y presentar sugerencias y recomendaciones

4. MARCO DE REFERENCIA

4.1. MARCO TEÓRICO

No es necesaria una falla técnica para entrar en un sistema de información, en la mayoría de los casos de crímenes cibernéticos, al intentarlo con ingeniería social, es mucho más fácil y así lograr obtener todo de una manera sencilla y sin violencia, así estemos hablando de un delito. Las políticas de seguridad de la información o los controles no garantizan la protección total de la información, por si solos, los servicios, los sistemas de información, o las redes. Se puede presentar que existan vulnerabilidades residuales después de hacer algunos controles y pueden hacer que la seguridad de la información sea ineficaz, y son posibles los incidentes de seguridad de la información.

Puede afectar comercialmente y económicamente a una organización indirecta o directamente. Además, pueden ocurrir nuevos casos de amenazas que no se hayan identificado con anterioridad. La poca o mínima preparación por parte de una organización para enfrentar este tipo de incidentes hace aumente el grado de impacto comercial potencialmente negativo. Por lo tanto, es esencial para cualquier organización seria acerca de la seguridad de la información tener un enfoque estructurado y planificado para realizar lo siguiente:

- Detectar, informar y evaluar los incidentes de seguridad de la información; responder a incidentes de seguridad de la información, activar controles apropiados para la reducción, prevención y recuperación de los impactos (por ejemplo, en el apoyo a las áreas de gestión de crisis).

- Reportar vulnerabilidades de seguridad de la información que no han tenido la suficiente incidencia para causar eventos de seguridad de la información y posiblemente incidentes de seguridad de la información, y evaluarlos y tratarlos apropiadamente.

- Aprender de los incidentes y vulnerabilidades de seguridad de la información, para que la gestión de incidentes de seguridad de la información, de puedan instituir control y tener conocimientos para poder prevenirlos y de algún modo atacarlos.

De ese modo, para el manejo legal en Colombia existen entidades que protegen y vigilan la integridad de los colombianos como es el DNI (Departamento Nacional de Inteligencia), cuya misión es “PRODUCIR INTELIGENCIA ESTRATÉGICA Y CONTRAINTELIGENCIA DE ESTADO en el ámbito nacional e internacional, desde

una perspectiva civil, orientada al cumplimiento de los fines esenciales del Estado, con fundamento en el respeto a la dignidad humana"[1].

En Latinoamérica, Colombia es uno de los países que cuenta con un comando de seguridad cibernética. Al incursionar en la revolución digital, el Caribe y América Latina, la región es el cuarto mayor mercado móvil del mundo, tanto que la mitad de la población usa internet y el volumen de compras por internet aumentan a grandes pasos.

Ahora bien, en la Fiscalía de las ciudades de Tunja, Duitama y Sogamoso existe una oficina llamada delitos informáticos, esta tiene a cargo algunos de los delitos que se presentan cuando sustraen dinero de las cuentas bancarias, para compras sin autorización de los tarjetahabientes, algunos de los casos en su mayoría buscan que tengan montos altos de dinero para comprar tiquetes de aviones o productos por internet. Otros se dan mediante engaños que hacen clonación de la tarjeta débito o que son engañados en la misma entidad bancaria. Algunos más son delitos contra la libertad que los maneja el Gaula, tales como la extorsión.

Cabe señalar que el inicio del proceso para determinar un delito informática se inicia con la actuación judicial por denuncia de la persona o de redes de *hackers* que están en Boyacá, se comienza de oficio como fiscalía y hay diferentes *modus operandi* de las redes que violan la seguridad informática de los bancos

4.1.1. Análisis del cibercrímen[2]

La evolución de las TIC va enlazada en los últimos años con la cibercriminalidad, en ocasiones no se dimensionan los riesgos que puede tener y en otras ocasiones se exagera. Han pasado más de 30 años desde que se conoció el cibercrímen y sus actores, pero para algunas entidades parece novedoso este tema y en gran proporción incomprendido. La aparición de cibercrímenes sociales convierte a cualquier persona vulnerable a ser víctima de estos, ya que por el hecho de compartir información en la red, fotos y datos personales están expuestos a un ciberataque personal, cibercrímen ideológico o político, ciberterrorismo o hacktivismo.

[1] DIRECCIÓN NACIONAL DE INTELIGENCIA. Misión y Visión. {En Línea}. s.f. Disponible en: http://www.dni.gov.co/index.php?idcategoria=51. párr. 1

[2] CENTRO CIBERNÉTICO POLICIAL. Informe amenazas de cibercrímen en 2016-2017. Bogotá, D.C.: Cairvirtual. 2017.

4.1.2. Caracterización del cibercrímen[3]

Cambio de selección de víctimas de personas a empresas público – privadas. Un incremento en el volumen de operaciones que afectan empresas como el sector financiero, en donde si el nivel de seguridad es más alto el volumen de ataque también aumenta.

Nuevas plataformas de comercio para ser utilizadas a través pishing. Hay una relación directa con el aumento del *e-commerce*, así lo demuestra el "Tercer Estudio de Transacciones no Presenciales 2015 y el estudio de Hábitos de comprador Online 2016"[4] presentado por la Cámara de Comercio Electrónico, donde señaló que el 76% de los internautas compraron al menos una vez en línea.[5]

Servicios del gobierno electrónico como vector de ataque para la distribución de malware. Con la estrategia implementada llamada Gobierno en Línea para dar trasparencia, seguridad y participación en las TIC, se ha generado que cibercriminales utilicen entidades estatales para enviar correos con archivos adjuntos que resultan ser *malware* que afectan los equipos logrando ver toda la información de la víctima. [3]

Estafa a través de BEC (*Business Email Compromise*). Es una modalidad de fraude para las empresas que realizan transferencias electrónicas para pagar productos o servicios.

Vinculación de ciudadanos extranjeros en crímenes informáticos. Esta modalidad se presenta en la clonación de tarjetas débito y crédito de entidades financieras y llegan bandas internacionales a cometer este tipo de delitos en el país.

Presencia de usuarios colombianos en *Deep Web*. *Deep Web* es "la parte de internet que no ha sido indexada en un buscador"[6], este tipo de páginas no siempre son ilícitas pero sí se suelen utilizar para vender sustancias alucinógenas y evadir los controles legales.

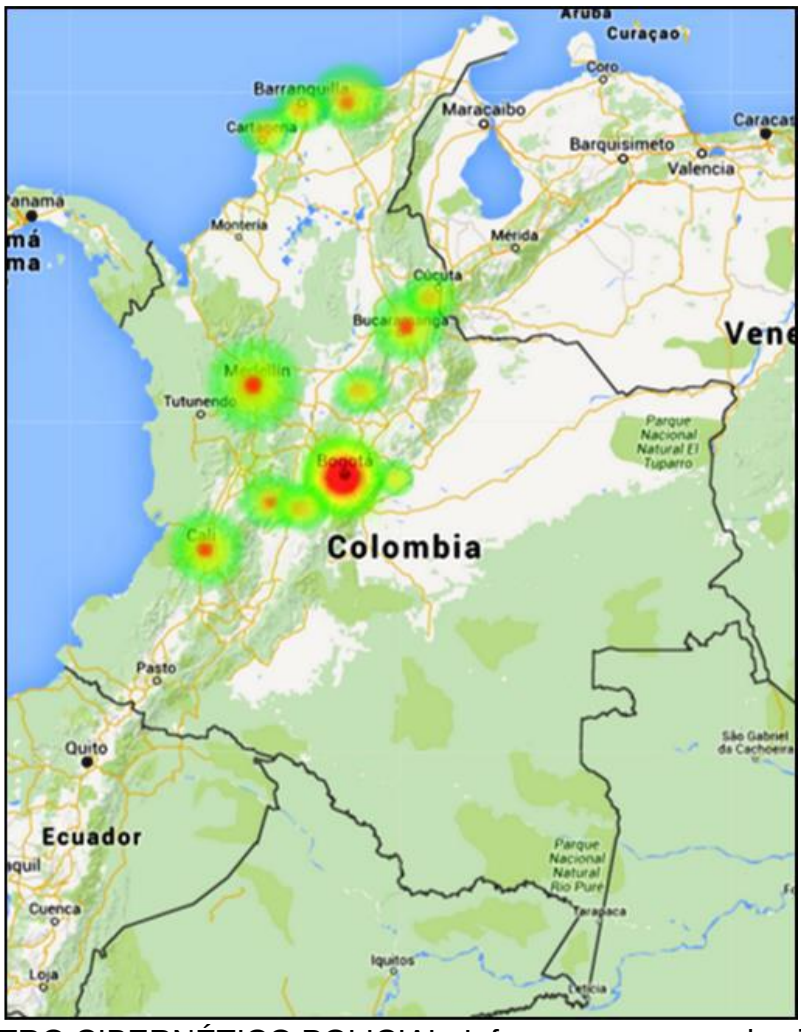
Uso de internet como herramientas de amenazas para instigar y delinquir. El uso de internet ha aumentado en un 28% según el Ministerio de TIC, pero muchas veces es mal utilizado para hacer ciberbullying.

Monedas virtuales como forma de pago. Las monedas virtuales tales como la más conocida que es el *bitcoin* son formas de pago virtual que no están supervisadas

[3] Ibíd.
[4] Ibíd. p. 4.
[5] Ibíd.
[6] Ibíd. p. 7.

por ninguna entidad, lo que genera un posible foco ilícito dado que pueden ser utilizadas para extorsión y al no conocerse la procedencia no se puede detectar.

Figura 1. Mapa de calor cibernético



Fuente: CENTRO CIBERNÉTICO POLICIAL. Informe amenazas de cibercrímen en 2016-2017. Bogotá, D.C.: Cairvirtual. 2017, p. 11

Tal como se ve en el mapa, las ciudades con mayor incidencia de crímenes son Bogotá, Cali, Barranquilla y Bucaramanga; en la región de Boyacá no está evidenciado como foco de altos crímenes pero esto no la hace exenta de que se presenten, o en el peor de los casos puede que no sean denunciados.

“El Centro Cibernético Policial es la dependencia de la Dirección de Investigación Criminal e INTERPOL son los encargados del desarrollo de estrategias, programas,

proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos"[7]; la Policía Nacional ha hecho alianzas con entidades internacionales para fortalecer el departamento a través capacitaciones con entidades internacionales como Interpol, Edupol, Ameripol y Europol, siendo esta último una alianza única en Latinoamérica[8].

4.1.3. Ataques de 2015[9]

En el año 2015 se presentaron diversos ataques tanto a nivel nacional como internacional de los cuales se destacan los que se describen a continuación. De esta manera se puede ver la importancia de conocer su impacto a nivel local en la ciudad de Sogamoso puesto que este tema no solo afecta a grandes metrópolis sino a la comunidad en general.

A. Fraude a Bavaria por 300 millones de pesos- 27 de mayo de 2015

Una entidad bancaria otorga un poder por parte de dos funcionarios de Bavaria para girar a una fundación más de nueve mil millones de pesos. En las investigaciones de las autoridades figura que "los autores del fraude lograron que en los sistemas se diera la autorización electrónica de Bavaria para realizar el movimiento financiero"[10], y de esa forma el banco autorizó el desembolso a la fundación. Una de las hipótesis es que podía tratarse de una red especializada en hackear y cometer este tipo de fraudes.

B. CTB *locker*

Es un virus que encripta los archivos y pide dinero para desencriptarlos, esto se hace a través de un correo electrónico que tiene un archivo oculto que resulta ser un troyano disfrazado y logra que terceros ingresen al sistema sin que el usuario se dé por enterados. Los usuarios que ejecuten el archivos verán cifrados todos los archivos, el *malware* descarga un *ransomware* que es un software malicioso, este le da la capacidad al ciberdelincuente de bloquear el equipo desde una ubicación remota y encriptar archivos, este *ransomware* es llamado Win32=FileCoder.DA, y exige dinero para recuperar la información, cuando termina de cifrar la información despliega la siguiente pantalla:

De acuerdo a algunos estudios, Colombia es el sexto país más afectado por este virus.

---

[7] Ibíd., p. 3.
[8] Ibíd.
[9] Trabajo Colaborativo II Fundamentos de Seguridad Informática Orduz Barrera Diana Maria Escuela de Ciencias Básicas, Tecnología e Ingeniería – UNAD
[10] Ibíd., párr. 3

C. El ciberdelincuente que viajó por el mundo con millas de famosos[11].

En el mes de junio de 2015 fue capturado Jaime Alejandro Solano Moreno de 23 años cuando hacia uno de sus tantos viajes, viajó a Miami, África, México y destinos nacionales, robó 5 millones de millas en tres años, y lo lograba utilizando *phishing*, correos electrónicos con el logo de *lifemiles*; solicitando información de actualización de datos, igualmente usaba ingeniería social para obtener más información. Tras esto, las investigaciones están en curso ya que sospechan también de cómplices en las aerolíneas.

D. Clonación de tarjetas de crédito[12]

Fueron clonadas más de 40 tarjetas por una banda llamada "los mellados", simplemente ofrecían ayuda a las personas que quieren retirar de los cajeros y con un dispositivo electrónico roban toda la información de la tarjeta para luego clonarla y retirar todo el dinero de la cuenta.

E. Capturada banda de ciberpiratas[13]

En barranquilla el 31 de agosto de 2015 fue capturada de una banda denominada "piratas del Caribe", 18 personas capturadas entre funcionarios de la Registraduría y empleados bancarios hacían fraudes electrónicos virtuales, logrando millonarios hurtos a entidades bancarias, el *modus operandi* consistía en que el líder siendo un *hacker* de gran reconocimiento en la costa obtenía información de titulares, luego este daba esta información al captador de información, entonces hacía la selección de víctimas y reclutaba personal bancario de la Registraduría y telefonía celular para hacer transferencia de cuentas y luego repartir el dinero. El hurto trascendió entre los siete mil millones y los 330 mil millones de pesos durante cuatro años.

F. Otras actividades graves que regularmente no son delitos través de la red, pero se comenten a través de la red.[14]

Terrorismo: cuando los terroristas están próximos a cometer un ataque utilizan la red de internet para intimidar a terceros y generar terror a través de sistemas informáticos, ya sea para comunicar sus acciones dando avisos, haciendo el plan a

---

[11] DIARIO EL COMERCIO. El ciberdelincuente que viajó por el mundo con millas de los famosos. {En línea}. 2015. Disponible en: http://www.elcomercio.com/actualidad/ciberdelincuente-viaje-mundo-millas-famosos.html

[12] TEGUI BLOG. Delitos informáticos. {En Línea}. 2016. Disponible en: https://teguiblog.wordpress.com

[13] PERIÓDICO EL HERALDO. Capturan en la costa y el interior a banda de 18 cibercriminales conocida como 'Piratas del Caribe'. {En Línea}. 2015. Disponible en: https://www.elheraldo.co/judicial/capturan-18-implicados-en-banda-de-piratas-informaticos-214691

[14] GARCÍA DE LA CRUZ, Juan Manuel. Delitos Informáticos. Maestría en Administración con Especialidad en Informática. Culiacán: Universidad Valle Del Bravo, 2005.

larga distancia por e-mail o por los servicios de comunicación a través de mensajes instantáneos.

Narcotráfico: si los narcotraficantes intercambian entre sí información a través de internet y hacen sus ventas y compras de material ilegal por medio de la red, pasa a ser un delito que se comete con la informática como medio, lo cual está prohibido.

Espionaje: el espionaje personal con intención de rastrear a una persona para observar sus acciones a través de internet, las cosas que ve, los sitios a los que accede, la información que procesa, sin ninguna clase de autorización jurídica está atentando contra la privacidad y deviene en cometer un delito.

Tráfico de armas: se pueden utilizar las redes sociales para comercializar armas de manera ilegal, publicando páginas para este fin.

Proselitismo de sectas: existen diferentes grupos en los cuales reúnen determinado grupo de personas y las convencen para propagar información fraudulenta, las incitan a cometer cualquier clase de delito, económico, social, y cualquiera que denote comportamiento inadecuado".

4.1.4 Penalización[15]

La ley 1273 de 2009 establecida por el entonces "presidente Álvaro Uribe, por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico denominado "De la protección de la información y de los datos". Económicamente las multas van entre 100 y 1000 SMMLV, dependiendo de que el delito no incurra en una falta más grave, y textualmente como lo cita el decreto se penaliza a quien "con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes"[16].

4.2. MARCO LEGAL

En Colombia la normatividad para delitos informáticos empezó a ser más significativa desde la creación de la Ley 1273 de 2009, conocida como la Ley de delitos informáticos. Uno de los primeros antecedentes jurídicos a esta ley es que desde hacía más de 20 años con el Decreto 2060 de 1989 se reglamentó:

[15] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009, no. 47.223

[16] Ibíd. Art. 269G

> “La inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas.[17]
>
> En el Decreto 2060 de 1989 de se comenzó a penalizar este tipo de delitos, al mismo tiempo se tomaron como base para la Reforma al Código Penal Colombiano del año 2000:
>
> Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.
>
> Ahora bien, el Código Penal colombiano (Ley 599 de 2000) en su capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones:
>
> Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles”.[18]

“Una norma posterior fue la Ley 679 de 2001 por medio de la cual se expidió un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución pero solo tiene sanciones administrativas” tal como lo cita el siguiente artículo:

> “ARTÍCULO 10. SANCIONES ADMINISTRATIVAS. El Ministerio de Comunicaciones tomará medidas a partir de las denuncias formuladas, y sancionará a los proveedores o servidores, administradores y usuarios responsables que operen desde territorio colombiano, sucesivamente de la siguiente manera: 1. Multas hasta de 100 salarios mínimos legales vigentes.

[17] OJEDA, Jorge; ARIAS, Miguel; RINCÓN, Fernando y DAZA, Libardo. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. Vol.11 No. 28. (enero-junio 2010)
[18] Ibíd., pp. 51-52

> 2. Cancelación o suspensión de la correspondiente página electrónica. Para la imposición de estas sanciones se aplicará el procedimiento establecido en el Código Contencioso Administrativo con observancia del debido proceso y criterios de adecuación, proporcionalidad y reincidencia.[19]
>
> [No obstante] el 21 de julio de 2009 se instauró la Ley 1336, "por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual, con niños, niñas y adolescentes". En forma específica, en su capítulo VI establece los "tipos penales de turismo sexual y almacenamiento e intercambio de pornografía infantil" con penas de prisión de diez (10) a veinte (20) años y multas de ciento cincuenta (150) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes (SMLMV)".[20]

"Igualmente, la "Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos, la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes"[21]. El primero de los dos capítulos en que está dividida la ley trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. El segundo capítulo se refiere a los atentados informáticos y otras infracciones".

> "[De ese modo] este Marco jurídico se ha convertido en una importante contribución y un instrumento efectivo para que las entidades públicas y privadas puedan enfrentar los "delitos informáticos" con definiciones de procedimientos y políticas de seguridad de la información; y en consecuencia, con las acciones penales que pueden adelantar contra las personas que incurran en las conductas tipificadas en la norma. Con ello, Colombia se ubica al mismo nivel de los países miembros de la Comunidad Económica Europea (CEE), los cuales ampliaron al nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países, mediante el Convenio 'Cibercriminalidad', suscrito en Budapest-Hungría en 2001 y vigente desde julio de 2004".[22]

"En las siguientes figuras se presenta a detalle el contenido de la ley y sus características aplicables a este análisis. La Figura 1 identifica las actuaciones con

---

[19] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 679. (3, agosto, 2001). Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Diario Oficial. Bogotá, D.C., 2001. No. 44.509. Art. 10

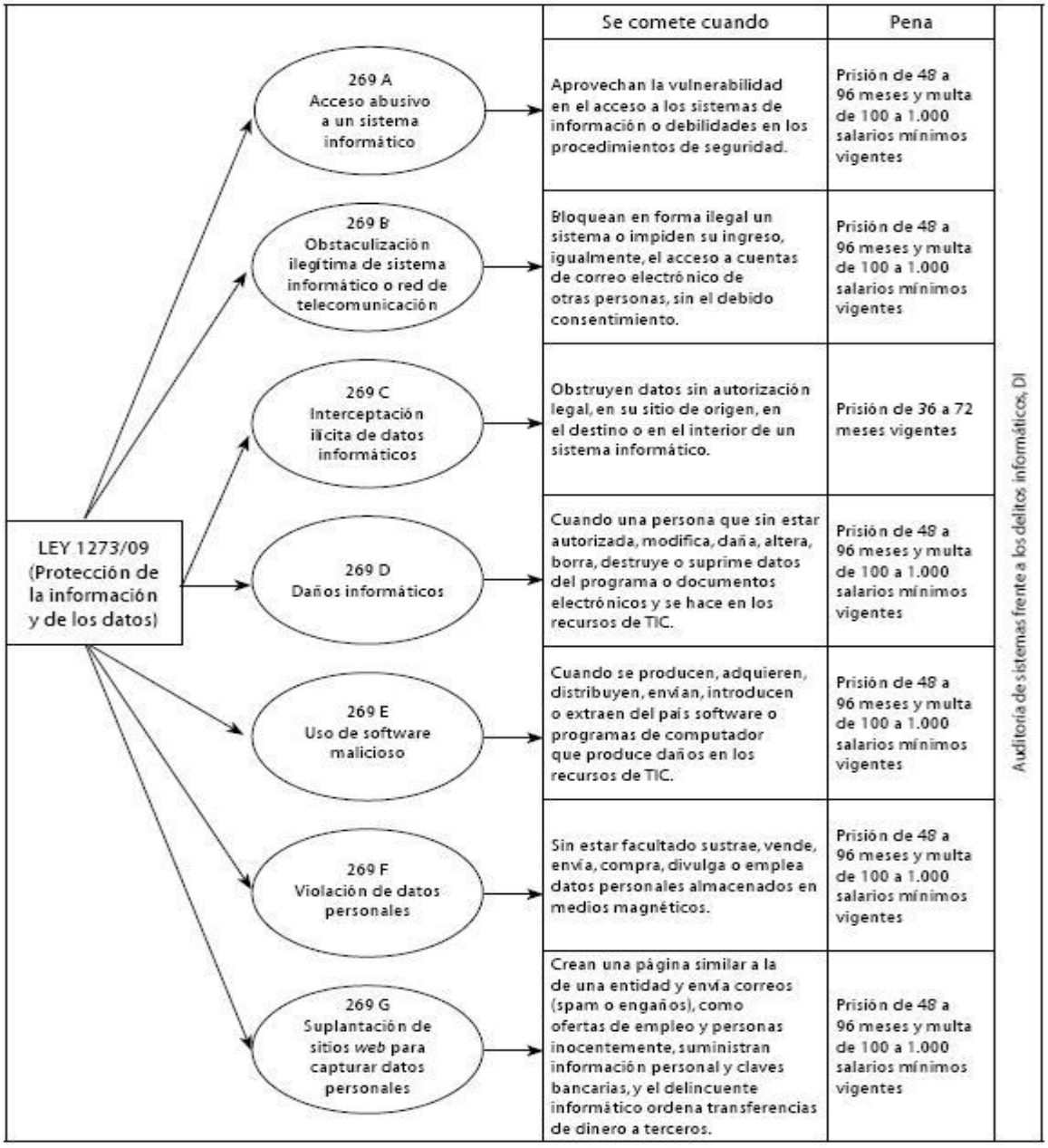
[20] OJEDA, op. cit, p. 52

[21] DACCACH, José Camilo. Ley de Delitos Informáticos en Colombia. {En Línea}. 2016. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/. párr. 1

[22] OJEDA, op. cit, p. 53

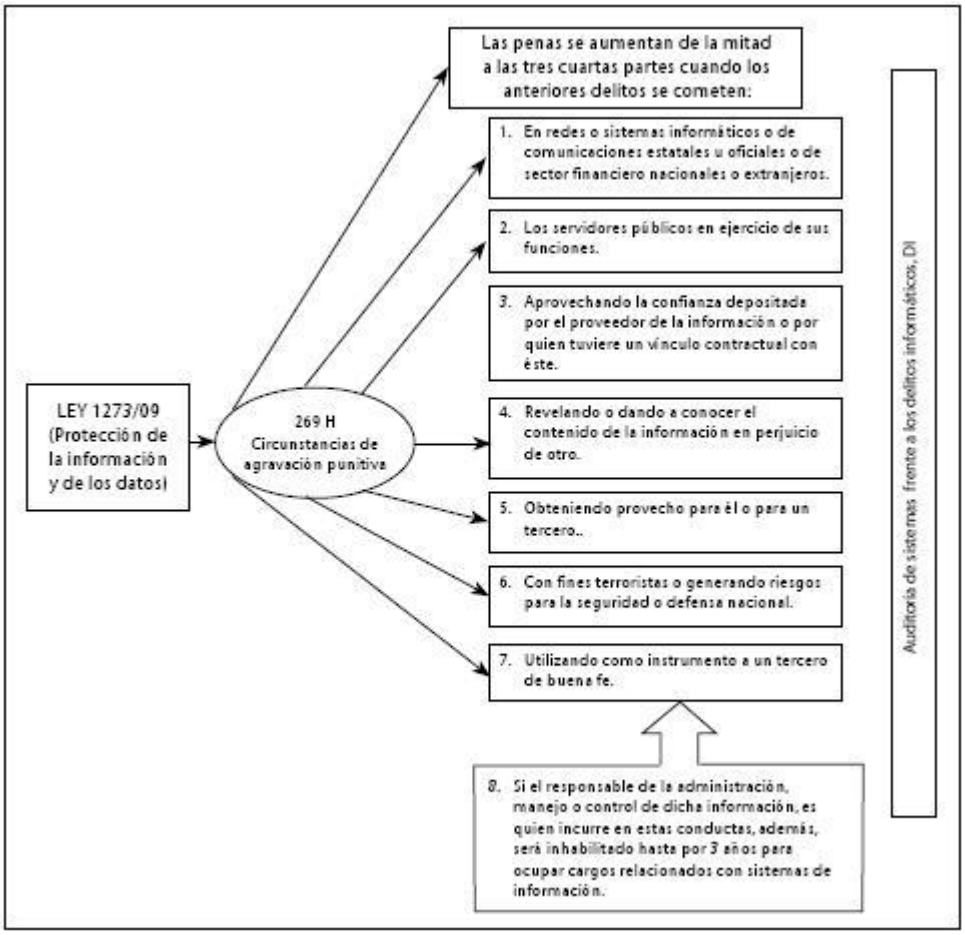
las cuales se tipifica el delito y la punibilidad aplicable (en su mayoría, penas de prisión entre 48 y 96 meses y multas de 100 a 1.000 SMLMV)".

Figura 2. Legislación penal colombiana frente a los delitos informáticos (artículo 1 de la Ley 1273 de 2009)



Fuente: OJEDA, Jorge; ARIAS, Miguel; RINCÓN, Fernando y DAZA, Libardo. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. Vol.11 No. 28. (Enero-junio 2010), p. 55

Figura 3. "Circunstancias de agravación punitiva", o aquellas situaciones que por agravantes aumentan la pena del delito (Artículo 269H/Ley 1273 de 2009).



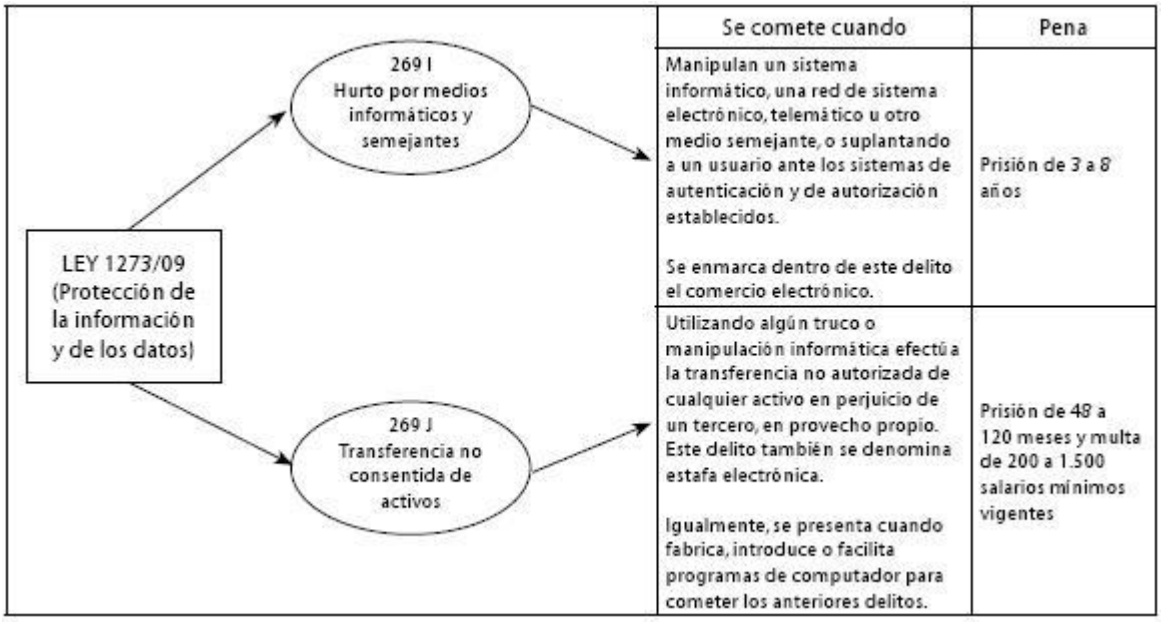
Fuente: OJEDA, Jorge; ARIAS, Miguel; RINCÓN, Fernando y DAZA, Libardo. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. Vol.11 No. 28. (Enero-junio 2010), p. 56

Por su parte, la Figura 3 se trata de:

> "Los atentados informáticos y otras infracciones" referidos en los artículos 269I "Hurto por medios informáticos y semejantes" y 269J "Transferencia no consentida de activos", entendidos normalmente como delitos 'ordinarios' en cuya realización es importante el uso de recursos tecnológicos contemplados en el capítulo II de la Ley 1273 de 2009 analizada.[23]

[23] Ibíd., p. 57

Figura 4. Legislación penal colombiana frente a los delitos informáticos (artículo 1 de la Ley 1273 de 2009)



Fuente: OJEDA, Jorge; ARIAS, Miguel; RINCÓN, Fernando y DAZA, Libardo. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. Vol.11 No. 28. (Enero-junio 2010), p. 57

4.3. MARCO CONCEPTUAL

4.3.1. Procesos de ingeniería social

La ingeniería social es la utilizar la psicología humana, manejarla a favor, para obtener información de forma engañosa, pero lo más importante sin ningún acto violento

- Pishing: es el proceso mediante el cual se puede obtener información confidencial de forma fraudulenta, como contraseñas e información bancaria confidencial. De esa forma, el *pisher* con un correo o un sitio web logra suplantar a una empresa y obtener la información alegando que está actualizando los datos del cliente, también enviando correos electrónicos donde piden información acerca de tarjetas de crédito y claves; se debe tener en cuenta que un administrador de la información nunca pide este tipo de datos. También a través de correos con archivos adjuntos con código malicioso pueden ejecutarse y robar información del PC.

Otro proceso es la manipulación cara a cara con el cliente para obtener información con simples preguntas pueden revelar la contraseña, en una conversación se puede revelar información de su pasado, y se presenta respondiendo esta pregunta ¿qué contraseña introduciría yo si fueses la víctima?

- *"Vishing*. Es igual al pishing pero se utiliza una llamada telefónica, en lugar de un correo o un sitio web. La persona que utiliza este método tiene que ser muy conversadora y tener poder de convencimiento, para obtener información durante toda la llamada como contraseñas, claves de tarjetas y números de tarjetas de crédito.

- *Baiting*. El delincuente de forma intencional deja un dispositivo extraíble como CD o una memoria USB, la cual contiene un programa malicioso que al ejecutarse puede abrir un programa para robar información sin que se dé cuenta el dueño del equipo.

- *Carding*. Es el proceso mediante el cual se utilizan tarjetas de crédito o los números de tarjeta de terceras personas, se relacionan con el *hacking* ya que se utiliza la ingeniería social para poder obtener información. En internet se encuentran manuales con los cuales se puede hacer *carding* ofreciendo *tips* tan sencillos como buscar un extracto en la basura o robar la correspondencia del vecino para obtener un número de tarjeta de crédito y de ahí en adelante se da el paso a paso para poder hacer fraudes.

- Criptomonedas: se debe hablar primero de monedas virtuales que hace referencia a un tipo de dinero virtual no regulado controlado por una comunidad digital específica; una moneda digital es una forma de moneda virtual que se crea y se almacena electrónicamente. "Una criptomoneda es un medio de intercambio que utilizan la criptografía para asegurar las transacciones y controlar la creación de nuevas unidades."[24]. Los riesgos que tiene las criptomonedas son volatilidad en su valor, riesgo de lavado de activos, no están vigiladas por el Estado, riesgo de que se trate de una pirámide u otro fraude".

Todos estos métodos de ingeniería social se pueden prevenir evitando correos electrónicos de fuentes no seguras, tener en cuenta que ninguna entidad solicita información confidencial por ningún medio, en las llamadas telefónicas de igual manera no hay que suministrar información personal, los dispositivos que no sean de fuentes seguras es mejor no utilizarlos en los equipos personales.

Vale resaltar que el partido político MIRA en su página virtual maneja una app que se puede descargar en celulares, la cual explica los diferentes delitos informáticos

[24]OROYFINANZAS.COM. Definición Criptomoneda: ¿Qué es una criptomoneda? {En Línea}. 2014. Disponible en: https://www.oroyfinanzas.com/2014/10/que-es-criptomoneda/. párr. 11

a los cuales están expuestos, describiéndolos y se retoman a continuación, como denunciar y las leyes que los protegen[25].

- *"Grooming*. Práctica realizada por un adulto que de manera deliberada y hasta sistemática engaña y establece relaciones de amistad con niñas, niñas y adolescente vía internet con el fin de obtener imágenes eróticas, personales o pornográficas.

- *Suplantación de identidad.* Sin autorización un tercero se roba información personal para cometer ilícitos.

- *Sexting*. Es el intercambio de mensajes de tipo sexual o erótico, sugerente o explícito vía teléfono celular

- Sextorsión. Consiste en acciones de acceso, hostigamiento o constreñimiento a otras personas con amenazas personales o la publicación de imágenes íntimas, con el propósito de tener un favor sexual o dinero

- *Ciberbullying*. Conforme a la Ley 1620 de 2013 se define como la forma e intimidación con uso deliberado de tecnología de información (internet, redes sociales y virtuales, telefonía móvil y videojuegos *on line*) para ejercer maltrato psicológico y continuado.

- *Pornografía infantil*. Es la reproducción, producción, venta, ofrecimiento, compra, almacenamiento, transmisión, etc., de fotografías, videos o cualquier medio de representaciones reales o modificadas de cualquier tipo de actividad sexual que involucre menores de 18 años de edad.

- *Morphing.* Es la producción de material sexual o pornográfico en el cual se incorporan imágenes editadas o se simula la voz de personas menores de 18 años de edad".[26]

[25] PARTIDO POLÍTICO MIRA. ¿Sabes cómo protegerte en la red contra delitos informáticos? {En línea}. s.f. Disponible en: https://partidomira.com/sabes-como-protegerte-en-la-red/

[26] COLOMBIA. CONGRESO DE LA REPÚBLICA. Proyecto de Ley 050. (28, septiembre, 2017). Por la cual se formulan los lineamientos de política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos, en contra de niñas, niños y adolescentes; se modifica el código penal y se dictan otras disposiciones. Bogotá, D.C.: Cámara de Representantes, 2017. Art. 2

4.3.2. Conceptos y definiciones[27]

"Ciberesfera: sistema formado por el conjunto de elementos digitales, personales y relacionales que conforman la envoltura o hábitat cibernético de la humanidad.

Ciber: (de Cibernética). 1. elem. compos. Significa 'cibernético'. Ciberespacio, cibernauta. (23ª edición 2014, del Diccionario de la Lengua Española).

Ciberactivismo: conjunto de técnicas de comunicación mediadas por el ciberespacio y su tecnología que permiten la dedicación intensa a una determinada línea de acción en la vida pública, en el área social, política o religiosa mediante el logro de una comunicación más rápida y difusión de gran audiencia.

Ciberarma: acción cibernética destinada a realizar funciones ofensivas o defensivas que se materialicen en un ataque y tengan por finalidad un daño intencional, con resultado de destrucción de las cosas, violencia en las personas, disfuncionalidad o disrupción temporal o permanente de redes, sistemas, equipos, funciones, servicios o instalaciones; o atente contra intereses, derechos y libertades.

Acción cibernética: cualquier acto, medida, instrumento, procedimiento o dispositivo susceptible de ser catalogado como medio idóneo para producir efectos cibernéticos adversos.

Ciberarma de guerra: ciberarma cuya utilización equivale al uso de la fuerza o de un ataque armado prohibido por el artículo 2.4 de la Carta de Naciones Unidas y el derecho internacional consuetudinario y pueden ser utilizadas:

1. Para el ejercicio del derecho inherente a la autodefensa individual o colectiva reconocida en el artículo 51 de la de la Carta de Naciones Unidas, de conformidad con el Derecho Internacional, incluido el Derecho Internacional Humanitario, en respuesta a un ataque armado a través del ciberespacio.

2. Como medida coercitiva adoptada por parte del Consejo de Seguridad, de acuerdo con lo dispuesto en los artículos 41de la Carta de Naciones Unidas.

[27] MOLINA, Mateos. Conceptos y definiciones. {En línea}. s.f. Disponible en: http://molinamateos.com/content/conceptos-y-definiciones-0

3. Como medida para mantener o restablecer la paz y la seguridad internacional según dispone el artículo 42, ambos del Capítulo VII de la Carta de Naciones Unidas.

Ciberataque: ofensiva, agresión o acción realizada en perjuicio de valores, personas, bienes, sistemas o servicios, mediados por el ciberespacio y su tecnología.

Ciberdelincuencia: conjunto de actos ejecutados mediante el uso del ciberespacio y su tecnología, con el fin de realizar actividades delictivas.

Ciberespacio: conjunto de interconexiones electrónicas dispuestas en red que conforma un espacio de relación integrado por componentes de naturaleza material de base tecnológica, de naturaleza inmaterial sustentada en la información y el conocimiento, a través del lenguaje y de naturaleza antropológica fundamentada en la sociabilidad del ser humano. Deviene en medio y procedimiento para prestar servicios y ha generado un nuevo marco espacio-cultural, modulado por los confines de la tecnología y la sociabilidad, con efectos económicos, políticos, jurídicos, sociales, culturales y de seguridad. El ciberespacio es un entorno universal y medio de vertebración mundial que tiene como límites la seguridad, el desarrollo y el respeto a los derechos humanos.

Ciberinteligencia: actividades de inteligencia y contrainteligencia realizadas en o desde el ciberespacio y mediadas por su tecnología.

Ciberseguridad: conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan (Art. 2.3 de la Orden Ministerial 10/2013 de 19 de febrero por la que se crea el Mando Conjunto de la Ciberdefensa).

A la vista de lo dispuesto en la Ley de Seguridad Nacional, se podría enriquecer la definición de Ciberseguridad y considerarla como 'la acción del Estado constituida por el conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, configurada como uno de los ámbitos de especial interés de la Seguridad Nacional. Que protege la libertad, los derechos y bienestar de los ciudadanos, garantiza la defensa de España y sus principios y valores constitucionales, así como contribuye junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos, mediante la defensa de la infraestructura tecnológica, los servicios que prestan y la información que manejan’.

Ahora, para ser plenamente efectiva la ciberseguridad requeriría lo que se puede denominar denominar *full cybersecurity*, consistente en la integración

y sincronización entre sí de los componentes cibernéticos, de la información, y sus operaciones; con otras medidas para situaciones de conflicto, todo ello dotado del marco legal y voluntad política apropiados. Para ser eficiente a nivel global demandaría una estrategia efectiva para alcanzar un equilibrio estable en el ciberespacio en el que los Estados se vean disuadidos de realizar operaciones maliciosas.

Ciberguerra: lucha con medios, organización y doctrina cibernética realizada a través de actos cibernéticos de guerra, llevada a cabo entre Estados enemigos con fines políticos irreconciliables o incompatibles que comporta siempre la posibilidad de una escalada al extremo, una intervención sin límites para alcanzar la victoria y la destrucción del adversario por medios cibernéticos. Adopta una forma organizada y representa el instrumento último de la política en el ámbito cibernético.

Ciberdiplomacia: conjunto de actuaciones diplomáticas realizadas utilizando el ciberespacio y mediadas por las Tecnologías de la Información y las Comunicaciones.

Diplomacia digital: conjunto de actuaciones diplomáticas orientadas a la protección de los intereses del Estado en el ciberespacio.

Resiliencia: capacidad de respuesta y recuperación ante ciberataques.

Ciencias Sociales Informáticas: nuevo campo de estudio surgido del cruce entre el análisis de datos y la sociología (también llamada cibersociología)".

5. DESARROLLO DEL TRABAJO DE GRADO

En las tres poblaciones se realiza un análisis y diagnóstico a una muestra de habitantes para identificar las posibles emergencias cibernéticas y el conocimiento que tiene la población en general acerca de este tema, y los controles que las entidades públicas y privadas tienen para proteger a la población y generar planes de contingencia en caso de presentarse alguna eventualidad.

Se dividen tres sectores importantes para el análisis que son la empresa privada, la empresa pública y las instituciones educativas.

5.1. DOCUMENTACIÓN QUE SUSTENTA LA CIBERSEGURIDAD Y EL CIBERCRIMEN

5.1.1. Cibercrimen

"El máximo objetivo de los delincuentes cibernéticos suele ser acceder sin previo consentimiento a la información y datos que son propiedad de personas, empresas o gobiernos"[28]. Tales ataques no suelen suceder de forma física sino que se llevan a cabo de forma virtual[29].

> El cibercrímen es cualquier crimen que se lleva a cabo u ocurre mayormente en línea; abarca desde el robo de identidad y otras violaciones de seguridad hasta actividades como la pornografía vengativa, el acoso cibernético, el hostigamiento, el abuso e incluso, la explotación sexual infantil. Los terroristas cada vez participan más en internet y trasladan los crímenes más aterradores al espacio cibernético.[30]

Cabe señalar que en ocasiones resulta muy sencillo poder cometer estos delitos ya que se hacen de forma silenciosa y con poco tiempo, y de acuerdo a lo avances tecnológicos en materia de seguridad permiten ocultar fácilmente la identidad; dándose la eterna persecución entre "el gato y el ratón".

Lo más común en cometer errores en cuanto a la definición de un ciberdelincuente y un *hacker*, siempre se refieren a los dos de la misma manera y o es así. Un *hacker* no es delincuente informático mientras que un ciberdelincuente sí lo es; los *hackers* de sombrero negro (*black hat*) son los que logran hacer intrusiones con fines lucrativos, los *hackers* sombrero blanco o hacker ético (*white hat*) suelen penetrar

---

[28] ÁL, José. ¿Qué es y cómo combatir el cibercrímen? {En Línea}. 2015. Disponible en: http://portaley.com/2015/04/que-es-y-como-combatir-el-cibercrimen/. párr. 3

[29] Ibíd.

[30] SYMANTEC. De qué manera distinguir el cibercrímen y protegerse. {En Línea}. s.f. Disponible en: https://ar.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html. párr. 3

la seguridad del sistema y trabajan para una empresa, y los *hacker* grises (*grey hat*) pueden penetrar en el sistema y encontrar problemas para después cobrar por solucionarlos

5.1.1.1 ¿Qué leyes funcionan mejor contra el cibercrímen?

Para poder ser castigado un delito de forma concisa resulta complicado ya que las pruebas que se puedan conseguir son muy volátiles, se necesita de una legislación integral que incluye el Derecho Sustantivo y el Derecho Procesal para que tenga una respuesta la justicia penal. Esta legislación debe cumplir con lo siguiente:

- Debe ser neutral tecnológicamente para poder aceptar cambios y evoluciones de la tecnología o corre el riesgo de ser obsoleta.
- Su aplicación debe ser flexible para garantizar Derechos Humanos y Estado de Derecho
- Ser compatible con las leyes de otros países para permitir la cooperación internacional.

A través del Convenio de Budapest sobre el Delito Cibernético existe una directriz internacional también ampliamente utilizada en las Américas que ayuda a los países a cumplir estos requerimientos, este documento es muy completo y coherente, y sirve como marco legal para la cooperación internacional, además ayuda a las naciones como lista de verificación para hacer leyes internas sustantivas y procesales, en América Latina varios países aplican este convenio y está incluida Colombia.

5.1.1.2 Contextualización del cibercrímen en Colombia

5.1.2 Ciberseguridad

Según el ISACA (*Information Systems Audit and Control Association* – Asociación de Auditoría y Control sobre los Sistemas de Información*)* ciberseguridad es la “protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.[31]

Cabe resaltar que es importante emplear buenas prácticas al hacer uso de correos, redes sociales, e internet en general, y educar a todos los integrantes de una empresa para poder proteger la información de la misma. La ciberseguridad es la

[31]CARVAJAL AZCONA, Javier. ICEMD. . {En Línea}. s.f. Disponible en: https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo/

práctica de defender a los equipos electrónicos, redes o servidores de ataques maliciosos, también se conoce como seguridad de tecnología de información y seguridad electrónica. Abarca temas tan amplios como seguridad informática, educación del usuario y recuperación de desastres.

A manera de ilustración, en Estados Unidos se invierten millones de dólares en ciberseguridad pero a pesar de todo recomiendan estar evolucionando y monitoreado continuamente los recursos electrónicos. Las amenazas que contrarrestan la ciberseguridad son tres: el cibercrímen que comprende a las personas que realizan ataques; ciberguerra que son ataques con motivaciones políticas; y ciberterrorismo que hace referencia a grupos que intimidan y generan terror.

Ahora bien, la ciberseguridad brinda protección a los usuarios dependiendo de los protocolos criptográficos que maneje, la ciberseguridad no solo protege al información que se transmite sino también en cuanto a pérdida o robo de información. La ciberseguridad es una disciplina que debe estar en constante evolución para contrarrestar el cambiante medio de amenazas que se presenten. Además, esta se enfoca en la protección de toda la infraestructura computacional y en proteger la información con una serie de protocolos y herramientas para dar protección a la información y a la infraestructura. Comprende software, hardware y toda la información que requiera confidencialidad y necesite ser protegida, conviertiéndose en información privilegiada.

“De acuerdo al documento del CONPES (Consejo Nacional de Política Económica y Social, de la República de Colombia) en la siguiente tabla se resumen los casos de incidentes de seguridad digital en el 2014, donde se evidencia que “afectan cualquier sector de la economía”[32]. Teniendo en cuenta que desde hace tres años se han incrementado con mayor riesgo estos casos, dado que las telecomunicaciones se encuentran evolucionando constantemente”.[33]

Figura 5. Casos de Incidentes en Seguridad Digital en el año 2014

[32] DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES No. 3854: Política nacional de seguridad digital. Bogotá, D.C.: Consejo Nacional de Política Económica y Social. 2016. p. 12.
[33] Ibíd.

Mes de 2014	Organización	Sector	Impacto
Enero	SNAPCHAT	Red social	4,5 millones de nombres y números móviles comprometidos
Febrero	KICKSTARTER	Crowd funding	5,6 millones de víctimas
Marzo	KOREAN TELECOM	Telecomunicaciones	12 millones de suscriptores comprometidos
Abril	HEARTBLEED	Software	Primera de tres vulnerabilidades de fuente abierta
Mayo	EBAY	Compras	Base de datos de 145 millones de compradores comprometida
Junio	PF CHANG´S	Comidas	Más alta violación de información de alto nivel del mes
Julio	ENERGETIC BEAR	Energía	Operación de ciber espionaje a la industria de energía
Agosto	CYBERVOR	Tecnología	1,2 billones de credenciales comprometidas
Septiembre	iCLOUD	Entretenimiento	Cuentas de celebridades comprometidas
Octubre	SANDWORM	Tecnología	Ataque a la vulnerabilidad de Windows
Noviembre	SONY PICTURES	Entretenimiento	Más alta violación de alto nivel del año
Diciembre	INCEPTION FRAMEWORK	Sector público	Operación de ciber espionaje a sector público

Fuente: DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES No. 3854: Política nacional de seguridad digital. Bogotá, D.C.: Consejo Nacional de Política Económica y Social. 2016. p. 12

5.1.3 Ciberseguridad y seguridad de la información

"Cuando se busca proteger el hardware, redes, software, la infraestructura tecnológica o los servicios, se hace referencia al ámbito de la seguridad informática o la ciberseguridad. Cuando se incluyen las actividades de seguridad que se relacionan con la información de forma que se manejan las personas, la seguridad física, el cumplimiento o la concienciación se habla sobre la seguridad de la información".[34]

De igual forma, cuando se aborda el tema de la ciberseguridad esto se refiere a la protección de sistemas interconectados o de información digital, se puede decir que en este campo se realizan prácticas ofensivas, y la seguridad de la información tiene que ver con el hecho de que sin importar el estado en el que se encuentre la información, ya sea digital, escrita en medio magnético o en papel, también requiere ser protegida. Por tanto, es pertinente hablar sobre prácticas defensivas.

[34]SGSI. ¿Cuál es la diferencia entre ciberseguridad y seguridad de la información? Blog especializado en Sistemas de Gestión de Seguridad de la Información. {En Línea}. 2017 Disponible en: https://www.pmg-ssi.com/2017/01/ciberseguridad-seguridad-informacion/

5.2. PLANES DE CONTROL DE INCIDENTES CIBERNÉTICOS EN LAS CIUDADES DE TUNJA, DUITAMA Y SOGAMOSO

5.2.1 Análisis de delitos informáticos en Boyacá en los dos últimos años

De acuerdo a los principales delitos informáticos presentados en Boyacá, se puede evidenciar que han disminuido en los dos últimos años, y en el campo de cibercrímenes se dan los más comunes y menos sofisticados pero de igual modo han disminuido. Todo esto gracias a la educación por parte de las autoridades para que la comunidad no incurra en estos fraudes y por la denuncia que es de vital importancia para determinar los focos a los cuales hay que dar el mayor interés, tal como se puede evidenciar en la página de la Policía Nacional y el CAI virtual.

“En la ciudad de Sogamoso – Boyacá, a partir del año 2017 se está creando el Departamento de Delitos Informáticos en la Policía Nacional, dado que los pocos casos que eran denunciados se centralizaban en la SIJIN de la ciudad”.

5.2.2 GEL (Gobierno en Línea)

En el gobierno del presidente Juan Manuel Santos se está implementando la política de Gobierno Digital para generar un ambiente evolucionado con las diferentes tecnologías, con el fin de fomentar valor público de manera que todas las sociedades actúen sobre este aspecto. En este sentido, el nuevo objetivo de la política de Gobierno Digital es el siguiente:

> “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”

Teniendo en cuenta lo anterior, las características competitivo, proactivo e innovador se entienden de la siguiente forma:

> “*Competitivo
>
> - Entidades idóneas, preparadas y con alta calidad en sus procesos y en la implementación de políticas
>
> - Ciudadanos que tienen capacidades y recursos efectivos, ágiles y fáciles de usar para interactuar con el Estado a través de los medios digitales.
>
> *Proactivo

- Entidades que se anticipan, son previsivas, mitigan riesgos y realizan seguimiento a las nuevas tecnologías o tecnologías emergentes para satisfacer sus necesidades y resolver problemáticas

- Ciudadanos que participan en el diseño de trámites y servicios; políticas; normas; proyectos y en la toma de decisiones por medios digitales

*Innovador

- Entidades que promueven la interacción y la colaboración entre diferentes actores, para la generación de valor público usando medios digitales

- Ciudadanos que ayudan a identificar y resolver problemáticas y necesidades comunes y participan en espacios de encuentro y colaboración con diferentes actores." [35]

Igualmente, valor público es la posibilidad de llegar a donde el mercado no llega, es decir que todos los ciudadanos tengan la posibilidad de aprovechar las diferentes tecnologías, el gobierno actualmente tiene el programa Internet para Todos y Vive Digital, dando cubrimiento a zonas aisladas de Colombia donde el acceso a tecnología era mínimo. "Para la implementación de la Política de Gobierno Digital se han definido varios elementos que brindan orientaciones generales y específicas que deben ser acogidas por las entidades, a fin de alcanzar los propósitos de la política". Estos elementos son los siguientes:

* Los dos componentes TIC para el Estado que buscan el buen funcionamiento y la relación con otras entidades públicas en el manejo de tecnologías de información y TIC para la Sociedad, teniendo como objetivo fortalecer la sociedad y la relación con el Estado en cuanto ambientes digitales, seguros, amigables y confiables; son líneas de acción que orientan el desarrollo y la implementación de la política

* Los tres habilitadores transversales Arquitectura, Seguridad y privacidad, y Servicios Ciudadanos Digitales son elementos de base que permiten el desarrollo de los componentes de la política.[36]

Por otro lado, Ciudadanos Digitales son elementos de base que permiten el desarrollo de los componentes de la política. El gobierno empleó estos elementos, y uno de los propósitos fue la Ley antitrámite, con la cual se busca disminuir procesos del Estado y generar confianza para poder realizarlos electrónicamente y digitalmente a través de las TIC.

[35] GOBIERNO EN LÍNEA. ¿Qué es la política de Gobierno Digital? Gobierno digital. {En Línea}. 2017 Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html
[36] Ibíd., párr. 15.

Es preciso señalar que el Ministerio de las Tecnologías de la Información y la Comunicación es el líder de la política digital, y además es el encargado de hacer las normas y leyes para el normal funcionamiento de todas las entidades públicas de orden territorial y nacional. La estructura de Gobierno en Línea comprende cuatro componentes de la estrategia que son TIC para Servicios, TIC para Gobierno Abierto, TIC para Gestión y Seguridad, y Privacidad de la Información. En la siguiente tabla se describe cada componente de la estrategia Gobierno en Línea:

Tabla 1. Descripción compontes Estrategia Gobierno en Línea

	ESTRATEGIA GOBIERNO EN LÍNEA			
COMPONENTES	DESCRIPCIÓN	LOGROS	CRITERIO	SUBCRITERIOS
TIC PARA LA GESTIÓN	Comprende la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información, gestión y aprovechamiento de la información para el análisis y toma de decisiones.	**Estrategia de TI.** Busca aportar valor al desarrollo sectorial e institucional de las entidades a través de una estrategia de TI. **Información.** Busca aportar valor estratégico a la toma de decisiones a partir de la gestión de la información como un producto y servicio de calidad.	Busca la comprensión de la situación actual de la entidad, contexto organizacional y entorno relacionado con el uso de las tecnologías. Entendimiento y direccionamiento estratégico. Diseño de componentes de la información. Análisis y aprovechamientos de componentes y información. Gestión de la Calidad y de Seguridad de los Componentes de Información.	La entidad cuenta con un diagnóstico del entorno nacional, sectorial o institucional, que incluya el entendimiento estratégico de la Arquitectura Empresarial, dinámica organizacional y análisis del desempeño estratégico.
TIC PARA GOBIERNO ABIERTO	Comprende las actividades encaminadas a fomentar la construcción de un Estado más transparente, participativo y colaborativo	**Transparencia**. Busca facilitar el acceso a la información pública de manera permanente y permitir	**Acceso a la información pública**. Busca poner a disposición del público toda la información del estado. A través de la rendición de cuentas se publica	Mantiene actualizada y disponible la información pública, habilitan canales electrónicos para realizar convocatorias y

	en los asuntos públicos mediante el uso de las TIC.	su aprovechamiento por parte de los usuarios ciudadanos y grupos de interés **Colaboración.** Busca la generación de soluciones provenientes de los usuarios, en cuanto a retos o problemáticas identificados por las entidades y/o por los usuarios. **Participación.** La entidad cuenta e implementa una estrategia de participación electrónica que busca promover la participación, conocer e involucrar a los usuarios en el quehacer público	de manera clara información entre el Estado y los usuarios a través de las TIC. **Innovación abierta.** Pretende la construcción de soluciones a problemas o retos públicos a través de acciones de colaboración con los usuarios, ciudadanos y grupos de interés. Participación en medios electrónicos, participación ciudadana y toma de decisiones.	tener disponible la información pública. La entidad gestiona las acciones de colaboración para obtener la(s) solución(es) o mejora(s) a los problemas Los retos identificados. La entidad habilita los canales electrónicos para involucrar a los usuarios, ciudadanos y grupos de interés dentro de procesos de toma de decisiones.
TIC PARA SERVICIOS	Comprende la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los usuarios y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo.	**Servicios centrados en los usuarios.** Los usuarios cuentan con una oferta de trámites, servicios y espacios de comunicación a través de canales electrónicos usables y accesibles que responden a sus necesidades y expectativas.	**Caracterización de usuarios**. Define el segmento al que se va a dar solución para responder a sus necesidades. **Accesibilidad.** Trámites y servicios disponibles para toda la población incluida la población con discapacidad. **Usabilidad.** Fácil	Deben contar con directrices de uso, accesibilidad y caracterización, al igual que el uso de internet. La entidad habilita a través de web, móvil e integrado el sistema de PQRD La entidad proporciona os formularios de acuerdo a la norma al igual un sistema para descarga de

		Sistema integrado peticiones, quejas, reclamos y denuncias (PQRD). Los usuarios cuentan con múltiples canales que operan de forma integrada, para la atención de peticiones, quejas, reclamos y denuncias. **Trámites y servicios en línea.** Los usuarios cuentan con múltiples canales que operan de forma integrada, para la atención de peticiones, quejas, reclamos y denuncias. Monitoreo y mejoramiento continuo. Pretende desarrollar actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información y los sistemas de información.	uso de las herramientas. **Promoción.** Aumentar el conocimiento y uso de las TIC. **Evaluación de la satisfacción del usuario.** Grado de satisfacción del usuario. **Mejoramiento continuo.** Aumentar niveles de satisfacción del usuario. Sistema web, móvil e integrado de contacto, peticiones, quejas, reclamos y denuncias (PQRD). Formularios diligenciables, transaccionales y descargables, certificaciones y constancias en línea Trámites y servicios en línea	certificaciones y tramites en línea.
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Comprende las acciones transversales a los demás componentes enunciados,	**Definición del marco de seguridad y privacidad de la información y de**	Diagnóstico, gestión de riesgos y plan de seguridad y	Definir acciones, mediciones, evaluación, seguimiento y contar con un plan de seguridad y

	tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.	**los sistemas de información.** Se quiere definir el estado actual del nivel de seguridad y privacidad y definir las acciones a implementar. **Implementación del plan de seguridad y privacidad de la información y de los sistemas de información.** Busca desarrollar las acciones definidas en el plan de seguridad y privacidad. **Monitoreo y mejoramiento continuo** Pretende desarrollar actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información y los sistemas de información	privacidad de la información. Evaluación de desempeño.	privacidad de la información.

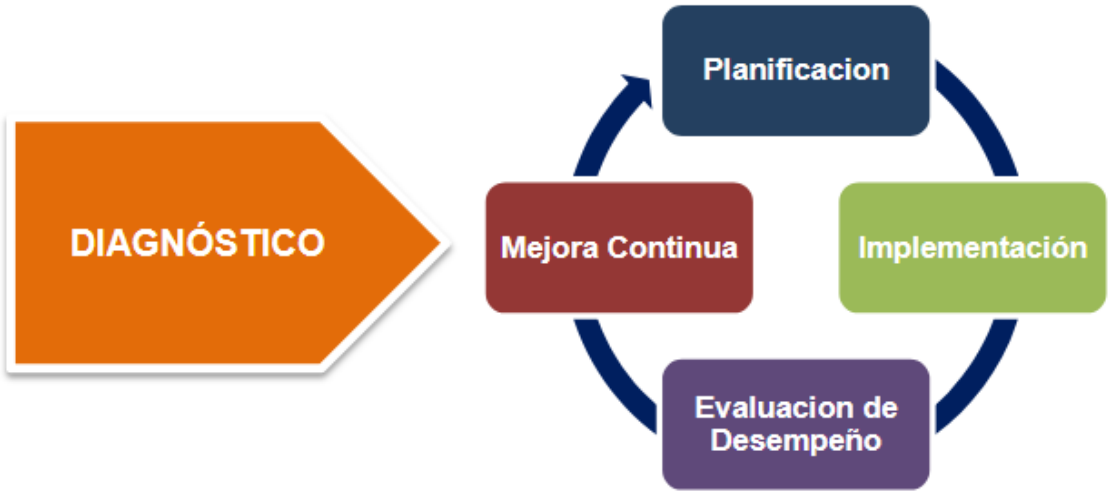
Fuente: El Autor con base en GOBIERNO EN LÍNEA. Manual/estrategia de Gobierno en Línea. {En Línea}. 2017 Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf

5.2.3 MSPI (Modelo de seguridad y privacidad de la información)

Dentro de la estrategia de Gobierno en Línea GEL se ha implementado un Modelo de Seguridad y Privacidad de la Información para fortalecer la seguridad de la

información de acuerdo a las nuevas tendencias tecnológicas. Este documento (MSPI) está basado en el ISO 27001 de 2013, y en cuanto al componente legal se basa en la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública[37]. El Modelo de Seguridad y Privacidad de la Información comprende cinco fases de su ciclo de operación y se describen a continuación.[38]

Figura 6. Ciclo de operación del modelo seguridad y privacidad de la información



Fuente: MINTIC. Seguridad y Privacidad de la Información. Modelo. {En Línea}, s.f. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Fase 1. Diagnóstico. Permite verificar el estado actual y alcanzar las siguientes metas:

- "Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.
- Determinar el nivel de madurez de los controles de la seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.

[37] GLOBALTEK. Implantación MSPI – Modelo de Seguridad y Privacidad de la Información. Consultoría. {En Línea}, s.f. Disponible en: https://www.globalteksecurity.com/mspi-implantacion-modelo-de-seguridad-y-privacidad-de-la-informacion-gel/

[38] MINTIC. Seguridad y Privacidad de la Información. Modelo. {En Línea}, s.f. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- Identificación del uso de buenas prácticas en ciberseguridad”.

“Para realizar dicha fase las entidades deben efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad. Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación.

Fase 2. Planificación. Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo. Esta fase tiene las siguientes metas:

- Políticas de seguridad y privacidad de la información, este documento debe ser aprobado por la entidad y debe contener objetivo, alcance y nivel cumplimiento.
- Política de la seguridad y privacidad de la información, manual de políticas de seguridad y privacidad de la información, se deben explicar políticas, principios y normatividad.
- Procedimientos de seguridad de la información, se desarrollan y formalizan procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.
- Roles y responsabilidades de seguridad y privacidad de la información, mediante acto administrativo se deben asignar los roles en los diferentes niveles, para la correcta toma de decisiones.
- Inventario de activos de información, generar un inventario de activo de información exacto para poder definir nivel de criticidad de los mismos.
- Integración del MSPI con el sistema de integración documental. La entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental emitido conforme a los parámetros generados por el archivo general de la nación.
- Identificación, valoración y tratamiento de riesgos, se define una metodología para dar seguimiento a los riesgos.
- Plan de comunicaciones, estrategia para generar cultura organizacional, con sensibilización y capacitación.
- Plan de transición de IPv4 a IPv6, para llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, se debe cumplir con la fase de planeación establecida en la Guía n°. 20.”

Fase 3. Implementación. Esta fase le permite a la entidad llevar a cabo la implementación de la planificación realizada en la fase anterior del MSPI. Comprende las siguientes actividades:

- “Planificación y control operacional, se debe tener toda la documentación documentada para verificar que los procesos se estén llevando bien, y tener soporte en caso de presentarse algún riesgo, poder solucionarse.
- Implementación del plan de tratamiento de riesgos, se debe implementar de acuerdo a los riesgos que se presenten y deben ser aprobado por cada uno de los dueños de los procesos.
- Indicadores de gestión, la entidad deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.
- Plan de transición de IPv4 a IPv6”.

Fase 4. Fase de evaluación de desempeño. El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas. Esta fase tiene las siguientes tareas:

- Plan de seguimiento y revisión a la implementación del MSPI, documento aprobado y revisado por la dirección de la entidad, donde tiene la revisión de actividades, controles de riesgo y ejecución e implementación del MSPI.
- Plan de ejecución de auditorías, la entidad debe generar un documento donde se especifique el plan de auditorías para el MSPI, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Fase 5. Fase de Mejora continua. Con los resultados obtenidos en la fase 4 se debe buscar un mejoramiento continuo de seguridad y privacidad de la información para mitigar debilidades encontradas.

Modelo de madurez

Dentro de una organización se puede identificar el nivel en que se encuentra el MSPI y se puede medir la brecha al nivel optimizado. En la siguiente tabla se encuentra la descripción de los niveles.[39]

[39] Ibíd., p. 32.

Tabla 2. Características de los niveles de madurez

Nivel	Descripción
Inexistente	• Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad. • No se reconoce la información como un activo importante para su misión y objetivos estratégicos. • No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
Inicial	• Se han identificado las debilidades en la seguridad de la información. • Los incidentes de seguridad de la información se tratan de forma reactiva. • Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
Repetible	• Se identifican en forma general los activos de información. • Se clasifican los activos de información. • Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. • Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. • La entidad cuenta con un plan de diagnóstico para IPv6.
Definido	• La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. • La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. • La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. • La Entidad tiene procedimientos formales de seguridad de la Información • La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. • La Entidad ha realizado un inventario de activos de información aplicando una metodología. • La Entidad trata riesgos de seguridad de la información a través de una metodología. • Se implementa el plan de tratamiento de riesgos. • La entidad cuenta con un plan de transición de IPv4 a IPv6.
Administrado	• Se revisa y monitorea periódicamente los activos de información de la Entidad. • Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. • Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. • Se utilizan indicadores de efectividad para establecer si la entidad

Fuente: MINTIC. Seguridad y Privacidad de la Información. Modelo. {En Línea}, s.f. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

5.2.4 Respuesta a incidentes de seguridad de TI[40]

Muchas veces las organizaciones únicamente toman medidas ante cualquier incidente hasta que estos se presentan, pero puede ser más costoso que hacer con

[40] MICROSOFT. Respuesta a incidentes de seguridad de TI. TechNet. {En Línea}, 2018. Disponible en: https://technet.microsoft.com/es-es/library/cc700825.aspx

anterioridad una estrategia para prevenirlas. Para responder correctamente a cualquier incidente se necesita lo siguiente:

- “Minimizar la cantidad y gravedad de los incidentes de seguridad.
- Crear un CSIRT principal (*Computer Security Incident Response Team*, Equipo de respuesta a incidentes de seguridad informática).
- Definir un plan de respuesta a incidentes.
- Es importante educar tanto a usuarios como empleados de una organización para proteger de posibles incidentes, puesto que muchas veces por desinformación y exceso de confianza se cometen errores y queda expuesta información a terceras personas que puedan hacer mal.
- Se debe educar en cuanto a encriptación, flujo de la información a través de redes, firewalls, supervisión de copias de seguridad, etc.

Se debe tener en cuenta que crear un CSIRT principal (*Computer Security Incident Response Team*, Equipo de respuesta a incidentes de seguridad informática). Crear este equipo es vital y es muy importante definirle a cada miembro del equipo la tarea que debe desempeñar para que no quede ningún área sin cubrir. Un equipo adecuado debe realizar las siguientes tareas:

- Supervisar los sistemas en busca de infracciones de seguridad.
- Servir como punto central de comunicación, tanto para recibir los informes de incidentes de seguridad como para difundir información esencial sobre los incidentes a las entidades correspondientes.
- Documentar y catalogar los incidentes de seguridad.
- Aumentar el nivel de conciencia con respecto a la seguridad dentro de la compañía para ayudar a evitar que se den incidentes en la organización.
- Posibilitar la auditoría de sistemas y redes mediante procesos como la evaluación de vulnerabilidades y pruebas de penetración.
- Obtener más información sobre las nuevas vulnerabilidades y estrategias de ataque.
- Investigar acerca de nuevas revisiones de software.
- Analizar y desarrollar nuevas tecnologías para minimizar los riesgos y vulnerabilidades de seguridad.
- Ofrecer servicios de consultoría sobre seguridad.
- Perfeccionar y actualizar continuamente los sistemas y procedimientos actuales”.[41]

No obstante, en caso de presentarse un incidente se debe informar al grupo y es importante seguir el proceso que se expone a continuación.

[41] Ibíd., párr. 18

Evaluación inicial: se debe determinar si es un verdadero incidente o es un falso positivo; se debe analizar qué tan grave es el incidente y registrar acciones minuciosamente.

Comunicación del incidente: se debe comunicar al equipo de CSIRT para que este dé las indicaciones y poder darle forma, con el fin de iniciar el proceso de coordinación de incidentes en el menor tiempo posible.

Contención de daños y minimización de riesgos: dependiendo la rapidez con la que se actúe para contrarrestar un ataque o incidente, así mismo será su resultado positivo y se sugieren las siguientes prioridades:

1. "Proteger la vida humana y la seguridad de las personas. Por supuesto, esta debe ser siempre la máxima prioridad.
2. Proteger la información secreta y confidencial. Como parte de su plan de respuesta a incidentes debe definir claramente qué información es secreta o confidencial. Esto le permitirá establecer prioridades a sus respuestas de protección de datos.
3. Proteger otra información como datos científicos, sobre propiedad o del ámbito directivo. Puede que otra información de su entorno también sea valiosa. Debe proteger en primer lugar los datos más valiosos antes de pasar a otros menos útiles.
4. Proteger el hardware y software contra el ataque. Esto incluye protegerlos contra la pérdida o la modificación de los archivos de sistema y contra daños físicos al hardware. Los daños en los sistemas pueden tener como consecuencia un costoso tiempo de inactividad.
5. Minimizar la interrupción de los recursos informáticos (incluidos los procesos). Aunque el tiempo de producción sea muy importante en la mayoría de los entornos, el hecho de mantener los sistemas en funcionamiento durante un ataque puede tener como consecuencia problemas más graves en el futuro. Por este motivo, la minimización de la interrupción de los recursos informáticos debe ser generalmente una prioridad relativamente baja."[42]

Identificación de la gravedad del ataque: se debe determinar la gravedad del incidente para contrarrestar el mismo y evitar pérdidas económicas y materiales y tener en cuenta lo siguiente.

- "Determinar la naturaleza del ataque (puede ser diferente a lo que sugiere la evaluación inicial).
- Delimitar el punto de origen del ataque.

[42] Ibíd., párr. 22

- Determinar la intención del ataque. ¿Estaba el ataque dirigido específicamente a su organización para conseguir información concreta o fue un ataque aleatorio?
- Identificar los sistemas puestos en peligro.
- Reconocer los archivos a los que se ha tenido acceso y determinar su grado de confidencialidad".

"Protección de pruebas: es importante que en el momento en que se descubra un incidente se realicen de inmediato copias de seguridad de la información y hacer la respectiva custodia de las pruebas, sellar con fechas y momentos en el que se está recolectando las pruebas; en caso de que en algún momento se desee hacer algún proceso para incriminar, estas pruebas deben cumplir con los requisitos de las leyes que estén vigentes para que sean válidas.

Recuperación de los sistemas: dependiendo del tipo de ataque, se debe tomar la decisión si se restaura el sistema o no es posible por el daño casado, por eso es de gran importante hacer copias de seguridad con regularidad ya que el sistema pudo haber sido dañado con un tiempo atrás y es clave determinar qué copia de seguridad es la adecuada para restaurar el sistema.

Recopilación y organización de las pruebas del incidente: se debe ser muy específico y detallada, y se recomienda que sea hecho por dos personas para que exista un control dual y no se pierda ningún registro que puede ser de gran importancia en el momento en que se quiera realizar algún proceso legal.

Valoración de los daños y costos del incidente: al determinar los daños que sufre la organización, se deben considerar tanto los costos directos como los indirectos. El daño y los costos del incidente constituyen una prueba importante y necesaria si decide emprender acciones legales.

Revisión de las encuestas y actualización de la directiva: una vez que se hayan finalizado las fases de documentación y recuperación, debe revisar el proceso minuciosamente. Determine con su equipo qué pasos se siguieron correctamente y qué errores se cometieron. En casi todos los casos se descubrirá que se deben modificar algunos procesos para controlar mejor futuros incidentes.

Encontrar debilidades en su plan de respuesta a incidentes: este análisis posterior tiene como objetivo encontrar oportunidades de mejora que iniciarán un nuevo proceso de planificación de la respuesta a incidentes".

5.2.4.1 CERT

A nivel internacional se conoce y se aplica el *Computer Emergency Respounse Team* (CERT), pero también se conoce con diferentes términos:

- CSIRT (*Computer Security Incident Response Team* - Equipo de respuesta a incidentes de seguridad informática).
- IRT (*Incident Response Team* - Equipo de respuesta a incidentes).
- CIRT (*Computer Incident Response Team*- Equipo de respuesta a incidentes informáticos).
- SERT (*Security Emergency Response Team* - Equipo de respuesta a emergencias de seguridad).
- ISIRT (*Information Security Incident Response Team* - Equipo de respuesta a incidentes de seguridad de la información).

"En Colombia se puede encontrar el colCert que es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, su objetivo principal es la coordinación de Ciberseguridad y Ciberdefensa nacional, proteger al Estado de emergencias de ciberseguridad. Ofrece servicios de prevención, y coordinan con mecanismos internacionales para coordinar este tema. Realizar protocolos y mecanismos de buenas prácticas de ciberseguridad y ciberdefensa.

Por otro lado, en Uruguay se denomina CERTuy, es el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay. El CERTuy protege los activos de información críticos del Estado y promueve el conocimiento en seguridad de la información para prevenir y responder a incidentes de seguridad. Sus principales objetivos son centralizar, coordinar y optimizar los procesos de respuesta a incidentes en seguridad de la información; difundir mejores prácticas en seguridad de la información y realizar tareas preventivas.

Por su parte, en Argentina se halla el ICIC, Programa Nacional de Infraestructura Crítica de Información y Ciberseguridad, busca proteger las infraestructuras tecnológicas del estado y del sector privado si así lo requiere. También tiene un sistema de capacitaciones que se realizan anualmente desde el 2011 llamado Ejercicio Nacional de Respuesta a Incidentes Cibernéticos (ENRIC), cuyo objetivo principal es capacitar en el marco legal relacionado con ciberincidentes. De la misma manera, en la página se encuentran cursos virtuales relacionados con informática y son totalmente gratis. El ICIC brinda cursos, talleres y charlas enmarcadas en la estrategia de capacitación diseñada por la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad.

También está el ecCert, siendo el Centro de Respuesta a Incidentes Informáticos y Control de las Telecomunicaciones del Ecuador, su compromiso es fortalecer el buen uso de internet y las comunicaciones, ofreciendo productos y servicios de calidad y con la cooperación a nivel internacional. En la página web se pueden reportar incidentes y también están constantemente actualizando diferente información de prevención en cuanto a ciberseguridad y ciberdefensa".

Además, en Perú se encuentra el PeCert, Coordinación de emergencias en Redes Teleinformáticas, lidera esfuerzo para contrarrestar ciber desafíos y coordina

defensa ante ciberataques para proveer a la nación ante una postura segura en el ámbito de la seguridad informática. En la página se pueden reportar incidentes y ofrecen servicios como *etichal hacking*, capacitación, análisis forense, *pentesting*, entre otros.

Del mismo modo, en Chile está ClCert, creado desde el 2001 como una alianza con el Laboratorio de Criptografía Aplicada y Seguridad.

5.2.5. Mecanismos de control en Colombia contra crímenes cibernéticos

En Colombia existe el CAI virtual en el cual se pueden hacer denuncias de delitos informáticos, a nivel nacional desde cualquier un computador.

- CAI VIRTUAL[43]

Es el Centro Cibernético de la Policía Nacional de Colombia, en esta página se pueden encontrar las formas más sencillas para hacer denuncias de crímenes cibernéticos, y muestran los diferentes operativos realizados a nivel nacional, donde dan captura a delincuentes después de un seguimiento, incurriendo en delitos como robo de celulares, clonación de tarjetas, *hackeos* ilegales, entre otros. También al realizar una navegación por la página muestra diferentes aplicaciones de seguridad y *tips* para protegerse de delitos informáticos, videos y documentos.

A través de dos páginas www.fiscalía.gov.co o www.policia.gov.co y en caso de no quieren revelar sus nombres lo pueden denunciar a través del correo denunciaanonima@fiscalia.gov.co

Los principales delitos informáticos que se presentan a nivel nacional, de acuerdo a los ciberincidentes generados en la página de CAI Virtual, tomando fecha de referencia de los dos últimos meses del año 2017 son los siguientes:

- *Pishing*
- Suplantación de identidad
- *Grooming*
- *Smishing*
- Sextorsión
- *Malware*

También con la aplicación se logró verificar que los casos presentados en el departamento de Boyacá fueron en la ciudad de Tunja, y el delito preponderante fue suplantación de identidad.

[43] CENTRO CIBERNÉTICO POLICIAL. CAI Virtual {En línea}. s.f. Disponible en: https://caivirtual.policia.gov.co/contenido/cai-virtual-0

- TE PROTEJO[44].

El 20 de febrero de 2008 la Red PaPaz convocó al Ministerio de Comunicaciones, Ministerio de Educación, varias empresas, ONG y a algunos padres y madres, a participar en un acuerdo para construir un sitio seguro el cual enseñe las normas derechos y deberes al utilizar las TIC, y proteger a la infancia y adolescencia; tomando en cuenta el continuo uso de estas herramientas y poder minimizar los delitos hacia esta población.

Esta página y esta organización han tenido grandes logros de modo que con sus estadísticas se puede analizar que en los últimos 5 años aumentaron los casos reportados, pero en el último año han ido disminuyendo gracias a la educación virtual y a la divulgación de formas de protección a través de estas organizaciones no conocidas.

Figura 7. Reportes procesados de denuncias virtuales

[44] TE PROTEJO. Logros y resultados. {En línea} s.f. Disponible en: http://www.teprotejo.org/index.php/es/logros-y-resultados

Fuente: TE PROTEJO. Logros y resultados. {En línea} s.f. Disponible en: http://www.teprotejo.org/index.php/es/logros-y-resultados

Figura 8. Categoría de reportes virtuales

Fuente: TE PROTEJO. Logros y resultados. {En línea} s.f. Disponible en: http://www.teprotejo.org/index.php/es/logros-y-resultados

Siendo el primer caso y con más porcentaje la pornografía infantil en el año 2017, se aclara que las mayores víctimas de estudio de esta página son los niños, niñas y adolescentes menores de 18 años.

Figura 9. Logros durante el 2017

Fuente: TE PROTEJO. Logros y resultados. {En línea} s.f. Disponible en: http://www.teprotejo.org/index.php/es/logros-y-resultados

Igualmente, se han logrado importantes capturas y bloqueos a páginas que promueven la pornografía infantil, así mismo las leyes del gobierno se han ido fortaleciendo y están siendo más duras para este tipo de crímenes cibernéticos que afectan directamente a la población más vulnerable que son los niños.

- TUS 10 COMPORTAMIENTOS DIGITALES[45]

En febrero de 2008 la Red PaPaz con el objetivo de "Promover el uso sano, seguro y constructivo de Tecnologías de la Información y las Comunicaciones (TIC) en la infancia y adolescencia"[46] convocó a una Mesa de Trabajo de Nuevas Tecnologías a las siguientes entidades:

- Ministerio de Tecnologías de la Información y las Comunicaciones
- Ministerio de Educación Nacional
- Oficina de Delitos Informáticos de la Policía Nacional

[45] RED PAPAZ. ¿Quiénes Somos? {En Línea} s.f. http://tus10comportamientosdigitales.redpapaz.org/index.php?option=com_k2&view=item&id=1:%c2%bfqui%c3%a9nes-somos?&itemid=2

[46] Ibíd., párr. 1

- Empresa de Telecomunicaciones de Bogotá ETB
- Fundación Telefónica
- Microsoft Colombia
- Fundación Alberto Merani
- Foro de Generaciones Interactivas
- Red PaPaz

En esta página se busca que todas personas que utilicen cualquier dispositivo digital, teléfono, computador, internet lo hagan de manera responsable, legal, respetuosa reconociéndose como un miembro del mundo virtual. Se define que los que utilizan las TIC no solo tiene derechos sino también deberes para la correcta utilización de estas tecnologías, y esto va dirigido a niños, niñas, adolescentes y adultos, al igual a instituciones que se comprometan a tener un adecuado comportamiento en la utilización de las TIC.

Los 10 comportamientos son los que se presentan a continuación:

- Respeto
- Libertad
- Identidad
- Integridad
- Intimidad
- Autonomía
- Calidad de vida
- Cuidado y acompañamiento
- Respeto por la ley
- Derecho de autor

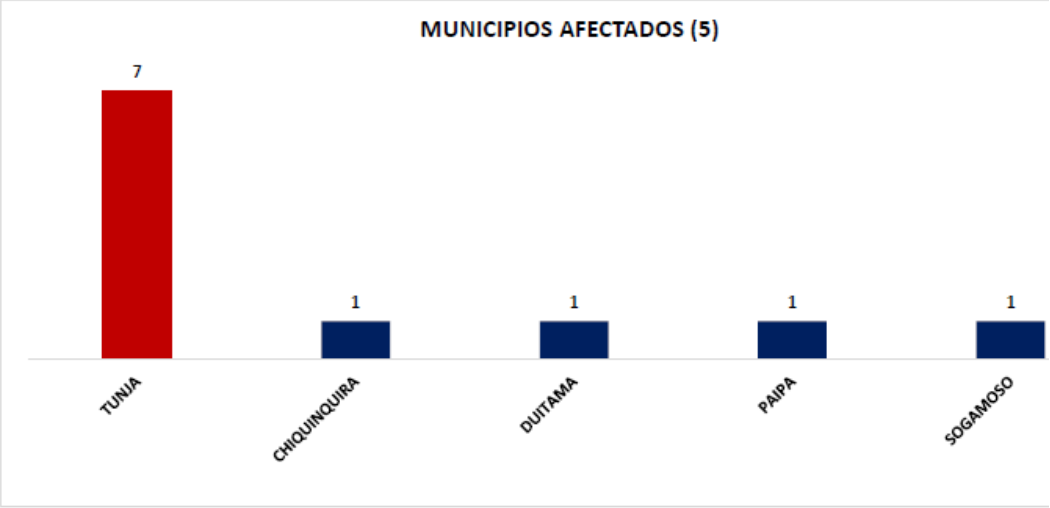
5.3. INCIDENTES PRESENTADOS EN LAS CIUDADES DE TUNJA, DUITAMA Y SOGAMOSO

Se han presentado delitos informáticos que se hacen virales en redes sociales, especialmente por la aplicación de Whatsapp, y se denomina estafa de colores de

whatsapp[47], es un enlace que invita a los usuarios a descargarlo para cambiar los colores del whatsapp siendo falso ya que realiza la descarga de un *malware* que infecta los dispositivos móviles, y hace que se genere una cadena al reenviar este tipo de información.

Gracias a información compartida por la Fiscalía General de la nación con sede en la ciudad de Tunja, que se utiliza en la presente monografía con fines académicos únicamente, en el siguiente grafico se muestra los principales municipios de Boyacá en los cuales se han presentado delitos informáticos siendo los principales Tunja, seguido de Chiquinquirá que no es el objetivo principal del estudio, pero se logra detectar que los delitos informáticos presentados en este municipio, tiene una participación importante, puede ser debido a su notable crecimiento a nivel económico e industrial y desafortunadamente es foco para delincuentes. Estas graficas tiene son de fecha Octubre de 2017, y es un censo realizado por parte de la fiscalía, y solo se analizan las noticias creadas por hechos ocurridos durante la semana del censo y no, de otras fechas.

Grafica No. Dinámica delitos informáticos, municipios afectados Octubre de 2017

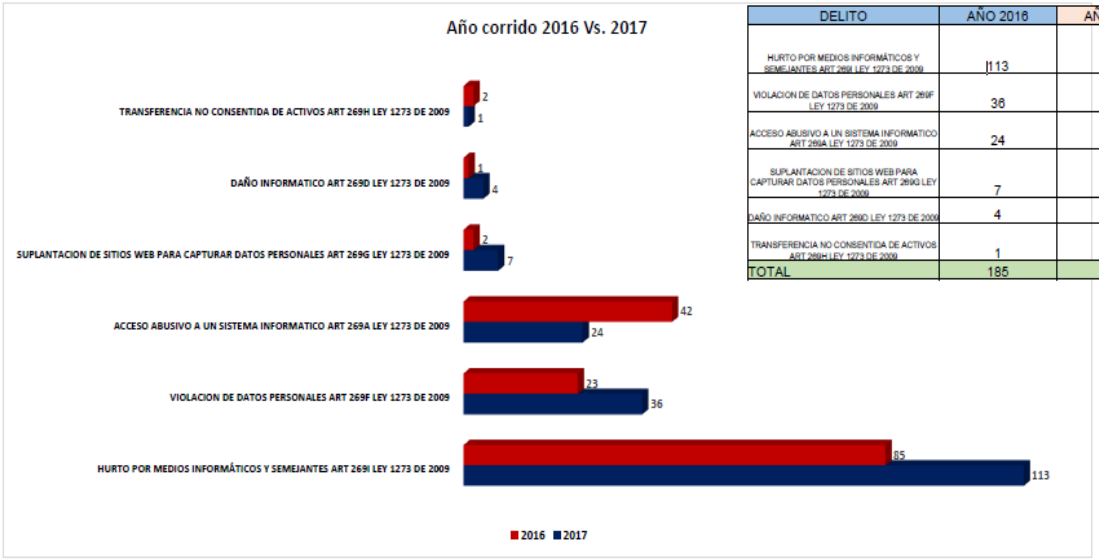


Fecha de la consulta: 07-11-2017_14:00 pm – Fuente: SPOA –SISAC – **Nota:** Solo se analizan las noticias creadas por hechos ocurridos durante la semana del censo y no, de otras fechas.

Fuente: Fiscalía General de la Nación Subdirección Seccional de Policía Judicial - Boyacá CTI-SAC Dinámica Delitos Informáticos

[47] EL GRUPO INFORMÁTICO. Cuidado en WhatsApp: vuelve el viral de "activar nuevos colores". [En Línea]. 2017. Disponible en: https://www.elgrupoinformatico.com/cuidado-whatsapp-vuelve-viral-activar-nuevos-colores-t37384.html

Grafica No. Año corrido 2016 – 2017



DELITO	AÑO 2016	AÑO 2017
HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES ART 269I LEY 1273 DE 2009	113	85
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009	36	23
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2009	24	42
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES ART 269G LEY 1273 DE 2009	7	2
DAÑO INFORMATICO ART 269D LEY 1273 DE 2009	4	1
TRANSFERENCIA NO CONSENTIDA DE ACTIVOS ART 269H LEY 1273 DE 2009	1	2
TOTAL	185	155

Fuente: Fiscalía General de la Nación Subdirección Seccional de Policía Judicial - Boyacá CTI-SAC Dinámica Delitos Informáticos

En la anterior grafico se analizan los principales delitos informáticos y su comparación en los dos últimos años, siendo los delitos informáticos presentados:

TRANSFERENCIA NO CONSENTIDA DE ACTIVOS ART 269H LEY 1273 DE 2009
HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES ART 269I LEY 1273 DE 2009
VIOLACION DE DATOS PERSONALES ART 269F LEY 1273 DE 2009
ACCESO ABUSIVO A UN SISTEMA INFORMATICO ART 269A LEY 1273 DE 2009
SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES ART 269G LEY 1273 DE 2009
DAÑO INFORMATICO ART 269D LEY 1273 DE 2009

De acuerdo con la entrevista con uno de los investigadores de la Fiscalía con sede en Sogamoso, Dario Rincón, quien lleva en la institución más de 15 años, declara que la institución, como otras entidades gubernamentales, tratan al máximo de generar conciencia en la ciudadanía para prevenir este tipo de delitos informático y han conseguido disminuir considerablemente, los casos presentados en el departamento de Boyacá, no obstante en este campo en el momento en que evolución la tecnología, de la misma manera los delincuentes crean nuevas formas de cometer delitos.

De la misma manera el gobierno está siendo muy estricto y severo con las leyes y condenando a los delincuentes, que cometen este tipo de actos, tal como lo define la ley 1273 de 2009 “De la protección de la información y de los datos”, que castiga económicamente las multas van entre 100 y 1000 SMMLV y penas hasta los 120 meses

5.3.3. Municipio de Tunja

Tunja es la capital del departamento de Boyacá, ubicada a 130 km del noreste de Bogotá a 2822 m s.n.m., con una población en el 2017 de 195.496 habitantes, siendo su principal actividad económica el ofrecimiento de bienes y servicios y en menor proporción la industria manufacturera. Es centro de estamentos gubernamentales, judiciales y ejecutivos, y se considera el centro de comercio de Boyacá, es también llamada la ciudad universitaria, se generan trabajos directos e indirectos, en los últimos años ha incrementado los ingresos del sector constructor.

“La estrategia de Gobierno en línea en el orden territorial apoya la modernización del Estado, promoviendo el acceso de los ciudadanos y servidores públicos a los servicios de este, en todos los municipios y departamentos”[48]. Gran parte de las entidades del orden territorial han recibido la conectividad a través del Programa Compartel en Banda Ancha para Instituciones Públicas del Ministerio de Comunicaciones; la plantilla del sitio web, siguiendo los lineamientos del sistema de Internet para la Rendición de Cuentas, un trabajo articulado entre el programa Gobierno en Línea, la Agencia Técnica de Cooperación Alemana - GTZ, Transparencia por Colombia, la Federación Colombiana de Municipios y Colnodo. Igualmente, reciben los correos electrónicos institucionales con el apoyo de Google y los equipos de cómputo necesarios para implementar el sitio web del municipio.

> De otra parte, la estrategia se centra en brindar el acompañamiento y la capacitación necesaria para que las administraciones locales puedan crear y mantener su propio sitio web, en el que se encuentre información dirigida a su comunidad y a su vez, cada comunidad puede darse a conocer dentro y fuera de Colombia. Pero, sobre todo, la Estrategia busca generar las capacidades locales que permitan sentar las bases institucionales para que los municipios y departamentos colombianos inicien el camino de Gobierno en línea y avancen en las fases de la estrategia de Gobierno en línea.”[49]

[48] ALCALDÍA DE BARRANCABERMEJA. Estrategia de Gobierno en línea en el Orden Territorial. {En Línea}. s.f. Disponible en: https://www.barrancabermeja.gov.co/estrategia-de-gobierno-en-l%C3%ADnea-en-el-orden-territorial. párr. 1

[49] ALCALDÍA DE MAGANGUÉ BOLIVAR. Estrategia de Gobierno en línea en el Orden Territorial. {En Línea}. s.f. Disponible en: http://www.maganguebolivar.gov.co/estrategia-de-gobierno-en-linea.html. párr. 3

Según la policía metropolitana de Tunja, a continuación se pueden encontrar las diferentes actividades que la institución realiza para prevención en la comunidad de diferentes delitos[50]:

- Top 1. Loterías falsas
- Top 2. Llamadas millonarias
- Top 3. Paquete chileno
- Top 4. Engaño
- Top 5. Estafas por internet

Frente a ello, es importante destacar que se puede ser víctima por ingenuidad, desesperación o ambición. Por tanto, brindan recomendaciones a los ciudadanos de obtenerse de dar información a través de redes sociales, desconfiar de transacciones a través de la red.

En un informe de la Policía Nacional, Departamento de delitos informáticos ubicado en la ciudad de Bogotá, donde consolidación en un informe de los delitos informáticos presentados en el departamento de Boyacá, desde enero hasta septiembre del año 2018, en el siguiente cuadro se presenta esta información de los delitos presentados en Tunja:

MUNICIPIO	DELITO	MODALIDAD	CANTIDAD
TUNJA (CT)	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	ACCESO REMOTO NO AUTORIZADO	4
TUNJA (CT)	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	APROVECHAMIENTO DE MALAS POLÍTICAS EN SEGURIDAD DE LA INFORMACIÓN	6
TUNJA (CT)	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	CORREO ELECTRONICO Y REDES SOCIALES SPAM, SCAM	19
TUNJA (CT)	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	SUPLANTACIÓN DE DOMINIO O URL - BLOG	1
TUNJA (CT)	ARTÍCULO 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN	IMPLEMENTACIÓN DE SOFTWARE MALICIOSO (MALWARE)	3

[50] POLICÍA NACIONAL DE COLOMBIA. Inicio. {En Línea} s.f. Disponible en: https://www.policia.gov.co

TUNJA (CT)	ARTÍCULO 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS	SUPLANTACIÓN DE SITIOS WEB (PHISHING)	2
TUNJA (CT)	ARTÍCULO 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS	SUPLANTACION SITIOS WEB	2
TUNJA (CT)	ARTÍCULO 269D. DAÑO INFORMÁTICO	DAÑO FÍSICO EQUIPO O MEDIO DE TRANSMISIÓN	2
TUNJA (CT)	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	ACCESO REMOTO NO AUTORIZADO	8
TUNJA (CT)	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	CORREO ELECTRÓNICO SPAM, SCAM	2
TUNJA (CT)	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	CORREO ELECTRONICO Y REDES SOCIALES SPAM, SCAM	4
TUNJA (CT)	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	EXTRACCIÓN DE DATOS O REGISTROS PERSONALES	12
TUNJA (CT)	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	MODIFICACIÓN DE DATOS O REGISTROS PERSONALES	1
TUNJA (CT)	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	SPOOFING	2
TUNJA (CT)	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	SUPLANTACIÓN DE SITIOS WEB (PHISHING)	2
TUNJA (CT)	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	SUPLANTACION SITIOS WEB	2
TUNJA (CT)	ARTÍCULO 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES	SUPLANTACIÓN DE IDENTIDAD POR CORREOS AJENOS	4
TUNJA (CT)	ARTÍCULO 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES	SUPLANTACION SITIOS WEB	2
TUNJA (CT)	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	AUDIORESPUESTA	2
TUNJA (CT)	ARTÍCULO 269I. HURTO POR MEDIOS	BANCA MOVIL	2

	INFORMÁTICOS Y SEMEJANTES		
TUNJA (CT)	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	CAJEROS AUTOMÁTICOS	32
TUNJA (CT)	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	CLONACIÓN DE TARJETA	2
TUNJA (CT)	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	DATAFONOS	2
TUNJA (CT)	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	INTERNET	27
TUNJA (CT)	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	PAGOS EN LÍNEA	31
TUNJA (CT)	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	PAGOS EN LÍNEA	1
TUNJA (CT)	ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	CRIPTOMONEDAS	2
TUNJA (CT)	ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	EXPLOTACIÓN DE VULNERABILIDADES (PHARMING)	6

Fuente: Policía Nacional, Dpto. delitos informáticos

5.3.2. Municipio de Duitama

Duitama está ubicado en el departamento de Boyacá, segundo municipio más poblado del departamento, con una población en el 2016 de 113.105 habitantes. Es uno de los mayores centros comerciales de la región donde unos de los principales ingresos son por transporte, y cuenta con las principales industrias de carrocerías reconocidas a nivel nacional e internacional. También su economía gira en torno a cosechas frutales como manzana, durazno, peras, curubas y ciruelas

El sitio oficial de la ciudad cuenta con un portal para realizar trámites, consulta, quejas, peticiones y reclamos virtualmente, y como Tunja tiene la estrategia de Gobierno en línea. En la ciudad de Duitama se presentaron delitos informáticos en julio del año pasado, y ocurrió realizando un “cambiazo” de tarjeta débito de una entidad financiera, logrando capturar a dos delincuentes que cometieron el ilícito. En estos casos las autoridades realizan las respectivas recomendaciones que por exceso de confianza y aceptar ayuda de terceros caen inocentemente en estos fraudes.

En un informe de la Policía Nacional, Departamento de delitos informáticos ubicado en la ciudad de Bogotá, donde consolidación en un informe de los delitos informáticos presentados en el departamento de Boyacá, desde enero hasta septiembre del año 2018, en el siguiente cuadro se presenta esta información de los delitos presentados en Duitama:

CIUDAD	DELITO	MODALIDAD	Cantidad
DUITAMA	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	ACCESO REMOTO NO AUTORIZADO	5
DUITAMA	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	APROVECHAMIENTO DE MALAS POLÍTICAS EN SEGURIDAD DE LA INFORMACIÓN	2
DUITAMA	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	CORREO ELECTRONICO Y REDES SOCIALES SPAM, SCAM	6
DUITAMA	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	MANIPULACIÓN DE CÓDIGO FUENTE	2
DUITAMA	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	SUPLANTACIÓN DE DOMINIO O URL - BLOG	4
DUITAMA	ARTÍCULO 269D. DAÑO INFORMÁTICO	ATAQUE CONJUNTO O RED DE ROBOTS INFORMÁTICO (BOTNET)	2
DUITAMA	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	EXTRACCIÓN DE DATOS O REGISTROS PERSONALES	4
DUITAMA	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	SUPLANTACION SITIOS WEB	6
DUITAMA	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	USURPACION DE IDENTIDAD	2
DUITAMA	ARTÍCULO 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES	SUPLANTACION SITIOS WEB	2
DUITAMA	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	AUDIORESPUESTA	2
DUITAMA	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	BANCA MOVIL	2
DUITAMA	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	CAJEROS AUTOMÁTICOS	19
DUITAMA	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	INTERNET	10
DUITAMA	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	PAGOS EN LÍNEA	18

DUITAMA	ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	EXPLOTACIÓN DE VULNERABILIDADES (PHARMING)	2
DUITAMA	ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	HARDWARE SKIMMING , KEYLOGGER	2
DUITAMA	ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	SENSOR DE ACTIVIDADES TECLADO O PANTALLA (KEYLOGGER)	7
DUITAMA	ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	TRANSACCIONES ELECTRONICAS (COMPRA VENTA DE PRODUCTOS POR INTERNET)	13

Fuente: Policía Nacional, Dpto. delitos informáticos

5.3.3. Municipio de Sogamoso

Ubicado en el centro oriente del departamento de Boyacá, con una población en 2016 de 112.190 habitantes, su actividad económica principal es la industria siderúrgica y materiales de construcción, con empresas importantes como Sidenal. En el sitio oficial de la ciudad se cuenta con un portal para realizar trámites, consulta, quejas, peticiones y reclamos virtualmente, y cuenta al igual que Tunja con Gobierno en línea.

Uno de los delitos informáticos presentados en el municipio fue la captura de un delincuente que estaba realizando tráfico de pornografía infantil a través de whatsapp, y pertenecía a una banda internacional de 43 integrantes ubicados en países europeos y de Latinoamérica que se dedicaban a difundir este tipo de contenidos; este delito en Colombia está dispuesto en el artículo 218 del Código Penal.

En un informe de la Policía Nacional, Departamento de delitos informáticos ubicado en la ciudad de Bogotá, donde consolidación en un informe de los delitos informáticos presentados en el departamento de Boyacá, desde enero hasta septiembre del año 2018, en el siguiente cuadro se presenta esta información de los delitos presentados en Sogamoso:

CIUDAD	DELITO	MODALIDAD	Cantidad
SOGAMOSO	ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	CORREO ELECTRONICO Y REDES SOCIALES SPAM, SCAM	5
SOGAMOSO	ARTÍCULO 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS	ATAQUES A DNS	2
SOGAMOSO	ARTÍCULO 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS	SUPLANTACION SITIOS WEB	2
SOGAMOSO	ARTÍCULO 269D. DAÑO INFORMÁTICO	MALWARE	2

SOGAMOSO	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	ACCESO REMOTO NO AUTORIZADO	5
SOGAMOSO	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	CORREO ELECTRONICO Y REDES SOCIALES SPAM, SCAM	2
SOGAMOSO	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	EXTRACCIÓN DE DATOS O REGISTROS PERSONALES	4
SOGAMOSO	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	IMPLEMENTACIÓN DE SOFTWARE MALICIOSO (MALWARE)	2
SOGAMOSO	ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES	SUPLANTACION SITIOS WEB	4
SOGAMOSO	ARTÍCULO 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES	SUPLANTACIÓN DE IDENTIDAD POR CORREOS AJENOS	2
SOGAMOSO	ARTÍCULO 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES	SUPLANTACION SITIOS WEB	2
SOGAMOSO	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	AUDIORESPUESTA	6
SOGAMOSO	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	BANCA MOVIL	9
SOGAMOSO	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	CAJEROS AUTOMÁTICOS	16
SOGAMOSO	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	DATAFONOS	2
SOGAMOSO	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	ENGAÑO	2
SOGAMOSO	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	INTERNET	31
SOGAMOSO	ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	PAGOS EN LÍNEA	12
SOGAMOSO	ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	EXPLOTACIÓN DE VULNERABILIDADES (PHARMING)	2
SOGAMOSO	ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	SENSOR DE ACTIVIDADES TECLADO O PANTALLA (KEYLOGGER)	2
SOGAMOSO	ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	TRANSACCIONES ELECTRONICAS (COMPRA VENTA DE PRODUCTOS POR INTERNET)	10

Fuente: Policía Nacional, Dpto. delitos informáticos

5.4. DIAGNÓSTICO A UNA MUESTRA DE LA POBLACIÓN DE TUNJA, DUITAMA Y SOGAMOSO

5.4.1. Sogamoso

En el anexo 1. Se pueden evidenciar las preguntas que se realizaron a entidades públicas y privadas como Entidades Financieras, colegios, entidades públicas y

privadas, cuyo objeto social está relacionado con el manejo de información tanto de terceras personas como manejo de información importante para dichas entidades.

El Banco Caja Social a través su sitio web ofrece a clientes del banco "el servicio de Banca Empresarial del Banco, este se publica a través del protocolo SSL, implementado mediante el uso de un certificado de servidor seguro, emitido al Banco Caja Social por Verisign, entidad de certificación digital abierta"[51].

El ingreso de la aplicación exige manejar altos niveles de cifrado, por lo que solo se pueden utilizar *browsers* de últimas versiones capaces de manejar llaves de cifrado de 128 bits o superiores. Se ha fortalecido el proceso de autenticación y operación de la aplicación mediante el uso de dispositivos de OTP (*Token*). Los equipos empleados para la prestación del servicio de banca empresarial forman parte de un esquema que permite mantener el servicio con un alto porcentaje de disponibilidad.

"Internet Empresarial Banco Caja Social cuenta con una moderna tecnología digital que brinda un manejo confidencial de la información y un alto nivel de seguridad. Mediante el *token* exclusivo para cada usuario registrado, su empresa obtiene comodidad y facilidad para llevar a cabo sus operaciones electrónicas en todo momento.

Características y beneficios

El portal utiliza el protocolo de seguridad SSL para transmitir documentos privados vía internet, encriptando la información por medio de códigos secretos y utilizando una llave privada para codificar los datos. Los navegadores Internet Explorer y Netscape soportan SSL. Certificado digital avalado por Certicámaras, filial de la Cámara de Comercio de Bogotá que garantiza que la información transmitida entre su empresa y el Banco sea segura y no pueda ser modificada por otro usuario".[52]

Los delitos más comunes presentados en la entidad son:

Clonación tarjetas débito y crédito

Cambiazo tarjetas débito y crédito

Suplantación de funcionarios

Compras con tarjeta de crédito no autorizadas

[51] BANCO CAJA SOCIAL, S.A. Plataforma de seguridad informática usada por el Banco. {En Línea} s.f. Disponible en: https://www.bancocajasocial.com/plataforma-de-seguridad-informatica-usada-por-el-banco. párr. 1

[52] BANCO CAJA SOCIAL, S.A. Seguridad en Internet Empresarial. {En Línea} s.f. Disponible en: https://www.bancocajasocial.com/seguridad-en-internet-empresarial. párr. 3-4

Con la entrevista realizada al funcionario, este informa que el banco cuenta con una plataforma segura para poder realizar transacciones por internet y los procesos operativos que realiza la entidad, puesto que siempre son revisados y supervisados para que no ocurran riesgos por el manejo de la información. Es obligación del banco y de todos los funcionarios, al realizar cualquier apertura de un producto entregar las recomendaciones de seguridad y en especial con las tarjetas de créditos que los incidentes más frecuentes no entregar el número de la tarjeta, ni ninguna clase de información, ni aceptar ayuda de extraños para manejo de medios electrónicos.

Cabe señalar que a nivel nacional hubo un incidente en la entidad hace alrededor de 8 años, en la cual hicieron fraude a muchos clientes substrayendo dinero, con este afectó mucho a la entidad por falta de controles internos, se vendió fraudulentamente información de clientes y suplantaron identidades, abriendo productos con documentos falsos.

ENTREVISTA REALIZADA AL SECTOR PÚBLICO

En el municipio de Sogamoso, su sistema de información está administrada por la empresa SYSMAN. Se han presentado en la entidad emergencias informáticas. No se han presentado casos de robo de información, pero en este momento se está realizando una auditoría y se ha detectado que la información no tiene los niveles de seguridad requerida y es manejada por la mayoría de funcionarios sin ninguna privacidad como lo necesita.

El municipio de Sogamoso cuenta con un software financiero que se utiliza en la dependencia Secretaría de Hacienda, dentro del cual maneja varios módulos que se alimentan de información generada por los impuestos del municipio, para proteger la información se trabaja a la par con dependencia de las TIC y el proveedor del software Sysman, esto con el propósito de cuidar la información para evitar perdida de información o alteración del sistema.

La administración tiene en cuenta lo siguientes requerimientos para salvaguardar la información.

- Evalúa y actualiza de manera permanente el software ya implementado, o la creación de nuevos módulos, de acuerdo con los cambios tecnológicos, organizacionales y las necesidades de servicios ofrecidos o demandados por el Municipio o la ciudadanía para mejorar los procesos.
- Maneja diferentes programas de protección de software que permite al administrador verificar los usuarios y llevar un paso a paso de las modificaciones o cambios que se realizan en el sistema.
- Se cuenta con un servidor para la seguridad de la información este incluye encriptación de datos, tokenización y claves que ayudan a proteger los datos en cada uno de los módulos y aplicativos que maneja el software. La

encriptación protege la red y otros activos físicos como el servidor, los equipos de cómputo que se manejan en Hacienda y bases de datos, también se protegen los datos y archivos reales almacenados en ellos o que viajan entre ellos a través de Internet.

ENTREVISTA A INSTITUCIONES EDUCATIVAS

Colegio CEDHU

Los equipos de la institución cuentan con antivirus, *firewall*, y los equipos de las áreas administrativas cuentan con usuarios y claves de seguridad para manejo de la información. Tiene un control de navegador de páginas web para que estén restringidas especialmente de pornografía y redes sociales. Se han presentado en la entidad o se han visto involucrados los estudiantes en algún tipo de emergencia cibernéticos

La mayoría de casos que se presentan son por ciberbullying de los estudiantes y se maneja con charlas para los estudiantes en las clases de informática y otras materias.

Ocurrió un incidente en el cual a través de una red social crearon un grupo donde participaban diferentes instituciones educativas de la ciudad de Sogamoso, generando bullying a determinado estudiante. De inmediato los docentes de la institución informaron a las directivas de la misma, y a su vez estas informaron a la policía de infancia y adolescencia para que se realicen las investigaciones pertinentes y lograr ubicar quién era el creador de la red para realizar las medidas pertinentes.

La educación que ofrecen a los estudiantes está orientada a la prevención de delitos informáticos. No está orientada a la prevención de delitos informáticos, se basan en manejo de software y programación.

5.4.2. Tunja

En la ciudad de Tunja se toma como referencia a Indeportes Boyacá, de acuerdo a un estudio realizado[53]:

> La información se encuentra en constante peligro ya que la mayoría de los documentos carece de contraseñas tal como lo específica la norma de seguridad NTC 5411-1:2006, además que el tratamiento de la información no

[53] RODRÍGUEZ CARRILLO, Ana María. Análisis y diagnóstico de la seguridad informática de indeportes Boyacá. Trabajo de grado para optar el título de Especialista en Seguridad informática. Tunja: Universidad Nacional Abierta y a Distancia, 2014. P. 74

tiene definido un Sistema de Gestión de Seguridad Informática como lo indica la norma NTC ISO/IEC 27001. Cada usuario dispone de su información sin tener un orden o restricción, además que los equipos se encuentran altamente vulnerables teniendo en cuenta que utilizan el servidor como medio de dispersión de archivos, lo que hace que cualquier usuario que ingrese a la red tenga acceso a esos documentos, no tienen un tratamiento adecuado de la información sino que solo la almacenan en equipos, memorias, impresiones etc., pero no cumplen con la confidencialidad ni la disponibilidad.

De acuerdo a lo anterior, se evidencia claramente que la monotonía y la idea que nunca ha pasado nada hace que los procesos de seguridad en la información no tengan la seguridad que exige la norma NTC, y los excesos de confianza producen un alto riesgo de que se pueda presentar un delito informático; en este informe se hicieron pruebas de vulnerabilidad y con proceso muy fáciles se puede acceder a la información.

5.4.3 Duitama

En el Municipio de Duitama la principal actividad económica es el transporte, seguida de establecimientos de comercio como ropa, zapatos, y víveres, los principales delitos que se presentan en la ciudad son hurtos y delincuencia común, no obstante el sector bancario es el que más se ve afectado en cuanto a delitos informáticos, a continuación se describen los más recientes delitos presentados en la ciudad.

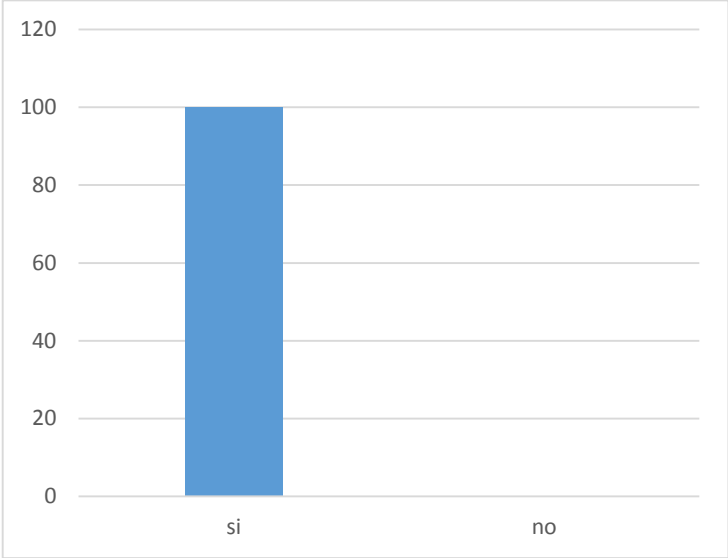
En la ciudad de Duitama, en Julio de 2017 se presentó un cambiazo de tarjeta débito de una cliente del Banco Popular, al momento los funcionarios de la entidad se percataron de los hechos a través de las cámaras de seguridad de la entidad, y de inmediato dieron aviso a las autoridades, las cuales dieron captura a los delincuentes cuando estaban intentando retirar del cajero automático. Estos hechos ocurren por la ingenuidad de los usuarios bancarios al recibir ayuda de extraños para realizar transacciones en cajeros automáticos.

En una entrevista con la Ingeniera de Sistemas de almacenes Paraíso, informa que no se han presentado ataque informáticos con mayor trascendencia, pero que la empresa cuenta con un sistema de seguridad para ataque informáticos en caso de presentarse.

6. TABULACION DE LA INFOMACION

Se va a realizar un análisis de cada pregunta de la encuesta anterior para poder definir y sacar conclusiones de la información recolectada en las ciudades de Tunja, Duitama y Sogamoso, a una población con conocimientos básicos en seguridad informática ya que se usan términos que son de esta área de conocimiento.

En la primera pregunta, se analiza si conocen sobre cibercrímen y ciberseguridad.

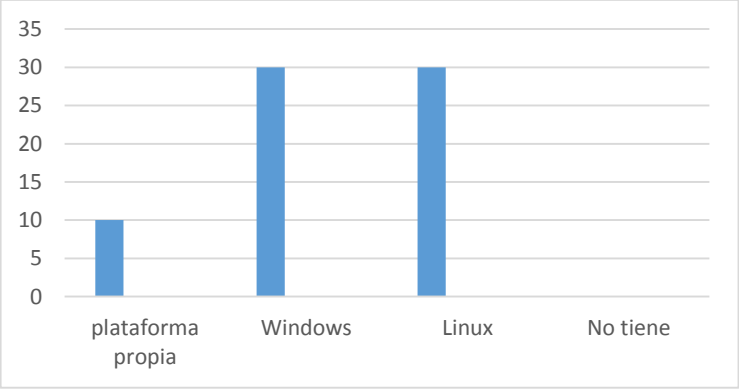


Gráfica 1. Conocimiento sobre ciberseguridad y cibercrímen

En la gráfica 1, podemos notar que todos los encuestados responden que si conocen sobre ciberseguridad y cibercrímen, y se aclarar que a todas las personas que se les realizo la encuestas son profesionales en sistemas.

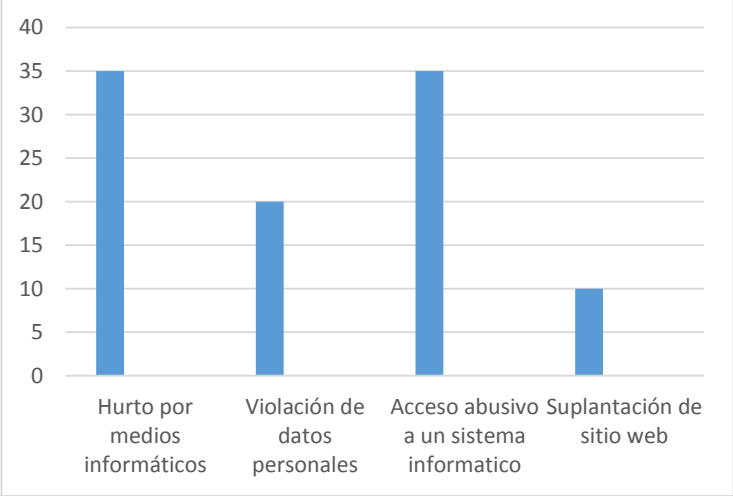
En la segunda pregunta, se pedía describir estos eventos dentro de su organización, los eventos más frecuentes que se presentaban en las empresas, eran virus, malware, con más frecuencia a través de internet por permitir páginas y descargar archivos sin autorización que afectan la seguridad de la empresa.

En la tercer pregunta se indaga sobre la plataforma de seguridad con la que cuenta la entidad a la que pertenece, y todos cuentan con una plataforma de seguridad bajo un sistema Linux, Windows y plataformas propias, la última la manejan empresas grandes, las cuales manejan más información sensible de la población como el Municipio de Sogamoso y almacenes Paraíso.



Grafica No. 2 Plataforma de seguridad

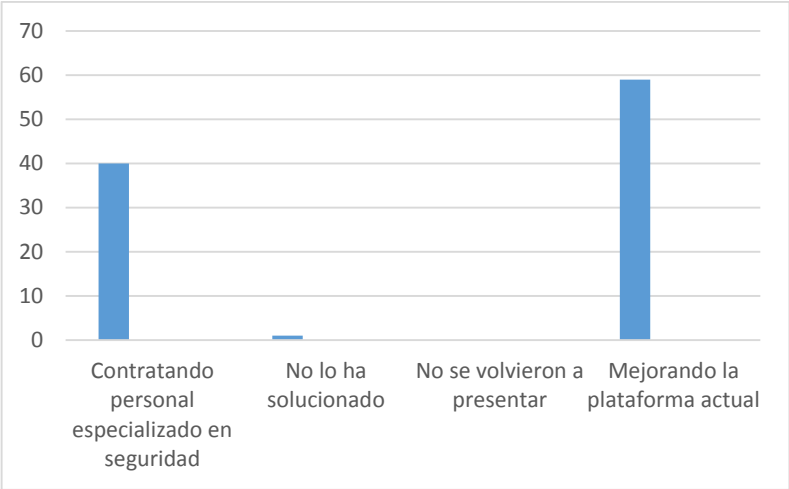
En la pregunta cinco, ¿Cuáles son las emergencias cibernéticas más frecuentes que se presentan en la organización?



Grafica No. 3 Emergencias cibernéticas

En la gráfica 3, vemos que los casos más frecuentes en las tres ciudades son acceso abusivo a sistema informático y hurtos por medios electrónico, cabe aclarar que en una de las encuestas informaron que dentro de la organización a la fecha no se han presentado ninguno de estos casos.

En la pregunta seis, Cómo han solucionado estos posibles evento NMs?



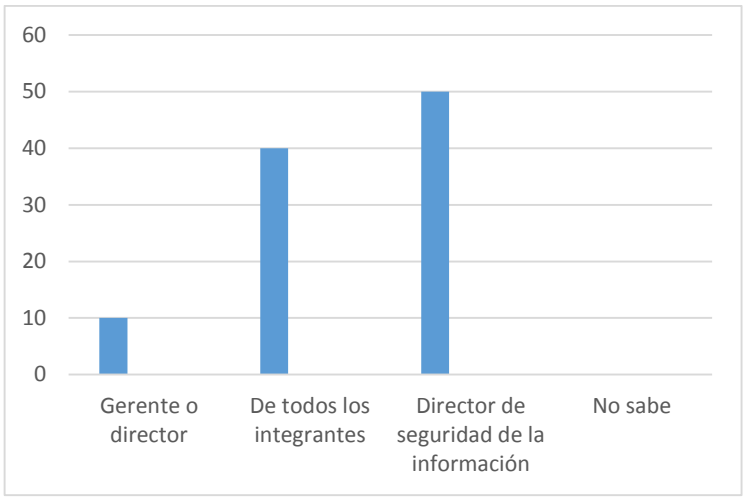
Grafica No. 4 Como soluciona problemas de seguridad

En esta grafica es claro que en las entidades donde se presenta este tipo de incidentes siempre buscan mejorar la plataforma, están siendo prevenidos ante posibles ataques, pero hay algunas que como no se presentan incidentes, no buscan actualizar y están corriendo riesgos, ya que los delincuentes si están siendo más agresivos con los ataques, y no hay que esperar a que sucedan los eventos, siempre es mejor prevenirlos.

En la pregunta No.6 se pregunta sobre los sistemas de seguridad maneja la entidad para proteger la información

Algunos no conoce el sistema, ya que la empresa no es tan amplia para compartir la información, los más comunes son: instalación de antivirus, encriptación de datos, software, hardware, red interna.

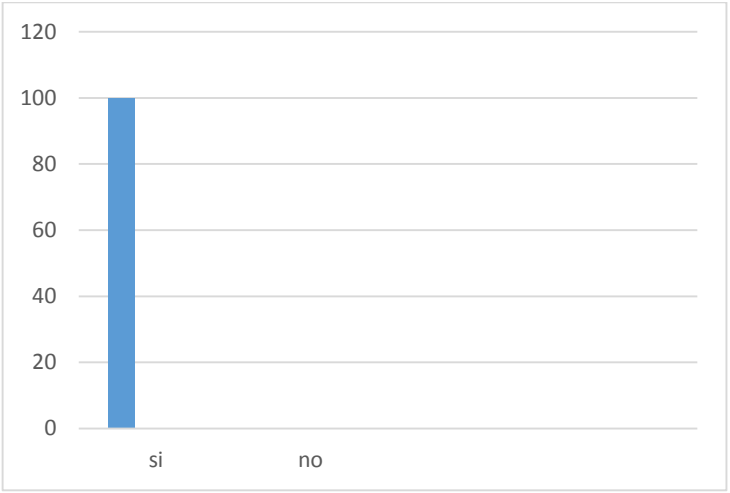
En la pregunta 7, el responsable de la seguridad dentro de la organización.



Grafica No 5. Responsabilidad de seguridad de la información

La grafica 5 nos muestra que es importante que todos los integrantes de una entidad estén comprometidos con cuidar y proteger información, liderados por el director de seguridad informática quien da las pautas y las normas que se deben seguir para proteger uno de los principales activos de una organización y es la información.

En la pregunta No. 8, se indaga sobre controles sobre internet ya acceso a correos y redes sociales

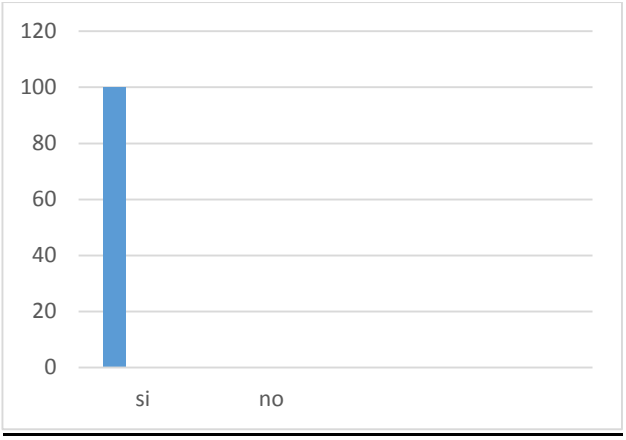


Grafica No. 6. Acceso a internet, correo y redes sociales

Es claro que la gráfica nos muestra que si hay restricciones para acceso a internet, en lagunas entidades permiten el acceso dependiendo la jerarquía dentro de la

entidad y también en una institución como el SENA permiten el acceso libre a internet ya que la forma de estudio es virtual

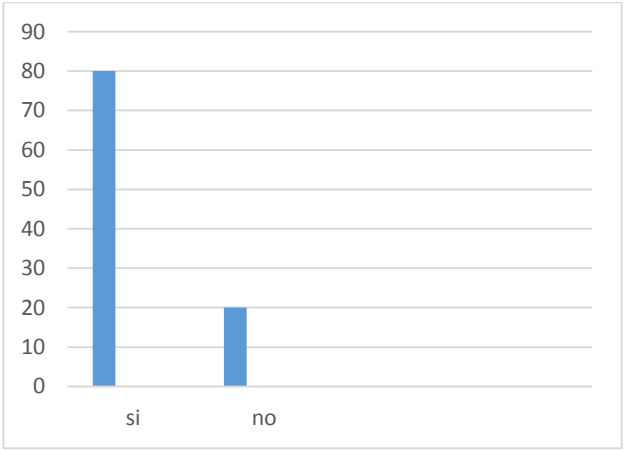
Pregunta No. 9, Se han presentado algún tipo de fallas debido a virus? Cuales?



Grafica No. 7 Fallas por virus

En todas las entidades se han presentado algún tipo de falla, desde la más sencilla como un virus hasta una más complicada pero no muy peligrosa como suplantación de identidad de una cuenta de correo electrónico.

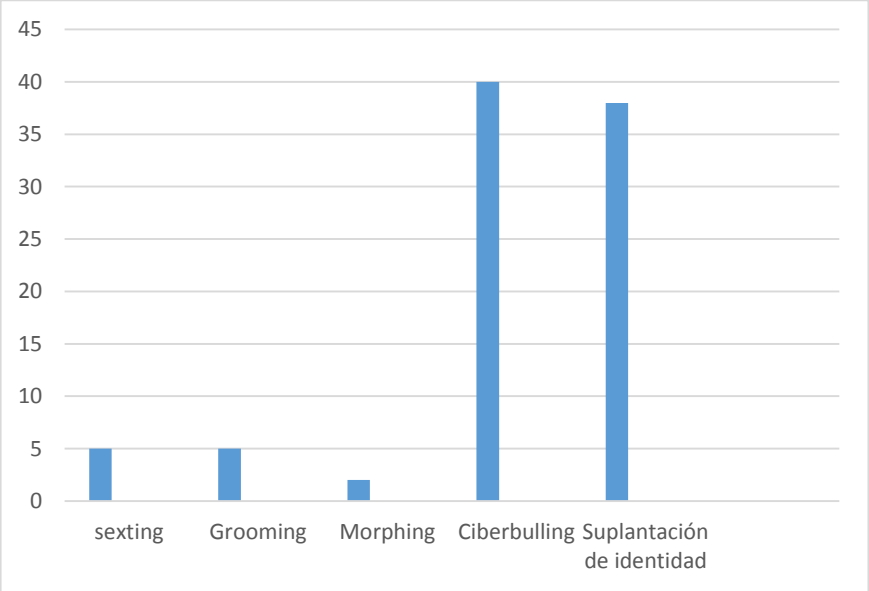
La pregunta 10. En caso de presentarse alguna emergencia cibernética, delito informático o evento similar, sabe a qué entidad del estado puede denunciar? Cuál?



Grafica No. 8 Conocimiento sobre a quién se deben denunciar cibercrímenes

La grafica nos muestra que a pesar de que en todos los medios de comunicación tratan de dar a conocer las formas para denunciar los delitos informáticos, no conocen a quien se debe denunciar, en los demás casos informan que si tienen conocimiento sobre la entidad a la cual se puede denunciar pero no mencionan la página virtual sino la institución en este caso La policía Nacional.

La pregunta No. 10 Existen delitos informáticos que están afectando al entorno (familia, colegio, trabajo, amigos etc) de una persona, De los siguientes delitos cuál conoce?



Grafica No. 9. Tipos de delitos informáticos

La grafica nos muestra que los delitos más comunes o más sonados en el medio son los que conocen, pero los tres primeros tienen muchísima incidencia en los últimos tiempos y en especial en población vulnerable como niños, adolescentes etc.

7. INFORME FINAL SOBRE INCIDENTES INFORMÁTICOS EN LAS CIUDADES DE TUNJA, DUITAMA Y SOGAMOSO, CON SUGERENCIAS Y RECOMENDACIONES

Las tecnologías de la información y la comunicación son una herramienta muy importante dentro de una organización, y en el departamento de Boyacá no dimensionan el valor que tiene los activos de información dentro de la misma, y dejan disponible datos a cualquier integrante de la empresa para que manipule información. Es una idea que se debe eliminar de las empresas puesto que en ellas se dice “acá nunca se ha presentado ese tipo de delitos”, y no esperar a que ocurra alguna pérdida de información esencial y se aprovechen los ciberdelincuentes para cometer delitos que pueden generar en ellos ingresos significativos, y para las empresas pérdidas irrecuperables.

El cibercrímen tiene inicios hace más de 30 años, pero para algunas entidades este tema es novedoso, y descuidan en muchas ocasiones la información que están administrando por desconocimiento de este tipo de delito, que en este momento no es necesario actuar con fuerza bruta sino simplemente ganando la confianza y aprovechando de la tranquilidad con que manejan los datos y con el pensamiento que nunca va a pasar nada hasta que en el menor tiempo sucede algo considerable que afecta mucho las finanzas de una entidad, o de la persona.

En los últimos años las TIC y su evolución, tocan el mercado del e-commerce y este se presta para que se active uno de los delitos más comunes y es el pishing que es el proceso mediante el cual se puede obtener información confidencial de forma fraudulenta, como contraseñas e información bancaria confidencial, otra de las modalidades de fraude frecuentes son Estafa a través de BEC (*Business Email Compromise*). Es una modalidad de fraude para las empresas que realizan transferencias electrónicas para pagar productos o servicios.

Vinculación de ciudadanos extranjeros en crímenes informáticos. Esta modalidad se presenta en la clonación de tarjetas débito y crédito de entidades financieras y llegan bandas internacionales a cometer este tipo de delitos en el país.

Presencia de usuarios colombianos en *Deep Web*. *Deep Web* es “la parte de internet que no ha sido indexada en un buscador”[i], este tipo de páginas no siempre son ilícitas pero sí se suelen utilizar para vender sustancias alucinógenas y evadir los controles legales.

Otros tipos de delitos no tan comunes pero que están activos y que muchas veces están sucediendo y en continua transformación por el nivel de maldad y malicia de los delincuentes son:

- *Vishing*. Es igual al pishing pero se utiliza una llamada telefónica, en lugar de un correo o un sitio web.

- *Baiting*. El delincuente de forma intencional deja un dispositivo extraíble como CD o una memoria USB, la cual contiene un programa malicioso que al ejecutarse puede abrir un programa para robar información sin que se dé cuenta el dueño del equipo.

- *Carding*. Es el proceso mediante el cual se utilizan tarjetas de crédito o los números de tarjeta de terceras personas, se relacionan con el *hacking* ya que se utiliza la ingeniería social para poder obtener información.

    - *Grooming*. Práctica realizada por un adulto que de manera deliberada y hasta sistemática engaña y establece relaciones de amistad con niñas, niñas y adolescente vía internet con el fin de obtener imágenes eróticas, personales o pornográficas.

    - *Suplantación de identidad.* Sin autorización un tercero se roba información personal para cometer ilícitos.

    - *Sexting*. Es el intercambio de mensajes de tipo sexual o erótico, sugerente o explícito vía teléfono celular

    - Sextorsión. Consiste en acciones de acceso, hostigamiento o constreñimiento a otras personas con amenazas personales o la publicación de imágenes íntimas, con el propósito de tener un favor sexual o dinero

    - *Ciberbullying*. Conforme a la Ley 1620 de 2013 se define como la forma e intimidación con uso deliberado de tecnología de información (internet, redes sociales y virtuales, telefonía móvil y videojuegos *on line*) para ejercer maltrato psicológico y continuado.

    - *Pornografía infantil*. Es la reproducción, producción, venta, ofrecimiento, compra, almacenamiento, transmisión, etc., de fotografías, videos o cualquier medio de representaciones reales o modificadas de cualquier tipo de actividad sexual que involucre menores de 18 años de edad.

    - *Morphing.* Es la producción de material sexual o pornográfico en el cual se incorporan imágenes editadas o se simula la voz de personas menores de 18 años de edad.

Todos estos tipos de delitos son los elementos del mundo del cibercrímen que en una definición amplia y muy específica, y es cualquier crimen o delito que se lleve a

cabo en línea es decir que se haga uso de internet para cometerlo y afectar información financiera y personal.

El común siempre comete un error al comparar un hacker con un ciberdelincuente y no es así ya que el primero su objetivo es entrar en un sistema, ya sea para mejorar la seguridad, o solo con fines lucrativos, mientras que el ciberdelincuente está cometiendo delitos que son castigados por la ley.

Resulta necesario concientizar a las empresas de que los activos de información son intangibles pero mucho más valiosos que los activos tangibles, y que deben cumplir con las normas mínimas que exige la ley para proteger la información, dado que los ciberdelincuentes están esperando a descubrir alguna posibilidad de cometer un delito con algo tan fácil como la ingeniería social, es decir basándose en la ingenuidad y el exceso de confianza para cometer el delito.

Es claro que en Colombia existen varios mecanismos de control que protegen a la comunidad, y al compararlos con las diferentes organizaciones a nivel latinoamericano estamos a la par en cuanto a controles, procesos y certificaciones.

En Colombia se creó GEL (Gobierno en Línea) que busca lograr que toda la comunidad este incluida en las TIC, y generar confianza y accesibilidad a un entorno digital de confianza, en todos este entorno del GEL, se conoce la ley anti trámites y que las diferentes organización facilitan los tramites de documentos al poder realizarlos a través del mundo digital, esto siempre con el respaldo de seguridad que da certicámara. Adicional a esto también se crea Internet para todos y Vive Digital, donde el ideal del gobierno es que todo el país pueda tener acceso al mundo digital, hasta los rincones más lejanos de Colombia.

En la mayoría de los casos cuando se maneja un sistema de información nunca se piensa en prevenir algún ataque, solo se espera a que ocurra y los costos en solucionarlo pueden ser mucho más altos, en lugar de pensar desde un principio en un plan de prevención, por esto es importante crear un CSIRT principal (*Computer Security Incident Response Team*, Equipo de respuesta a incidentes de seguridad informática). Crear este equipo es vital y es muy importante definirle a cada miembro del equipo la tarea que debe desempeñar para que no quede ningún área sin cubrir. Un equipo adecuado debe realizar tareas como monitorear, controlar, dirigir, planear, prevenir, y en caso de presentarse algún incidente logar identificar la alerta, un plan de prevención, de recuperación de la estabilidad del negocio, analizar las pruebas encontradas.

En Colombia contamos con el respaldo de entidades de Estados Unidos y la Unión Europea para control fraudes informáticos.

También existen entidades que controlan y protegen a la sociedad cuando se presenten casos de delitos informáticos, facilitando el proceso para realizar la denuncia porque todo el proceso es virtual, está el CAI Virtual, donde no solo se pueden poder las quejas y denuncios, sino también educan a la comunidad para prevenir estos delitos realiza jornadas de educación repartiendo volantes a la comunidad, la Policía Nacional que tiene contacto directo con la comunidad para prevenir estos delitos y "no dar papaya", ya que los delincuentes se aprovechan de la ingenuidad y la inocencia para poder cometer los delitos, no obstante en cualquier oficina de la Fiscalía reciben el denuncio de forma presencial, también existe una página que llama teprotejo.com Esta página y la organización Red PaPaz han tenido grandes logros de modo que con sus estadísticas se puede analizar que en los últimos 5 años aumentaron los casos reportados, pero en el último año han ido disminuyendo gracias a la educación virtual y a la divulgación de formas de protección a través de estas organizaciones no conocidas.

En el diagnóstico que se realiza en la tres ciudades Tunja Duitama y Sogamoso, es evidente que todos conocen los términos sobre ciberseguridad y cibercrímen, pero es claro que no se han presentado casos de delitos de alta complejidad, simplemente los más comunes como virus, gusanos entre otros, y es de mucha importancia que las personas especialistas en el tema que trabajan y tiene contacto en una organización, no conozcan a que entidades se debe denunciar estos delitos, y la forma de hacerlo, tan sencilla como en una página, que facilita los procesos a través de internet.

"No solo se debe conocer todos los términos y forma de prevenir los delitos informáticos, están las leyes que protegen a la sociedad y lo mejor que castigan a los delincuentes, la "Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos, la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes"[54]. El primero de los dos capítulos en que está dividida la ley trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. El segundo capítulo se refiere a los atentados informáticos y otras infracciones".

[54] DACCACH, José Camilo. Ley de Delitos Informáticos en Colombia. {En Línea}. 2016. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/. párr. 1

8. CONCLUSIONES

- Los delitos informáticos están catalogados como una fuente muy fuerte para poder perjudicar económicamente, socialmente a un individuo o a una empresa, y lograr acabar con la misma de una forma no violenta en algunas ocasiones, y si en un tiempo muy corto.
- En Boyacá, se presentan delitos informáticos en su gran mayoría violando datos personales para cometer ilícitos, pero hay una ventaja que el tipo de delito no ha crecido con respecto los ocurridos a nivel mundial, en este tiempo solo se presentan intrusiones sencillas que nos representan un grado de pérdida económica grande, no obstante los delincuentes conocen los procesos y hay que prevenir estos hechos.
- En Colombia, desde hace 4 años aproximadamente está tomando fuerzas las TIC, para que puedan llegar al alcance de toda la población del país, con la buena noticia que también cuenta con todos los procesos para educar y prevenir a los directamente involucrados en el medio, y que tengan la tranquilidad de usar medios digitales, un claro ejemplo es el as gobierno en línea, GEL.
- En cuanto a las leyes que castigan a los delincuentes en este tipo de delitos, están normadas a nivel nacional, y en el departamento de Boyacá, en las ciudades de Tunja, Duitama y Sogamoso, tiene claro la forma de aplicarlas y sobre todo divulgarlas para poder proteger a la comunidad, de esta manera estas leyes están sincronizadas no solo localmente sino el gobierno busca tener alianzas con entidades de otras naciones para mejorar los procesos.
- Con la posibilidad que se tuvo de interactuar con varias personas de las tres ciudades, que estaban empapados del tema de seguridad informática, también hay una alerta importante, y es que muchos no tenían claro a qué entidad debían denunciar en caso de presenta un caso de emergencia informática, y también la tranquilidad que los invade por no presentarse delitos ni emergencias informáticas en los entornos a los cuales pertenecen.

9. BIBLIOGRAFÍA

ÁL, José. ¿Qué es y cómo combatir el cibercrímen? {En Línea}. 2015. Disponible en: http://portaley.com/2015/04/que-es-y-como-combatir-el-cibercrimen/

ALCALDÍA DE BARRANCABERMEJA. Estrategia de Gobierno en línea en el Orden Territorial. {En Línea}. s.f. Disponible en: https://www.barrancabermeja.gov.co/estrategia-de-gobierno-en-l%C3%ADnea-en-el-orden-territorial

ALCALDÍA DE MAGANGUE BOLIVAR. Estrategia de Gobierno en línea en el Orden Territorial. {En Línea}. s.f. Disponible en: http://www.maganguebolivar.gov.co/estrategia-de-gobierno-en-linea.html.

BANCO CAJA SOCIAL, S.A. Inicio {En Línea} s.f. Disponible en: www.bancocajasocial.com.co

BANCO CAJA SOCIAL, S.A. Plataforma de seguridad informática usada por el Banco. {En Línea} s.f. Disponible en: https://www.bancocajasocial.com/plataforma-de-seguridad-informatica-usada-por-el-banco.

BANCO CAJA SOCIAL, S.A. Seguridad en Internet Empresarial. {En Línea} s.f. Disponible en: https://www.bancocajasocial.com/seguridad-en-internet-empresarial.

CARVAJAL AZCONA, Javier. ICEMD. . {En Línea}. s.f. Disponible en: https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo/

CENTRO CIBERNÉTICO POLICIAL. Informe amenazas de cibercrímen en 2016-2017. Bogotá, D.C.: Cairvirtual. 2017.

CENTRO NACIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA. Qué es el CERTuy. {En línea}. 2013. Disponible en: https://www.cert.uy/inicio/institucional/que_es_el_cert/

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009, no. 47.223

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 679. (3, agosto, 2001). Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación,

la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Diario Oficial. Bogotá, D.C., 2001. No. 44.509

COLOMBIA. CONGRESO DE LA REPÚBLICA. Proyecto de ley 050. (28, septiembre, 2017). Por la cual se formulan los lineamientos de política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos, en contra de niñas, niños y adolescentes; se modifica el código penal y se dictan otras disposiciones. Bogotá, D.C.: Cámara de Representantes, 2017.

DACCACH, José Camilo. Ley de Delitos Informáticos en Colombia. {En Línea}. 2016. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES No. 3854: Política nacional de seguridad digital. Bogotá, D.C.: Consejo Nacional de Política Económica y Social, 2016.

DIARIO EL COMERCIO. El ciberdelincuente que viajó por el mundo con millas de los famosos. {En línea}. 2015. Disponible en: http://www.elcomercio.com/actualidad/ciberdelincuente-viaje-mundo-millas-famosos.html

DIARIO EL TIEMPO. El intento de fraude en el que Bavaria casi pierde $ 9.000 millones. {En Línea}. 2015. Disponible en: http://www.eltiempo.com/archivo/documento/CMS-15961636

DIRECCIÓN NACIONAL DE INTELIGENCIA. Misión y Visión. {En Línea}. s.f. Disponible en: http://www.dni.gov.co/index.php?idcategoria=51

EL GRUPO INFORMÁTICO. Cuidado en WhatsApp: vuelve el viral de "activar nuevos colores". [En Línea]. 2017. Disponible en: https://www.elgrupoinformatico.com/cuidado-whatsapp-vuelve-viral-activar-nuevos-colores-t37384.html

GARCÍA DE LA CRUZ, Juan Manuel. Delitos Informáticos. Maestría en Administración con Especialidad en Informática. Culiacán: Universidad Valle Del Bravo, 2005.

GLOBALTEK. Implantación MSPI – Modelo de Seguridad y Privacidad de la Información. Consultoría. {En Línea}, s.f. Disponible en: https://www.globalteksecurity.com/mspi-implantacion-modelo-de-seguridad-y-privacidad-de-la-informacion-gel/

GOBIERNO EN LÍNEA. Manual/estrategia de Gobierno en Línea. {En Línea}. 2017 Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf

GOBIERNO EN LÍNEA. ¿Qué es la política de Gobierno Digital? Gobierno digital. {En Línea}. 2017 Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html

MICROSOFT. Respuesta a incidentes de seguridad de TI. TechNet. {En Línea}, 2018. Disponible en: https://technet.microsoft.com/es-es/library/cc700825.aspx

MINTIC. Seguridad y Privacidad de la Información. Modelo. {En Línea}, s.f. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MOLINA, Mateos. Conceptos y definiciones. {En línea}. s.f. Disponible en: http://molinamateos.com/content/conceptos-y-definiciones-0

OJEDA, Jorge; ARIAS, Miguel; RINCÓN, Fernando y DAZA, Libardo. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. Vol.11 No. 28. (Enero-junio 2010)

OROYFINANZAS.COM. Definición Criptomoneda: ¿Qué es una criptomoneda? {En Línea}. 2014. Disponible en: https://www.oroyfinanzas.com/2014/10/que-es-criptomoneda/

PARTIDO POLÍTICO MIRA. ¿Sabes cómo protegerte en la red contra delitos informáticos? {En línea}. s.f. Disponible en: https://partidomira.com/sabes-como-protegerte-en-la-red/

PERIÓDICO EL HERALDO. Capturan en la costa y el interior a banda de 18 cibercriminales conocida como 'Piratas del Caribe'. {En Línea}. 2015. Disponible en: https://www.elheraldo.co/judicial/capturan-18-implicados-en-banda-de-piratas-informaticos-214691

POLICÍA NACIONAL DE COLOMBIA. Inicio. {En Línea} s.f. Disponible en: https://www.policia.gov.co

POWER DATA. Seguridad de datos: En qué consiste y qué es importante en tu empresa. {En línea}. s.f. Disponible en: https://www.powerdata.es/seguridad-de-datos

RED PAPAZ. ¿Quiénes Somos? {En Línea} s.f. http://tus10comportamientosdigitales.redpapaz.org/index.php?option=com_k2&view=item&id=1:%c2%bfqui%c3%a9nes-somos?&itemid=2

RODRÍGUEZ CARRILLO, Ana María. Análisis y diagnóstico de la seguridad informática de indeportes Boyacá. Trabajo de grado para optar el título de Especialista en Seguridad informática. Tunja: Universidad Nacional Abierta y a Distancia, 2014.

SGSI. ¿Cuál es la diferencia entre ciberseguridad y seguridad de la información? Blog especializado en Sistemas de Gestión de Seguridad de la Información. {En Línea}. 2017 Disponible en: https://www.pmg-ssi.com/2017/01/ciberseguridad-seguridad-informacion/

SYMANTEC. De qué manera distinguir el cibercrímen y protegerse. {En Línea}. s.f. Disponible en: https://ar.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html

TEGUI BLOG. Delitos informáticos. {En Línea}. 2016. Disponible en: https://teguiblog.wordpress.com

TE PROTEJO. Logros y resultados. {En línea} s.f. Disponible en: http://www.teprotejo.org/index.php/es/logros-y-resultados

WIKIPEDIA. Hacker. {En Línea}. s.f. Disponible en: https://es.wikipedia.org/wiki/Hacker

: Fiscalía General de la Nación Subdirección Seccional de Policía Judicial -Boyacá CTI-SAC Dinámica Delitos Informáticos

10. ANEXOS

Anexo 1. Entrevista realizada a una muestra de la población en las ciudades de Tunja, Duitama y Sogamoso, con el fin de hacer el diagnóstico.

A continuación se presentan las preguntas realizadas a entidades en las ciudades de Tunja, Duitama y Sogamoso, para analizar la situación actual de las mismas en cuanto a ciberseguridad y cibercrímenes y la apreciación general que pueden tener en cuanto a estos temas.

1. Sabe usted que es ciberseguridad y cibercrímen?

Si

No

2. Si su respuesta es afirmativa describa estos eventos dentro de su organización.

_____

3. ¿Cuál es la plataforma de seguridad con la que cuenta la entidad a la que pertenece?

Plataforma propia

Windows

Linux

No tienen

4. ¿Cuáles son las emergencias cibernéticas más frecuentes que se presentan en la organización?

Hurto por medios informáticos

Violación de datos personales

Acceso abusivo a un sistema informático

Suplantación de sitio web

5. ¿Cómo han solucionado estos posibles eventos?

Contratando a personal especializado en seguridad

No lo ha solucionado

No se volvieron a presentar

Mejorando la plataforma actual

6. ¿Qué sistema de seguridad maneja la entidad para proteger la información?
   _____

7. ¿De quién es la responsabilidad de la seguridad dentro de la organización?

Gerente o Director __

De todos los integrantes __

Director de seguridad de la información __

No sabe __

8. En la empresa hay algún control para el uso de internet y en especial el acceso a redes sociales y uso de correo electrónico. Cuales?

SI __

NO __

_____

9. Se han presentado algún tipo de fallas debido a virus? Cuales?

SI __

NO __

_____

10. En caso de presentarse alguna emergencia cibernética, delito informático o evento similar, sabe a qué entidad del estado puede denunciar? Cuál?
    SI __
    NO __
    _____

11. Existen delitos informáticos que están afectando al entorno (familia, colegio, trabajo, amigos etc) de una persona, De los siguientes delitos cuál conoce?

    Sexting ___
    Grooming ___
    Morphing ___
    Ciberbullying ___
    Suplantacion de identidad ___