ANÁLISIS DE LA EVOLUCIÓN DEL ASEGURAMIENTO INFORMÁTICO EN ENTIDADES DEL SECTOR GOBIERNO COLOMBIANO

WILLIAM HERNANDO MARTINEZ RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA
2020

ANÁLISIS DE LA EVOLUCIÓN DEL ASEGURAMIENTO INFORMÁTICO EN ENTIDADES DEL SECTOR GOBIERNO COLOMBIANO

WILLIAM HERNANDO MARTINEZ RODRIGUEZ

Monografía de grado para optar al título de Especialista en Seguridad Informática

Ingeniera Yolima Esther Mercado Palencia
Directora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA
2020

Nota de aceptación:

_____
_____
_____
_____
_____
_____
_____

_____
Firma del director

_____
Firma del jurado

_____
Firma del jurado

Bogotá, 20 de mayo de 2020

DEDICATORIA

A Dios todopoderoso quien nos da la fortaleza, la salud, la vida y todo lo necesario para alcanzar nuestros propósitos y nuestras metas, infinitas gracias.

A mis padres que desde pequeño me han enseñado a valorar todo en la vida, desde lo más pequeño hasta lo más grande, a ellos que siempre me han inculcado la humidad y el respeto por los demás, a ellos que siempre me han enseñado a salir adelante en la vida.

A mi esposa, la mujer que Dios puso en mi camino, ella que siempre me brinda sus palabras de aliento, ella que es el soporte en el que se apoya mi vida, ella con la que miramos juntos el mismo horizonte, gracias por estar siempre ahí cuando lo necesito.

A mi hermosa hija, mi princesa, el motor que revoluciona mis días, el regalo más preciado que me ha dado Dios, mi princesa que le pone su toque de alegría y ternura, lo más hermoso de mi vida.

William Hernando Martínez Rodríguez

AGRADECIMIENTOS

A la Universidad Nacional Abierta y a Distancia – UNAD, de la cual soy egresado de Ingeniería en Telecomunicaciones por todos los conocimientos adquiridos en todos estos años de estar vinculado a ella.

A la Contraloría de Bogotá D.C., mi lugar de trabajo, donde me han brindado la oportunidad de extender mis conocimientos y quienes han aportado la experiencia para ser el profesional que soy hoy en día.

A la Ingeniera Yolima Mercado Palencia, por aportarme su experiencia y conocimiento en el apoyo y desarrollo de esta monografía, gracias por el aporte y dirección que ha brindado en este documento.

A los Ingenieros Luis Fernando Zambrano y Katerine Marceles, docentes de la UNAD, quienes me han orientado en el tema del documento y han aportado con las sugerencias para el buen desarrollo de la monografía.

William Hernando Martínez Rodríguez

CONTENIDO

pág.

LISTA DE GRAFICOS

pág.

LISTA DE CUADROS

pág.

RESUMEN

Se indagará sobre los principios e inicios que ha tenido la seguridad informática a través del tiempo y como esta ha influido en las organizaciones, buscando proteger los activos de información y haciendo que las empresas encuentren la mejor manera de adoptar un sistema de seguridad.

Con relación a lo anterior, se investigarán sobre los tipos de protección informática que se han venido utilizando, más específicamente en las entidades del sector gubernamental, verificando sus características, beneficios y sobre todo la protección que brindan frente a un posible ataque a los sistemas de información o accesos no autorizados.

Frente al sector gubernamental, se determinará en un acercamiento a algunas entidades, que beneficios les ha brindado la implementación de mecanismos, protocolos, políticas, entre otros y se identificara su uso con sus respectivas ventajas y desventajas con relación a la protección en este tipo de entidades.

Finalmente, y como aporte de la temática planteada, se pretende dar una orientación hacia importancia de la implementación de un sistema de seguridad informático en las entidades del sector gobierno, generando un documento de recomendaciones que guíe con mejores prácticas en cuanto a la protección de los activos de información y mejorando la defensa frente a los riesgos y amenazas los que están expuestas.

Palabras clave: Ciberseguridad, ciberdefensa, Mecanismos de seguridad digital, SGSI, ataques cibernéticos.

ABSTRACT

The principles and beginnings that computer security has had over time and how it has influenced organizations will be investigated, seeking to protect information assets and making companies find the best way to adopt a security system.

In relation to the above, investigate the types of computer protection that you have used, more specifically in the entities of the governmental sector, verifying their characteristics, benefits and over all the protection we provide against a possible attack on the information systems or accesses not allowed.

Faced with the government sector, it will be determined in an approach to some entities, which benefits have been provided by the implementation of mechanisms, protocols, policies, among others, and their use will be identified with their respective advantages and disadvantages in relation to protection in this type of entities.

Finally, as part of the theme, it is an orientation towards the importance of implementing the information security system in government sector entities, generating a document of recommendations that guide best practices in terms of asset protection. Of information and improving the defense against the risks and threats that are exposed.

Keywords: Cybersecurity, cyber defense, Digital Security Mechanisms, ISMS, cyber attacks.

INTRODUCCION

La seguridad de la información es un tema que hoy por hoy ha tomado una alta relevancia en todo tipo de organización tanto privada como pública, siendo estas últimas propensas a brindar información a la ciudadanía como usuario final. Esta información podría estar catalogada como sensible y es de gran importancia su cuidado con los controles y medios adecuados. Por esta y por otras tantas razones, los servicios y los sistemas de información de las entidades gubernamentales están más expuestas a ataques cibernéticos, enfrentando problemas como pérdidas o daños en la información y la infraestructura tecnológica.

En los últimos años, con el progreso en cuanto a tecnología y la utilización importante de las TIC, se han podido optimizar muchas actividades encaminadas y orientadas hacia la prestación de los servicios vitales y de gran importancia para la nación, de igual forma, el ingreso a internet ha tenido una función clave en muchos partes del gobierno, con lo cual se convierte en una herramienta de interacción continua entre muchas pretensiones entre la ciudadanía, las entidades y el propio gobierno, pero por otro lado, se ha venido incrementando el uso de las TIC para realizar actos delictivos, forjar amenazas informáticas, buscando con ello, afectar de una u otra forma a las infraestructuras tecnológicas, los sistemas de información e incluso desestabilizar e impactar los procesos que se lleven en algunas entidades gubernamentales.

Por estas razones es que las entidades gubernamentales han aumentado sus esfuerzos por detectar los riesgos informáticos a los que se encuentran expuestas y poner en consideración incluir dentro de los procedimientos de estrategia, guías de ciberseguridad y de ciberdefensa que se enfoquen a robustecer la seguridad informática de las entidades y de esta manera mantener disponibles los recursos y servicios que presten.

El tema abordado busca poder analizar la protección y seguridad que se está dando a la información en algunas entidades gubernamentales Colombianas frente al aseguramiento informático, recopilando datos y documentos que sirvan como base para la confrontación sobre los inicios que ha tenido la seguridad informática en las entidades del sector gobierno de Colombia y su influencia para enfocar los parámetros establecidos en las políticas de ciberseguridad y ciberdefensa establecidas por el Ministerio de Defensa y MinTIC. De igual forma se busca determinar cuál es el impacto y los beneficios que han tenido las acciones y la tecnología enfocada hacia la gestión de riesgos informáticos y la mitigación de las amenazas cibernéticas

Finalmente, se pretende poder aportar con un documento de recomendaciones que logre orientar en la importancia de implementar los sistemas de aseguramiento informático en las entidades del sector gobierno de Colombia y de esta forma contribuir en la optimización de la defensa contra los riesgos y amenazas a los que están expuestas.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCION DEL PROBLEMA

La pérdida o robo de la información, los ataques a los sistemas de información o el acceso no autorizado a la infraestructura tecnológica, son algunas de las situaciones que se pueden presentar en las organizaciones sean estas públicas o privadas y que frente a esta problemática se deben tomar las medidas pertinentes y adecuadas para minimizar los riesgos y las amenazas que se posean con relación a la seguridad informática y de la información.

Principalmente las entidades públicas y el sector gubernamental, están alineados con la Política de Ciberseguridad y Ciberdefensa decretado en el documento CONPES 3701 de 2011 y el actual CONPES 3854 de 2016 “Política Nacional de Seguridad Digital, cuyo objeto es fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital”[1].

En el transcurso de los años, el sector gubernamental ha venido fortaleciendo las medidas en cuanto a la protección de la información con sistemas de seguridad perimetral, procesos y procedimientos incluidos en los sistemas de gestión integrales, pero sin embargo, según un análisis de Comparitech[2], Colombia tiene problemas significativos en ciberseguridad, entre 60 países estudiados, nuestro país ocupo el puesto 39 en cuanto a índices de ciberseguridad colocándolo en un rango medio de la seguridad en la red. De acuerdo con el MinTIC[3] y los resultados obtenidos del FURAG (Formulario Único Reporte de Avances de la Gestión) de 186 entidades consultadas, el 66% a iniciado un proceso de implementación de un sistema de gestión de seguridad informática, el 21% informo aun no tener implementado algún sistema o no ha migrado a las nuevas generaciones de seguridad informática que brindan detener los ataques mediante la inspección de tráfico y la detección y control de aplicaciones y el 13% no respondió.

El gobierno Nacional en conjunto con las diferentes entidades responsables de la seguridad de la información de las personas y/o entidades han desarrollado estrategias que permitan contrarrestar la afectación de los delitos informáticos, siendo estos el principal tema que afecta a toda la sociedad en temas cibernéticos, y es que día a día se evidencia un aumento considerable de esta afectación y lo

[1] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL.CONPES 3854 Política Nacional de Seguridad Digital. Colombia. 2016. P.6.

[2] PROFITLINE, Actualmente Como se encuentra Colombia en Seguridad Informática. https://profitline.com.co/actualmente-como-se-encuentra-colombia-en-seguridad-informatica/ 2019

[3] Ministerio de Tecnologías de la Información y las Comunicaciones. “¿Y de seguridad TI qué hacen las entidades?” https://www.mintic.gov.co/gestionti/615/w3-article-7083.html?_noredirect=1 2019

que es más preocupante, se configuran nuevas modalidades, lo que obliga al estado Colombiano a reformar de manera periódica la normatividad pues esta debe adaptarse a las nuevas necesidades.

De acuerdo a la problemática planteada y con relación al análisis de la evolución del aseguramiento informático en entidades del sector, se pretende generar un documento de recomendaciones que permitan guiar con mejores prácticas, sobre la importancia que conlleva la utilización de mecanismos, políticas y protocolos de seguridad digital y la implementación de un SGSI, minimizando el impacto que podría producir los ataques informáticos y los beneficios de detección y prevención de intrusiones en las entidades del sector gobierno y cuya información en su mayoría, por ser de dominio público es de vital importancia conservando la triada CID (Confidencialidad, Integridad y Disponibilidad).

1.2 FORMULACION DEL PROBLEMA

Con relación al planteamiento anterior, se da definición al siguiente cuestionamiento:

¿Cómo ha evolucionado el aseguramiento informático en entidades del sector gobierno Colombiano con la implementación de políticas y lineamientos de estado?

2. JUSTIFICACION

Las organizaciones en general están expuestas constantemente al riesgo de enfrentar un ataque cibernético y como consecuencia tener una pérdida o daño en su información, particularmente y de acuerdo con grandes compañías especializadas en seguridad informática, los sectores con más vulnerabilidad frente a ataques cibernéticos son el sector financiero, gubernamental, entretenimiento y comercio, a lo cual nos centraremos principalmente en el sector gobierno, del que se analizara más detalladamente, el auge que ha tenido a través de los años y la importancia que se ha venido dando desde el Ministerio de Tecnologías de la Información y las Comunicaciones para que las entidades públicas estén alineadas en cuanto a la gestión de la seguridad informática y llevando consigo la necesidad de fortalecer, proteger y asegurar la información con sistemas de seguridad perimetral que desde sus inicios hasta el presente, ha venido evolucionando a pasos agigantados y buscando conservar la confidencialidad, integridad y disponibilidad de la información, cuya consulta generalmente está dada a la ciudadanía en general y siempre estar disponible en el momento que se requiera.

Hace algunos años, para el caso de las entidades públicas el progresivo uso de las TIC, las conexiones a internet, las redes de comunicaciones esenciales para la realización de actividades propias de las instituciones y principalmente el crecimiento de la oferta de servicios brindados a la ciudadanía y utilizables en línea, demuestran un incremento importante en la colaboración de la ciudadanía en los medios electrónicos, sin embargo, este uso de los entornos digitales dispuestos por las entidades públicas han conducido también a el aumento de riesgos en cuanto al componente informático, los cuales tenían una gestión inadecuada que pudieron derivar en amenazas, incidentes y ataques cibernéticos, teniendo consecuencias importantes no solo para la entidad afectada sino para el país en general.

En el entorno actual, el país ha realizado una tipificación de la problemática a solucionar, definiendo políticas lideradas por los ministerios de defensa y minTIC, las cuales han acogido las recomendaciones para la gestión de riesgos informáticos, de igual forma hacer un uso responsable de los entornos digitales y fortalecer las capacidades de encargarse y mitigar las posibles amenazas en los servicios ofrecidos y los sistemas de información de uso propio.

Se pretende orientar a través de un documento de recomendaciones que permita guiar, sobre la importancia que el sector gubernamental debe tener en cuanto a las medidas de protección y de seguridad informática que actualmente se manejan, para afrontar de manera adecuada los posibles ataques informáticos.

La realización del presente documento, busca brindar un escenario en el que se pueda analizar la necesidad y en ciertos casos la obligación de las organizaciones del sector gobierno, en poder dar una protección optima a los activos de información con la utilización de equipos de última generación que ofrecen una serie de prestaciones definidas en los campos de seguridad perimetral y que permitirán entregar a las entidades una protección integral en términos de prevención de intrusiones, filtrado web, antimalware y control de aplicaciones (incluido el tráfico cifrado), todo esto enmarcado en firewalls de próxima generación y adoptando las mejores prácticas de seguridad.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar la evolución del aseguramiento informático en algunas instituciones gubernamentales del sector gobierno Colombiano, generando un documento de recomendaciones que permita guiar en lo referente a seguridad informática.

3.2 OBJETIVOS ESPECIFICOS

- Recopilar información y producciones documentales de seguridad informática determinando su influencia en algunas entidades del sector gobierno colombiano.

- Determinar el impacto del uso y tipo de tecnología de seguridad informática en algunas entidades del sector gobierno colombiano, identificando cual puede ser el mejor modelo y que beneficios ha brindado frente a la mitigación de amenazas cibernéticas.

- Presentar un documento de recomendaciones que contribuya y oriente sobre la importancia de la implementación de un sistema de aseguramiento informático.

4. MARCO REFERENCIAL

4.1 MARCO TEORICO

Se encuentra información sobre el tema de análisis, la cual da soporte a este documento, en donde los siguientes autores con sus aportes dan definición del estado actual en cuanto a las políticas públicas de ciberseguridad y ciberdefensa en Colombia y sobre la evolución que está ha tenido en el país. Rodrigo Cortes Borrero (Especialista en Derecho Administrativo)[4] quien aporta un informe en el que de acuerdo a los desafíos en los sectores de seguridad informática y de la información, describe como se ha implementado en los últimos años las políticas públicas de ciberseguridad y ciberdefensa, los organismos y las entidades encargados de hacerlas cumplir, garantizando que los sectores públicos como privados puedan basarse en ellos y buscar la implementación de buenas prácticas a través de procesos, procedimientos y dispositivos que protejan uno de los activos más valiosos en los últimos tiempos como es la información.

El apoyo documental del informe "Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia" de Rodrigo Cortes Borrero, puede dar ilustración de como desde el campo legislativo y normativo permite dar bases jurídicas al tema de seguridad informática, tomando como sustento que a partir de los últimos años con el aumento acelerado en la época informática, internet y las comunicaciones, han surgido nuevos retos para la nación y todos sus sectores tanto privados como públicos, necesitando crear y poner en funcionamiento políticas públicas puesto que pueden afrontar a estos recientes retos en el campo digital, es así como nuestro país no está exento de estos fenómenos y por ello en el informe del autor se da una descripción de la política pública de ciberseguridad y ciberdefensa que en los recientes años se ha implementado en la nación, de igual forma identifica los organismos, instituciones encargadas de estas funciones, así como los instrumentos jurídicos que garanticen la seguridad cibernética tanto en los sectores públicos y privados buscando alcanzar la salvaguarda de los derechos, el patrimonio y por supuesto la información.

Por otra parte, Juan Diego Camacho García (Oficial del Ejército Colombiano y Especialista en Administración de la Seguridad)[5] en su informe acerca de la evolución de la ciberdefensa y la seguridad de la información en Colombia, ilustra sobre el aumento de las amenazas cibernéticas y de cómo el concepto de ciberdefensa ha tenido una notable evolución en el transcurso de los años en nuestro país, de igual forma cómo el concepto de seguridad de la información ha

[4] CORTES BORRERO, Rodrigo, ESTADO ACTUAL DE LA POLITICA PÚBLICA DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA, https://repository.usta.edu.co/bitstream/handle/11634/14032/2015rodrigocortes.pdf?cv=1&sequ= 2015

[5] CAMACHO GARCIA, Juan Diego. Evolución de la ciberdefensa y la seguridad de la información en Colombia. https://repository.unimilitar.edu.co/handle/10654/14382 2016

pasado del manejo de la protección que se daba a la documentación física hacia la evolución que se ha tenido ahora al manejarla en forma digital, permitiendo a la nación a buscar las formas de protegerse e implementar controles como políticas de estado y apoyo en los entes que proveen capacidad operativa e inteligencia cibernética, para buscar mitigar los riesgos y amenazas a los que se pueden enfrentar las instituciones y más específicamente las entidades gubernamentales.

Juan Diego Camacho en su informe “Evolución de la ciberdefensa y la seguridad de la información en Colombia” da cuenta que en los últimos años las amenazas cibernéticas han ido en aumento aproximadamente desde el año 2000, sumándose a ello los ataques como malware, spyware, exploits, denegación de servicios (DDOS), intrusiones, fraudes entre otros, haciendo que en ocasiones veamos el campo de la ciberseguridad como algo blando y con amenazas que día tras día son más difíciles de predecir pudiendo vulnerar la infraestructura cibernética y de esta forma materializar los riesgos a los que están expuestas las empresas y entidades sin importar su naturaleza. Debido a lo anterior, en nuestro país la ciberdefensa y seguridad informática y de la información ha tenido una gran evolución contando que el ministerio de defensa pueda apoyar con semilleros, profesionalización y financieramente en la adquisición de tecnología hacia los sectores de defensa por medio de organismos como el comando conjunto cibernético y el centro cibernético policial encargados de la seguridad ciudadana en el ciberespacio, y que puedan ayudar en forma activa a solventar de cierta forma los incidentes que se puedan encaminar hacia los activos y sistemas de información estratégicos para la nación.

De acuerdo a lo expuesto anteriormente, Juan Diego Camacho presenta varios aspectos que se deben tener en cuenta para poder enfrentarse en nuevos escenarios contra el delito cibernético y como contraprestación a ello se exige la creación de nuevas herramientas de prevención, reacción y defensa, para consolidar una capacidad suficiente de ciberseguridad y ciberdefensa contando con las siguientes áreas de concentración:

- Sistemas seguros y resistentes
- Doctrina y normatividad
- Sensibilización y cambio cultural
- Roles y misiones
- Compromiso internacional
- Educación y capacidades de investigación y desarrollo
- Infraestructura y equipamiento

Los anteriores aspectos están en la capacidad de poder darle protección a la infraestructura cibernética, siendo una obligación del estado colombiano proteger a los ciudadanos de los posibles ataques cibernéticos transformándose estas siete áreas en maniobras para resguardar la ciberdefensa en la nación.

Respecto a lo identificado en la información recopilada en los informes que soportan este documento, se puede contextualizar como ha sido esa evolución que el país ha tenido en el campo de ciberseguridad y cuales han sido esas herramientas que hasta el momento han permitido enfrentar esos riesgos y amenazas que potencialmente puede tener la nación en temas de delitos y ataques informáticos, de acuerdo al artículo del El Periódico el Tiempo (Colombia se prepara para enfrentar los ciberataques, 2014): "Seis millones de personas fueron víctimas de alguna modalidad de crimen digital en Colombia el año pasado, según la firma de seguridad digital Norton. La compañía calcula que el costo de los delitos informáticos en 2013 alcanzó 874 mil millones de pesos. La situación para las entidades públicas y privadas no es mejor, pues el más elemental diagnóstico sugiere que existe un alto reto en temas de ciberseguridad. Durante el 2013 se detectaron 1.551 defaces, una modalidad de ataque cibernético que cambia la página principal de un sitio de internet. En lo que va del 2014 se han reportado 801 de esos ataques: 507 a portales comerciales, 186 de sitios web educativos y 108 de sitios web de entidades", demostrando de esta forma una delicadísima dificultad que está perturbando mucho al Sector público de la misma manera a las entidades privadas, intranquilidad que viene redundada en la administración del país en los recientes cinco años.

Desde esta óptica el gobierno colombiano ha establecido una sucesión de tácticas desde la inserción de recientes características penales según las contravenciones informáticas inclusive la solidificación de la Política Publica expresada en el CONPES 3701 "LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA". (Consejo Nacional de Política Económica y Social del 2011), justamente, debido a estos contextos, estas tácticas han sido trasformadas en una Política Publica la cual admitiría que el gobierno nacional y las organizaciones privadas enfrentaran las nuevas conminaciones del ambiente digital, fortificando las organizaciones, los medios tangibles y de capital humano, entre varios, para desempeñarse y afrontar a las recientes amenazas que no son algo inferior en los diferentes direcciones que siguen perturbando el capital y la seguridad del país.[6]

4.2 MARCO CONCEPTUAL

4.2.1 La seguridad perimetral. Es un método de defensa de red, que se basa en el establecimiento de recursos de seguridad en el perímetro de la red y a diferentes niveles, permitiendo definir niveles de confianza, el acceso de usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.[7] Algunos de los dispositivos utilizados para la protección y

[6] CORTES BORRERO, Rodrigo, ESTADO ACTUAL DE LA POLITICA PÚBLICA DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA, https://repository.usta.edu.co/bitstream/handle/11634/14032/2015rodrigocortes.pdf?cv=1&sequ= 2015

[7] TURMERO, Pablo. Elementos básicos de la seguridad perimetral. https://www.monografias.com/trabajos106/elementos-basicos-seguridad-perimetral/elementos-basicos-seguridad-perimetral.shtml. 2015

seguridad perimetral son inicialmente los firewalls, los IDS / IPS sistemas de detección y prevención de intrusos, antivirus, antimalware, honeypots o honeynets, que son el punto de partida para entender cómo funciona un UTM.

4.2.2 Firewall. Un firewall es básicamente la primera línea de defensa de la red. El propósito de un firewall es proteger la red contra el acceso no deseado. Puede ser en forma de un dispositivo físico o en un programa virtual, por lo general en calidad de "guardián" del tráfico que entra y sale de la red.

Por lo general, los firewalls le permiten establecer ciertas reglas para determinar lo que está permitido o no en su red privada. Dependiendo de su tipo, el firewall puede restringir el acceso sólo a determinadas direcciones IP, dominios, sitios y otros que pueden ser peligrosos.[8]

4.2.3 Sistemas de detección de intrusos y sistemas de prevención de intrusiones. Históricamente los IDS surgen antes que los IPS, con la función principal de detectar situaciones anómalas y usos indebidos de los recursos y servicios de la infraestructura tecnológica. Como consecuencia de la dificultad para reaccionar oportunamente a las alertas de intrusión generadas por los IDS, nacen los IPS que se encargan de reaccionar proactivamente a las intrusiones detectadas por el IDS tan pronto se identifican.

La detección de intrusos consiste en un conjunto de métodos y técnicas para revelar actividad sospechosa sobre un recurso o conjunto de recursos computacionales. Es decir, eventos que sugieran comportamientos anómalos, incorrectos o inapropiados sobre un sistema.[9]

4.2.4 Antivirus y Antimalware. Los software de Antivirus no logran divisar toda infección y amenaza presente ya que estas progresan continuamente. A cambio de esto, son prácticos para descubrir el malware que se propaga por intermedio de técnicas acostumbradas como las unidades USB, archivos adjuntos de Correo Electrónico, y para los que necesitan del reconocimiento de firmas para su localización. La localización de amenazas por firmas representa que únicamente las amenazas (firmas) conocidas logran ser descubiertas por la mayoría de programas de Antivirus.

El Anti-Malware es esbozado para impedir la propagación de malware nuevo a través de debilidades de día cero, malvertising o cualquier forma tergiversada de

---

[8] RODRIGUEZ, Victoria. Cómo funciona un firewall. https://www.segurisoft.es/encriptacion/como-funciona-firewall/. 2017

[9] LEHMANN, Armin Dieter. Intrusion Detection FAQ. http://www.sans.org/resources/idfaq/what_is_id.php

comunicación como las redes sociales y la mensajería. Para la defensa frente al malware adelantado y nuevas amenazas peligrosas, el Anti-Malware es una preferencia.[10]

4.2.5 Honeypot y Honeynet. Son honeypots las aplicaciones que simulan, de una forma más o menos interactiva, servicios o aplicaciones que registran la actividad sospechosa que un atacante pueda realizar sobre ellos. Al conjunto de honeypots que presentan una arquitectura lógica de red simulando un conjunto de sistemas, servicios y aplicaciones relacionadas, se le denomina honeynet. Por supuesto, en este tipo de entornos simulados no existe información real sensible ni relativa a la organización, pero si información aparentemente interesante que motive al atacante y le haga "perder" tiempo, al mismo tiempo que proporciona información sobre técnicas y métodos de ataque.[11]

4.2.6 Ciberseguridad. "Se define como la capacidad del Estado para minimizar el nivel de riesgo cibernético al que están expuestos los ciudadanos, en áreas como transacciones financieras, protección a la información y propiedad intelectual". (BNamericas, 2014)

4.2.7 Ciberdefensa. Esta especificada como la facultad del gobierno de advertir y neutralizar diferentes sucesos o conminaciones cibernéticas que perturbe el gobierno nacional, en la utilización de la internet con alcances terroristas, hechos de acechanza y ofensiva digital, lema de una presentación del Ministerio de Defensa.

4.2.8 Política pública. Estas son un acumulado de objetivos, decisiones y acciones que el gobierno ejecuta, para poder dar solución a una problemática que este enfrentando y que en dado caso, la ciudadanía y el mismo gobierno considere que son prioritarios. De acuerdo a su importancia, estas políticas públicas pueden determinar la evaluación de las acciones para poder mitigar, eliminar o variar la problemática que se presenta.

Con relación a lo anterior y para el tema a tratar en el presente documento, las políticas públicas definidas para salvaguardar y gestionar el riesgo en cuestión del entorno digital, están enmarcadas en los CONPES 3701 de 2011 y 3854 de 2016, cuyos objetivos principales son la defensa de país, y la lucha contra el cibercrimen, y para su plan de acción para ponerla en marcha y en ejecución para

[10] GONZALO, Leonardo. Antivirus vs Anti-Malware. https://www.malwarefox.com/es/antivirus-vs-anti-malware/

[11] RODRIGUEZ, Raúl. Para aprender, perder… o no: Introducción. https://www.securityartwork.es/2010/03/26/para-aprender-perder%E2%80%A6-o-no-introduccion/. 2010

los años 2016 a 2019 tuvo una financiación de $ 85.070 millones de pesos, buscando para el año 2020 impactar de manera positiva en la economía.

En cuanto a las tendencias en temas de ciberseguridad se puede definir por lo siguiente:

- Movilidad: Los beneficios de describir con información en espacios reales han dispuesto un espacio para la ejecución de iniciativas en torno a del BYOD (Bring Your Own Device) porque buscan aumentar la producción de los funcionarios, acrecentando su nivel de conexión, disminuyendo de esta manera los períodos de contestación. Como resultado de esto, hallamos en Colombia una mejor preparación a adaptar el contorno de las agrupaciones por medio de la instauración de medidas encaminadas a incitar, y resguardar, el teletrabajo.
- Internet de las Cosas: La mayoría de usos de aparatos acoplados a internet y que logran acabar formando una fracción de una conexión colectiva aumenta la exhibición de información personal y confidencial a los ciberdelincuentes esperando la inadvertencia de los cibernautas.
- Cloud Computing: en la búsqueda de economizar en precios, las organizaciones han escogido por contratar servicios para algunos métodos e instrumentos, esperando la acumulación de la información y el manejo de aplicaciones a organizaciones foráneas a las entidades, con la demanda de poseer una ejecución más orientada a las labores fundamentales del comercio.[12]

En el transcurso de los años la ciberseguridad y ciberdefensa han tenido una alta utilidad en el espacio político global, debido a que el ciberespacio y las Tecnologías de la Información y las Comunicaciones se tornan constantemente más fundamentales para el progreso social y económico. De igual forma, se incrementa la trascendencia por infraestructura de las Tecnologías de la Información y las Comunicaciones y las conminaciones cibernéticas progresan a una manera veloz, con relación a un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

4.2.9 CONPES. Es la mayor jurisdicción a nivel estatal de planeación y se desenvuelve como entidad asesora del Gobierno en muchas las vertientes relacionadas con el progreso económico y social de la nación. Para conseguirlo, dirige y encamina a las entidades comisionadas de la gestión económica y social en el país, por medio del análisis y el consentimiento de documentos acerca del adelanto de políticas ordinarias que son mostrados en sesión. (Consejo Nacional de Política Económica y Social de 2011)

[12] CORTES BORRERO, Rodrigo, ESTADO ACTUAL DE LA POLITICA PÚBLICA DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA, https://repository.usta.edu.co/bitstream/handle/11634/14032/2015rodrigocortes.pdf?cv=1&sequ= 2015

Con lo anterior, se logra afianzar que consta un contexto y es que los Estados y Colombia no es extraño, están o han establecido Políticas Públicas que se orientan a la Ciberseguridad y la Ciberdefensa, que de esta forma lo muestra el Ministerio de Defensa Nacional (2009):

"Al beneficiarnos de los ilimitados recursos de las redes públicas de datos como Internet y de la infraestructura tecnológica interconectada, también nos enfrentamos a nuevos escenarios para el delito, el terrorismo y la guerra, lo cual exige la Creación de nuevas herramientas de prevención, reacción y defensa".[13]

De acuerdo a los dominios de control, se verifican la existencia de cuatro elementos de seguridad contenidos en las Normas ISO 27001:

- Seguridad organizativa

    a. Políticas de seguridad: Reglas y protocolos que se definen para propender por la seguridad informática de las entidades.
    b. Aspectos organizativos para la seguridad: Busca establecer la estructura de la gestión y controlar la implementación de la seguridad informática en las organizaciones.
    c. Clasificación y control de activos: Este procedimiento se lleva a cabo con el análisis de riesgos, responsabilidad sobre los activos, inventario de los activos buscando definir el tipo de activo al que pertenece, propiedad de los activos y su uso adecuado.
    d. Seguridad ligada al personal: establecer puntos de control sobre el talento humano que opera la información en la organización, evitando con ello fugas de información, errores de manejo, fisuras de confidencialidad.
    e. Gestión de la continuidad del negocio: Tratar de garantizar que las entidades puedan sobrellevar a un acontecimiento que potencialmente pueda colocar en riesgo su infraestructura física y tecnológica.

- Seguridad lógica

    a. Control de accesos: Poder limitar el acceso a la información y también a las instalaciones de procesamiento de información, otorgando autorización de a los usuarios de acceso a un servicio o una información.
    b. Desarrollo y mantenimiento de sistemas: Aplica a los sistemas información, desarrollos propios o de terceros, sistemas operativos y sistemas que integren los ambientes administrados en la entidad donde se encuentren los desarrollos.

[13] CORTES BORRERO, Rodrigo, ESTADO ACTUAL DE LA POLITICA PÚBLICA DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA, https://repository.usta.edu.co/bitstream/handle/11634/14032/2015rodrigocortes.pdf?cv=1&sequ= 2015

c. Gestión de comunicaciones y operaciones: La forma como se administra y supervisa todo en cuanto a las actividades y comunicaciones de las organizaciones por medio del control de la información o la entrega de ella.

- Seguridad física

  Seguridad física y del entorno: Este aspecto hace referencia en cuanto a las barreras físicas y los mecanismos que controlan el entorno de los sistemas informáticos buscando proteger el hardware de posibles amenazas físicas la cual contrasta de cierta forma con la seguridad lógica.

- Seguridad legal

  Conformidad y cumplimiento del sistema de gestión: Este aspecto es importante en cuanto a la identificación de las partes interesadas, cumplimiento de los requisitos legales y regulatorios, objetivos y metas y las obligaciones contractuales.

En conformidad con lo anterior, no es necesario realizar una gran senda sobre la seguridad, sino por las principales por las que se guiara el análisis de la evolución informática en el presente trabajo, en general sobre la normatividad nacional que buscan el aseguramiento de la información en las organizaciones de la nación, el compromiso del país y la dedicación de algunas entidades hacia el tema de la protección de la información.

4.2.10 Tipos de Delitos Informáticos. Los delitos informáticos son una representación de la necesidad de obtención de la propiedad que no pertenece al individuo a través de mecanismos electrónicos que afectan la privacidad de las personas desde sus datos personales como del abuso intelectual, para definir los tipos de delitos informáticos es importante hacer referencia al Convenio sobre la Ciberdelincuencia el cual fue presentado en Noviembre de 2001[14], este tuvo lugar en el marco tecnológico en la Unión Europea, el cual fue firmado en Budapest, por lo cual se definen los siguientes grupos de delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.

[14] DIVISION COMPUTER FORENSIC, Tipos de delitos informáticos, Clasificación según el "Convenio sobre la Ciberdelincuencia", https://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html 2001

Este tipo de delitos usualmente son cometidos a través de usos de mecanismos como el robo de identidades, conexión a redes no permitidas, y la utilización de software ilegal como son keyloggers y software espía.

Los delitos informáticos cometidos dentro de este grupo son aquellos cuando de manera no autorizada se borra información o se corrompen ficheros para beneficio propio, ellos son:

- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

Delito relacionado con contenido, toda aquella propagación, creación, edición, difusión, producción de contenido pornográfico infantil, a través de sistemas electrónicos.

4.3 MARCO HISTORICO

4.3.1 La evolución de los firewalls. Desde hace más de 20 años cuando Check Point Software Technologies ingresó su primer cortafuego de red corporativo, sellando el principio de un mercado grande para cortafuegos que ha salvaguardado muchas de redes en todo el planeta. El FireWall-1 de Check Point, descubierto en el NetWorld+Interop en el año 1994, no había sido el primer cortafuegos, por supuesto.

El cortafuego estaba comenzado a arrancar forma con el levantamiento de Internet. Las organizaciones y los establecimientos educativos entre los años 80 y los años 90 advirtieron la necesidad de bloquear el tráfico IP no apetecido, estableciendo un muro de acceso perimétrico. En aquel periodo, algunas veces ellos mismos “implementaban” sus propios routers u otros dispositivos, incluso que los constructores definitivamente llegaron al salvamento con servicios de cortafuegos que les facilitaran este trabajo. Marcus Ranum, actualmente director de seguridad en Tenable Network Security, es estimado el más sobresaliente de los principales descubridores de cortafuegos comerciales, ya que esbozó el firewall DEC SEAL en el año 1990, y se ocupó con el cortafuego Gauntlet y el juego de instrumentos TIS en Trusted Information Systems. Otros esfuerzos anticipados, como el cortafuego Raptor, asimismo estaban. Pero fue el lanzamiento del FireWall-1 de Check Point lo que acabó estableciendo una variedad de mercado masivo al que rápido se acoplaron no solo los magnos

distribuidores de redes, como Cisco y Juniper, sino un conjunto de otros proveedores, como WatchGuard.[15]

4.3.2 Seguridad de red antes de UTM. Los sistemas de seguridad de red tradicionales son construidos a propósito. Debido a que existen docenas de tipos de amenazas para la red de la organización, las compañías tuvieron que comprar uno o más de cada tipo de sistema para garantizar la protección adecuada de su red y sus datos. Cada vez que se compra un sistema específico, el equipo de TI debe desempaquetar e instalar el equipo en el centro de datos. A medida que surgían amenazas de hackers y delincuentes más sofisticados, nuevos tipos de plataformas de seguridad entraron en el mercado. De hecho, no era raro que una empresa mediana tuviera uno o dos docenas de tipos de sistemas de seguridad instalados. Esto requería espacio, refrigeración, electricidad, equipos de red adicionales y, especialmente, capacitación del personal de TI. Creó una carga financiera y administrativa para las organizaciones.

Para resolver este problema, los sistemas UTM entraron en escena e integraron múltiples tipos de sistemas de seguridad en una sola plataforma. Los tipos de sistemas de seguridad de red integrados incluían firewalls, detección y prevención de intrusiones, antimalware, filtrado de contenido web, VPN, prevención de pérdida de datos, seguridad de correo electrónico y otros tipos de sistemas de seguridad. Esto simplificó enormemente la administración de estos sistemas de seguridad porque se integraron en una interfaz de administración todo en uno. El sistema UTM era una pieza única de hardware, lo que significa que había un valor agregado adicional de menos gasto en refrigeración, electricidad y menos espacio requerido en el centro de datos.

Además, un sistema de seguridad de red integrado, como un UTM, hace que la administración y administración de la seguridad de la red sea un proceso más eficiente y ágil. Donde con los sistemas tradicionales, el personal de seguridad de TI tenía que ser entrenado individualmente en cada sistema, con una capacitación UTM solo para un sistema único. Debido a esta eficiencia, es posible que se necesite menos personal de TI para administrar la seguridad de la red.

Los sistemas UTM han suplantado al firewall tradicional en la seguridad de la red. Si se tratara de comprar un sistema UTM, buscarían estos sistemas en el mercado de firewall. Los fabricantes de firewall han adoptado este cambio y ahora hacen que los sistemas de firewall tengan más capacidad de procesamiento. Los sistemas de hardware más potentes admiten la funcionalidad UTM agregada mencionada anteriormente. Los fabricantes de firewall para empresas más comunes, como FortiNet, Cisco, Dell SonicWall, Sophos y Barracuda, venden exclusivamente firewalls tipo UTM. En el mercado de seguridad de redes

[15] CORTES, Mireya. La evolución del firewall. http://cio.com.mx/la-evolucion-del-firewall/. 2014

empresariales de hoy en día, es difícil encontrar el cortafuegos tradicional que hace estrictamente el control de acceso basado en reglas.[16]

4.3.3 Panorama de Latinoamérica y Colombia frente a la seguridad informática. Los asaltos informáticos en América Latina cada vez crecen por causa de la vulnerabilidad de sus sistemas financieros y empresariales. En una revisión realizada por Fortinet, una compañía de ciberseguridad a nivel mundial, resolvió hacer un estudio del horizonte de la seguridad de la información de Colombia, en el cual halló que alrededor del 80% de las organizaciones en Colombia tienen sistemas sumamente vulnerables. Nuno Mantinhas, vicepresidente de Fortinet para el Caribe y Latinoamérica, afirmó que no obstante la cantidad parece impresionante, tal vez lo malo es que el otro 20% sobrante no tiene un cifrado de su información sensible, sino intermedio, de la que hacen parte las entidades gubernamentales.

De acuerdo a un estudio hecho por Eset, la "Infección por malware" ocupa el primer lugar con el 40% de contestaciones positivas, mientras que en segundo lugar se sitúan los casos de "Phishing" con el 16% y en el tercero el "fraude interno/externo" con el 13%. De acuerdo a lo anterior y con relación a los resultados de la encuesta de Eset, las organizaciones en América Latina reservan presupuestos para la implementación de soluciones de aplicaciones antivirus en primer lugar con el 77 %, seguidas de cortafuegos con 71 % y respaldos de información con 63 %. No obstante, se debe recalcar que si las organizaciones proponen sus sistemas de protección a software antivirus, los temas de malwares tendrían que disminuir, algo que no se manifiesta en el estudio, es decir que las organizaciones no están asistiendo al mejor aplicativo sino al más barato.[17]

A diferencia de la última década, los problemas de seguridad de la información son una preocupación para los líderes de las organizaciones colombianas. Los responsables de la operación de las entidades son más conscientes y más sensibles a la necesidad de salvaguardar la información y tienen presupuestos oficiales para hacerlo. Pero a veces esto no es suficiente y debe continuarse a favor de la profesionalidad y la conciencia, no solo de las personas que pertenecen al departamento de TI, sino también de cada miembro de la organización.

La humanidad es el eslabón más frágil entre todas las cadenas para almacenar información. Hay personas que saben que realmente es un activo valioso para su negocio y lo cuidan; Otros son conscientes, pero lo ignoran. Y otras personas definitivamente no tienen idea de la importancia de la seguridad de la información.

[16] CRUZ, Luis. ¿Qué es la gestión unificada de amenazas (UTM)?. https://study.com/academy/lesson/what-is-unified-threat-management-utm.html.

[17] CONTRERAS, Nicolás. Más del 80 por ciento de las compañías en Colombia son vulnerables a ataques informáticos. https://caracol.com.co/radio/2016/06/09/tecnologia/1465469190_389745.html. 2016

Se busca conciencia y cómo interesar a las personas que tienen parte o toda la información confidencial sobre la empresa. Aquí está la idea de generar una cultura organizacional y una cultura que las personas sean responsables de la información.

Definitivamente, el "phishing" (mensajes falsos para robar información) sigue siendo un dolor de cabeza para muchas organizaciones. Esto abre muchas puertas a amenazas conocidas y desconocidas para captar rápidamente información confidencial o, dependiendo del ataque, incluso negar el servicio que brindan a sus usuarios.

El ransomware (secuestro de computadoras para rescate) también ha dañado a muchas compañías en Colombia. Estos tipos de amenazas pueden incluso secuestrar equipos informáticos o equipos de Internet de las cosas (IoT) y llegar a extremos extremadamente peligrosos en varios sectores. Uno de los más vulnerables a esto, con la modernización de las herramientas técnicas conectadas a Internet, puede ser, por ejemplo, el sector de la salud. Estas son las amenazas más importantes y relevantes en Colombia en este momento.

Existen varios mitos en el campo de la seguridad de la información. El primero es "Tengo un firewall y con eso estoy protegido". Pero no: la seguridad de la información ya no tiene perímetros. Se debe implementar una estrategia que, de acuerdo con las necesidades de la empresa, ofrezca protección integral al usuario final y proteja todo el acceso al ecosistema digital. El otro mito es "Tengo el antivirus actualizado, por lo que no estaré infectado". Esto también es falso. Es bueno tener protección de punto final, pero eso no es todo. Muchos programas antivirus funcionan con firmas y, por ejemplo, no detectan amenazas de día cero. Dependiendo de la criticidad y la gestión de la información, existen varias alternativas en el mercado.[18]

4.4 MARCO LEGAL

La categorización legal colombiana contiene una gran diversidad de disposiciones de clases constitucionales, legales y reglamentarias, que manejan numerosas acciones con relación al medio de la seguridad digital y que reflejan ser importantes en el avance de la gestión de riesgos de seguridad informática:

En el marco legal colombiano a través de la constitución política se contempla en el artículo 15 el derecho fundamental de habeas data y el artículo 20 acerca de la libertad de información.

[18] DUEÑAS, Jaime. COLOMBIA ES MÁS CONSCIENTE FRENTE A LA SEGURIDAD DE LA INFORMACIÓN. https://www.enter.co/especiales/empresas/colombia-seguridad-informacion/. 2018

Ley 1273 de 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”.[19] La referencia en cuanto a la ley, se regula en el código penal los delitos cibernéticos y agregando la sanción correspondiente en los casos que se incurra en la materialización de alguno de las infracciones allí descritas, a través de esta se reconocieron y se clasificaron los delitos informáticos en Colombia e interpreta el accionar del delincuente y se acoge a la determinación de judicialización nombrada por el Código Penal, de igual forma dicta otra serie de disposiciones que los jueces deberán tener en cuanta al momento de aplicar la totalidad del articulado del Código Penal y regula el tiempo máximo de privación de la libertad que se aplicaran en el estado colombiano.

“Colombia tiene una nueva Política de Seguridad Digital, hoja de ruta para que el Gobierno, las organizaciones públicas y privadas, la fuerza pública, la academia y los ciudadanos en general, cuenten con un entorno digital confiable y seguro. Conpes es la sigla que hace referencia al Consejo Nacional de Política Económica y Social. Ésta es la máxima autoridad nacional de planeación y se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país”.[20]

CONPES 3701 DE 2011. “Lineamientos de política para ciberseguridad y ciberdefensa”.[21] Este documento está encaminado a desplegar una estrategia nacional que neutralice el aumento de amenazas informáticas que perturben a nuestro país.

CONPES 3854 DE 2016. “Política nacional de seguridad digital”[22]Este documento se orienta hacia una gestión de riesgos de seguridad digital, buscando que los ciudadanos, las entidades públicas y privadas establezcan e identifiquen los riesgos y amenazas a los que posiblemente podrían estar expuestos, así mismo como su protección y prevención ante ataques y delitos informáticos.

[19] Alcaldía de Bogotá. Ley 1273 de 2009 nivel nacional. Diario Oficial 47.223 de enero 5 de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. 2009

[20] Ministerio de Tecnologías de la Información y las Comunicaciones. “Lo que usted debe saber del Conpes de Seguridad Digital https://www.mintic.gov.co/portal/604/w3-article-15410.html. 2016

[21] Ministerio de Tecnologías de la Información y las Comunicaciones. “Documento CONPES 3701 de 2011” https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf. 2011

[22] Departamento Nacional de Planeación. “Documento CONPES 3854 de 2016” https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf. 2016

4.5 MARCO CONTEXTUAL

4.5.1 Entidades a nivel Nacional. A continuación se relacionan las entidades que tienen las competencias del manejo y reglamentación en el territorial nacional en cuanto a la seguridad y defensa informática del país y con relación a la puesta en marcha y disposición de herramientas para tal fin.

- Presidencia de la Republica.

Dentro de las competencias constitucionales y reglamentarias, el poder ejecutivo y como primer superior el Presidente de la Republica, Supremo Mando administrativo y primer dirigente de las fuerzas militares, ha dirigido el cálculo de una Política Publica de ciberseguridad y ciberdefensa en nuestro país, a partir del arribo del Presidente Juan Manuel Santos a la máxima cartera, se ha verificado un inmenso arranque político, para afrontar los nuevos retos que la colectividad y la nación colombiana enfrenta, poniendo en marcha diferentes herramientas y elementos para disponer a Colombia para muchos nuevos ambientes de seguridad digital.

- Ministerio de Defensa Nacional

El cometido del Ministerio de Defensa, la concreta como una obligación de “Asistir a la gobernanza demócrata, el bienestar social y la supresión de la violencia, a través de la instrucción de la defensa y la seguridad, la adaptación apropiada y orientada de la fuerza y el progreso de competencias suficientes convincentes” (MinDefensa, 2014).

En sus oficios definidos Según el Decreto 1512 de 2000 Art. 5 se encuentra contribuir en la ilustración, avance y cumplimiento de las políticas de defensa y seguridad nacional, buscando asegurar la dominio nacional, la libertad, la integridad de país y el orden reglamentario, el sostenimiento de las situaciones necesarias para la función y el derecho de autonomías públicas, y para garantizar que la sociedad de Colombia residan en paz.

Estando este organismo el convocado a especificar las directrices que realicen la Ciberseguridad y la Ciberdefensa en la nación colombiana, incorporado con las Fuerzas Militares y de Policía Nacional, las entidades de seguridad e Inteligencia

- Ministerio de Tecnologías de la Información y las Comunicaciones

De acuerdo a la Ley 1341 o Ley de TIC, es el organismo que se delega de delinear, acoger y fomentar las políticas, propósitos, programas e ideas del sector de las Tecnologías de la Información y las Comunicaciones.

Está definido en sus funciones el aumentar y proveer el acercamiento de todos los residentes de la nación, a las Tecnologías de la Información y las Comunicaciones y a sus servicios.

Su encargo es brindar el acceso, uso seguro y adquisición masivos de las TIC, por medio de políticas y programas, para optimar el bienestar y calidad social de cada habitante del territorio nacional y el aumento razonable del progreso del país. (Min Tic, 2014)

Estado esta organización como la institución especializada para asistir a la realización de las Políticas de Ciberseguridad y ciberdefensa, por a su representación especializada y su operatividad, siendo un socio fundamental en conjunto al Ministerio de Defensa para que la política pública de Ciberseguridad y Ciberdefensa logre establecerse, desplegarse y formar los resultados deseados al norte de estos recientes inconvenientes que la actualidad nos manifiesta.

4.5.2 Organismos Especializados. En nuestro territorio nacional tenemos una terna de Ciberseguridad y Ciberdefensa en Colombia conformado por una delegación intersectorial armonizada por las siguientes (3) tres instituciones establecidas a partir del documento CONPES 3701 de 2011:

- CCOC - Comando Conjunto Cibernético de las Fuerzas Militares

Es una unidad elite adscrita al Comando de las Fuerzas Militares, la cual se comisiona en regular la réplica a sucesos de seguridad cibernética que afecten la seguridad del país.

En cuanto a algunas de sus funciones encontramos:

- Fortalecer las capacidades técnicas y operativas del país que permitan afrontar las amenazas informáticas y los ataques cibernéticos, a través de la ejecución de medidas de defensa a nivel de hardware y/o software y la implementación de protocolos de ciberdefensa.
- Defender la infraestructura crítica y minimizar los riesgos informáticos asociados con la información estratégica del país, así como reforzar la protección de los sistemas informáticos de la Fuerza Pública de Colombia.

- Desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional.[23]

➢ CCP - Centro Cibernético Policial

Esta es una dependencia de la Dirección de Investigación Criminal e INTERPOL encomendada del adelanto de tácticas, programas, proyectos y otras acciones solicitadas en asuntos de investigación criminal frente a las agresiones que perjudican la información y los datos. (2014)

Objetivos:

- Implementación del Centro Cibernético Policial C.C.P.
- Respuesta en línea a incidentes de Ciberseguridad Cuadrante Virtual - CAI VIRTUAL.
- Coordinación internacional del Grupo de trabajo sobre delitos tecnológicos de INTERPOL EUROPOL
- Atención a incidentes informáticos en laboratorios forenses móviles DIJIN.
- Implementación CSIRT PONAL (Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional).
- Laboratorio de investigación de malware (Sector Bancario).
- Análisis forense equipos Tablet Mac-Servidores-Smarthphones.
- Atención, litigios sobre delitos cibernéticos (impacto en varios niveles y sectores).
- Unidades de investigación tecnológica UDITE (44) Cobertura nacional de la problemática.

➢ COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT)

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, tendrá la responsabilidad central de coordinar la Ciberseguridad y la Defensa Cibernética Nacional, que formará parte del Proceso de Misión de Gestión de Seguridad y Defensa del Ministerio de Defensa Nacional. Su objetivo principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano contra emergencias de seguridad cibernética que amenacen o comprometan la seguridad y defensa nacional.[24]

[23] COMANDO CONJUNTO CIBERNETICO. Funciones y deberes. https://www.ccoc.mil.co/quienes_somos_funciones_deberes. 2018

[24] colCERT, Grupo de respuesta a emergencias cibernéticas de Colombia. http://www.colcert.gov.co/?q=acerca-de 2017

Objetivos:

- Coordinar y asesorar a CSIRT y entidades tanto públicas, privadas y de la sociedad civil para responder a incidentes informáticos.
- Ofrecer servicios para prevenir amenazas cibernéticas, responder a incidentes cibernéticos, así como información, conciencia y capacitación en seguridad informática.
- Actuar como un punto de contacto internacional con sus homólogos en otros países, así como con organizaciones internacionales involucradas en esta tecnología.
- Promover el desarrollo de la capacidad local / sectorial, así como la creación de CSIRT sectoriales para la gestión operativa de incidentes de seguridad cibernética en infraestructura nacional crítica, el sector privado y la sociedad civil.
- Desarrollar y promover las mejores prácticas, protocolos y guías de buenas prácticas y recomendaciones para ciberdefensa y ciberseguridad para las infraestructuras críticas de la nación en asociación con los agentes correspondientes y garantizar su implementación y cumplimiento.
- Coordinar la implementación de políticas e iniciativas público-privadas para crear conciencia y capacitar talento humano especializado, relacionado con la defensa cibernética y la seguridad cibernética.
- Apoyar a las agencias estatales de seguridad e investigación para la prevención del delito y la investigación donde las tecnologías de información y comunicación median
- Promover un sistema de gestión del conocimiento relacionado con la ciberdefensa y la ciberseguridad destinado a mejorar los servicios de colCERT.

4.5.3 Aproximación hacia algunas entidades públicas. Como ejemplificación e ilustración de las acciones y procedimentación, orientadas para la mitigación de los riesgos y amenazas en cuestión de ciberataques, se adentrara en mecanismos, manuales y protocolos de seguridad de la información de algunas entidades públicas del sector gobierno, así como en el plan estratégico de tecnologías de la información y las comunicaciones de una entidad del sector público, con el que se encaminara y dará soporte de como se ha instaurado desde el sector gubernamental las estrategias, actividades, proyectos e iniciativas de aseguramiento informático en nuestro país.

- El Banco de la Republica, de acuerdo a la constitución política de Colombia establece que es un órgano independiente de las demás ramas del poder público y por ello se beneficia de una autonomía en el campo administrativo, patrimonial y técnico y está sometido a un régimen legal propio. Su misión es apoyar a la prosperidad de los colombianos a través de la conservación del poder adquisitivo de la moneda, el soporte al

progreso económico sostenido, la contribución a la permanencia financiera, el buen desarrollo de los sistemas de pago y la apropiada gestión cultural. Sus órganos decisorios son la junta directiva quienes dirigen y ejecutan las funciones del banco, está compuesta por siete miembros los cuales sesionan, deliberan y deciden; además pueden crear y reglamentar comités decisorios y asesores de política cuando se estime conveniente. El otro órgano decisorio es el consejo de administración que tiene funciones principalmente con políticas de administración y operación del banco, este consejo administrativo puede crear y reglamentar comités decisorios y asesores de administración los cuales funcionan como instancias técnicas de planeación, consultoría, recomendación o evaluación así como comités relacionados con temas internos de carácter laboral.[25]

Dentro del desempeño del banco se han desarrollado temas estratégicos que apoyan temas tácticos como capital humano y cultura organizacional, tecnología e infraestructura, uno de estos temas estratégicos es el de Gobierno Corporativo que en uno de sus literales menciona el fortalecimiento de la resiliencia de los procesos críticos del banco para asegurar la prestación de sus servicios misionales ante la ocurrencia de riesgos en situaciones normales o de desastres enmarcado en los siguientes parámetros: consolidación de una red de manejo de desastres de operación en conjunto con otras entidades financieras y del sector público, optimización del SGSI desarrollando alianzas de colaboración de conocimiento y experiencias con otras entidades centrales e instituciones locales en temas de ciberseguridad para poder actuar proactivamente a cara de nuevas amenazas y riesgos en esta modalidad delictiva, identificación de cargos críticos del banco para asegurar la continuidad de sus servicios.[26]

- La Contraloría de Bogotá D.C. es la entidad que vigila la gestión fiscal de la Administración Distrital y de los particulares que manejan fondos o bienes públicos, en aras del mejoramiento de la calidad de vida de los ciudadanos del Distrito Capital, es un organismo de carácter técnico, provisto de autonomía administrativa y presupuestal. Dentro de sus objetivos para el cumplimiento de la vigilancia del control fiscal distrital están el ejercicio como representante de la ciudadanía en la gestión de la administración en cuanto a bienes o fondos del Distrito Capital, generar la cultura del patrimonio público distrital, contribuir con los informes de auditoría para el mejoramiento de la gestión administrativa y fiscal de las entidades distritales, establecer responsabilidades fiscales e imponer sanciones y demás acciones derivadas del ejercicio de vigilancia y control fiscal,

[25] BANCO DE LA REPUBLICA. Quienes somos. https://www.banrep.gov.co/es/somos-el-banco-central-de-colombia

[26] BANCO DE LA REPUBLICA. Plan estratégico 2017 – 2021, Temas estratégicos. https://www.banrep.gov.co/es/plan-estrategico_2017-2021/temas-estrategicos

procurando el resarcimiento del daño al patrimonio público. Su sede principal está ubicada en la capital de la república y cuenta con alrededor de 1300 empleados entre funcionarios de planta y contratistas quienes cumplen funciones misionales y de apoyo. Además cuenta con 4 sedes en las que se encuentran las siguientes:

- Sede capacitación: Es un sitio donde los funcionarios pueden tomar capacitaciones y cursos de temas de la misionalidad de la entidad, así como de variedad de temas enfocados hacia el buen desempeño de las funciones de sus empleados.
- Sede San Cayetano: En esta sede se encuentran el almacén general y el archivo de la entidad, es un lugar que brinda custodia no solo a la parte de bienes materiales sino a la documentación histórica y actual de la entidad.
- Sede Condominio: ubicada en el centro de la ciudad, en esta sede se encuentra la dependencia de estudios de economía y política pública, encargados de proponer, dirigir e implementar políticas, lineamientos, estrategias y orientaciones para la evaluación macroeconómica del Distrito Capital.
- Sede Participación Ciudadana: allí funciona la dependencia de participación ciudadana y desarrollo local, quienes además de las funciones de fiscalización ejecutan de manera transversal las políticas orientadas a propiciar la participación ciudadana y el ejercicio del control fiscal en los entes locales del distrito capital.

En las competencias misionales de la Contraloría de Bogotá D.C. están la auditoria a las entidades distritales públicas o privadas que manejan presupuesto del distrito capital. De igual forma, hacen parte de estas auditorías y de la vigilancia del control fiscal, los entes locales, es decir, las alcaldías locales en cada una de las 20 localidades; así mismo se realiza la gestión en hallazgos de auditoria determinando responsabilidades fiscales según sea el caso. Dentro de sus pilares fundamentales orientados en el su plan estratégico se encuentra la *Tecnología* como uno de los ejes principales, en éste escenario la Contraloría de Bogotá, D.C., busca la apropiación y el uso de las Tecnologías de la Información y las Comunicaciones como herramienta que potencialice el ejercicio del control fiscal, hacia el conocimiento y la innovación.[27]

Uno de los objetivos específicos del plan estratégico de tecnologías de la información y las comunicaciones (PETI) es continuar con la implementación de la Política de Gobierno Digital difundida por el Gobierno

[27] CONTRALORIA DE BOGOTA D.C., Planes y programas, Plan Estratégico 2016 – 2020. http://www.contraloriabogota.gov.co/sites/default/files/Contenido/Planes/Planes%20y%20Programas/Planes/Estrategico/2016-2020/Versi%C3%B3n%203.0/PLAN%20ESTRATEGICO%20INSTITUCIONAL%202016-2020%20Ver%203.0.pdf

Nacional y la Alta Consejería Distrital de TIC, para afianzar el uso y aprovechamiento de las tecnologías y así contribuir a promover la participación ciudadana y el control social en los procesos de control y vigilancia fiscal.[28]

Uno de los motivadores en cuanto al PETI, es continuar con los recursos, estrategias y esfuerzos encaminados a la implementación y gestión de la plataforma tecnológica que da un soporte eficiente a la infraestructura y los sistemas de información, encaminando desde uno de sus objetivos estratégicos proteger la información institucional, buscando mantener la triada de la información en cuanto a la confidencialidad, la disponibilidad y la integridad, de igual forma que la seguridad de los datos de la entidad. De esta forma uno de los proyectos de la Contraloría de Bogotá D.C. frente a las estrategias de Política de Gobierno Digital es el de dar continuidad con el desarrollo del subsistema de la información, realizando actividades para su implementación, gestión, verificación y mejora continua.

- La Contaduría General de la Nación es una unidad administrativa especial creada por la constitución política de Colombia, dentro de sus principales funciones se encuentra determinar políticas, principios y normas sobre contabilidad que deben regir en la nación para el sector público, centralizar y consolidar la contabilidad pública, llevar la contabilidad de la nación así como establecer el balance general para su presentación ante el congreso de la república, entre otras. Dentro de sus políticas de gestión y desempeño institucional el gobierno digital y la seguridad digital las cuales hacen parte del desarrollo administrativo y orientan a la gestión y manejo de los recursos humanos, técnicos, materiales, físicos y financieros de las entidades de la administración pública.[29]

  La Contaduría establece estrategias y controles en el marco del SGSI asegurando la disposición de recursos requeridos y un enfoque basado en la gestión de objetivos de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información y mejora continua, con lo anterior, se compromete a garantizar, verificar y cumplir los requerimientos operativos, normativos, legales aplicables a la seguridad de la información, a través de la concientización de los funcionarios en seguridad de la información.[30]

[28] CONTRALORIA DE BOGOTA D.C., Planes y programas, PETI 2016 – 2020 Versión 5.0 http://www.contraloriabogota.gov.co/sites/default/files/Contenido/Planes/Planes%20y%20Programas/Planes/PETI/2016-2020/Versi%C3%B3n%205.0/PETI%202016-2020%20v5.pdf

[29] CONTADURIA GENERAL DE LA NACION, Nuestra entidad. “Direccionamiento estratégico”. http://www.contaduria.gov.co/direccionamiento-estrategico

[30] CONTADURIA GENERAL DE LA NACION. Manual y políticas del sistema integrado de gestión institucional. http://www.contaduria.gov.co/manual-y-politicas-del-sistema-integrado-de-gestion-institucional

- La Alcaldía Municipal de Fusagasugá es un ente del orden territorial que administra los recursos públicos del Estado en busca del bienestar de la ciudadanía Fusagasugueña a través de la prestación de servicios de calidad. Entre sus funciones principales esta satisfacer las necesidades y requerimientos de la comunidad, la implementación de procesos de las actividades propias del municipio, el fortalecimiento de las competencias laborales y la cultura de la atención oportuna y transparente, la gestión y administración de los recursos y el cumplimiento de las competencias y normas legales para la ejecución del mandato legal y transparente.[31] Está ubicada en el municipio de Fusagasugá conocido como "La ciudad jardín", provincia del Sumapaz del departamento de Cundinamarca a 59 km al suroccidente de Bogotá

  La Alcaldía ha determinado la necesidad de establecer, implementar y mantener el Modelo de Seguridad y Privacidad de la Información (MSPI) con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información que procesa, almacena, crea y/o transporta en su operación diaria, es por esto que la entidad pone a disposición de empleados, contratistas, proveedores y ciudadanía en general el manual de seguridad de la información el cual contiene los elementos del MSPI y su interacción para el cumplimiento de las políticas de seguridad de la información.

[31] ALCALDIA DE FUSAGASUGA, Nuestra Alcaldía. Objetivos y funciones. http://www.fusagasuga-cundinamarca.gov.co/NuestraAlcaldia/Paginas/Objetivos-y-Funciones.aspx

5. METODOLOGIA

Para llevar a cabo la realización del presente documento, se desarrollaron las siguientes fases para el cumplimiento de cada uno de los objetivos propuestos:

5.1 FASE 1

En esta fase y de acuerdo con el planteamiento del primer objetivo específico, se realizó una búsqueda de información y de producciones documentales, las cuales contenían en gran parte de su desarrollo un acercamiento al tema de la seguridad informática enfocado hacia como las entidades públicas se han desempeñado en materia, como ha sido su evolución teniendo en cuenta que es un tema que en los últimos años ha tenido un crecimiento exponencial y como el gobierno nacional ha puesto la lupa emitiendo normativas y políticas publicas buscando alinear a las instituciones y entidades a buscar la mitigación de riesgos y amenazas cibernéticas, así como motivando a la implementación de procesos, procedimientos, controles, mecanismos y dispositivos que coadyuven a estas en el trabajo de la protección y seguridad informática y de la información.

Con relación a la información recopilada, se pudo destacar que existe en la actualidad mucha información que logra poner en contexto el tema del presente documento, al ser este un tema de gran relevancia no solo para el mundo sino para también para nuestro país, varios autores en proyectos ya presentados, en artículos y publicaciones en internet, hacen referencia de como se ha venido trabajando la seguridad informática en las entidades del sector gobierno colombiano y cuál ha sido su influencia para contrarrestar los riesgos y amenazas que potencialmente puedan tener frente a los ataques cibernéticos.

5.2 FASE 2

En esta segunda fase, se logró hacer un análisis del impacto en materia de seguridad informática que ha tenido en el transcurso de los años el país y como las entidades del sector gobierno colombiano han asimilado estas políticas públicas de ciberseguridad y dando continuidad con el segundo objetivo específico, se realizó un acercamiento a una entidad pública identificando cual podría ser un buen modelo y que beneficios ha brindado esa implementación de procesos y procedimientos orientados a la seguridad informática y frente a la mitigación de los riesgos y amenazas cibernéticas a los cuales se encuentra expuesta.

5.3 FASE 3

Para la tercera fase y de acuerdo a la documentación recopilada y observada en las anteriores fases, se tuvo en cuenta cual ha sido el desempeño de las entidades del sector gobierno y con relación al acercamiento al plan estratégico de tecnologías de la información y las comunicaciones (PETI) de la entidad pública que se analizó en la anterior fase, se determinaron las recomendaciones que podrían contribuir y orientar hacía la importancia de la implementación del aseguramiento informático en busca de la mitigación de riesgos y amenazas cibernéticas y la mejora continua frente a los potenciales ataques informáticos que puedan tener las entidades del sector gobierno colombiano.

6. ANALISIS DE LA SEGURIDAD INFORMATICA Y SU INFLUENCIA EN ALGUNAS ENTIDADES PÚBLICAS EN EL PAIS

En relación a la política de ciberseguridad y ciberdefensa definida en el CONPES 3854, se concentra en contrarrestar y minimizar el aumento de las amenazas cibernéticas en bandera de dos objetivos de gran relevancia: la defensa del país y la lucha contra el cibercrimen.

De acuerdo con los lineamientos del CONPES 3854, se pretende que esta política nacional de seguridad digital, busca cambiar el enfoque tradicional que se había dado al aseguramiento y protección digital hacia la inclusión de la gestión del riesgo siendo uno de los elementos de más relevancia al abordar la seguridad digital, a través de cuatro principios fundamentales y cinco dimensiones estratégicas que son la base de la política del documento CONPES 3854:

Principios fundamentales

- Salvaguardar los derechos humanos
- Enfoque incluyente y colaborativo
- Responsabilidad compartida
- Enfoque de gestión de riesgo

Dimensiones estratégicas

- Gobernanza
- Marco legal y regulatorio
- Gestión de riesgos de seguridad digital
- Cultura ciudadana
- Capacidades para la gestión del riesgo

El panorama actual en términos generales de la seguridad informática en Colombia, presenta problemas significativos de ciberseguridad, sin embargo, estas falencias no son de tal criticidad comparadas con otros países de la región e inclusive con otros fuera de la región latinoamericana. Este balance lo entrego Comparitech, una plataforma especializada en el análisis de servicios tecnológicos.[32]

La muestra de este estudio se realizó en 60 países, dentro de los cuales Argelia ocupo el primer puesto con los peores índices de ciberseguridad. En contraste con este resultado Japón fue el país con los mejores índices con el tema en mención. De acuerdo con lo anterior Colombia ocupo el puesto 39, situándolo en un rango

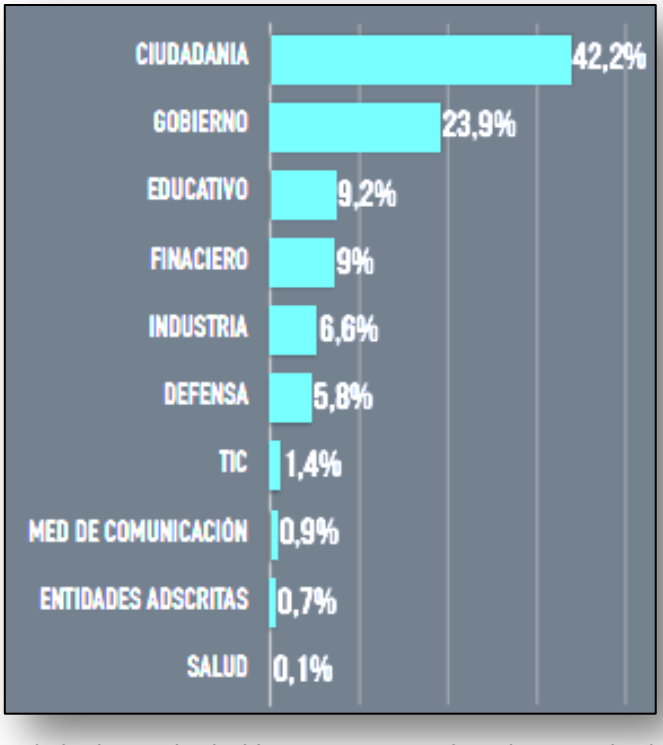
[32] PROFITLINE, SERVICIOS IT OUTSOURCING. ACTUALMENTE COMO SE ENCUENTRA COLOMBIA EN SEGURIDAD INFORMÁTICA. https://profitline.com.co/actualmente-como-se-encuentra-colombia-en-seguridad-informatica/

medio, en cuanto a los índices analizados por la plataforma encargada de realizar el estudio.

En cuanto a la medición realizada por el estudio en la parte legislativa, no tuvo un resultado muy alentador, sobre una calificación sobre 10 Colombia obtuvo una apreciación de 4, sin embargo, y no siendo conformistas, ninguno de los países analizados en el estudio sobrepaso la calificación de 7. Justamente en el presente gobierno se han intentado modernizar la ley de las TIC pero las propuestas han recibido varios reproches sobre todo en el tema del trato a la televisión pública, razón por la cual el Congreso de la Republica las coloco en lista de espera para su respectiva observación.

De acuerdo al análisis y lo diagnosticado en el CONPES 3854, el país ha tenido un incremento en cuanto a temas de conectividad aproximadamente desde el año 2010, dado esto, también ha aumentado las vulnerabilidades y riesgos en temas de seguridad de la información. Como se muestra en el Grafico 1, se puede apreciar a los sectores más afectados en el país con relación a incidentes digitales:

Grafico 1. Afectación incidentes digitales por sectores

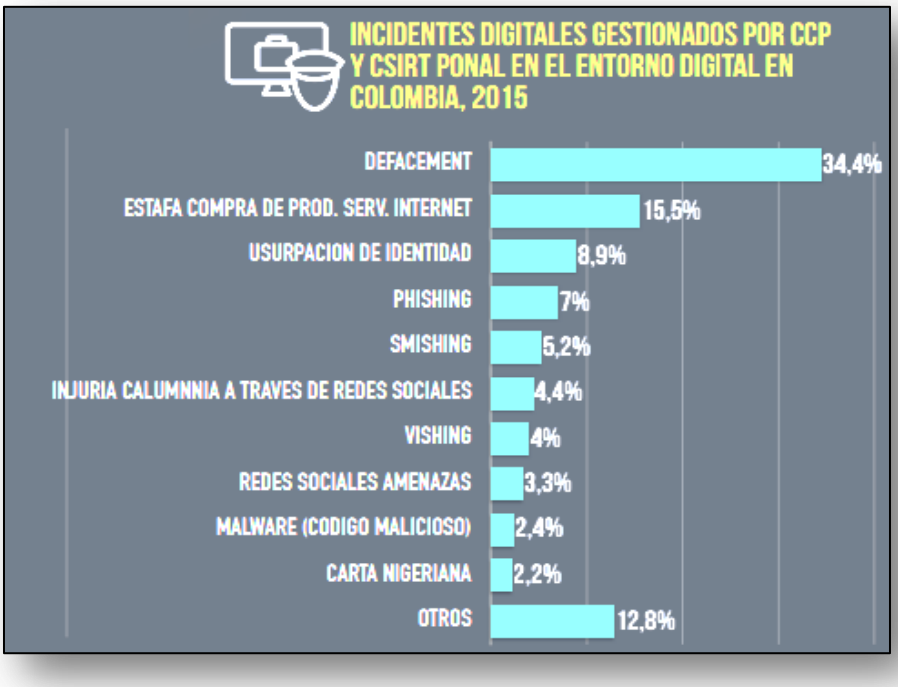


Fuente: MEJIA, María Isabel. Diagnostico incidentes: Sectores afectados en Colombia por incidentes digitales, 2015 (colCERT) [Grafico]. Nueva política pública de seguridad digital: Desafíos y oportunidades en el escenario de posconflicto. Colombia. MINTIC. 2016. [Consultado: 12 de mayo de 2019]. Disponible en: https://mintic.gov.co/portal/604/articles-15570_recurso_2.pdf

Con relación al análisis realizado por el MinTIC, se evidencia que la ciudadanía en general es la más afectada en incidentes informáticos, seguido del sector gobierno con un 23,9% del cual se hace un énfasis en el análisis del comportamiento de la seguridad informática del país. Es importante tener la concienciación de los riesgos en cuanto a seguridad digital y poder establecer los correctivos necesarios al respecto.

De igual forma se analizaron cuáles fueron los incidentes digitales más gestionados por CCP y CSIRT PONAL en el entorno digital en el país, se puede apreciar que en el Grafico 2 se encuentran los diferentes porcentajes de cuales han sido estos incidentes digitales que se han presentado en el país:

Grafico 2. Incidentes digitales más gestionados por CCP y CSIRT PONAL.



Fuente: MEJIA, María Isabel. Diagnostico incidentes: Sectores afectados en Colombia por incidentes digitales, 2015 (CCP y CSIRT PONAL) [Grafico]. Nueva política pública de seguridad digital: Desafíos y oportunidades en el escenario de posconflicto. Colombia. MINTIC. 2016. [Consultado: 12 de mayo de 2019]. Disponible en: https://mintic.gov.co/portal/604/articles-15570_recurso_2.pdf

En el anterior gráfico, se destaca el Defacement con un porcentaje de 34,4%, la estafa por internet con el 15,5%, la usurpación de identidad y el phishing con 8,9% y 7% respectivamente, como los incidentes digitales con mayor gestión y por los cuales se ven más atacadas las entidades.

Estos riesgos de seguridad digital en las entidades del sector gubernamental, pueden causar incertidumbres y vulnerabilidades que durante los últimos años se han ido incrementando a medida que también crece la infraestructura tecnológica de las entidades, generando como consecuencias altos costos de la actividad maliciosa y afectación de la infraestructura critica cuando no se tienen los debidos controles y procedimientos para la protección tanto de la seguridad perimetral así como la salvaguarda de la información con la implementación de los sistemas de gestión de seguridad de la información.

De acuerdo al enfoque dado por el informe "Nueva política pública de seguridad digital: desafíos y oportunidades en el escenario de posconflicto", [33] se dio un diagnóstico institucional en el cual se identificaron los siguientes ítems en las entidades públicas:

- No cuentan con una visión estratégica establecida en la gestión de riesgos.
- Se requiere robustecer las capacidades de ciberdefensa dando una orientación a la gestión de riesgos de seguridad.
- La cooperación, colaboración y asistencia tanto nacional como en el campo internacional, deben estar ligados con la seguridad digital, que al momento del diagnóstico no son suficientes y deben estar articulados.

Es debido a estas y otras tantas causas que el gobierno nacional en cabeza del Ministerio de Tecnologías de la Información y las Comunicaciones lanzo en su momento el primer documento CONPES 3701 como lineamientos de política para ciberseguridad y ciberdefensa, esperando con ello poder contrarrestar las amenazas cibernéticas en el entorno digital, ayudando a fortalecer las capacidades de los probables afectados en cuanto a la identificación y gestión de los riesgos de seguridad de la información.

También uno de los tantos logros obtenidos por esta política de ciberseguridad y ciberdefensa, ha sido el fortalecimiento de la institucionalidad en cuanto a seguridad se refiere, creando nuevas instancias como las siguientes:

- colCERT: Grupo de respuesta a emergencias cibernéticas de Colombia (Ministerio de Defensa Nacional).
- CCOC: Comando Conjunto Cibernético (Comando General de las Fuerzas Militares de Colombia).
- CCP: Centro Cibernético Policial (Policía Nacional de Colombia).
- CSIRT PONAL: Equipos de respuesta a incidentes de seguridad informática de la Policía Nacional.
- Delegatura de protección de datos de la Superintendencia de Industria y Comercio.

[33] Mintic. NUEVA POLÍTICA PÚBLICA DE SEGURIDAD DIGITAL: DESAFIOS Y OPORTUNIDADES EN EL ESCENARIO DE POSCONFLICTO. https://www.mintic.gov.co/portal/604/articles-15570_recurso_2.pdf

- Subdirección técnica de seguridad y privacidad de tecnologías de información (MinTIC).
- Comité de ciberdefensa (Fuerzas Militares).
- Unidades cibernéticas (Ejército Nacional, Armada Nacional y Fuerza Aérea Colombiana)[34]

En tanto el documento CONPES 3854 de 2016 ha tenido como aspectos relevantes:

- Definir las acciones a partir de su año de expedición ya que el anterior documento solo tenía acciones definidas hasta el 2015.
- Contiene la oportunidad de establecer recomendaciones y seguimiento de alto nivel.
- Establece los lineamientos y orientaciones de la política pública.

Es un instrumento que con el cual los miembros de alto nivel del gobierno nacional tengan en cuenta las instrucciones directamente de la presidencia de la república.

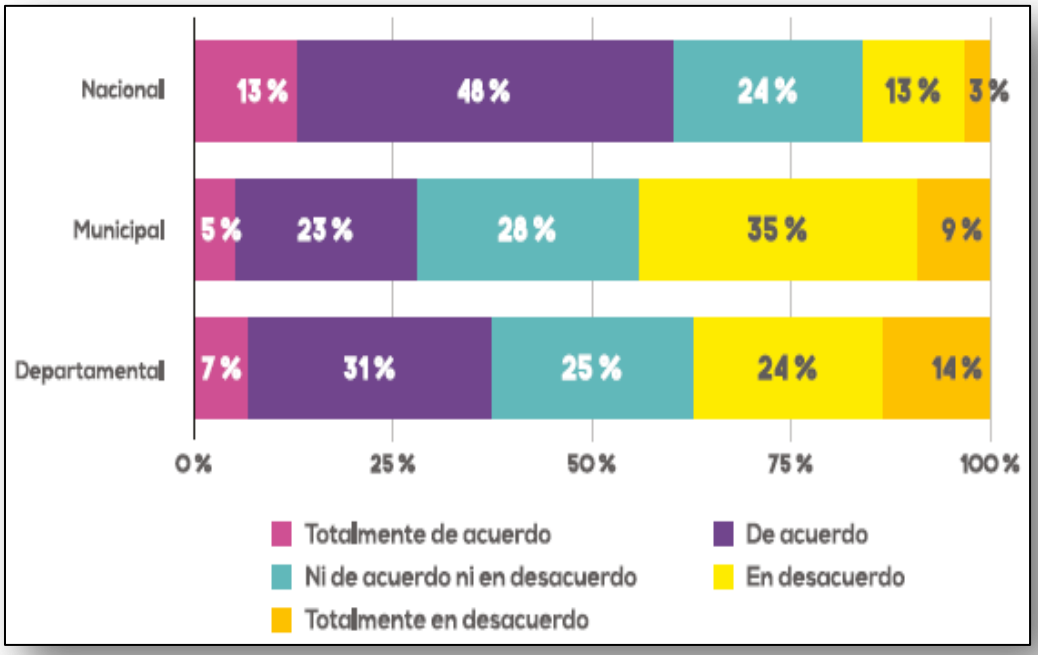
El aseguramiento informático en las entidades del sector gubernamental Colombiano cuenta con los siguientes datos de acuerdo al informe "Impacto de los incidentes de seguridad digital en Colombia 2017"[35] realizado entre la OEA, el Ministerio de Tecnologías de la Información y las Comunicaciones y el BID, en el que se destacan como han estado preparadas las entidades frente a un incidente de carácter digital, cual es la proyección en cuanto a temas de protección de activos de información y como se ha gestionado el presupuesto para prepararse frente a un potencial ataque de cirberdelincuentes.

Las practicas se seguridad digital en las entidades públicas son un mecanismo para gestionar los riesgos y amenazas detectados, frente a esto se evidencio que a nivel nacional el 13% y 48% se sentían en cierto sentido muy preparados o preparados frente a un incidente digital, a nivel territorial estos porcentajes son más bajos con el 28% y 38% respectivamente, en el Grafico 3 se puede apreciar los porcentajes de cómo se sienten preparadas las entidades para enfrentar un incidente digital:

[34] Documento CONPES 3854. POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[35] BID. Impacto de los incidentes de seguridad digital en Colombia 2017. https://publications.iadb.org/es/publicacion/17294/impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017

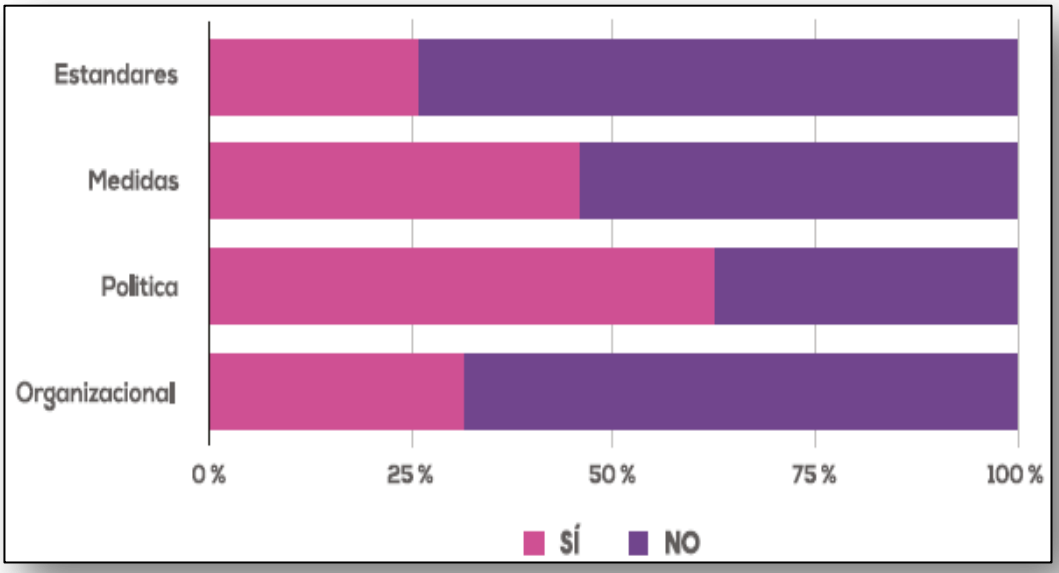
Grafico 3. Preparacion frente a un incidente digital



Fuente: OEA, MINTIC, BID. Prácticas de seguridad digital en las entidades: Nivel de preparación de la entidad para hacer frente a un incidente digital. [Grafico]. Impacto de los incidentes de seguridad digital en Colombia 2017. Colombia. MINTIC. 2017. [Consultado: 12 de mayo de 2019]. Disponible en: http://dx.doi.org/10.18235/0000843

Con relación a los anteriores niveles de preparación de las entidades públicas, se traslada al siguiente cuestionamiento y es qué buenas practicas han sido implementadas entre estándares o normatividad, medidas técnicas, políticas de funcionamiento y medidas organizativas; de acuerdo a los resultados del informe, un gran porcentaje de entidades han implementado políticas de funcionamiento (62%), seguido de medidas técnicas con un porcentaje de 46% y 31% de las entidades han implementado medidas organizativas, como se muestra en el Grafico 4, existe un alto porcentaje de prácticas en seguridad que no se han implementado en las entidades públicas:

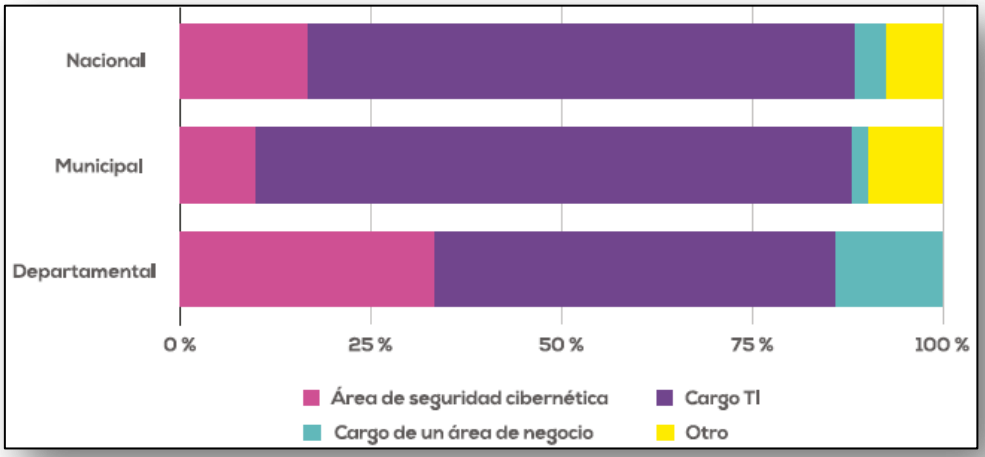
Grafico 4. Practicas en seguridad digital implementadas en las entidades publicas



Fuente: OEA, MINTIC, BID. Prácticas de seguridad digital en las entidades: Practicas de seguridad digital implementadas por las entidades. [Grafico]. Impacto de los incidentes de seguridad digital en Colombia 2017. Colombia. MINTIC. 2017. [Consultado: 12 de mayo de 2019]. Disponible en: http://dx.doi.org/10.18235/0000843

Como se puede considerar en el anterior gráfico, muchas de las entidades no han implementado prácticas de seguridad porque no tienen definido un departamento o un grupo de seguridad informático que responda a estas medidas para enfrentar incidentes de carácter digital, es probable que para dar respuesta a la implementación de estándares, políticas de funcionamiento y medidas técnicas y organizativas, se traslade este tipo de responsabilidades directamente al departamento de tecnologías de la información como una función general o se lleve incluso a otras áreas de la entidad que simplemente no tengan mucho que ver frente a estos temas del aseguramiento informático. Con relación a lo anterior, se evidencia que un alto porcentaje de entidades públicas tiene el rol de seguridad digital a cargo del departamento TIC frente a un pequeño porcentaje que tiene definido un área dedicada a la seguridad informática, como se visualiza en el Grafico 5, solo el 17% de las entidades a nivel nacional cuentan con esta área definida, así como el 10% y 33% para las entidades a nivel municipal y departamental respectivamente:

Grafico 5. Entidades con rol o area de seguridad digital



Fuente: OEA, MINTIC, BID. Prácticas de seguridad digital en las entidades: Entidades con área, cargo(s) o rol(es) dedicado(s) a la seguridad digital. [Grafico]. Impacto de los incidentes de seguridad digital en Colombia 2017. Colombia. MINTIC. 2017. [Consultado: 12 de mayo de 2019]. Disponible en: http://dx.doi.org/10.18235/0000843

En cuanto al tema de inversión y presupuesto que realizan las entidades públicas a la seguridad de la información, se evidenciaron principalmente 4 categorías. Con un porcentaje de 46% las entidades asignaron su presupuesto de recursos de TI a plataformas y medios (Hardware y Software), el 30% de las entidades asigno el presupuesto de TI a la contratación de recursos humanos (empleados/contratistas) y el 9% y 15% lo asignaron a la generación de conocimiento (capacitaciones, investigación) y servicios especializados (gestión de seguridad, soporte) respectivamente. En el Cuadro 1, se representa como se realizó la asignación de recursos de TI en los presupuestos de las entidades en general:

Cuadro 1. Porcentaje de recursos asignados a TI en las entidades

Categoría	**Porcentaje**
Recursos Humanos (ej. empleados, contratistas)	30%
Plataformas y Medios Tecnológicos (ej. hardware, software)	46%
Generación de Capacidades (ej. capacitación, concientización, investigación)	9%
Servicios Especializados (ej. gestión de seguridad, externalización, soporte)	15%

Fuente: OEA, MINTIC, BID. Presupuesto para la seguridad digital en las entidades: Asignación del presupuesto para la seguridad digital por entidad que asignaron recursos a TI (2016). [Cuadro]. Impacto de los incidentes de seguridad digital en Colombia 2017. Colombia. MINTIC. 2017. [Consultado: 12 de mayo de 2019]. Disponible en: http://dx.doi.org/10.18235/0000843

6.1 ATAQUES A ENTIDADES DEL ESTADO COLOMBIANO

De acuerdo al servicio de inteligencia de amenazas de la firma Fortinet, realizaron un estudio en el que publico que entre los meses de abril y julio del año 2019, el territorio colombiano sufrió algo más de 40 millones de intentos de ataques cibernéticos colocando a la nación en uno de los países de esta región con uno de los índices más altos en intentos de intrusión a la seguridad informática.

Estos intentos de ataques cibernéticos la mayoría fueron producidos por exploits, códigos que aprovechan las debilidades de las aplicaciones o de algunos sistemas para ser controlados remotamente, dándoles a los atacantes la llave para acceder a los sistemas. Dentro de los ataques cibernéticos recibidos por las entidades públicas, se encuentran muchos catalogados en la interrupción de servicios y/o robos de información, causando fallas en la prestación de los servicios prestados por las instituciones, daños en su infraestructura y obviamente pérdidas ascendiendo a millones de pesos.

Algunos ejemplos de estos ataques presentados en los últimos 10 años son los siguientes:

- Registraduria Nacional del Estado Civil (2010) Ataque masivo de hackers durante las elecciones parlamentarias que hizo colapsar al sistema de datos.[36], de acuerdo a las revelaciones realizadas por Colprensa, al parecer lo ataques generados provinieron del Ministerio de Defensa, el Departamento Administrativo de Seguridad DAS y desde la Policía Nacional, es por esto que el CTI de la fiscalía decidió archivar la investigación considerando que no habían pruebas suficientes; para este caso la defensa de la Registraduria Nacional llevaría el caso hasta últimas instancias debido a que consideraron que para este ataque presentado se estaría mostrando una muestra de impunidad.

- Registraduria Nacional del Estado Civil (2011) Confirmó el primer ataque de 'hackers' al sitio web de la entidad las consultas de bases de datos del Censo Electoral y la de jurados de votación, intentaron ser bloqueadas por Anonymus.[37], de acuerdo a las declaraciones dadas por el registrador de ese entonces Carlos Ariel Sánchez, se intentó bloquear las bases de datos del censo electoral y la de jurados de votación, este ataque fue frustrado debido a que se logró detectar a tiempo las direcciones IP desde donde provenían los actos delictivos y se dio informe a tiempo a la fiscalía y a la policía, estos prepararon un completo plan de seguridad informática en el

[36] EL UNIVERSAL. Investigación sobre ataques de hackers a la Registraduría será cerrada. https://www.eluniversal.com.co/home/investigacion-sobre-ataques-de-hackers-la-registraduria-sera-cerrada-65604-HVEU147563 2012

[37] El Espectador. Confirman primer ataque de ' a la Registraduría. https://www.elespectador.com/noticias/politica/confirman-primer-ataque-de-hackers-registraduria-articulo-300731

que en los puntos de información de los resultados electorales fueran neutralizados hechos que pudieran afectar el proceso de las elecciones de ese entonces.

- Empresa de Acueducto y Alcantarillado de Bogotá (2012) Ataque informático de 3 días a la página oficial de contrataciones de la entidad, con interrupciones en su funcionamiento e inscripción de proveedores en los procesos de contratación.[38], en noviembre de 2012 se presentó luego de presentar una publicación de un proceso contractual por cerca de 80 mil millones para realizar la compra de vehículos para la operación de servicio público de aseo, el ataque cibernético completo tres días y solo tuvo afectación en la página de contrataciones de la EAAB.

- Fiscalía de Tibú (2013) En asonada incendiaron casa del alcalde y la Fiscalía de Tibú, Norte de Santander Quemaron los archivos de la Fiscalía, los manifestantes ingresaron por el parqueadero y le prendieron fuego a la estructura.[39], los manifestantes entraron por el parqueadero de la Fiscalía de Tibu y como acciones intentaron incendiar la infraestructura, a pesar que la lluvia logro apaciguar el fuego, la turba sin embargo ingresó al lugar, tomaron archivos y documentos prendiéndoles fuego, causando con ello perdida de información propia y reservada de la institución.

- Superintendencia Financiera (2014) Superfinanciera NO hace llamadas para solicitar información personal.[40], hacia mediados del año 2014, la Superintendencia Financiera lanzo un comunicado advirtiendo al público y ciudadanía en general, que personas inescrupulosas estaban realizando llamadas telefónicas y solicitando información y datos personales, así como datos de tarjetas de crédito en nombre de esa entidad. Advirtió que ellos no realizan este tipo de gestión e invito a los ciudadanos se requerían algún tipo de información a dirigirse a los canales dispuestos por parte de la superfinanciera.

- Municipios de Aguada, Santander (2015) En menos de tres meses el presupuesto de estos municipios había desaparecido, en septiembre de 2015, unos delincuentes habían desocupado las cuentas por medio de un virus informático, el robo superó los 1142 millones de pesos.[41], Ricardo Ariza alcalde de Aguada, afirmo que el presupuesto de su municipio alcanzaba los 3000 millones, lo que quiere decir que el robo ascendió cerca del 40% del total, el modo de operación de los ciberatacantes fue enviar un

[38] CM&. Hacker ataca sitio web EAAB, link de contratación. http://www cmi com co/?n= 92235 2012

[39] Vanguardia. En asonada incendiaron casa del alcalde y la Fiscalía de Tibú, Norte de Santander. https://www.vanguardia.com/colombia/en-asonada-incendiaron-casa-del-alcalde-y-la-fiscalia-de-tibu-norte-de-santander-CAvl212231

[40] Superfinanciera. Superfinanciera NO hace llamadas para solicitar información personal. https://www.superfinanciera.gov.co/inicio/10083259

[41] Infolaft. Un ataque informático. https://www.infolaft.com/en-vivo-un-ataque-informatico/

correo al tesorero del municipio con un anexo el cual contamino el computador, de esta forma aprovecharon cuando movió el dinero para robar información y datos contables. Gracias al accionar de la Policía y Fiscalía, se logró montar un operativo que dio como resultado la captura de 8 personas que conformaban la banda delincuencial que hurtaba a través de medios informáticos.

- Fiscalía General de la Nación (2016) Piratas informáticos han hecho circular correos con logos de la Fiscalía para robar los datos de usuarios desprevenidos.[42], una compañía de seguridad (Eset) informo sobre una amenaza a través de la web, se trataba de un correo electrónico fraudulento de una supuesta citación por parte de la Fiscalía General de la Nación el cual contenía los logos de dicha entidad para hacerlo parecer un correo oficial el cual contenía un enlace que supuestamente descargaba un archivo con la citación que en realidad era un archivo malicioso. Este tipo de archivos roban información valiosa de los usuarios que los atacantes la utilizan en muchos casos para ingeniería social.

- Dirección de Impuestos y Aduanas Nacionales (2017) Alerta a los ciudadanos sobre falsos correos que están circulando a nombre de la DIAN y utilizando el nombre de funcionarios, notifican a los ciudadanos contribuyentes sobre la apertura de presuntas investigaciones por evasión de Impuesto Sobre las Ventas -IVA y Retefuente.[43], a través de correos electrónicos los atacantes invitaban a consultar a través de links el estado y causales de un supuesto proceso de evasión de impuestos y a ponerse en contacto con un aparente funcionario, con logos del Ministerio del Interior, de la DIAN y un número de expediente que se encontraba en un link, los delincuentes tomaban la información personal de los incautos. La entidad reitero a la ciudadanía a verificar en los canales oficiales la autenticidad de la información que recibían.

- Alcaldía de Ibagué (2018) Incendio en la Alcaldía provoca daños en computadores y destrucción de algunos documentos.[44], la conflagración se presentó en el segundo piso de la Alcaldía de Ibagué justamente en el área donde se estructuran y revisan procesos de contratación de la secretaria administrativa. Se tuvo reporte de la emergencia alrededor de la 1:00 a.m. pero en el momento que arribo el cuerpo de bomberos, ya el incendio había ocasionado daños materiales en esa dependencia, afectado equipos de cómputo, impresoras y sobre todo papelería que no se precisó que tipo de información se perdió en el incendio. Al parecer el incendio se produjo por

[42] Semana. No se deje engañar: estos son los correos falsos de la Fiscalía. https://www.semana.com/tecnologia/articulo/correos-falsos-de-lafiscalia/489435

[43] DIAN. Circula Otra Versión De Falsos. http://www.dian.gov.co/descargas/EscritosComunicados/2017/033_Comunicado_de_prensa_23022017.pdf

[44] El olfato. Incendio en la Alcaldía de Ibagué provoca daños en computadores y destrucción de algunos documentos. https://elolfato.com/incendio-en-laalcaldia-de-ibague-provoca-danos-en-computadores-y-destruccion-de-algunos-documentos

un corto circuito que genero una impresora que quedo encendida, sin embargo en el sitio donde se produjo el suceso, ha tenido variados escándalos en cuanto a la participación en pagos irregulares que se hicieron a la firma Infotic que presuntamente tenia lazos familiares y presentaba conflicto de intereses al momento de realizar la contratación con la Alcaldía de Ibagué.

- Secretaria de Movilidad (2019) Falso: fotocomparendos no se notifican vía correo electrónico.[45], ante múltiples quejas de muchos ciudadanos, la Secretaria de Movilidad informo que ciberdelincuentes estaban haciendo llegar correos a la ciudadanía con falsas notificaciones de comparendos que no existían, los correos no tienen ningún fundamento legal, con cuentas de correo falsas, citando leyes y números de comparendo que no correspondían a la codificación oficial, además del texto del correo incluía un archivo adjunto que al descargarse en los computadores de los ciudadanos producía perdida de información así mismo como el robo de la misma. La Secretaria de Movilidad fue enfática en que las notificaciones de los comparendos no se hacen vía correo electrónico sino por correspondencia física, por lo que recomendaron no descargar ningún tipo de archivo procedente de estas cuentas, de igual forma no suministrar ningún tipo de información personal por ningún otro medio ni telefónico ni electrónico y asegurarse de realizar transferencias de datos en sitios protegidos visualizando los protocolos HTTPS y SSL en las URL de los sitios cuando naveguen en internet.

Teniendo en cuenta que el estado colombiano promulgó una política pública, donde la principal finalidad fue la entregar acciones para la ciberdefensa y ciberseguridad de la información, a través de la creación de entidades estatales apoyadas por las instituciones de seguridad ya existentes en Colombia que permitieran la intersección de las acciones que atentan contra la información de la nación y más cuando se trata de información confidencial, asignó una suma importante de recursos económicos que permitieron el desarrollo de estas estrategias y así posicionar a Colombia como país pionero en la implementación de acciones para la protección de las entidades gubernamentales, mediante el análisis de esta se pudo constatar que aunque la nación avanzó en temas de seguridad de la información, desconoció la importancia de las entidades territoriales y lo más importante, olvidó al habitante de Colombia como pilar importante del territorio nacional.

Con la promulgación de la segunda política pública en el año 2016, los errores del pasado fueron corregidos y de manera importante se reconoció a las personas como centro de atención nacional y se le brindaron las condiciones óptimas para

[45] EL NUEVO SIGLO. Falso: fotocomparendos no se notifican vía correo electrónico. https://www.elnuevosiglo.com.co/articulos/02-2019-falsofotocomparendos-no-se-notifican-correo-electronico

el manejo de la información, adicional de manera importante se involucran las entidades territoriales y se le da a Colombia el posicionamiento internacional merecido de acuerdo a los esfuerzos realizados año tras año para conseguir el blindaje de la información o en el menor de los casos las acciones necesarias para procesar legalmente a las personas que pasan por encima de la normatividad colombiana.

Es de mencionar que la Política Pública, está basada en garantizar los principios fundamentales, permitiendo crear acciones de garantizar los derechos humanos de cada uno de los colombianos y preservar los valores fundamentales a los que son acreedores cada individuo, adicional se basa en la adopción de un enfoque incluyente y colaborativo, asegurara una responsabilidad compartida entre todos los actores involucrados del estado y permitir la adopción de estrategias previendo posibles riesgos y de esta manera garantizar que los colombianos interactúen dentro del entorno digital de una forma libre, confiable y segura.

En términos generales, el ingreso que se ha dado a la tecnología en los últimos años ha ido avanzando de igual forma por lo que está relacionado directa y proporcionalmente, es decir, que a medida que avanza la tecnología, de la misma manera progresa la facilidad de acceso a las redes. Con relación a lo anterior la gran mayoría de la población estaría expuesta a ser una potencial víctima de ciberdelincuentes y es por esto que también la población debe contar con los aspectos mínimos de ciberseguridad y tener algún conocimiento al respecto.

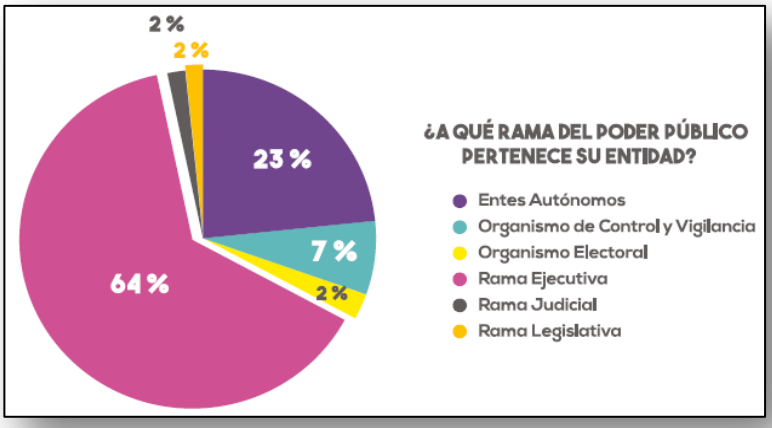
7. IMPACTO DEL USO Y TIPO DE TECNOLOGÍA DE SEGURIDAD INFORMÁTICA SEGÚN LO ESTABLECIDO EN LAS POLÍTICAS DE CIBERSEGURIDAD Y CIBERDEFENSA

El Ministerio de Tecnologías de la Información y las Comunicaciones en conjunto con la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), realizaron un estudio con visión a la preparación de las entidades privadas como empresas publicas colombianas para hacer frente en cuanto a la mitigación de las amenazas y vulnerabilidades en referente a la seguridad digital.[46]En este estudio también se permite visualizar los costos económicos que los incidentes en cuanto a seguridad digital han repercutido en varios sectores de la economía colombiana, representando las observaciones encontradas con relación a los perfiles de las empresas examinadas. Dentro del espectro de las entidades públicas colombianas consultadas para la realización del informe, se discriminaron de la siguiente forma en cuanto al siguiente perfil:

- 64% Rama Ejecutiva
- 23% Entes Autónomos.
- 13% Organismo Electoral, las Rama Judicial y Legislativa, y Organismos de control y vigilancia

La relación de las entidades públicas frente a la rama de poder público se aprecia en el Grafico 6:

Grafico 6. Distribución de entidades con relación a la rama de poder público a la que pertenece



Fuente: OEA, MINTIC, BID. Perfil de las entidades: Rama del poder público a que pertenece la entidad [Grafico]. Impacto de los incidentes de seguridad digital en Colombia 2017. Colombia. MINTIC. 2017. [Consultado: 12 de mayo de 2019]. Disponible en: http://dx.doi.org/10.18235/0000843

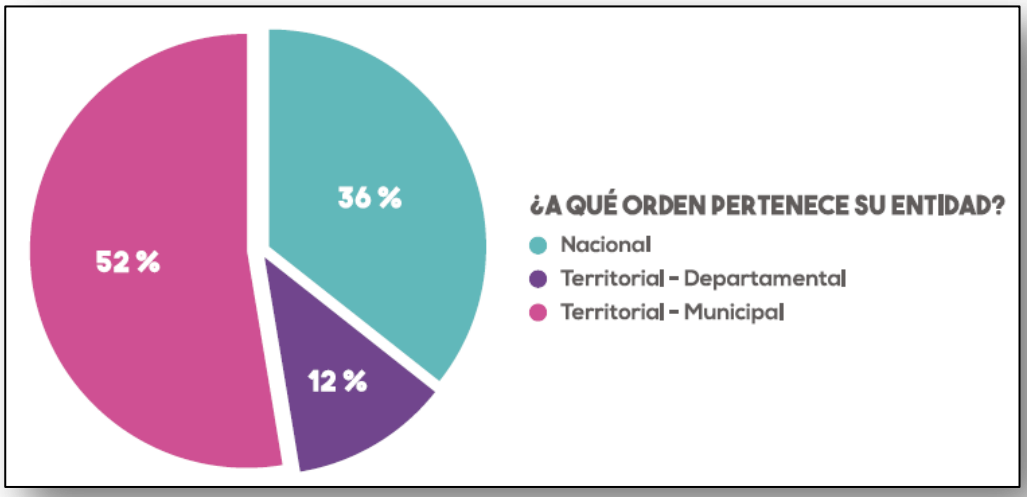
[46] BID. Impacto de los incidentes de seguridad digital en Colombia 2017. https://publications.iadb.org/es/publicacion/17294/impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017

Con relación al orden en que pertenecen las entidades públicas consultadas se tienen los siguientes datos:

- 52% Nivel Territorial-Municipal
- 36% Entidades nacionales
- 12% Territorial-Departamental.

En el Grafico 7 se puede apreciar cómo se encuentra el porcentaje en cuanto al orden al que pertenecen las entidades públicas consultadas:

Grafico 7. Distribución del orden al que pertenecen las entidades publicas



Fuente: OEA, MINTIC, BID. Perfil de las entidades: Orden a que pertenece la entidad [Grafico]. Impacto de los incidentes de seguridad digital en Colombia 2017. Colombia. MINTIC. 2017. [Consultado: 12 de mayo de 2019]. Disponible en: http://dx.doi.org/10.18235/0000843

El informe advierte sobre la poca asignación presupuestal en cuanto a los temas de seguridad digital de las organizaciones, sin embargo, cerca del 37% de las empresas consultadas se sienten preparadas para enfrentar en algún momento un suceso relacionado con la seguridad informática, y el 33% relacionado con el sector público de nivel nacional, tienen un área dedicada al desempeño de la seguridad digital.[47]

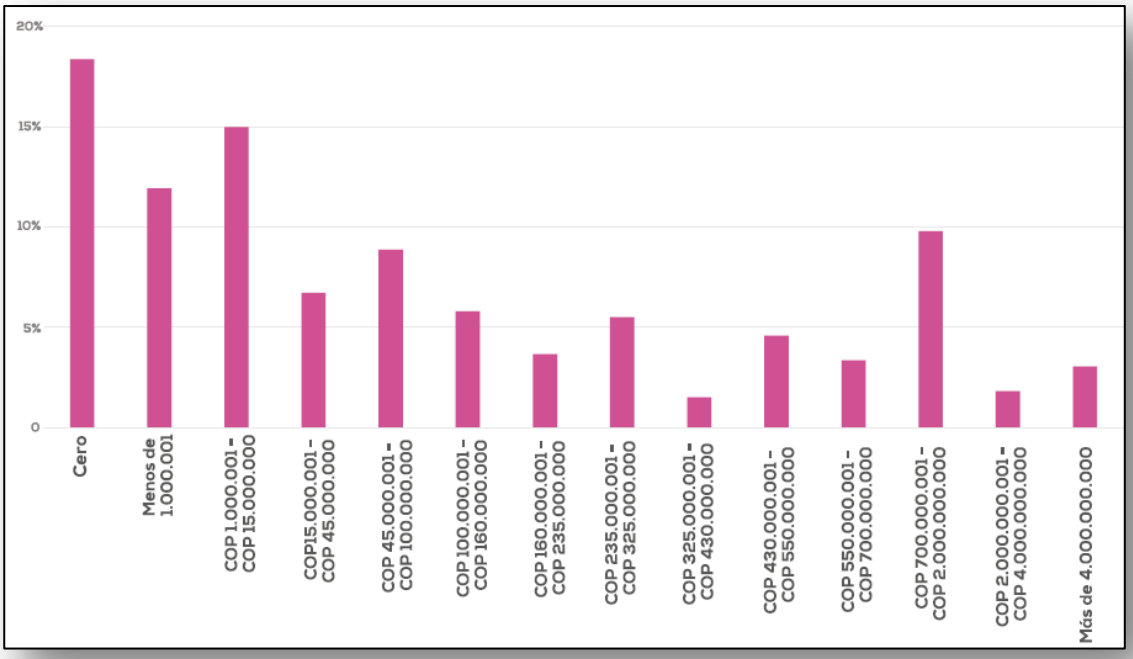
De acuerdo a un estudio realizado por Certicamara y Symantec en el año 2017, concluyeron que las empresas y entidades del sector gubernamental en Colombia a pesar del crecimiento de amenazas cibernéticas que podría llegar a un 60%, el presupuesto asignado para estas compañías apenas y llega al 10% del total de los

[47] EL TIEMPO, Tecnosfera. El 63 % de las grandes empresas identificaron incidentes digitales. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/resultados-del-estudio-impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017-137222

gastos.[48] Sin embargo, en el informe sobre los impactos de los incidentes de seguridad digital en Colombia (2017), se destaca que la mayoría de entidades públicas que asignaron presupuesto para Tecnologías de Información, también lo hicieron para el tema de Seguridad Digital. Alrededor del 82% de las entidades estatales realizaron asignación para TI y para Seguridad Digital,[49] con relación a los presupuestos asignados (en pesos) se obtuvieron los siguientes valores:

Con relación a los presupuestos que se asignan hacia la seguridad informática en el sector público en el Grafico 8 se aprecia los montos de distribución en porcentajes en pesos que se asignaron a las entidades públicas:

Grafico 8. Presupuestos asignados en pesos en las entidades publicas



Fuente: OEA, MINTIC, BID. Perfil de las entidades: Presupuesto para la seguridad digital (2016) [Grafico]. Impacto de los incidentes de seguridad digital en Colombia 2017. Colombia. MINTIC. 2017. [Consultado: 12 de mayo de 2019]. Disponible en: http://dx.doi.org/10.18235/0000843

[48] SEMANA. Tecnología. Las empresas en Colombia no invierten en seguridad digital. https://www.semana.com/tecnologia/articulo/colombia-no-invierte-en-seguridad-digital/492724

[49] BID. Impacto de los incidentes de seguridad digital en Colombia 2017. https://publications.iadb.org/es/publicacion/17294/impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017

7.1 ORGANIZACIÓN TECNOLÓGICA EN LAS ENTIDADES DEL ESTADO PARA LA SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN

Si bien es importante que la alta dirección apoye de manera activa la seguridad digital en las entidades, este compromiso debe ser demostrado en todos los niveles definiendo responsabilidades y roles que garanticen dentro de las entidades y organizaciones la planeación y la implementación de técnicas de protección para mitigar los riesgos y amenazas en cuestión de ciberseguridad. Estas deben darse desde los procesos misionales o los procesos que sean el núcleo de las instituciones.

A continuación se consideran algunas ilustraciones de como a partir de las directrices de estándares y arquitectura de TI dadas por el Ministerio de Tecnologías de la Información y las Comunicaciones, las entidades públicas al trascurso de los últimos años han dado cumplimiento en la implementación de estrategias acordes a las buenas prácticas de seguridad de la información. El Modelo de Seguridad y Privacidad de la Información (MSPI) publicado por MINTIC, se encuentra enfilado con el marco de referencia de arquitectura TI y sustenta los otros componentes de la estrategia GEL: TIC para servicios, TIC para gobierno abierto y TIC para gestión.

El modelo MSPI está permanentemente actualizado reuniendo los cambios técnicos de la norma 27001:2013, la normatividad de la ley de protección de datos personales, transparencia y acceso a la información pública, las cuales se deben tener en cuenta para la gestión de la información. De igual forma este modelo cuenta con una colección de guías que apoyan a las entidades a ejecutar lo solicitado en cada una de las fases del modelo, buscando los resultados y como desplegarlos. La implementación del MSPI en las entidades está definido por las necesidades de objetivos, requisitos de seguridad, procesos, tamaño y estructura, con el objetivo de conservar triada de la seguridad confidencialidad, integridad y disponibilidad, garantizando el buen uso y privacidad de la información.

El Instrumento de Evaluación MSPI es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente “Seguridad y Privacidad de la Información”. Fue creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con uso libre.[50]

[50] MINTIC. Modelo de seguridad. https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

7.1.1 Mecanismos de seguridad de los servicios informáticos del Banco de la Republica. Buscan garantizar la seguridad informática de los sistemas de información del banco, este modelo de seguridad está conformado por políticas, estándares, procedimientos y mecanismos de seguridad, basados en los siguientes fundamentos:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación
- Autorización
- No repudiación
- Observancia

Los mecanismos de seguridad informática en correspondencia con los anteriores fundamentos, buscan garantizar el aseguramiento digital de modo que en el momento de ejecutar alguno de los mecanismos este soportando un fundamento. A continuación se muestra como están implementadas estas tecnologías y su impacto frente a los servicios informáticos que presta el banco:[51]

- Políticas, estándares y procedimientos: Están diseñados, implementados y divulgados de forma clara, para que la infraestructura de seguridad se ejecute firmemente frente al modelo de seguridad. Algunos controles al no ser automatizados son de tipo procedimental para lo cual se siguen políticas y estándares particulares a ellos.
- Plan de continuidad de negocio: Este pretende garantizar las operaciones de la entidad, sorteando los eventos o desastres fortuitos que puedan presentarse. Aquí definen las responsabilidades, alertas, acciones, recuperación, y puesta en marcha a la normalidad de los servicios logrando la disponibilidad en tiempos y momentos requeridos.
- Procedimientos de contingencia y backup: Frente a eventos adversos, la entidad cuenta con un plan que permite actuar y ejecutar de forma adecuada y oportuna en el momento que se atente con el buen rendimiento de los servicios. En este punto es muy importante la participación de los usuarios en el cumplimiento de las acciones dispuestas en el plan de contingencia con el fin que se pueda garantizar la disponibilidad de servicios y poder monitorear las máquinas y no tener una sobrecarga en ellas. El manejo de backups contiene unas políticas y estándares solidos debido a que es un procedimiento demasiado sensible para la entidad.
- Alta disponibilidad y tolerancia a fallas: se cuentan con equipos de tolerancia a fallas y alta disponibilidad por la necesidad de sostener los servicios y aplicaciones críticas en operación, permitiendo mantener la

[51] BANCO DE LA REPUBLICA. Mecanismos de seguridad de los servicios informáticos. https://www.banrep.gov.co/sites/default/files/paginas/Mecanismos_de_Seguridad_Informatica.pdf 2007

disponibilidad para que los servicios se puedan ofrecer de manera adecuada, buscando que el impacto frente a la operación sea mínimo.

- Contraseñas: estas deben ser de uso exclusivo para cada persona en particular, y su buena utilización así como el cumplimiento de las políticas aplicadas a estas, significan el desempeño de la autenticación en los servicios.
- Sistemas de autenticación (Tarjetas o biométricos): estos mecanismos exigen a las personas presentar un elemento ya sea que este en su poder o que lo caracteriza en su cuerpo, permitiéndole autenticarse de forma más segura en su identidad, mitigando de esta manera una posibilidad de suplantación frente al sistema.
- Códigos de autenticación: son números que de forma aleatoria identifican de manera única un individuo o entidad. Estos se encuentran en un sobreflex que se entrega a la entidad o individuo que se vaya a autenticar con el banco, de manera que el poseedor del sobreflex puede seleccionar secuencialmente uno de los códigos, se envía hacia el banco y mediante un software GAC valida a que entidad pertenece.
- Políticas de acceso: Luego de ejecutar la autenticación de un individuo y comprobar que está dentro del sistema, se determina a que tiene derecho a acceder y que procesos puede ejecutar, de forma que a través de perfiles de acceso se define cual es el comportamiento que cada persona puede tener en el sistema.
- ACL o Listas de control de acceso: estas tablas dan informe de cuales usuarios pueden ingresar al sistema y a que derechos de acceso tienen estos. Este mecanismo está provisto en el servidor web del banco dando restricción en el acceso a un sitio web. Estas ACL tienen asociada una clave (contraseña encriptada) a cada carga (usuario), permitiendo que para ingresar al sistema protegido por una ACL se introduzcan las credenciales, si están pertenecen a la ACL y la clave pertenece a la carga, el usuario puede acceder a los servicios.
- Cifras de control: este mecanismo hace referencia a números que se calculan a través de algoritmos denominados HASH, recurriendo la información que se procura proteger, relacionando el número de forma única con esta información, de manera que al modificarse la información, la cifra de control ya no es válida.
- Encripción simétrica y asimétrica: brinda confidencialidad a la información a través de algoritmos matemáticos y datos especiales, que solo el individuo que los conozca podrá tener acceso a la información. En la parte de simétrica la clave debe ser conocida por el individuo que encripto como por el que requiere desencriptar, para lo cual debe existir una manera confiable que ambos tengan la clave habiendo un riesgo de vulnerabilidad. En la parte asimétrica se tienen mecanismos de clave pública y privada, de manera que se encripta con la clave privada (dueño de la información) y se desencripta con la clave pública.

- Llaves públicas y privadas: Cada participante posee estas dos llaves, la pública que se dará a conocer y la privada que no se compartirá. Este mecanismo será utilizado en los siguientes eventos: El primer evento para encriptar información con la llave publica y se pueda desencriptar con la privada que le corresponda. El segundo evento se utiliza para la firma de información, donde el individuo firma con la llave privada y el receptor puede verificar quien lo firmo con la llave pública, garantizando con este mecanismo los fundamentos de autenticación, confidencialidad, integridad y no repudiación.
- Firmas digitales: este mecanismo permite garantizar la procedencia de la información con el uso de las llaves públicas y privadas, el individuo emplea su llave privada para realizar la firma de la información y el que recibe utiliza la llave pública para verificar quien firmo la información.
- Certificados digitales: el uso de estos certificados se asemeja al uso de una tarjeta de crédito electrónica, en cuanto busca establecer la identidad cuando se realiza alguna transacción web y que es validada por una autoridad de certificación (CA). El certificado digital como mecanismo de seguridad contiene los siguientes elementos: una serie, fecha de expiración, llave pública y firma digital de la entidad emisora del certificado.
- Infraestructura de llaves públicas (PKI): esta tecnología de seguridad (Public Key Infraestructure) es la base para garantizar la seguridad en el manejo de la información electrónica que tiene gran alcance en servicios de técnicas y conceptos de llaves públicas, buscando brindar interoperatividad entre sistemas, seguridad en las operaciones electrónicas, desarrollo de mecanismos de comercio electrónico y la administración de llaves, su registro, su revocación, llaves históricas, almacenamiento, control, auditorias, entre otros.
- Secure Socket Layer (SSL): este protocolo se utiliza como mecanismo de seguridad en la transmisión de mensajes vía HTTP. SSL coloca una capa adicional entre las capas HTTP y la IP, garantizando fundamentos de seguridad punto a punto: Autenticación (cliente - servidor), confidencialidad, integridad y autenticación. Avala la identidad de la persona que solicita la información, dando la certeza en una de las partes que la persona es quien dice ser.
- Firewalls: esta barrera de protección filtra el acceso a los servidores privados a través de reglas que habilitan o prohíben el ingreso de un punto a otro, garantizando los fundamentos de autenticación y autorización.
- Antivirus: este mecanismo de seguridad es el software que controla la presencia de programas maliciosos en los sistemas, detección de intrusiones, y controlan tanto la parte de servidores como las estaciones de trabajo del banco.
- Monitoreo, Sistemas de detección de intrusos y de vulnerabilidades: son herramientas que permiten realizar tareas orientadas a obtener datos e información con relación a posibles intrusos que puedan atacar un sistema de igual forma la forma en cómo podrían realizarlo, identificando las

vulnerabilidades a fin de controlarlas y corregirlas. Este mecanismo de seguridad permite la proactividad en cuanto al control de todos los fundamentos de seguridad informática debido a que las vulnerabilidades y los atacantes que se detecten para referirse a cualquiera de ellos.

- Atención de incidentes: este esquema busca garantizar la actuación en forma adecuada al momento de presentarse un incidente contra cualquiera de los fundamentos de seguridad, en casos como fallas de equipos y servicios, así como para eventos que se presenten y atenten la seguridad informática del banco.
- Análisis de riesgos e impactos: mediante este mecanismo se pretende identificar y analizar los riesgos y amenazas latentes de los sistemas y servicios y los respectivos impactos que tengan sobre estos. La importancia de realizar este tipo de análisis para tener prevención en la aplicación de controles y no esperar a que ocurra algún tipo de incidente para actuar.

Estos mecanismos de seguridad implementados por el Banco de la Republica, han permitido ofrecer sus servicios de manera segura, y buscando en la tecnología de seguridad de la información un adecuado soporte no solo para funcionarios sino para sus clientes. Para el banco es importante que los clientes sepan que estas medidas de seguridad le proveen la confianza requerida en sus operaciones así como en el cuidado de sus productos, de esta forma encaminan los esfuerzos en la mitigación de riesgos de eventuales fallas técnicas, de posibles fraudes, de potenciales ataques informáticos que no solo pondrían en riesgo la seguridad de la información propia del banco sino también el manejo que tienen sobre la información y activos puestos en custodia de los clientes.

7.1.2 Protocolos de seguridad informática de la Alcaldía Municipal de Fusagasugá. La Alcaldía del municipio de Fusagasugá es una entidad gubernamental del orden territorial la cual está regida por la legislación y normatividad del estado Colombiano y de acuerdo con su Sistema de Gestión de Calidad se encuentra enrolado con los requisitos del MSPI y el manual de gobierno en línea. Luego de la verificación e identificación de riesgos se realizó la definición de protocolos que definen y reglamentan las políticas de seguridad de la información en los diferentes ámbitos de la Alcaldía. A continuación se relacionan algunos de los protocolos con los cuales se da tratamiento a los posibles riesgos y amenazas en materia de seguridad de la información:[52]

- Generales: todos los funcionarios y usuarios deben adoptar las medidas de control establecidas así como los ordenamientos legislativos aplicables para la protección de la información. La infraestructura tecnológica y la

[52] PULIDO BARRETO, Ana Milena. MANTILLA RODRIGUEZ, Jenith Marsella. Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina tic de la alcaldía municipal de Fusagasugá, basados en la gestión el riesgo informático. http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/6327/1/35250 2016

información de la Alcaldía son de su propiedad por lo cual no se puede copiar, duplicar, transmitir o divulgar. Los usuarios y contraseñas asignados son personales, intransferibles y confidenciales, y es único para cada usuario. La infraestructura de sistemas, aplicaciones y recursos deben ser utilizados para fines propios de la Alcaldía y no para provecho personal. No es permitido el uso de programas o herramientas de mensajería para el envío y recepción de información confidencial. Se debe realizar el bloqueo de la terminal de trabajo cuando se ausente, para los casos de inactividad se bloquearan después de 5 minutos automáticamente. No está permitido el compartir carpetas de los equipos de la entidad.

- Aplicaciones: aquellas que contengan componentes de seguridad como claves de acceso, autenticaciones, PIN, entre otros, deben ser avaladas por la oficina TIC. Los funcionarios no deben realizar modificaciones a las configuraciones generales de las aplicaciones o a los sistemas operativos, en especial a las configuraciones específicas de seguridad.
- Manejo de claves: debe contener 8 caracteres alfanuméricos y diferentes a la utilizada durante los últimos 3 meses. La vigencia de la contraseña es de 30 días calendario, transcurrido ese tiempo el sistema obliga a su respectivo cambio. La oficina de TIC realizara el respectivo bloqueo en los casos especiales de licencias, incapacidades, vacaciones, permisos, entre otros.
- Segmentación de redes: La Alcaldía realiza la segmentación lógica y física de los servidores (Capa presentación) y estos se protegen en una DMZ que se encuentra resguardada por el firewall. Con relación a los servidores de aplicaciones, la comunicación entre estos segmentos se realizaran por protocolos seguros HTTPS con certificado digital. Para el servidor de bases de datos de la Alcaldía, estará ubicado en un sitio distinto al del servidor de la aplicación, habilitando la comunicación únicamente entre ellos.
- Servidores para prestar el servicio: se tienen las reglas de acceso detalladas de acuerdo al servicio al que se pretende ingresar, así como el cumplimiento de las políticas de DMZ en los procedimientos establecidos.
- Hardware: la pérdida o daño de los equipos de la Alcaldía debe ser reportada al área encargada y su reparación debe estar a cargo por el personal o funcionarios de la Alcaldía, no está autorizado el personal ajeno a la entidad. El software y hardware que adquiera la Alcaldía debe ser adquirido en canales de compra confiables y deberá contar con su respectivo contrato de mantenimiento.
- Acceso lógico y físico: los equipos multiusuario y de comunicaciones son ubicados en lugares seguros mitigando alteraciones o usos no autorizados. Se establece una autenticación de múltiple factor. El acceso a los recursos y sus permisos se realiza de acuerdo a la asignación de los usuarios y sus funciones dentro del sistema.
- Respaldo y continuidad del negocio: se realiza respaldo a través de diferentes fuentes de energía (UPS, filtros eléctricos) que puedan mantener la disponibilidad de la información de los diferentes servidores de la

Alcaldía. Se tiene un programa de mantenimientos preventivos mitigando los riesgos de fallas y baja probabilidad de ocurrencia. El plan de contingencia y recuperación de debe probar y documentar regularmente.

- Parches de seguridad: las estaciones de trabajo, aplicativos y servidores tendrán que estar actualizadas con el ultimo nivel de parches tanto de sistema operativo como del producto.
- Tratamiento de documentación impresa: esta no podrá ser accesible por personal no autorizado, se debe evitar la mala práctica de dejar documentos sin recoger en las impresoras y/o fotocopiadoras, de igual forma en los lugares de paso o de atención al usuario.
- Control de la información: los funcionarios que utilicen recursos de los sistemas de la Alcaldía, deber preservar la confidencialidad, integridad, disponibilidad de la información que maneje en especial si es información clasificada como crítica.
- Escritorio limpio: los funcionarios de la Alcaldía mantienen la política de escritorio limpio buscando prevenir el acceso no autorizado a los activos de información de los equipos desatendidos, así como los soportes documentales físicos que se encuentren disponibles deberán estar bajo llave.
- Activación y actualización de programas antivirus: se tienen instalados en todas las terminales y los funcionarios no deben interferir en la actualización de estos.
- Seguridad del centro de datos, de cableado y cuartos de equipos tecnológicos: está restringido el acceso a personal no autorizado y se debe mantener una planilla de registro al iniciar y finalizar cualquier actividad. Se debe contar con ingreso de dispositivos electrónicos y accesos biométricos.

Los anteriores son algunos de los protocolos de seguridad adoptados por la Alcaldía municipal de Fusagasugá que ayudan con la gestión del riesgo y amenazas informáticas generando medidas de respuesta que puedan permitir una nueva valoración del riesgo, evaluándolos y reclasificándolos buscando mitigar al máximo la ocurrencia de incidentes de seguridad frente a los riesgos detectados.

7.1.3 Manual de seguridad informática – Contaduría General de la Nación. Esta entidad incorpora una gestión segura y brinda un ambiente óptimo para la operación de los activos informáticos y la infraestructura tecnológica que da soporte a los procesos misionales preservando los fundamentos de confidencialidad, integridad y disponibilidad. La Contaduría General de la Nación (CGN) se apega hacia el cumplimiento de la normatividad y las directrices dadas por el gobierno nacional en cuanto a la seguridad de la información, la protección de datos, el buen nombre de la CGN y de las organizaciones con las que pueda tener vínculos, empleando metodologías de evaluación y tratamiento de riesgos y amenazas de acuerdo a las necesidades de la entidad.

El en manual de seguridad informática de la CGN se pretende dar una administración hacia la protección de activos informáticos, la implementación del SGSI y al soporte en cuanto a la concepción e implementación de las políticas, procedimientos e instructivos. A continuación se muestran algunos aspectos tenidos en cuenta por la CGN para aseguramiento informático como entidad gubernamental dando cumplimiento con los lineamientos que el estado a través de sus entidades ha dispuesto para propender con un ambiente óptimo de seguridad de la información:[53]

- Activos de información: están catalogados en activos físicos (Infraestructura de TI, Controles de entorno TI, Hardware de TI, Documentación), activos de servicios TI (administración de usuarios, aplicaciones, firewall, servidores, servicios de red, servicios web, antivirus, bases de datos, entre otros) activos humanos (empleados, personal externo).
- Acceso a los recursos de información: custodia y cuidado de la información, vigilancia y salvaguardar los recursos que les han sido encomendados, el acceso a los servicios de red debe ser autorizado por el jefe inmediato, el acceso y uso de la información debe ser exclusiva a funciones propias de la entidad, los modem, cable-modem no están permitidos a excepción de una política de firewall y uso de VPNs, en cuanto a la terminación laboral con la CGN se deben retirar los derechos de acceso y de igual forma la devolución de los activos al personal autorizado.
- Uso de los recursos de información: los bienes y recursos entregados deben ser utilizados únicamente para el desempeño de las funciones de cada empleado así como la información reservada a la que tenga acceso. Los sistemas de información a los que tenga acceso se deben utilizar con los propósitos de la entidad y no para otros fines. No se permite la instalación y uso de aplicativos ajenos a la CGN. Solo el personal autorizado puede realizar las tareas de instalación y cambios en el software y hardware de los equipos de la entidad. Todos los cambios que se realicen en la infraestructura debe ceñirse a la política de seguridad de la entidad. Se deben realizar análisis de riesgos a todo software y hardware que llegue a la entidad. No está permitida la navegación a sitios web de uso social así como el uso de emisoras de radio por internet, ni la descarga de audio y/o video debido al incremento del uso de ancho de banda.
- Uso del correo electrónico: este es el medio oficial de comunicación de la entidad. Los correos electrónicos deben tener configurada su firma con el estándar de la entidad. La conexión al correo y su uso debe ser para

[53] CONTADURIA GENERAL DE LA NACION. Manual de seguridad de la Información. http://www.contaduria.gov.co/documents/20127/35873/MANUAL%2BDE%2BSEGURIDAD%2BDE%2BLA%2BINFORMACI%C3%93N-%2BMAYO%2B31%2B2019.pdf/cf9d72ad-ad76-cdff-afdb-a1a6459360f4?t=1565109226933 2019

propósito oficial de la entidad y no para fines propios. Debe ser de uso personal e intransferible. El contenido de los mensajes se considera confidencial y solo perderá ese carácter en las investigaciones oficiales o incidentes de seguridad informática que requieran de esta información.

- Administración de contraseñas: se tienen unos parámetros de construcción de contraseñas con las cuales se brindara la seguridad pertinente al acceso a la red o al aplicativo que se requiera, entre estos se encuentran que debe tener al menos 8 caracteres, no contener información como nombres de familia, mascotas, ciudades, solo números, o palabras de diccionario, se debe incluir caracteres alfanuméricos mezclados con mayúsculas y minúsculas.
- Protección de contraseñas: estas son de uso personal e intransferible y solo para acceso de miembros o empleados de la CGN, cada usuario es responsable del uso y custodia de su contraseña.
- Criptografía y llaves criptográficas: las llaves deben ser cambiadas por lo menos cada año o en sospecha de perdida de confidencialidad, los certificados SSL se deben cambiar entre un periodo de 1 a 2 años. La administración tanto de llaves como de certificados digitales la realiza la oficina de TIC.
- Áreas seguras: se cuenta con vigilancia privada en la entrada y salida de las instalaciones quien llevara el control de los elementos que salgan o ingresen. Sistema cerrado de monitoreo (cámaras).
- Ubicación y protección de equipos: el datacenter de la entidad está ubicado de forma que el personal que no esté autorizado no pueda ver la información durante su uso. De igual forma el ingreso a esta ubicación se controla con acceso biométrico.
- Servicios de suministro: la CGN cuenta con suministro constante de energía UPS asegurando que ante alguna falla se cuenta con el tiempo necesario de funcionamiento para los servidores. La instalación también cuenta con una planta eléctrica.
- Control de virus: el sistema de antivirus debe estar instalado en cada una de las terminales de trabajo y en los servidores, por tanto los usuarios no deben manipular ni desactivar esta funcionalidad. Cada funcionario debe hacer uso del software para verificar la presencia de virus en la información y medios que utilice (internet, memorias, carpetas, entre otros). Los sistemas que se detecten o se sospeche que han sido comprometidos con virus o software malicioso debe ser apagado y desconectado de la red inmediatamente.
- Seguridad en los equipos móviles: los equipos de cómputo móviles de la entidad que se utilicen dentro o fuera de ella, no se deben utilizar para fines personales ni el en hogar. Durante los traslados y viajes los computadores no se deben dejar desatendidos en lugares públicos y deben llevarse como equipaje de mano. Al ser equipos susceptibles a robo, se deben tener las medidas correspondientes como contraseñas de encendido, encriptación, con el fin de proveer seguridad y prevenir el

acceso no autorizado. Los equipos que contengan algún tipo de información sensible no podrán ser prestados a ninguna otra persona y su uso será exclusivo del funcionario que lo tenga asignado.

- Confidencialidad de la información: el sistema de clasificación de la información está definido en tres grupos (publica, publica clasificada, publica reservada), para el caso que la información no sea pública no puede ser entrega a ninguna entidad externa sin un acuerdo de confidencialidad. Se debe dar aviso al encargado de la seguridad de la información en caso que esta sea revelada o extraviada.
- Gestión de incidentes de seguridad de la información: todos los reportes y evaluación de los eventos de seguridad son reportados al encargado de la seguridad de la información, en los incidentes pueden estar incluidos fallas en el sistema, perdida de servicio, errores, pérdida de confidencialidad.
- Pantalla despejada y escritorio limpio: Los funcionarios de la CGN deberán bloquear sus equipos cuando se retiren del mismo, de igual forma, por política del directorio activo se bloqueara el equipo después de cinco minutos de inactividad y solo se podrá desbloquear con la contraseña del usuario. Después de la jornada laboral se deberán apagar o hibernar los equipos. Toda información pública clasificada y pública reservada debe permanecer bajo llave y si está en el equipo no deberá estar en el escritorio.
- Respaldo de datos: se realizan copias de respaldo y las pruebas de estas ceñido al procedimiento para tal fin. De igual forma se hace el seguimiento a la ejecución de las copias de respaldo y en caso de fallas para certificar la validez y su correcto funcionamiento. El procedimiento de copias de respaldo tiene como objetivos poder restaurar información por borrado, incidentes de seguridad, defectos en discos de almacenamiento y del mismo modo para la recuperación de desastres.
- Control de acceso: los sistemas de información de la CGN deben tener usuario y contraseña para ingresar y se permite hasta tres intentos de fallidos. El usuario o contraseña son únicos e intransferibles para cada funcionario y solo se permite un inicio de sesión es decir que no se permiten las sesiones simultaneas con el mismo usuario. Los casos de vacaciones, incapacidades, permisos, entre otros, se realizara la deshabilitación del usuario. Cada usuario solo tendrá acceso y permisos para el desarrollo de sus funciones y de acuerdo a la autorización otorgada. Para los casos de teletrabajo se deberá solicitar acceso a través de VPNs que solo son autorizadas y creadas en la oficina de TIC.
- Transferencia de información: esta deberá realizarse salvaguardando la confidencialidad e integridad de los datos con relación a la clasificación de la misma. Para el caso de requerir información clasificada y reservada se debe hacer uso y firma de actas de confidencialidad. Se deben utilizar mecanismos criptográficos para garantizar los fundamentos de confidencialidad, integridad y disponibilidad durante su transferencia.

- Gestión de la vulnerabilidad técnica: se realizar por lo menos una vez al año un plan de análisis de vulnerabilidades para las plataformas de la entidad y de esta manera realizar los correctivos a los que haya lugar en cuanto a la identificación de vulnerabilidades.
- Notificación de incidentes de seguridad de la información: cualquier incidente se debe notificar al proceso de gestión TIC para poder resolver el inconveniente, buscando reducir riesgos de seguridad protegiendo las personas así como la entidad. Se deben notificar situaciones como personas ajenas a la CGN, correos maliciosos, equipos infectados, mala utilización de recursos, uso ilegal del software, alteración de información, entre otros.

De esta forma la CGN busca dar cumplimiento al aseguramiento informático y su impacto se traduce en minimizar el riesgo en las funciones importantes de la entidad, cumplir con los principios de seguridad de la información, conservar la confianza en los funcionarios, soportarse en la innovación tecnológica, salvaguardar los activos tecnológicos, robustecer la cultura de la seguridad de la información, garantizar la continuidad del negocio frente a incidentes de seguridad informáticos.

7.1.4 Política General de Seguridad de la Información – Contraloría de Bogotá D.C. Dentro del objetivo principal del Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI - de la Contraloría de Bogotá D.C. esta la definición de las estrategias, actividades, proyectos e iniciativas de tecnología que la entidad requiere para el cumplimiento del Plan Estratégico Institucional. Entre ellos esta continuar con la implementación de la Política de Gobierno Digital divulgada por el Gobierno Nacional y la Alta Consejería Distrital de TIC, gestionar y administrar de manera eficiente la infraestructura tecnológica con el propósito de soportar y apoyar las exigencias y necesidades de los procesos de la entidad para su cumplimiento de las metas institucionales. La Contraloría de Bogotá D.C. reconoce la importancia de la protección de los activos de información que soportan los procesos de la entidad por esta razón está en el compromiso de la implementación de medidas para salvaguardar su confidencialidad, integridad, disponibilidad y privacidad con relación a la normatividad vigente, por lo cual acoge políticas, procedimientos y lineamientos para la gestión de la seguridad digital:

- Organización de la seguridad de la información: se definen roles y responsabilidades en los cuales se segregaran las funciones y las áreas de responsabilidad para prevención de conflictos de intereses que puedan llevar a oportunidades de modificaciones no autorizadas o el uso no adecuado de los activos de la información. Se tiene el comité SIGEL (Comité Técnico de Seguridad de la Información y Gobierno en Línea) el cual establece políticas para garantizar la seguridad y la integridad de la

información, la implementación de la estrategia de gobierno en línea de acuerdo a los lineamientos nacionales y distritales para la coordinación del proceso de gestión documental. La dirección de TIC establece las responsabilidades de operación y administración de los sistemas de información de la entidad. La entidad establece acuerdos de cooperación de seguridad de la información con entidades de seguridad del estado.

- Gestión de activos: esta política establece los lineamientos en relación a la identificación, clasificación, uso, administración y responsabilidad frente a los activos de información. De igual forma la metodología para la identificación, clasificación y etiquetado de los activos. Se mantendrá el inventario actualizado. Cada activo de información deberá tener asignado un propietario que estará al tanto de su correcta instalación.
- Devolución de activos: los usuarios deberá realizar la devolución de todos los activos de información físicos y/o electrónicos asignados por la entidad en sus procesos de desvinculación de la Contraloría.
- Gestión de medios removibles: estos deberán ser supervisados, tendrán acceso y uso restringido en la entidad.
- Dispositivos móviles: se establecen lineamientos para el acceso de dispositivos móviles a redes inalámbricas, así como las responsabilidades que deben tener los usuarios frente al uso de la información almacenada en ellos. Deben tener contraseña de ingreso, bloqueo de equipo manual y/o automático y función de borrado remoto. Deben permanecer encendido y cargado en las horas laborales.
- Control de acceso: se tienen medidas de control en los niveles de sistema operativo, red, sistemas de información y demás servicios TI y se delimitan de acuerdo a las funciones y cargos que desempeñen los usuarios. La gestión de usuarios y accesos a la información en todos los niveles contemplando la restricción y control de accesos privilegiados a la información.
- Criptografía: la información transmitida o almacenada será cifrada de acuerdo a la criticidad de la misma, las cuales incluyen llaves criptográficas y servicios que se implementan con medidas de seguridad que apliquen a los controles criptográficos.
- Seguridad física y del ambiente: se identifican las áreas que almacenen, manejen o generen información sensible a las cuales se les establecen perímetros de seguridad que permitan controlar el acceso a personal no autorizado. Los lineamientos de trabajo en áreas seguras deben incluir controles de punto de acceso a estas.
- Políticas de escritorio: la información física, magnética que contenga información pública reservada, pública clasificada, confidencial o sensible de la entidad debe guardarse en un lugar seguro cuando el funcionario se ausente de su lugar de trabajo. Se debe conservar el escritorio del equipo libre de información que pueda ser alcanzada, copiada o utilizada por personal ajeno a ella.

- Pantalla limpia: los equipos de la entidad deben tener aplicado protector de pantalla que se activara durante el tiempo de inactividad. Solo se podrá desbloquear con el usuario y contraseña del usuario. Los usuarios deben bloquear los equipos cuando se retiren de su puesto de trabajo.
- Seguridad de las comunicaciones: los mecanismos de protección de la información en las redes de datos aseguran su disponibilidad con una adecuada gestión de seguridad y control de tráfico. Estos mecanismos deben asegurar el control y gestión de red de datos, servicios de red, segregación de tráfico, de usuarios y sistemas de información.
- Gestión de incidentes de seguridad de la información: este procedimiento permite evaluar y decidir los eventos de seguridad correspondientes a incidentes, asegurando una respuesta rápida frente a los incidentes detectados.
- Gestión de la información de la continuidad del negocio: se debe restablecer las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante los eventos catastróficos y se deben mantener los sistemas de comunicación adecuados.
- Privacidad de la información: la protección de la información personal de usuarios y ciudadanos se mantendrá con acuerdos de confidencialidad, aceptando el registro y tratamiento de la información, así como la confidencialidad de la información que por la funciones de su cargo llegase a conocer.

Estas políticas de seguridad de la información, establecen parte del cumplimiento de los controles instaurados en el sistema de gestión de seguridad de la información con los que la Contraloría de Bogotá D.C. busca proteger la información. Estas medidas se complementan con aseguramiento en la protección perimetral, firewall de nueva generación, sistema de antivirus y procedimientos de respaldo de información, con los cuales se realiza el backup de la información y los sistemas de información de la entidad, los cuales soportan y pueden restaurar la información así como permiten la recuperación en el plan de continuidad del negocio de la entidad.

7.2 IDENTIFICACION DEL MEJOR MODELO FRENTE A LOS USOS, TIPOS DE TECNOLOGIAS Y LOS BENEFICIOS BRINDADOS EN CUANTO A LA MITIGACION DE AMENAZAS CIBERNETICAS

Es importante resaltar que luego de determinar los usos y tipos de tecnologías de seguridad informática en algunas entidades gubernamentales del orden nacional y territorial, es significativo que la instauración de las diferentes políticas, procesos, procedimientos, protocolos, entre otros, están dirigidos hacia la protección y seguridad de la información de cada entidad, sin embargo cabe destacar que de

acuerdo a la misionalidad de las entidades consultadas, de esa misma forma están orientados los mecanismos y controles implementados, es decir, por ejemplo los mecanismos del Banco de la Republica también están alineados no solo a los funcionarios y colaboradores, sino también hacia sus clientes usuarios externos buscando dar protección y seguridad a los datos en las transacciones que realizan, evitando que haya algún tipo de suplantación y más adelante el robo no solo de las inversiones que se tengan en el banco sino de los datos personales con los que puedan afectar en otras instancias y plataformas.

Del conjunto de controles adoptados por las entidades consultadas, y que para cada una de ellas han servido de fundamento, guía y claramente para la protección y seguridad de la información, buscando siempre la confidencialidad, integridad y disponibilidad, se puede establecer un modelo que cumpla con los parámetros y beneficios en el que cualquier entidad gubernamental pueda dar el paso inicial para realizar una evaluación de cómo se encuentra y hacia dónde quiere llegar en términos de seguridad de información y protegiéndose de posibles riesgos y/o amenazas cibernéticas. La siguiente es una recopilación de mecanismos, controles y demás parámetros encontrados en las que las entidades analizadas, los cuales tuvieron más reiteración en la implementación que se tiene actualmente, de igual forma se incluyen otros que por su complejidad son de gran utilidad para los componentes de seguridad y privacidad de la información:

- Políticas, estándares y procedimientos: alineadas a la implementación y ejecución del SGSI.
- Organización de las seguridad de la información: roles y responsabilidades.
- Gestión de activos: aprobados por cada entidad incluyendo físicos, servicios TI y recurso humano que los administre.
- Controles de acceso: accesos físicos, lógicos, uso de biométricos, así como el acceso a los recursos
- Gestión de usuarios y contraseñas: incluye políticas de autenticación, bloqueos.
- Alta disponibilidad: tolerancia a fallos, servidores, reglas de acceso y DMZ.
- Seguridad de las comunicaciones: segmentación de redes, SSL transmisión segura, transferencias seguras de información.
- Encriptación: Criptografía, llaves de acceso públicas – privadas.
- Seguridad física y del ambiente: ubicación y protección de equipos, áreas seguras.
- Respaldo de la información: contingencia, respaldo de datos.
- Continuidad del negocio: gestión de la información y sistemas críticos, plan de continuidad del negocio.
- Antivirus: control de virus, programas de antivirus.
- Firewall: aseguramiento perimetral, VPN, restricciones de acceso lógico.
- Monitoreo: IDS, gestión de vulnerabilidades, parches de seguridad, análisis de riesgo e impactos.

- Firmas digitales: firmas y certificados digitales.
- Dispositivos móviles: seguridad en equipos móviles.
- Políticas de escritorio: pantalla y escritorio limpio.
- Gestión de incidentes: notificación, atención y gestión de incidentes de seguridad.
- Control de la información: confidencialidad, privacidad de la información. Tratamiento documental, información impresa.
- Usos de sistemas de información y aplicativos: correo electrónico, software propio o contratado.
- Servicios de suministro: Centros de datos, cableado, cuartos de equipos, UPS.
- Gestión de medios removibles: discos extraíbles, USB.

Lo anterior, teniendo en cuenta la revisión realizada y de acuerdo a lo implementado en las entidades públicas analizadas, son los aspectos que más se tuvieron en cuenta en cada una de ellas para la conservación y protección de la información.

Adicionalmente y de acuerdo a la implementación del sistema de gestión de seguridad de la información, es importante tener en cuenta que dentro de la norma ISO 27001 se encuentra el anexo A, en el que se encuentran relacionados los controles a implementar y que son de obligatoriedad su cumplimiento para la certificación del SGSI. En el anexo A se encuentran un total de 114 controles de seguridad, los cuales la entidad debe seleccionar cuales aplican a su necesidad, estos no solo se designan al área TI, sino que incluso se involucra otras áreas como recurso humano, financiero, entre otros. Estos 114 controles se fraccionan a su vez en 14 dominios que son los siguientes:

- Políticas de seguridad de la información.
- Organización de la seguridad de la información.
- Seguridad de los recursos humanos.
- Gestión de Activos.
- Controles de acceso.
- Criptografía – Cifrado y gestión de claves.
- Seguridad física y ambiental.
- Seguridad operacional.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento del sistema.
- Gestión de incidentes de seguridad de la información.
- Cumplimiento.

8. RECOMENDACIONES SOBRE LA IMPORTANCIA DE LA IMPLEMENTACION DE UN SISTEMA DE ASEGURAMIENTO INFORMATICO

En el panorama nacional e internacional ninguna entidad está exonerada de un ataque cibernético. Desde grandes empresas como Telefónica, Yahoo! y Renault pasando por pymes locales, empresas privadas y entidades públicas, han estado como víctimas alrededor del mundo en las manos de ciberdelincuentes, que las ha pasado a desperdiciar no únicamente altas cifras económicas, sino uno de los activos más significativos de una organización: la información. De acuerdo a un informe realizado en el año 2016 por la firma Kroll, el 82% de los empresarios alrededor del mundo informo haber tolerado algún tipo de estafa informática durante el 2016, un 75% más que en el año 2015, , que destacó también que los primordiales delincuentes informáticos son funcionarios existentes y ex funcionarios.

Por este motivo, los fines para resguardarse frente a un potencial ataque van más allá de tener un sistema de antivirus en los equipos. Actualmente, contienen estrategias como cifrado de las comunicaciones, políticas de seguridad completas y protección de los equipos móviles. Poder sobresalir del deterioro de un ciberataque lleva tiempo, posee un impacto en la imagen organizacional y causa poderosas pérdidas, a lo cual se presentan algunas recomendaciones con medidas imprescindibles para mitigar estas amenazas y riesgos que pueden alcanzar a ser irremediables.[54]

- Modelo de Seguridad y Privacidad de la Información (MSPI)

El Modelo de Seguridad y Privacidad de la Información (MSPI) publicado por MINTIC, se encuentra enfilado con el marco de referencia de arquitectura TI y sustenta los otros componentes de la estrategia GEL: TIC para servicios, TIC para gobierno abierto y TIC para gestión.

El modelo MSPI está permanentemente actualizado reuniendo los cambios técnicos de la norma 27001:2013, la normatividad de la ley de protección de datos personales, transparencia y acceso a la información pública, las cuales se deben tener en cuenta para la gestión de la información. De igual forma este modelo cuenta con una colección de guías que apoyan a las entidades a ejecutar lo solicitado en cada una de las fases del modelo, buscando los resultados y como desplegarlos. La implementación del MSPI en las entidades está definido por las necesidades de objetivos, requisitos de seguridad, procesos, tamaño y estructura,

[54] PORTAFOLIO, Innovación. Siete consejos para proteger los sistemas informáticos de su compañía. https://www.portafolio.co/innovacion/siete-recomendaciones-para-proteger-los-sistemas-informaticos-de-su-compania-506755 2017

con el objetivo de conservar triada de la seguridad confidencialidad, integridad y disponibilidad, garantizando el buen uso y privacidad de la información.

El Instrumento de Evaluación MSPI es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información". Fue creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con uso libre.[55]

Dentro de las guías anexas con las que cuenta el MSPI se encuentran las siguientes:

- Guía 1 - Metodología de pruebas de efectividad
- Guía 2 - Política General MSPI v1
- Guía 3 - Procedimiento de Seguridad de la Información
- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 6 - Gestión Documental
- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 9 - Indicadores Gestión de Seguridad de la Información
- Guía 10 - Continuidad de Negocio
- Guía 11 - Análisis de Impacto de Negocio
- Guía 12 - Seguridad en la Nube
- Guía 13 - Evidencia Digital (En actualización)
- Guía 14 - Plan de comunicación, sensibilización, capacitación
- Guía 15 - Auditoria
- Guía 16 - Evaluación de Desempeño
- Guía 17 - Mejora continua
- Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
- Guía 19 - Aseguramiento de protocolo IPv4_IPv6
- Guía 20 - Transición IPv4_IPv6
- Guía 21 - Gestión de Incidentes
- Modelo de Seguridad y Privacidad

- Establecer políticas de seguridad

Estas deben ser el punto de partida de las entidades, deben tener un plan trazado a partir de la actividad y las necesidades de cada entidad. Con las políticas de

[55] MINTIC. Modelo de seguridad. https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

seguridad se debe salvaguardar la información, garantizar su confidencialidad y normalizar su uso y el de los sistemas de información a través del cual se accede a la misma. El objetivo principal es amortiguar el riesgo de pérdida, disminución o acceso no autorizado. Adicionalmente de la información, en las políticas de seguridad de la información se envuelven elementos como el hardware, el software y los usuarios; se identifican probables amenazas y vulnerabilidades externas e internas, además se instauran medidas de defensa y planes de acción ante un incidente o un ataque cibernético.

Es importante tener en cuenta las siguientes pautas de lo mínimo que debe contener la política de seguridad:

- Contener en parte del texto el reconocimiento en el que se indica lo que se desea hacer, que regula, las directrices que deben seguir los empleados y personas que deban cumplirla, todo esto alineado con la estrategia de la organización.
- Debe estar alineada al alcance del MSPI.
- Especificar a quien va dirigida la política, identificando quienes deben cumplir la política.
- Hacer referencia sobre la regulación por la cual se soporta, las excepciones y a quienes aplican las excepciones (cuando aplique).
- Los roles de la organización que puedan dar información sobre la misma.
- Las consecuencias para quienes incumplan la política.
- Fecha de inicio de la vigencia de la política.

- Capacitar a los funcionarios

Favorece para prevenir grietas de seguridad, por eso es preciso incorporar las mejores prácticas que los funcionarios deben perseguir para mitigar el riesgo y cerciorarse al máximo de la seguridad informática de la entidad. Esto involucra la exclusión de acceder a sitios web dudosos, preferir constantemente por los protocolos HTTPS y no introducir unidades de memoria externas USB sin alguna autorización, entre otros. Básicamente se debe concentrar en la formación del personal y a quienes aplique, en temas correspondientes con la seguridad de la información, cuya importancia y propósito sea reducir las vulnerabilidades y amenazas concernidas con el recurso humano.

Estas capacitaciones deben estar alineadas con un plan de capacitación en el que se deban incluir los temas más relevantes y que los funcionarios reconozcan en su día a día como por ejemplo uso de contraseñas, escaneos de antivirus, utilización del correo, usos permitidos y no permitidos de la web, copias de seguridad, ingeniería social, que son incidentes informáticos y a quien reportar, controles de acceso, seguridad en el escritorio, entre otros. De igual forma es recomendable hacer un plan de comunicaciones en el que se invite a la participación activa

mostrando las problemáticas, los beneficios y como crear cultura de la seguridad de la información, mostrar la temática a los grupos objeto de capacitación y controlar el proceso con evaluaciones que muestren el avance de los funcionarios en los temas recibidos.

- Respaldar la información y poder recuperarla

Las entidades que realizan copias de seguridad habituales de la información están preparadas para recuperarse más pronto de algún ciberataque. Se pueden realizar copias físicas (que deben ser modificados cada determinado tiempo), en la nube o una mezcla de las dos. La opción que se seleccione depende de las obligaciones y funciones de la entidad, sin embargo, lo mejor es que se describa realización de forma automática y reiterada. Asimismo puede encriptar las copias de respaldo con una contraseña, en el momento que se debe salvaguardar información confidencial.

- Cifrar las comunicaciones de la entidad

El cifrado es una habilidad a través de la cual se transforma la información para que no sea comprensible para los que alcancen a obtener acceso a los datos. En las entidades, el resguardo de las comunicaciones a través de las cuales se divulga información sensible debe ser una prelación de las entidades.

De lo anterior se debe tener en cuenta cifrar passwords de usuarios, datos personales y económicos, llamadas, contactos, el acceso a sitios web, al correo electrónico y enlaces a equipos remotos, entre otros, se ha transformado en una obligación de primera mano. Se encuentran procedimientos y técnicas que cifran la información enviada a partir un sitio web e impiden el acceso de potenciales atacantes y hoy incluso los mensajes que se remiten por WhatsApp son cifrados.

- Utilizar sistemas antivirus (Equipos, servidores y móviles)

Las entidades continúan siendo las afectadas principales de los virus informáticos por la información financiera y económica o por la información confidencial que operan, por tal razón resulta importante que los equipos tengan instalado un antivirus. En el mercado se hallan muchas opciones de antivirus, en cuanto a elegir alguna obedecerá de las funciones u obligaciones de cada entidad. En este punto, se debe tener en consideración puntos de vista como actualizaciones reiteradas, soporte técnico y la disposición en el momento de realizar la instalación. Adicionalmente, si los funcionarios se enlazan a la información de la entidad desde dispositivos móviles, asimismo se debe instalar un sistema antivirus en equipos como tablets y smartphones.

- Proteger los equipos conectados a la red

Algunas entidades continúan en el error de pensar que están protegidas en presencia de potenciales ataques simplemente por tener una solución de antivirus en sus equipos, sin embargo ponen a un costado diferentes equipos enlazados a la red como impresoras o Smart TV, dispositivos que se han transformado en recientes punto de riesgos y amenazas cibernéticas. No obstante, aún no están en el mercado elecciones de sistemas de antivirus para estos equipos en especial, se podría mitigar el riesgo con ciertas operaciones. Para el caso de las impresoras, se podrían colocar atrás del segmento del firewall de la entidad y sin enlace directo a Internet, de igual forma mantener renovado su software, cifrar el disco duro y controlar por medio de claves que funcionario utiliza las impresoras. Para el caso de los Smart TV, solo utilizar la navegación en ellos por páginas web seguras, de igual forma descargar las aplicaciones autorizadas y mantener el software siempre renovado.

- Adquirir herramientas de seguridad

Los firewalls son otra forma de conservar a los delincuentes cibernéticos apartados de la información de las entidades, por tanto favorecen a advertir ataques externos a las redes de la entidad. No obstante, los equipos ya incluyen esta elección preinstalada, también hay otros mucho más seguros que se logran contener por hardware (equipos que se amplían a la red) o por software (aplicaciones que se instalan en los equipos) y lo que realizan es analizar y filtrar el intercambio de información que ingresa y sale con el fin de bloquear potenciales amenazas. El contraste radica en que el primero lo ejecuta en cada uno de los equipos que estén enlazados con la red local, entre tanto el segundo únicamente en el equipo en el que esté instalado.

Se encuentra también la protección de la red inalámbrica, que es una de las puertas distinguidas por los ciberdelincuentes a través de la cual logran acceder a la red de las entidades. Para resguardarla de atacantes digitales, se debe iniciar por cambiar la contraseña que trae por default en el equipo por una contraseña más elaborada y de alto nivel de seguridad, también como el nombre de la red inalámbrica.

- Implementación del SGSI

Por otro lado y de acuerdo a una investigación realizada en el año 2019 por la firma Infometrika Ltda, para el MINTIC, cuatro (4) de cada diez (10) entidades públicas no han realizado la implementación de un sistema de gestión de seguridad de la información, así las cosas, una (1) de cada diez (10) se encuentra en un proceso avanzado de “Actuar” y las otras cinco (5) restantes se encuentran en “Planear” y “Hacer” lo que quiere decir que la entidades han demostrado un

aumento en el grado de conciencia en la importancia de salvaguardar la información.[56] Los SGSI brindan a las entidades públicas la correcta utilización de la información para advertir que sea utilizada en espacios inseguros. No obstante y de acuerdo a la investigación, varios directivos en especial de entidades del ente territorial, no hallan las ocasiones ni identifican la necesidad de apropiar presupuestos para el tema de la seguridad digital, ello sin contar que a muchas entidades les faltan recursos para invertir en seguridad y en general, la capacitación en estos temas dilatan el acogimiento de un SGSI. Con relación a las anteriores apreciaciones es justo hacer la recomendación en aumentar el acompañamiento por parte de MINTIC mas enfáticamente a las entidades con carácter territorial y que se busque garantizar en avanzar más eficientemente y de manera continuada para conseguir las transiciones al SGSI de manera controlada evitando la resistencia al cambio y suscitando la cultura de la seguridad digital por parte de los funcionarios y directivos.

Las entidades del estado deben tener en cuenta que la implementación del SGSI debe ir acorde a la normatividad legal vigente colombiana y a los estándares de seguridad de la información como la norma ISO/IEC 27001/2013, contemplada también en la estrategia de gobierno en línea y en el MSPI. La propuesta del estado dada en el MSPI, tiene las bases para la implementación del SGSI en cinco (5) fases, las cuales admiten a las entidades del estado encargarse de carácter eficiente de la seguridad y privacidad de la información. La operación y desarrollo de estas fases permitirán cumplir con los objetivos, metas y herramientas que reconocerán que la seguridad de la información sea sustentable en los SGSI de las entidades.

Las cinco fases propuestas en el MSPI que se deben tener en cuenta para una correcta implementación del SGSI en las entidades son las siguientes:

- Diagnóstico: busca precisar el estado de las entidades frente los requerimientos de S.I., teniendo en cuenta la infraestructura tecnológica con la que cuentan, el nivel de madurez en S.I., identificando los problemas internos y externos que envuelven la entidad en cuanto a S.I., enmarcado en el numeral cuatro (4) de la norma.
- Planificación: el objetivo es generar el plan de S.I. relacionando la misionalidad de la entidad, precisando el alcance, objetivos, políticas, procesos y procedimientos para la gestión del riesgo. De igual forma la definición de controles de seguridad que dan cumplimiento a las metas del SGSI. Basados en la norma se define en los numerales cuatro (4) Contexto de la información, cinco (5) Liderazgo, seis (6) Planeación y siete (7) Soporte, formando la estructura organizacional, establece responsabilidades y compromiso de la alta dirección, se definen las

[56] MINTIC. Hora de implementar buenas prácticas de seguridad de información pública. https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/5414:Hora-de-implementar-buenas-practicas-de-seguridad-de-informacion-publica 2019

políticas, procesos y procedimientos que establezcan las mejores medidas de seguridad de la información.

- Implementación: después de la planeación estratégica de S.I. se procede a la ejecución específica del SGSI, llevando a cabo el cumplimiento de las actividades y metas definidas. Para esta fase se define el numeral ocho (8) de la norma Operación.
- Gestión: para esta fase de realiza la trazabilidad del desempeño del SGSI calificando la eficiencia y eficacia del sistema, y definiendo los niveles de cumplimiento. Así mismo, se implementan acciones de mejora que garanticen el cumplimiento de las metas. Se define el numeral nueve (9) de la norma en cuanto a la evaluación de desempeño del SGSI midiendo la efectividad, donde es de vital importancia la realización de auditorías internas.
- Mejora continua: permite a las entidades realizar las mejoras al SGSI implementando las acciones correctivas de acuerdo a los resultados de la fase de evaluación de desempeño. De acuerdo con la norma en su numeral diez (10) Mejora, garantizando que las no conformidades encontradas tengan su trazabilidad permitiendo que no se repitan siendo las acciones correctivas efectivas.[57]

- Análisis de brechas (GAP)

Como recomendación para la implementación o el mantenimiento durante el proceso de implementación del SGSI, se encuentra un método que sirve para evaluar el cumplimiento de requisitos de la norma ISO/IEC 27001 así mismo de los controles, se asemeja a una especie de auditoria inicial en la que se puede obtener una imagen del grado de implantación de la norma en la entidad y puede contener dos fines importantes:

- Constituir un espacio de inicio para empezar la implementación de la norma y de esta forma verificar el recurso necesario en la entidad con el fin de elaborar de manera eficiente el plan de implementación de la ISO/IEC 27001.
- Establecerla como una herramienta de evaluación que mida el grado de implantación durante el proceso de la implementación y valorar el progreso del proyecto de establecimiento de la norma en la entidad.

Para la elaboración del análisis de brechas es conveniente manejar un modelo de madurez para la evaluación del cumplimiento de la norma. Estos modelos proponen de 5 o 6 niveles de madurez o de cumplimiento que se manejan como instrumento de la gestión de servicios TI y de igual forma, para evaluar si los

[57] CAMPOS RAMIREZ, Jefferson Faruk. SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO COLOMBIANO. http://polux.unipiloto.edu.co:8080/00002657.pdf

procesos de gestión se están desarrollando de la mejor manera frente a los controles implementados en la entidad.[58]

- Continuidad del negocio

En el marco procedimental que responde a las interrupciones de los servicios de la entidad y buscando proteger y recuperar las actividades criticas de las organizaciones que puedan verse implicadas por eventos naturales y/o ocasionados por el hombre, se debe contemplar poner en marcha un modelo de operación de continuidad del negocio que apoye a las entidades en la gestión de la seguridad de la información, buscando robustecer la protección de los datos definiendo tiempos mínimos de recuperación e identificando procesos, aplicaciones y plataformas que se consideren críticas para la operación de la entidad.

En el MSPI se contempla su implementación en cuatro (4) fases, las cuales deben contener objetivos, metas e instrumentos que admitan que la continuidad del negocio dentro de las entidades sea un sistema sustentable y permita:

- Dar respuesta al variable contexto de riesgos.
- Cerciorar la continuidad de las operaciones críticas de la entidad soportadas por los servicios TIC.
- Disponerse para responder antes que una alteración en los servicios TIC pueda ocurrir, identificando los sucesos dependidos con dicho incidente.
- Responder y recobrarse de incidentes, fallas y desastres.

Las fases del modelo vienen dadas por la planificación, implementación, gestión y mejora continua de los cuales se debe tener en cuenta lo siguientes:

- Planificación: Análisis de impacto del negocio, requerimientos, políticas para la preparación de los servicios TIC y entendimiento de los servicios TIC, todo esto enmarcado en la identificación GAPs.
- Implementación: se deben garantizar y proporcionar los recursos, procedimientos y operaciones necesarias, así como los programas de entrenamiento y concientización. En esta fase se establece la infraestructura de los sistemas de recuperación de TIC y la información critica separada del sitio de operaciones de la entidad.
- Gestión: se debe hacer una evaluación de desempeño y eficacia de la implementación, determinando un plan de seguimiento, evaluación y análisis para la preparación de las TIC para la continuidad del negocio de la entidad.
- Mejora continua: se definen las acciones correctivas identificando fallas. Se establecen las auditorías internas, se monitorea el rendimiento y la

[58] ISO 27001. FASE 1 AUDITORIA INICIAL ISO 27001 GAP ANALYSIS, QUE ES UN ANÁLISIS DE BRECHAS GAP EN ISO 27001. https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/

disponibilidad de los servicios TIC, así mismo, se debe realizar una revisión anual de pruebas y ejercicios y que el plan de continuidad de negocio funcione correctamente.

De otro lado, en el “Manual de Gobierno Digital” emitido por MINTIC y el Departamento Nacional de Planeación y dirigido principalmente a entidades públicas nacionales y territoriales, se dan pautas en el proceso de implementación de la política digital a través de cuatro importantes momentos:

1. Conocer la política

    - Evolución
    - Que es gobierno digital
    - Propósitos
    - Elementos
    - Actores

2. Planear la política

    - ¿Cómo planear la política en la entidad?

3. Ejecutar la política

    - TIC para el estado y TIC para la sociedad
    - Habilitadores transversales
    - Apoyo a la implementación

4. Medir la política

    - Seguimiento y evaluación en la entidad
    - Seguimiento y evaluación MinTIC

La política del gobierno digital se define como una política pública que tiene como objetivo promover el uso y la explotación de las TIC para consolidar un estado y ciudadanos competitivos, proactivos e innovadores que generen valor público en un entorno de confianza digital. Se hace esta recomendación para implementar esta política digital, ya que uno de sus facilitadores transversales es la seguridad de la información, que busca implementar pautas de seguridad de la información en todos sus procesos, procedimientos, servicios y sistemas en las entidades públicas, información, infraestructura y, en general, todos los activos de información, para salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador es compatible con el Modelo de seguridad y privacidad de la información (MSPI).

9. CONCLUSIONES

Durante el transcurso de los últimos tiempos, el avance tecnológico que se ha dado en el mundo y su repercusión a nivel nacional, ha venido a pasos agigantados, hemos tenido adelantos en equipos y dispositivos de todo nivel, las comunicaciones cableadas e inalámbricas cada vez son más rápidas, el desarrollo en cuanto a sistemas de información y su soporte a gran escala, entre otros tantos adelantos, también han tenido en contraste un avance en criminalidad cibernética, muchos individuos con formación académica o en ocasiones empíricos, retan por varias motivaciones la seguridad informática y de la información de las entidades y organizaciones sean de cualquier índole (privadas y públicas), quienes a su vez deben estar en guardia y la vanguardia para mitigar esos riesgos y amenazas a las que diariamente se enfrentan.

Dentro del análisis efectuado en el tema del presente documento, se logró evidenciar que el problema principal en cuanto al aseguramiento informático de las entidades gubernamentales ha sido que se poseen sistemas altamente vulnerables, algunas de ellas con deficiencias en cuanto a tecnología, ya sea por falta de recursos destinados a la seguridad informática o por la falta de capacitación o conocimiento del tema orientado al recurso humano. Sin embargo, en una publicación sobre el Índice Mundial de Ciberseguridad (IMC) realizada por la UIT (Unión Internacional de Telecomunicaciones), Colombia se destacó por sus resultados estando por encima de países como Chile y México. En este estudio se tuvieron encuentra cinco (5) aspectos de evaluación: medidas legales, técnicas, organizacionales, generación de capacidades y cooperación, buscando destacar a los países que fomentan la cultura de la ciberseguridad y su integración con las TIC, un trabajo que viene desde las directrices gubernamentales a través del MINTIC dirigido hacia todos los sectores público y privados del país.

Después del análisis realizado con relación a la evolución que ha tenido el país en materia de seguridad informática y más específicamente en algunas entidades gubernamentales, se puede destacar y concluir lo siguiente:

- El país ha estado en constante desarrollo de normativas y legislación que apoyan y dan soporte para que las entidades públicas tomen las medidas pertinentes para su seguridad informática, buscando con ello la mitigación de los riesgos que se presenten evitando ataques informáticos o en caso de materializarse, su impacto sea el menor posible para el desempeño de la entidad. A través de la política de seguridad digital, el gobierno, las organizaciones y la ciudadanía en general, se encaminan para tener un entorno digital confiable y seguro. Así mismo se destacan las entidades que tienen las competencias en el manejo de la seguridad y la defensa informática en el país que van desde la Presidencia de la República, el MINTIC, MINDEFENSA y la creación de entidades especializadas en

materia ciberseguridad tales como el Comando Conjunto Cibernético de las Fuerzas Militares, el Centro Cibernético Policial, COLCERT, entre otros.

- Se destaca que las entidades públicas han estado en concordancia con el cumplimiento de la normatividad y los modelos de seguridad que por ejemplo desde el MINTIC se han emitido, uno de ellos es el Modelo de Seguridad y Privacidad de la Información (MSPI) que contiene una serie de guías anexas que ayudan a las entidades a cumplir lo necesario, admitiendo de la mejor manera cada fase del modelo. Se pudo constatar con algunas entidades públicas, como se ha venido cumpliendo desde cada una de ellas con la implementación de mecanismos y protocolos de seguridad, políticas y procedimientos, SGSI, entre otros. Con las anteriores acciones y buenas prácticas se da acatamiento a los requisitos de seguridad, evitando de esta forma mitigar los riesgos y amenazas detectados con el objetivo principal de buscar salvaguardar los fundamentos principales de la triada de la información: Confidencialidad, Integridad y Disponibilidad, garantizando el buen uso y la privacidad de los datos.

- Si bien es cierto que a través de las políticas públicas el gobierno da respuesta a diversas demandas de la ciudadanía, para el caso de los CONPES de seguridad digital, se convierten en un instrumento para enfrentar las amenazas pero no puede ser lo único, la ciberseguridad es un asunto que nos compete a todos, no solo a las entidades públicas sino a la empresa privada, la academia y la ciudadanía en general. Para esta investigación en particular, la tarea del gobierno ha sido propender un uso responsable del entorno digital, aprendiendo a identificar las posibles amenazas y peligros y tener un plan de acción para poder reaccionar ante cualquier incidente, es por esto que mediante las directrices y recomendaciones de las entidades especialidades en seguridad digital tales como MINDEFENSA con el CCOC y el COLCERT, el MINTIC, la Policía Nacional con el CCP, buscan que las entidades se mantengan alerta sobre información de nuevas amenazas, implementar nuevas tecnologías que permitan defender sus equipos y dispositivos contra la explotación de vulnerabilidades y efectuar la instalación de mecanismos de detección de amenazas a nivel de red. De igual manera es importante contar con protecciones en la infraestructura para prevenir y mitigar la ejecución de amenazas.

- A pesar que todavía falta mucho, se destaca que el país va por buen camino en aspectos de seguridad informática, de acuerdo a la publicación de la UIT y según el MINTIC, Colombia y sus organizaciones han obtenido buenos resultados, y a pesar de no ser los mejores, confirman que las estrategias para la protección de la información están dando resultados y que ante posibles ataques cibernéticos, robo de información, entre otros, el

país tiene un nivel de preparación para responder ante ellos. De igual forma, se obtuvo buena calificación en los aspectos legales y regulatorios que posee el país para la prevención y promoción de la seguridad, protección de datos y judicialización de delitos informáticos, y en los aspectos organizacionales que tiene que ver con la creación de instancias como el Centro Cibernético Policial – CCP, el Comando Conjunto Cibernético – CCOC y el Grupo de Respuesta a Incidentes Informáticos – ColCERT.

10. RECOMENDACIONES

Es importante precisar que de acuerdo al análisis efectuado con relación a la evolución del aseguramiento informático en las entidades del sector gobierno en Colombia, se puede inferir que de acuerdo a la normatividad impartida por el gobierno nacional, existen una serie de directrices y modelos que las entidades públicas deben seguir para establecer el buen funcionamiento y asegurar su entorno digital, para con ello poder mitigar los riesgos y amenazas a los que estén expuestos y prevenir ante posibles ataques cibernéticos que puedan recibir; es por esto que existen una serie de mecanismos, procesos y procedimientos que las entidades públicas y en general, pueden tener en cuenta para controlar los riesgos y amenazas en materia de ciberseguridad:

- Establecer políticas de seguridad: con estas se busca darle protección a la información, salvaguardar su confidencialidad y reglamentar su uso y el de los sistemas de información a través de los cuales se accede a ella. Estas políticas buscan mitigar los riesgos de pérdida o acceso no autorizado a la información y pueden incluir elementos de hardware, software y por supuesto lo usuarios.
- Respaldo de la información y su recuperación: se debe estimar un sistema de copias de seguridad de la información y de los sistemas de información que la contienen o a través de los cuales se puede acceder, además se debe tener un plan de restauración de la información y de recuperación ante el caso de algún incidente o ataque cibernético en el menor tiempo posible. Se recomienda que la herramienta pueda encriptar los backups.
- Cifrado de las comunicaciones: en caso de interceptación de la información a través de los canales dispuestos para su transmisión, se debe tener una protección en las comunicaciones cifrando los datos personales, información sensible, llamadas, contactos, entre otros, buscando la confidencialidad e integridad de la información de la entidad.
- Sistemas de antivirus: es necesario que exista un sistema que proteja la información tanto en equipos de alto nivel (servidores) como en las estaciones de trabajo, que además contenga detección y protección de intrusos.
- Herramientas de seguridad perimetral: son una manera de mantener a los delincuentes cibernéticos alejados de la información y los activos de las entidades y las organizaciones en general, ayudan a prevenir y mitigar ataques que provengan fuera de la entidad. Es recomendable el uso de firewalls de nueva generación, estos son capaces de ofrecer niveles más profundos de seguridad en la red, pueden incluir inspección SSL, IPS con tecnología anti-evasión, control de aplicaciones, protección contra malware, estas características tiene como objetivo detener el número de ataques y filtrar tráfico proveniente de la red.

- Sistema de Gestión de Seguridad de la Información - SGSI: estos sistemas ayudan a las entidades a analizar posibles riesgos, establecer medidas de seguridad necesarias e implementar los controles que permitan evaluar la efectividad de esas medidas. Generalmente la normatividad utilizada está basada en los requisitos de las normas internacionales ISO/IEC 27000.

BIBLIOGRAFIA

ALCALDÍA DE BOGOTÁ. “Ley 1273 de 2009 nivel nacional. Diario Oficial 47.223 de enero 5 de 2019” {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492)

ALCALDÍA DE BOGOTÁ. “Ley 1581 de 2012 Nivel Nacional. Diario Oficial 48587 de octubre 18 de 2012.” {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276)

ALCALDÍA DE BOGOTÁ. “Ley 1712 de 2014 nivel nacional. Diario Oficial 49084 de marzo 6 de 2014” {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882)

ALCALDÍA DE BOGOTÁ. “Decreto 2952 de 2010 nivel nacional. Diario Oficial 47793 de agosto 6 de 2010” {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=40120)

ALCALDÍA DE BOGOTÁ. “Decreto 1377 de 2013 nivel nacional. Diario Oficial 48834 del 27 de junio de 2013” {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646)

ALCALDÍA DE BOGOTÁ. “Decreto 886 de 2014 nivel nacional. Diario Oficial 49150 de mayo 13 de 2014” {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57338)

.

ARMIROLA R, Daniel. “Bogotá, puesto 46 de 60 en ranking de seguridad en ciudades”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.elcolombiano.com/colombia/bogota-puesto-46-de-60-en-ranking-de-seguridad-en-ciudades-KA7561682)

ARMIROLA R, Daniel. “Ciberataque global prende las alarmas en Colombia”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.elcolombiano.com/internacional/ciberataque-global-prende-las-alarmas-en-colombia-IE6521831)

BANCO DE LA REPUBLICA. “Mecanismos de seguridad de los servicios informáticos”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.banrep.gov.co/sites/default/files/paginas/Mecanismos_de_Seguridad_Informatica.pdf)

BID. “Impacto de los incidentes de seguridad digital en Colombia 2017”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://publications.iadb.org/es/publicacion/17294/impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017)

CAMACHO GARCIA, Juan Diego. “Evolución de la ciberdefensa y la seguridad de la información en Colombia”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://repository.unimilitar.edu.co/handle/10654/14382)

CAMELO, Leonardo. “Seguridad de la Información y Seguridad Informática”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (http://seguridadinformacioncolombia.blogspot.com/2010/02/seguridad-de-la-informacion-y-seguridad.html)

CAMPOS RAMIREZ, Jefferson Faruk. “SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO COLOMBIANO”. {En línea}. {Revisado 19 noviembre de 2020} disponible en: (http://polux.unipiloto.edu.co:8080/00002657.pdf)

CERTICAMARA S.A. “Panorama del Cibercrimen en Colombia”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://blogs.portafolio.co/seguridad-informatica-certicamara-sa/panorama-del-cibercrimen-colombia/)

CENTRO CIBERNÉTICO POLICIAL. “Ciberincidentes” {En línea}. {Revisado 12 mayo de 2019} disponible en: (http://www.ccp.gov.co/ciberincidentes/tiempo-real/historico)

CM&. “Hacker ataca sitio web EAAB, link de contratación.” {En línea}. {Revisado 12 mayo de 2019} disponible en: (http://www.cmi.com.co/?n= 92235)

COLOMBIA DIGITAL.NET, Corporación Colombia Digital. “¿Cómo está Latinoamérica en temas de seguridad informática?”. {En línea}. {Revisado 12 mayo de 2019} disponible en:

(https://colombiadigital.net/actualidad/noticias/item/8250-como-esta-latinoamerica-en-temas-de-seguridad-informatica.html)

COLPRENSA “Colombia, el sexto país con más ciberataques en 2017”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174)

COLCERT, Grupo de respuesta a emergencias cibernéticas de Colombia. “Acerca de” {En línea}. {Revisado 23 marzo de 2020} disponible en: (http://www.colcert.gov.co/?q=acerca-de)

COMANDO CONJUNTO CIBERNETICO. “Funciones y deberes”. {En línea}. {Revisado 23 marzo de 2020} disponible en: (https://www.ccoc.mil.co/quienes_somos_funciones_deberes)

COMPUTERWORLD, Seguridad “Predicciones en seguridad informática y privacidad”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://computerworld.co/predicciones-en-seguridad-informatica-y-privacidad/)

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL “Lineamientos de política para Ciberseguridad y Ciberdefensa”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.)

CONTADURIA GENERAL DE LA NACION. “Manual de seguridad de la Información” {En línea}. {Revisado 12 mayo de 2019} disponible en: (http://www.contaduria.gov.co/documents/20127/35873/MANUAL%2BDE%2BSEGURIDAD%2BDE%2BLA%2BINFORMACI%C3%93N-%2BMAYO%2B31%2B2019.pdf/cf9d72ad-ad76-cdff-afdb-a1a6459360f4?t=1565109226933)

CONTRALORIA DE BOGOTA D.C., “Planes y programas, Plan Estratégico 2016 – 2020.” {En línea}. {Revisado 12 mayo de 2019} disponible en: (http://www.contraloriabogota.gov.co/sites/default/files/Contenido/Planes/Planes%20y%20Programas/Planes/Estrategico/2016-2020/Versi%C3%B3n%203.0/PLAN%20ESTRATEGICO%20INSTITUCIONAL%202016-2020%20Ver%203.0.pdf)

CONTRALORIA DE BOGOTA D.C., “Planes y programas, PETI 2016 – 2020 Versión 5.0” {En línea}. {Revisado 12 mayo de 2019} disponible en: (http://www.contraloriabogota.gov.co/sites/default/files/Contenido/Planes/Planes%20y%20Programas/Planes/PETI/2016-2020/Versi%C3%B3n%205.0/PETI%202016-2020%20v5.pdf)

CONTRERAS, Nicolás. “Más del 80 por ciento de las compañías en Colombia son vulnerables a ataques informáticos”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://caracol.com.co/radio/2016/06/09/tecnologia/1465469190_389745.html)

CORPORACIÓN COLOMBIA DIGITAL. “Entrevistas Colombia Digital: Seguridad informática, el valor de la información y el rol de las empresas.” {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://colombiadigital.net/actualidad/noticias/item/10005-entrevistas-colombia-digital-seguridad-informatica-el-valor-de-la-informacion-y-el-rol-de-las-empresas.html)

CORTES, Mireya. “La evolución del firewall”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://cio.com.mx/la-evolucion-del-firewall/)

CORTES BORRERO, Rodrigo. “ESTADO ACTUAL DE LA POLITICA PÚBLICA DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA” {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://repository.usta.edu.co/bitstream/handle/11634/14032/2015rodrigocortes.pdf?cv=1&sequ=)

CRUZ, Luis. “¿Qué es la gestión unificada de amenazas (UTM)?”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://study.com/academy/lesson/what-is-unified-threat-management-utm.html)

DAZA, Lizeth. “Las claves del futuro para la seguridad informática en Colombia”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://www.canalinformatico.net/software-y-la-nube/75-seguridad/2268-las-claves-del-futuro-para-la-seguridad-informatica-en-colombia)

DEPARTAMENTO NACIONAL DE PLANEACIÓN. “Documento CONPES 3854 de 2016” {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf)

DIAN. “Circula Otra Versión De Falsos” {Revisado 23 marzo de 2019} disponible en: (http://www.dian.gov.co/descargas/EscritosComunicados/2017/033_Comunicado_de_prensa_23022017.pdf)

DINERO, Tecnología. “Los sectores económicos más impactados por el cibercrimen en Colombia”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321)

DINERO, Tecnología. “Empresas. Colombia, débil en seguridad informática”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.dinero.com/edicion-impresa/tendencias/articulo/empresas-colombia-debil-seguridad-informatica/66085)

DINERO, Tecnología. “El 2015 fue un año de “altas y bajas” para la seguridad informática”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.dinero.com/pais/articulo/informe-certicamara-sobre-seguridad-informatica-colombia-para-2016/217635)

DIVISION COMPUTER FORENSIC. “Tipos de delitos informáticos, Clasificación según el Convenio sobre la Ciberdelincuencia”, {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html)

DUEÑAS, Jaime. “COLOMBIA ES MÁS CONSCIENTE FRENTE A LA SEGURIDAD DE LA INFORMACIÓN”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.enter.co/especiales/empresas/colombia-seguridad-informacion/)

EL ESPECTADOR. “Confirman primer ataque de 'hackers’ a la Registraduría” {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.elespectador.com/noticias/politica/confirman-primer-ataque-de-hackers-registraduria-articulo-300731)

EL NUEVO SIGLO. “Falso: fotocomparendos no se notifican vía correo electrónico” {Revisado 23 marzo de 2019} disponible en: (https://www.elnuevosiglo.com.co/articulos/02-2019-falsofotocomparendos-no-se-notifican-correo-electronico)

EL OLFATO. “Incendio en la Alcaldía de Ibagué provoca daños en computadores y destrucción de algunos documentos.” {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://elolfato.com/incendio-en-laalcaldia-de-ibague-provoca-danos-en-computadores-y-destruccion-de-algunos-documentos)

EL TIEMPO, Tecnosfera. “El 63 % de las grandes empresas identificaron incidentes digitales”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/resultados-del-estudio-impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017-137222.)

EL UNIVERSAL. “Investigación sobre ataques de hackers a la Registraduría será cerrada.” {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.eluniversal.com.co/home/investigacion-sobre-ataques-de-hackers-la-registraduria-sera-cerrada-65604-HVEU147563)

GONZALO, Leonardo. “Antivirus vs Anti-Malware”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.malwarefox.com/es/antivirus-vs-anti-malware/)

INFOLAFT. “un ataque informático” {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.infolaft.com/en-vivo-un-ataque-informatico/)

ISO 27001. “FASE 1 AUDITORIA INICIAL ISO 27001 GAP ANALYSIS, QUE ES UN ANÁLISIS DE BRECHAS GAP EN ISO 27001” {En línea}. {Revisado 19 noviembre de 2020} disponible en: (https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/)

LA REPÚBLICA. “Colombia es uno de los países más rigurosos en temas de seguridad y fraude” {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.larepublica.co/internet-economy/colombia-es-uno-de-los-paises-mas-rigurosos-en-temas-de-seguridad-y-fraude-2593165)

LATINPYME, Noticias. “SEGURIDAD INFORMÁTICA EN COLOMBIA POR BUEN CAMINO”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.latinpymes.com/seguridad-informatica-en-colombia-por-buen-camino/)

LEHMANN, Armin Dieter. “Intrusion Detection FAQ”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://www.sans.org/resources/idfaq/what_is_id.php)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Lo que usted debe saber del Conpes de Seguridad Digital” {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.mintic.gov.co/portal/604/w3-article-15410.html)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Documento CONPES 3701 de 2011” {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Guía encuesta de Diagnóstico Modelo de Seguridad de la Información para las Entidades del Estado”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (http://www.mintic.gov.co/gestionti/615/articles-5482_diagnostico.pdf)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Guía para la preparación de las TIC para la continuidad del negocio”. {En línea}. {Revisado 19 noviembre de 2020} disponible en: (https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Modelo de seguridad”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “NUEVA POLÍTICA PÚBLICA DE SEGURIDAD DIGITAL:

DESAFIOS Y OPORTUNIDADES EN EL ESCENARIO DE POSCONFLICTO". {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.mintic.gov.co/portal/604/articles-15570_recurso_2.pdf)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. "¿Y de seguridad TI qué hacen las entidades?". {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.mintic.gov.co/gestionti/615/w3-article-7083.html?_noredirect=1)

NAJAR P, José C, SUAREZ S, Nubia E. "La seguridad de la información: un activo valioso de la organización". {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://revistas.udistrital.edu.co/ojs/index.php/vinculos/article/view/10518/11605)

OCDE "Evaluar el impacto del gobierno digital en Colombia". {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.oecd.org/countries/colombia/evaluar-el-impacto-del-gobierno-digital-en-colombia-9789264284272-es.htm)

PEÑA CASTAÑEDA, Camilo. "Los principales retos que afronta el país en seguridad informática". {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/desafios-que-afronta-colombia-en-seguridad-informatica-50410)

PÉREZ G., Camilo. "¿En Colombia se investigan los delitos informáticos?" {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html.)

PORTAFOLIO, Innovación. "Siete consejos para proteger los sistemas informáticos de su compañía" {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.portafolio.co/innovacion/siete-recomendaciones-para-proteger-los-sistemas-informaticos-de-su-compania-506755)

PRESIDENCIA DE LA REPÚBLICA. "Manual de la política de seguridad para las Tecnologías de la Información y las Comunicaciones – TICS". {En línea}. {Revisado 12 mayo de 2019} disponible en: (http://wp.presidencia.gov.co/sitios/dapre/sigepre/manuales/M-TI-

01%20Manual%20general%20Sistema%20de%20Seguridad%20de%20la%20Informacion.pdf)

PROFITLINE, Servicios IT Outsourcing. “ACTUALMENTE COMO SE ENCUENTRA COLOMBIA EN SEGURIDAD INFORMÁTICA.”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://profitline.com.co/actualmente-como-se-encuentra-colombia-en-seguridad-informatica/)

PROFITLINE, Servicios IT Outsourcing. “Tendencias en seguridad informática para el 2019”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://profitline.com.co/tendencias-en-seguridad-informatica-para-el-2019/)

PULIDO BARRETO, Ana Milena. MANTILLA RODRIGUEZ, Jenith Marsella. “Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina tic de la alcaldía municipal de Fusagasugá, basados en la gestión el riesgo informático”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/6327/1/35250)

SECRETARÍA DEL SENADO. Congreso de la República. Colombia. “Ley estatutaria 1266 de 2008. Diario Oficial No. 47.219 de 31 de diciembre de 2008.” {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html)

SECRETARÍA DEL SENADO. Congreso de la República. Colombia. “Ley estatutaria 1621 de 2013. Diario Oficial No. 48.764 de 17 de abril de 2013.” {En línea}. {Revisado 23 marzo de 2019} disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley_1621_2013.html)

SEMANA, Economía. “Las empresas colombianas no están preparadas para los ciberataques”. {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.semana.com/tecnologia/articulo/las-empresas-colombianas-no-estan-preparadas-para-los-ciberataques/466430)

SEMANA, Tecnología. “Las empresas en Colombia no invierten en seguridad digital”. {En línea}. {Revisado 12 mayo de 2019} disponible en:

(https://www.semana.com/tecnologia/articulo/colombia-no-invierte-en-seguridad-digital/492724)

SEMANA, Tecnología. “No se deje engañar: estos son los correos falsos de la Fiscalía.” {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.semana.com/tecnologia/articulo/correos-falsos-de-lafiscalia/489435)

SUPERFINANCIERA. “Superfinanciera NO hace llamadas para solicitar información personal.” {En línea}. {Revisado 12 mayo de 2019} disponible en: (https://www.superfinanciera.gov.co/inicio/10083259)

RODRIGUEZ, Raúl. “Para aprender, perder… o no: Introducción”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.securityartwork.es/2010/03/26/para-aprender-perder%E2%80%A6-o-no-introduccion/)

RODRIGUEZ, Victoria. “Cómo funciona un firewall”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.segurisoft.es/encriptacion/como-funciona-firewall/)

TURMERO, Pablo. “Elementos básicos de la seguridad perimetral”. {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.monografias.com/trabajos106/elementos-basicos-seguridad-perimetral/elementos-basicos-seguridad-perimetral.shtml)

VANGUARDIA. “En asonada incendiaron casa del alcalde y la Fiscalía de Tibú, Norte de Santander.” {En línea}. {Revisado 23 marzo de 2019} disponible en: (https://www.vanguardia.com/colombia/en-asonada-incendiaron-casa-del-alcalde-y-la-fiscalia-de-tibu-norte-de-santander-CAvl212231)