LA IMPORTANCIA DEL HACKING EN LA CIBERSEGURIDAD A NIVEL ORGANIZACIONAL EN ENTIDADES DE ORDEN PUBLICO EN COLOMBIA.

JUAN FELIPE ROZO DÍAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
20 DE ABRIL DEL 2022

LA IMPORTANCIA DEL HACKING EN LA CIBERSEGURIDAD A NIVEL ORGANIZACIONAL EN ENTIDADES DE ORDEN PUBLICO EN COLOMBIA.

JUAN FELIPE ROZO DÍAZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Msc. Katerine Márceles Villalba
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
20 DE ABRIL DEL 2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., Fecha sustentación

AGRADECIMIENTOS

Agradezco a mi madre, quien con su dedicación y afecto contribuyó enormemente a mi interés y capacidad para cursar el presente programa de formación.

Agradezco a la coordinadora de mi grupo laboral, quien con su ejemplo y aprecio me ha impulsado cada día a ser un mejor profesional.

Agradezco a los directivos de la Universidad Nacional Abierta y a Distancia UNAD, que participaron activamente en mi formación y me brindaron el acompañamiento necesario para cumplir está meta profesional.

CONTENIDO

pág.

GLOSARIO

HACKER: El termino aparece en la década de los 50, es definido como aquella persona con suficientes conocimientos informáticos para vulnerar los esquemas de seguridad y lograr un acceso no autorizado a un sistema de información. Por definición un “hacker” debe preocuparse por conocer a fondo el funcionamiento de un sistema con el fin vulnerar su seguridad, demostrar los errores y poder corregirlos. Sin embargo, el término coloquialmente se ve asociado a los ciberdelicuentes, es por eso que surge la necesidad de especificar los tipos de hackers que existen.

CRACKER: Son hackers que utilizan la aplicación de sus conocimientos para la intrusión en sistemas informáticos con el fin de obtener un beneficio propio ilícito, o bien causar un perjuicio al sistema en mención. También conocidos como piratas informáticos, los crackers trabajan de forma malintencionada usualmente para robar información, descifrar claves de acceso o alterar de forma ilícita el contenido de un sistema.

PHREACKER: Es un término derivado de hacker, pero contextualizado a redes telefónicas. Los prehackers son personas con altos conocimientos de infraestructura y dispositivos de telefonía que se dedican a interceptar comunicaciones e identificar fallas en los protocolos de telefonía. Por lo general se orientan hacia la telefonía celular y las intrusiones son realizadas utilizando dispositivos artesanales de frecuencia.

WHITE HACKER: Llamados en español HACKERS DE SOMBRERO BLANCO son aquellos individuos que aplican sus conocimientos de seguridad para trabajar de la mano con los propietarios de los sistemas de información, con el fin de identificar vulnerabilidades y fortalecer el esquema de seguridad implementado. Usualmente los WHITE HACKERS diseñan herramientas y procesos ejecutables para contrarrestar acciones de los CRACKERS.

BLACK HACKER: Llamados en español HACKERS DE SOMBRERO NEGRO son aquellos individuos que violan la seguridad de un sistema con el fin de perjudicarlo u obtener un beneficio propio mediante el hurto de información, la destrucción de datos o la inhabilitación del sistema.

LAMMERS: Llamados también zomber. Es un término utilizado para expresarse sobre aquellos usuarios con conocimientos insuficientes en un campo particular o frente al uso de una herramienta específica, pero que promueven la idea que ser expertos y altamente capacitados. Asociados al mundo del HACKING, los LAMMERS son usuarios amateurs que se autoproclaman auténticos hackers

solo por el hecho de haber tenido un acercamiento vago al conocimiento de ciberseguridad e intrusión.

ICCN: Infraestructura Crítica Cibernética Nacional. Aquellos sistemas de administración pública o relacionados, definidos como activos nacionales y que son protegidos por la política de ciberseguridad, en busca de garantizar la prosperidad de la nación.

INGENIERÍA SOCIAL: Método de manipulación con fines ilícitos, donde por medio de la persuasión o suplantación de identidad se persuade a un usuario de suministrar información privada, o bien, de ejecutar una acción sobre un sistema la cual concede control al atacante. Existen diferentes tipos de ingeniería social, los cuales se aplican de acuerdo a la población objetivo y el fin último del ataque.

BOTNET: Red de equipos informáticos o BOTS controlados de forma remota con el fin de ejecutar ciberataques. También conocida como red de computadoras “zombie”

GOBERNANZA TI: Es la definición oportuna de estructuras y procesos organizativos que dirigen el uso de las tecnologías de la información (TI) a la contribución eficiente, para que la organización alcance el valor máximo valor de negocio mediante la gestión de riesgos y control de desempeño relacionados a las tecnologías de la información.

RESUMEN

La presente investigación resalta la importancia del área de conocimiento asociada al hacking e intrusión como herramienta para robustecer el esquema de ciberseguridad de las entidades públicas en Colombia.

El tema en mención se desarrolla a partir de un marco referencial que contextualiza histórica y conceptualmente la situación de Colombia frente a seguridad informática y ciberataques, resaltando la necesidad de fortalecer este aspecto en la gestión pública.

En un segundo momento, se justifica la necesidad identificada a partir del análisis del tipo de información que se gestiona al interior de las entidades de orden público en Colombia, de la importancia de la misionalidad de estas entidades para los intereses del estado colombiano, y finalmente, a partir de los riesgos que pueden evitarse al direccionar la gestión pública hacia procesos que garanticen seguridad en la información y las comunicaciones.

Posteriormente se enmarcan de forma teórica las ventajas implícitas en la inclusión de procesos asociados al hacking, en la gestión de la ciberseguridad de entidades del estado colombiano. Finalmente se consolidan recomendaciones dirigidas a directivos y jefes de departamentos de TI, las cuales brindan sugerencias útiles asociadas a ciberseguridad, divididas en recomendaciones referentes a infraestructura TI, y recomendaciones referentes a perfiles profesionales TI.

La investigación termina con conclusiones asociadas a la revisión y análisis teórico realizado, que reafirman la importancia del hacking a nivel organizacional en entidades públicas colombianas.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En Colombia, la ciberseguridad y la ciberdefensa son conceptos que han venido tomando fuerza a nivel gubernamental. El teniente Juan Carlos García, define la ciberseguridad a nivel nación como “la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. Así mismo, el teniente define ciberdefensa como “la capacidad del Estado para prevenir, detectar y neutralizar cualquier amenaza de naturaleza cibernética que atente contra la soberanía nacional, independencia, integridad y orden de constitucionalidad”.[1]

En este orden de ideas, el mundo digital puede ser entendido como un campo hostil, donde un gobierno y sus recursos están constantemente expuestos a ataques de diferentes tipos. Es deber del Gobierno Colombiano fortalecer los esquemas de ciberseguridad de la nación mediante el aumento presupuestal y el desarrollo de nuevas tecnologías al interior del país.

A nivel histórico, el gobierno colombiano ha sido blanco de varios ciberataques los cuales son en su mayoría documentados. A partir de la experiencia obtenida en estos eventos y las consecuencias de los mismos, es posible resaltar la importancia de la formación de profesionales que contribuyan al desarrollo de tecnologías y procedimientos relacionados a la seguridad informática.

Algunos ejemplos de ciberataques en el pasado, reconocidos a entidades gubernamentales en Colombia son:

- Octubre 2012. Ataque a la página web de la Policía Nacional. Al colectivo de piratas informáticos Anonymus se le atribuye el ciberataque mediante el cual la página web de la Policía Nacional de Colombia estuvo caída presuntamente por más de 18 horas. El ataque tuvo lugar a raíz de los enfrentamientos ocurridos durante las manifestaciones de la “semana de los indignados”.[2]

---

[1] GARCÍA, Juan Carlos. Conferencia: estado de la ciberseguridad y la ciberguerra en el contexto latinoamericano. Universidad Externado de Colombia. Bogotá. 2018.

[2] EL ESPECTADOR. Anonymous Colombia se atribuye ataque a la web de la policía nacional. 13 de octubre de 2012. Disponible en https://www.elespectador.com/colombia/mas-regiones/anonymous-colombia-se-atribuye-ataque-a-la-web-de-policia-nacional-article-381102/

- Abril 2012. Ataque a varios portales web del gobierno. Nuevamente al grupo de hackers Anonymus se le atribuye el ciberataque mediante el cual se inhabilitaron al menos 12 páginas web de entidades estatales entre las cuales estaban la página del Senado de la República y del Ministerio de Justicia. El ataque tuvo lugar como protesta ante la intención del gobierno de Juan Manuel Santos de regular la navegación en internet. [3]
- Septiembre 2016. Ataque a la aplicación de información al votante de la Registraduría. Un ciberataque de origen desconocido tuvo lugar durante el periodo de plebiscito del año 2016, a través del cual el aplicativo quedó offline. [4]

Adicional a los ataques registrados, en el transcurso de la última década se han realizado importantes estudios y datos oficiales que destacan la necesidad del gobierno colombiano de prestar especial atención al tema de ciberseguridad. Algunos ejemplos de estas publicaciones y estudios relacionados a Colombia son:

- Periódico El TIEMPO publica un artículo en el año 2017 donde señala que Colombia es el tercer país con más ciberataques en américa latina. El informe se basa en reportes oficiales de la compañía de ciberseguridad Kaspersky.

- En el año 2016 en un Informe de la OEA (Organización de los Estados Americanos) y BID (Banco Interamericano de Desarrollo) se concluye que América Latina y el Caribe presentan vulnerabilidades en materia de ciberseguridad consideradas potencialmente devastadoras. Puntualmente el informe menciona que Colombia tiene un nivel intermedio de madurez, pero que permanece muy distante de países desarrollados como Estados Unidos o la República de Corea.

Con base a los hechos mencionados con anterioridad es posible reconocer una trayectoria del esfuerzo y el interés del gobierno colombiano en materia de ciberseguridad. Sin embargo, es claro que aún falta mucho por hacer. El uso de las telecomunicaciones orientadas a la seguridad de la información debe ser la base para fomentar el desarrollo y la innovación, de esta forma se promueve una cultura de ciberseguridad que beneficia los intereses de la nación y protege a la ciudadanía.

---

[3] EXPANCIÓN. Anonymous ataca al gobierno de Colombia. 11 de abril de 2012.Disponible en https://expansion.mx/tecnologia/2012/04/11/anonymous-ataca-al-gobierno-de-colombia

[4] EL UNIVERSO. Hackean portal del gobierno de Colombia a 4 días del plebiscito.28 de septiembre de 2016. Disponible en https://www.eluniverso.com/noticias/2016/09/28/nota/5827507/hackean-portal-gobierno-colombia-4-dias-plebiscito/

1.2 FORMULACIÓN DEL PROBLEMA

Actualmente el gobierno colombiano avanza en la inclusión de la ciberseguridad dentro de las políticas públicas y los planes de desarrollo de las distintas entidades gubernamentales. Sin embargo, se hace necesario fortalecer la cultura de ciberseguridad para que se atienda con más entusiasmo las necesidades de seguridad informática en las instituciones de orden público.

Lo anterior implica comprender la importancia de contar con profesionales en hacking que supervisen, monitoreen y mejoren de forma continua los esquemas de ciberseguridad de las organizaciones gubernamentales de Colombia. En consecuencia, los órganos administrativos deben adquirir consciencia sobre los riesgos de sufrir ciberataques por intrusión y las consecuencias que estos pueden acarrear para los interés políticos, sociales y económicos del país.

A partir de la problemática descrita es posible consolidar la pregunta de investigación asociada al presente trabajo:

¿Qué ventajas implica la contratación de profesionales TI especializados en hacking, para las entidades de orden gubernamental en Colombia?

2 JUSTIFICACIÓN

El desarrollo de la presente investigación permite sustentar desde un punto de vista objetivo, la importancia del hacking en la gestión de recursos TI para el fortalecimiento del esquema de ciberseguridad en entidades estatales de Colombia.

A medida que se desarrolla la investigación es posible reconocer las serias implicaciones que han tenido los ciberataques en Colombia. Así mismo, es posible identificar el valor añadido que proporciona un" hacker" como miembro del equipo TI corporativo, profundizando en el caso de las entidades públicas colombianas.

En este orden de ideas, la presente investigación promueve una visión real de la ciberseguridad en entidades gubernamentales, consolidando recomendaciones y perfiles profesionales que permiten robustecer el esquema de seguridad informática, orientando las entidades públicas hacia el desarrollo y el aumento considerable de eficiencia en los procesos relacionados directamente con los intereses de la nación.

La presente monografía promueve la innovación en el sector público colombiano, y justifica la inclusión de procesos TI asociados al hacking como herramientas útiles para robustecer la defensa nacional y salvaguardar los activos del estado en un entorno digital. Las ideas consolidadas apuntan a la transformación de la gestión pública, convirtiendo al estado colombiano en un agente capaz de proveer confianza y proteger la integridad de sus recursos en ambientes electrónicos.

Las conclusiones obtenidas a partir de la presente investigación reafirman la importancia de formar y emplear profesionales en hacking que, desde la aplicación ética de sus habilidades, permitan contrarrestar intentos de delitos informáticos o eventos fortuitos de pérdida de información. Esta premisa se entiende como un llamado a las entidades de orden público en Colombia a tomar acciones frente a los posibles riesgos que implica el avance de la tecnología, con el fin de brindar confiabilidad al uso de nuevas herramientas que facilitarán las operaciones de la gestión pública.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar la importancia del hacking en la ciberseguridad a nivel organizacional en entidades de orden público en Colombia, mediante una revisión en fuentes bibliográficas especializadas con el fin de proponer recomendaciones que permitan fortalecer la gestión de la seguridad de la información, evidenciando la necesidad de vincular expertos en el área.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar las necesidades en Ciberseguridad a nivel organizacional en entidades de orden público en Colombia, con base al análisis de los antecedentes relacionados a ataques informáticos con el fin de reconocer la existencia de aspectos mejorables.

- Establecer la importancia del hacking a nivel organizacional en entidades de orden público en Colombia mediante una revisión en fuentes bibliográficas especializadas para distinguir las ventajas que implica el proceso en cuanto a la creación de un esquema de ciberseguridad.

- Proponer recomendaciones que permitan fortalecer la gestión de la seguridad de la información en entidades de orden público en Colombia con base a lineamientos y directrices relacionados con el área resaltando la necesidad de contar con más profesionales expertos en ciberseguridad.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Importancia del hacking en la ciberseguridad en las entidades de orden público. En la actualidad, las empresas y los gobiernos buscan orientar su funcionamiento hacia una constante evolución, con el fin de ser más competitivos y eficientes a la hora de ejecutar sus procesos. Está necesidad conlleva una permanente preocupación por asegurar los datos y la información que se almacena.

Este proceso de aseguramiento implica varias ventajas organizacionales como son la protección de políticas propias, el aseguramiento de data sensible, la obtención de confianza por parte de usuarios y finalmente un esfuerzo constante por utilizar mecanismos y tecnologías eficientes y actualizados.

Para lograr este objetivo es importante definir un modelo de gobernanza TI, el cual reconozca la importancia de la ciberseguridad como elemento indispensable para la gestión efectiva de los recursos TI en coherencia con las metas organizacionales.

El hacking es una rama importante del conocimiento en ciberseguridad y se centra en la búsqueda y explotación de vulnerabilidades de un sistema. Coloquialmente se asocia el término “hacker” con un ciberdelicuente; sin embargo, un “hacker” en realidad es aquella persona con suficientes conocimientos en seguridad informática, como para detectar y promover soluciones a debilidades que se encuentran en los sistemas de información.

En consecuencia, un “hacker” es la persona encargada de respaldar los sistemas de información generando constantemente mecanismos de protección y recomendaciones para salvaguardar la infraestructura TI de una organización.

A nivel gubernamental, la importancia del hacking como herramienta para contrarrestar posibles ciberataques, adquiere una importancia más alta, debido a que los sistemas y la data que se protege están directamente relacionados con el bienestar público y los intereses de la nación.

Sin embargo, para el caso del gobierno colombiano, la determinación de un equipo de profesionales hacking en las entidades de orden público no ha tomado la suficiente fuerza, principalmente por un desconocimiento de los riesgos y daños que

pueden tener lugar a nivel de ciberseguridad. Es importante que los órganos directivos de entidades gubernamentales comprendan la necesidad de protegerse de los ciberataques con objetivos como hurto de información, daño de los sistemas, alteración de la data o espionaje; debido a que este tipo de intrusiones pueden originar escenarios nefastos para el bienestar general de la nación.

Con el ánimo de prevenir situaciones críticas en materia de seguridad informática, un “hacker” es responsable de evaluar y monitorear de forma constante los sistemas de la entidad, así como de mantener actualizada la infraestructura y tecnologías que se utilizan. Estos procesos se ejecutan de forma periódica a través de pruebas de intrusión o Pentesting.

El pentesting no es más que una prueba de forma ordenada, ejecutada por un grupo de profesionales TI a partir de una metodología predefinida, en la cual se busca comprometer la seguridad de un sistema con el fin de emitir un diagnóstico asertivo de vulnerabilidades que permita promover la mejora del esquema de ciberseguridad.

A partir de una correcta ejecución de pruebas de testing, es posible atribuir a la organización un valor de confiabilidad en materia TI. De esta forma no solo se logra la protección de la información y los sistemas del gobierno colombiano, sino que además se fomenta la formación de profesionales orientados al hacking, como miembros útiles para garantizar la eficiencia de las entidades públicas.

4.1.1 Efectos negativos de la no inclusión de la Seguridad informática adecuada en las organizaciones de orden público. Al ignorar los riesgos existentes y no tomar medidas oportunas, pueden tener lugar ciberataques con efectos desastrosos sobre la gestión pública nacional. En las entidades públicas es de alta relevancia prestar atención a este tipo de necesidades, con el fin de salvaguardar los intereses y activos de la nación.

Inicialmente, es posible reconocer un efecto negativo sobre la privacidad de información clasificada del gobierno colombiano. Las entidades de orden público en Colombia consolidan y publican un índice de información donde se diferencian los datos que son abiertos al público y los datos que son reservados.

Entre los datos reservados se encuentran resultados de auditorías y procesos de evaluación estatales, estrategias y lineamientos militares, histórico de procesos disciplinarios e investigaciones, disposición de recursos, entre otros.[5] Exponer este tipo de información se considera perjudicial debido a su alta sensibilidad y la

[5] MINTIC. Índice de información clasificada y reservada [sitio web] Colombia. Consulta realizada el 2 de septiembre del 2021. Disponible en https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135889:Indice-de-informacion-clasificada-y-reservada

posibilidad de utilizarse para manipular procesos estatales o incluso con fines terroristas.

Un segundo punto importante, es el efecto negativo asociado directamente a la capacidad de progreso e innovación en el sector tecnológico colombiano. La realización de pruebas de intrusión y evaluación de vulnerabilidades sobre los sistemas de información obliga a los administradores de sistemas a considerar la implementación de tecnologías más actuales con el fin de solventar vulnerabilidades y no generar sistemas obsoletos.

En este orden de ideas, la no preocupación por consolidar une esquema de ciberseguridad eficiente basado en identificación asertiva de riesgos, orienta a las entidades de orden público a quedar obsoletas, debido al uso de tecnologías no consideradas como eficientes en el mercado, generando una exposición de los recursos y activos de información.

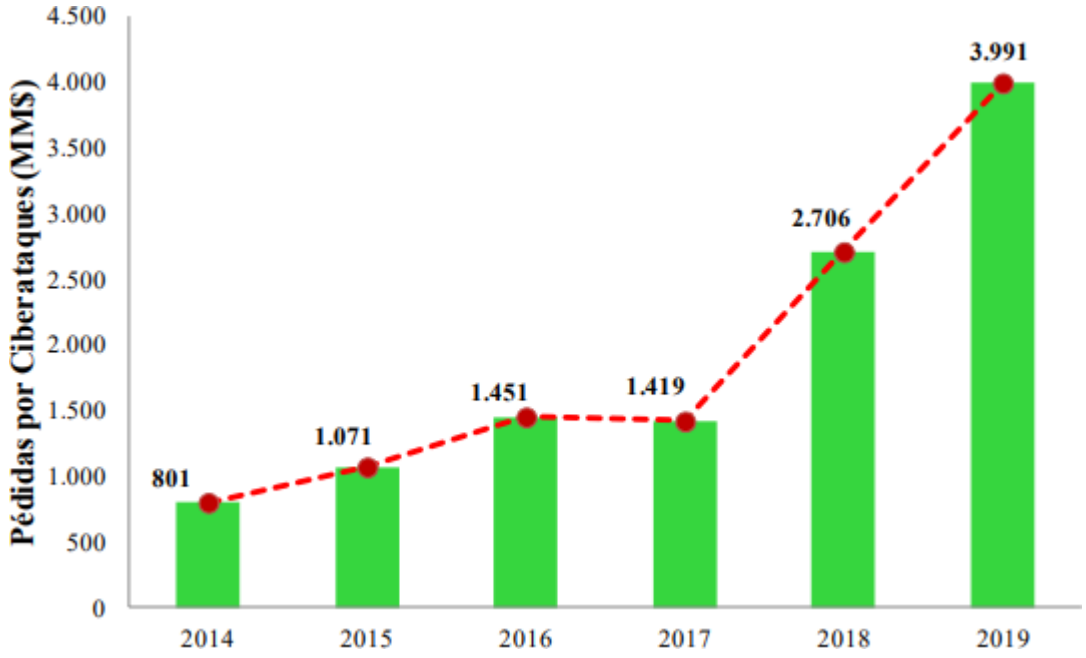
Finalmente, un último efecto negativo que vale la pena mencionar es el asociado con la confiabilidad que la ciudadanía y organizaciones internacionales perciben sobre las entidades de orden público en Colombia.

La gestión pública presenta evidencias de su labor tanto a la ciudadanía como a organismos de control internacional, con el fin de mantener un concepto de transparencia y generar una supervisión de procesos y métodos ejecutados. Al momento de presentar una gestión pública que carece de consideraciones y medidas eficientes asociadas a la ciberseguridad, se pone en evidencia una negligencia administrativa.

Actualmente, la ciberseguridad debe por obligación ser un tema de alto interés para los estados; de no ser así se producirá un incremento de cibercrimenes y eventos siniestros que afecten directamente los intereses de la nación. En consecuencia, se verá cuestionada la capacidad del estado y de las entidades públicas de realizar eficazmente sus funciones.

Así mismo, se genera un decremento de la cultura de ciberseguridad a nivel general, evento que repercute directamente sobre la economía de las naciones. IC3 (Internet Crime Complaint Center) genera anualmente un reporte de fraudes y crímenes cibernéticos y sus efectos a nivel mundial, para el año 2019 (año nefasto para la ciberseguridad mundial a raíz de la situación de pandemia) como se aprecia en la Ilustración 1, se registraron cerca de medio millón de delitos informáticos reportados, los cuales generaron pérdidas por más de 3000 mil millones de dólares.

Ilustración 1. Reporte pérdidas anuales por ciberdelitos a nivel mundial



Fuente. IC3. Internet Crime Report. 2019. Disponible en https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

Lo anterior evidencia un efecto altamente nocivo asociado un déficit de ciberseguridad. Se destaca la importancia de robustecer las capacidades de mitigación de riesgos y respuesta frente a ciberataques por parte de entidades gubernamentales, con el fin de proveer confiabilidad y bienestar sobre la información y los recursos que se administran.

4.1.2 Necesidades de implementación de un esquema de ciberseguridad que respalde procesos en TI en organizaciones de orden público. En primer lugar, es importante reconocer que el estado colombiano es un estado social de derecho organizado en forma de Republica Unitaria. Se divide en tres ramas del poder (ejecutiva, legislativa y judicial) y adicionalmente posee organismos de control independientes (Procuraduría, Contraloría, entre otros).

De otra parte, en Colombia se entiende por entidad estatal a toda aquella institución con personería jurídica creada por constitución, ley, ordenanza o acuerdo, o autorizadas por estas, que tengan participación pública donde se cumpla una función administrativa, comercial o industrial.

En este orden de ideas, es posible afirmar que en Colombia existe una amplia variedad de entidades públicas en cada uno de los sectores, las cuales puedes ser diferenciadas por su función y alcance. Se encuentran desde los Ministerios hasta

las entidades adscritas y organismos de control. Todas y cada una de estas entidades presentan un esquema organizacional y una asignación presupuestal para infraestructura TI y contratación de profesionales de las TIC.

Las tecnologías de la información y la comunicación juegan un papel importante en las entidades públicas, a tal grado que se consolida una oficina de tecnologías de la información mediante la cual se pretende gerenciar los servicios TI y alinearlos a los objetivos institucionales para alcanzar el cumplimiento de la misión.

Para lograr tal objetivo, la oficina de tecnologías o área de telecomunicaciones debe ofrecer a su entidad una serie de servicios útiles y comunes a cualquier tipo de institución o sector:

- Gestión de TI
- Atención de mesa de servicio
- Sistemas de información
- Gestión de Cambios
- Provisión de equipos
- Intercambio de datos con entidades de control
- Seguridad de la información

Los servicios mencionados, a pesar de ser citados de forma independiente, llevados a la práctica presentan una constante cooperación. Sin embargo, se destaca la seguridad de la información como un proceso transversal a todos los servicios, mediante el cual se garantiza el cumplimiento eficiente del objetivo de cada uno de ellos.

Esto significa que la implementación de un esquema de ciberseguridad que respalde cada proceso, garantiza el uso seguro y aprovechamiento de los recursos TI, reduciendo el riesgo a sufrir pérdidas de información, daños de activos o sistemas comprometidos por cualquier tipo de ciberataque.

De esta forma es posible asegurar que toda entidad estatal en Colombia requiere contar con un grupo de profesionales TI orientados a la ciberseguridad, que, mediante conocimiento avanzado de hacking e intrusión, propongan una estrategia de seguridad efectiva a partir de la cual sea posible:

- Garantizar la integridad, disponibilidad y confidencialidad de la información.
- Establecer una categorización de los activos de información de la empresa
- Establecer una estrategia que mitigación de riesgos en materia de ciberseguridad.
- Establecer políticas de prevención y procesos que promuevan la seguridad informática en la entidad.
- Establecer un consolidado de riesgos estimados para la entidad y sus activos

- Establecer un plan de respuesta a posibles incidentes que se presenten en materia de ciberseguridad.

4.2 MARCO CONCEPTUAL

4.2.1 Ciberseguridad. Inicialmente es importante reconocer que el concepto de ciberseguridad hace referencia a la práctica asociada a la defensa de dispositivos tecnológicos y a los datos que se gestionan sobre ellos. [6]

En el conjunto de dispositivos TI se encuentra una amplia variedad de elementos como computadoras, dispositivos móviles, servidores, sistemas de vigilancia, entre otros. Así mismo, los datos y la información por lo general están clasificados y se le asignan diferentes niveles de criticidad.

En consecuencia, la ciberseguridad se aplica a distintos niveles, depende del tipo de dispositivo y la data que se busque proteger.

- Ciberseguridad a nivel de red: seguridad asociada a asegurar el tráfico y los dispositivos intermedios como enrutadores y switches.
- Ciberseguridad a nivel de aplicación: seguridad asociada a asegurar los servidores de aplicación y entornos accesibles de dispositivos de usuario final.
- Ciberseguridad a nivel de base de datos: seguridad asociada a proteger la integridad confidencialidad y disponibilidad de los datos almacenados sobre una base.
- Ciberseguridad a nivel operativo: seguridad asociada a los procesos y decisiones consolidadas en cuanto a la gestión y uso de recursos TI.
- Ciberseguridad a nivel de usuario final: Seguridad asociada a capacitar y proveer medios de notificación a los usuarios finales de los sistemas, comúnmente reconocidos como el eslabón más débil en un esquema de ciberseguridad.

4.2.2 Amenazas, riesgos y vulnerabilidades. Un esquema de ciberseguridad busca consolidar un conjunto de reglas y procesos, cuyo fin es generar una estructura de prevención y respuesta contra amenazas identificadas con base a los activos. Un activo es aquel recurso tangible o intangible que posee un valor para la

[6] KASPERSKY. ¿Qué es la ciberseguridad? [sitio web]. Colombia. Consulta realizada el 28 de junio de 2021. Disponible en https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

organización y/o el usuario. En consecuencia, los activos son identificados, valorados, e inventariados. [7]

Se hace necesario reconocer tres conceptos importantes que complementan la idea expuesta sobre el objetivo de un esquema de ciberseguridad:

- Amenaza: Es el evento puntual identificado, el cual en caso de ocurrir puede desencadenar un incidente y perjudicar a la organización y/o a los usuarios de un sistema.

- Riesgo: Es la posibilidad calculada de que una amenaza se materialice y genere un evento siniestro sobre el sistema.

- Vulnerabilidad: es la debilidad asociada a un activo, la cual puede ser explotada de forma que se identifique una amenaza sobre la cual puedan cometerse agresiones.

4.2.3 Hacking. Muy asociado a la gestión de ciberseguridad, se encuentra el termino de hacking y el termino puntual hacking ético. Hacking es el conjunto de prácticas que implican el análisis de sistemas de información con fin de reconocer vulnerabilidades que puedan ser explotadas por un atacante. [8]

Hacking ético especifica el uso de estas prácticas de forma autorizada y con el único fin de solventar la vulnerabilidad detectadas para hacer más seguro el sistema. El hacking permite reconocer mediante pruebas de intrusión y testing, el nivel de seguridad con el que cuenta un sistema, específicamente cuales son las vulnerabilidades y su nivel de criticidad, y las posibles soluciones que solventen estas amenazas.

El hacking es un campo del conocimiento que recientemente ha adquirido importancia a nivel organizacionales y estatal, de modo que los gobiernos y empresas buscan auditar sus sistemas de información con el fin de identificar falencias de seguridad y poder protegerse contra ellas.

---

[7] CASTRO BOLAÑOS Duvan, ROJAS MORA Ángela. Riesgos, amenazas y vulnerabilidades de los sistemas de información geográfica. Trabajo de grado. Universidad Católica de Colombia. 2013.pp 25-26

[8] IONOS. Ethical hacking: solucionar fallos de seguridad y prevenir la cibercriminalidad [sitio web] Ionos digital guide. 2020. Consulta realizada el 2 de diciembre de 2021. Disponible en https://www.ionos.es/digitalguide/servidores/seguridad/que-es-el-ethical-hacking/

4.2.4 Entidad de orden público colombiana. En primer lugar, es importante reconocer que el estado colombiano es un estado social de derecho organizado en forma de Republica Unitaria. Se divide en tres ramas del poder (ejecutiva, legislativa y judicial) y adicionalmente posee organismos de control independientes (Procuraduría, Contraloría, entre otros).[9]

En Colombia se entiende por entidad estatal a toda aquella institución con personería jurídica creada por constitución, ley, ordenanza o acuerdo, o autorizadas por estas, que tengan participación pública donde se cumpla una función administrativa, comercial o industrial. [10]

En este orden de ideas, es posible afirmar que en Colombia existe una amplia variedad de entidades públicas en cada uno de los sectores, las cuales puedes ser diferenciadas por su función y alcance. Se encuentran desde los Ministerios hasta las entidades adscritas y organismos de control. Todas y cada una de estas entidades presentan un esquema organizacional y una asignación presupuestal para infraestructura TI y contratación de profesionales de las TIC.

4.2.5 Oficina de tecnologías de la información. Las tecnologías de la información y la comunicación juegan un papel importante en las entidades públicas, a tal grado que se consolida una oficina de tecnologías de la información mediante la cual se pretende gerenciar los servicios TI y alinearlos a los objetivos institucionales para alcanzar el cumplimiento de la misión.

Para lograr tal objetivo, la oficina de tecnologías o área de telecomunicaciones debe ofrecer a su entidad una serie de servicios útiles y comunes a cualquier tipo de institución o sector:

- Gestión de TI
- Atención de mesa de servicio
- Sistemas de información
- Gestión de Cambios
- Provisión de equipos
- Intercambio de datos con entidades de control
- Seguridad de la información

---

[9] LA ENCICLOPEDIA - RED CULTURAL DEL BANCO DE LA RÉPUBLICA. Estructura del Estado Colombiano. [sitio web]. Colombia. Consulta realizada el 12 de noviembre del 2021. Disponible en https://enciclopedia.banrepcultural.org/index.php/Estructura_del_Estado_colombiano#:~:text=El%20Estado%20colombiano%20est%C3%A1%20organizado,ejecutiva%20y%20la%20rama%20judicial.

[10] FUNCIÓN PÚBLICA. Glosario [sitio web] Colombia. Consulta realizada el 5 de noviembre de 2021. Disponible en https://www.funcionpublica.gov.co/glosario/-/wiki/Glosario+2/Entidad+Estatal

Los servicios mencionados, a pesar de ser citados de forma independiente, llevados a la práctica presentan una constante cooperación. Sin embargo, se destaca la seguridad de la información como un proceso transversal a todos los servicios, mediante el cual se garantiza el cumplimiento eficiente del objetivo de cada uno de ellos.

Esto significa que la implementación de un esquema de ciberseguridad que respalde cada proceso, garantiza el uso seguro y aprovechamiento de los recursos TI, reduciendo el riesgo a sufrir pérdidas de información, daños de activos o sistemas comprometidos por cualquier tipo de ciberataque.

De esta forma es posible asegurar que toda entidad estatal en Colombia requiere contar con un grupo de profesionales TI orientados a la ciberseguridad, que, mediante conocimiento avanzado de hacking e intrusión, propongan una estrategia de seguridad efectiva a partir de la cual sea posible:

- Garantizar la integridad, disponibilidad y confidencialidad de la información.
- Establecer una categorización de los activos de información de la empresa
- Establecer una estrategia que mitigación de riesgos en materia de ciberseguridad.
- Establecer políticas de prevención y procesos que promuevan la seguridad informática en la entidad.
- Establecer un consolidado de riesgos estimados para la entidad y sus activos
- Establecer un plan de respuesta a posibles incidentes que se presenten en materia de ciberseguridad.

4.3 MARCO HISTÓRICO

En 2016, Colombia adopta una nueva política de ciberseguridad cuyo objetivo es fortalecer la capacidad del estado para responder oportunamente a las amenazas y ciberataques. Se crea el Comité de Seguridad Digital dirigido por el coordinador Nacional de Seguridad Digital. Por primera vez la política de seguridad digital es incluida como parte integral de la operación estratégica de las entidades públicas y privadas.

Así mismo Colombia cuenta con:

- El Ministerio de Tecnología y las Comunicaciones el cual tiene desplegado a nivel nacional el modelo de seguridad y privacidad para apoyar la implementación de buenas prácticas y estándares que protejan los activos de información, infraestructura TI y sistemas de información.

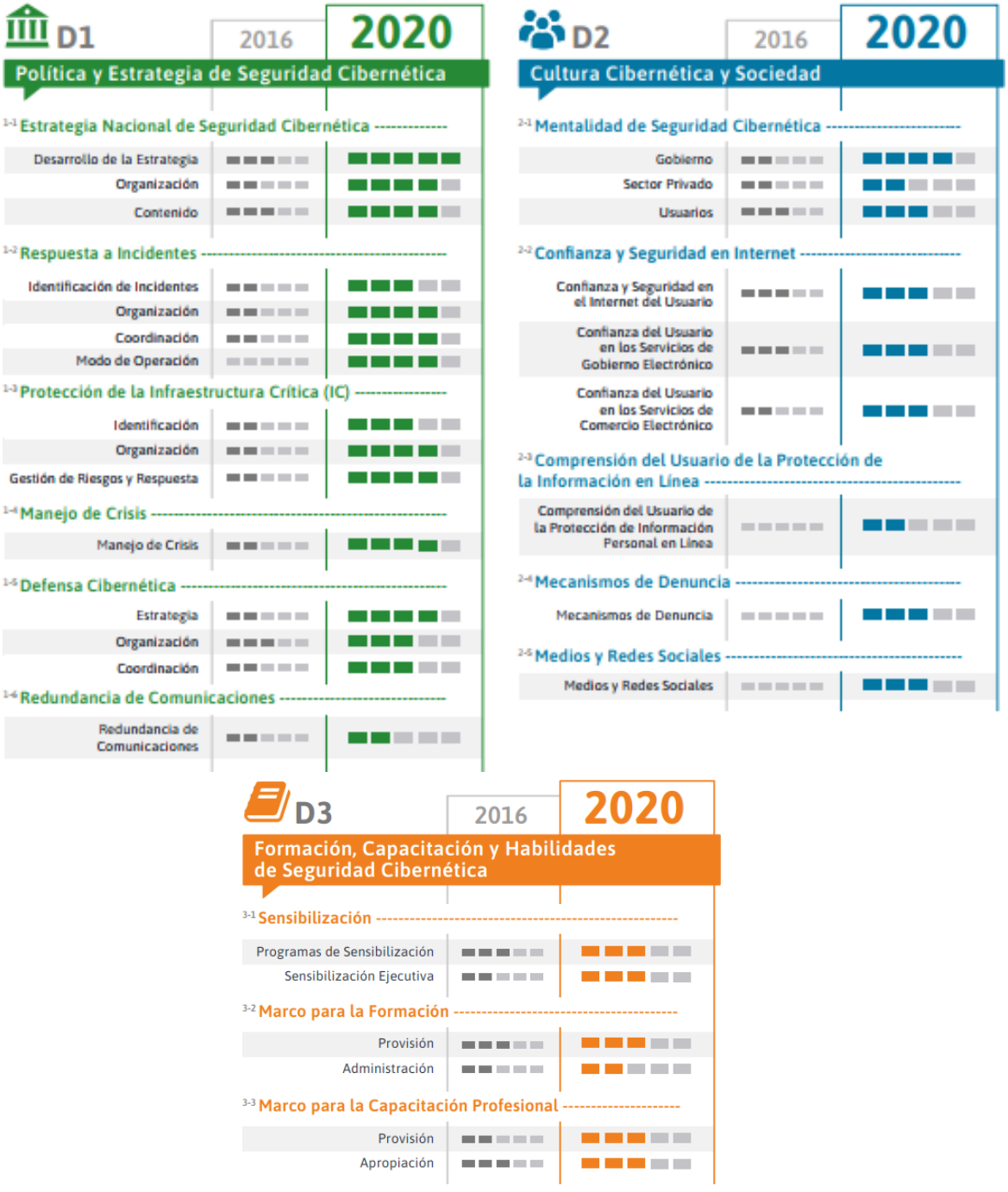
- EL ColCERT el cual es el equipo nacional de respuesta a incidentes de ciberseguridad. Uno de los CSIRT gubernamentales implementado por el Ministerio de Defensa para la centralización, documentación y atención a ciberataques que atentes contra intereses de la nación.

- El “Programa para la mejora de la conectividad y digitalización de la economía”. Estrategia aprobada en 2018, que concreta iniciativas de fortalecimiento de las capacidades nacionales en ciberseguridad.

Referente a temas de formación, los colombianos tienen la posibilidad de formarse en programas de pregrado y postgrado relacionados a TI y ciberseguridad. Así mismo, el MINTIC patrocina la formación en esta área mediante la entrega de becas educativas, campañas gratuitas educativas dirigidas a la población y la promoción de cursos y capacitaciones en ciberseguridad.

En el año 2020 el BID y la OEA publican su más reciente estudio respecto al desarrollo en materia de ciberseguridad en América Latina. En este documento se analiza el progreso de Colombia en materia de seguridad informática mediante cinco indicadores principales desglosados en varios datos de progreso cuantificados. Este análisis nos permite reconocer una tendencia de nivel medio en el perfeccionamiento de los procesos. Los datos en mención se consolidan en un reporte gráfico con indicadores de progreso, el cual es mostrado en la Ilustración 2.

Ilustración 2. Reporte indicadores ciberseguridad América Latina - Colombia



Fuente. CIBERSEGURIDAD Riesgos, Avances y el camino a seguir en América Latina y el Caribe. 2020. BID-OEA. [sitio web] Consulta realizada el 28 de abril de 2021. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Del reporte mostrado es importante reconocer que se tienen puntuaciones de nivel medio y alto en ítems asociados a diseño de estrategias, generación de cultura y legislación, lo cual es bastante favorable. Sin embargo, las puntuaciones más bajas son apreciables en la sección D5. ESTÁNDARES, ORGANIZACIONES Y TECNOLOGÍAS, donde se ubican los ítems directamente asociados a la calidad en soluciones reales implementadas.

Este hecho permite afirmar que, si bien se tiene iniciativas y estrategias orientadas a fortalecer y documentar lo relacionado a ciberseguridad, falta la consolidación de proyectos y la implementación de soluciones con el fin de culminar de forma contundente los procesos de planeación que se llevan a cabo. Mejorar los indicadores mencionados en la sección D5 implica directamente destinar más recursos y preparar a más profesionales en la materia, de esta forma se alcanzarán metas tangibles y se elevarán los indicadores asociados a soluciones ya efectuadas.

4.4 ESTADO ACTUAL

En el presente año 2021, la rigurosidad a nivel de ciberseguridad se ha hecho muy necesaria. Este hecho está directamente relacionado al escenario de pandemia actual que se vive a causa del virus COVID-19; evento que ha desencadeno una reforma a la metodología de trabajo en las entidades públicas y privadas, llevando la mayoría de operaciones a plataformas de teletrabajo.

Este fenómeno ha originado un escenario propicio para los ciberdelicuentes, donde es posible realizar ataques y desplegar actividades ilícitas a un mayor número de entornos digitales empresariales. En la Tabla 1 se relaciona el ranking de puntaje asociado a nivel de ciberseguridad por naciones establecido por la UIT donde se aprecia a Colombia entre las primeras posiciones de América Latina; sin embargo, es un posicionamiento muy lejano de los países con puntaje más alto a nivel mundial.

Tabla 1. Posicionamiento puntaje de ciberseguridad por país

Americas region

Member State	Score	Regional Rank	Global Rank
United States of America*	0.926	1	2
Canada*	0.892	2	9
Uruguay	0.681	3	51
Mexico	0.629	4	63
Paraguay	0.603	5	66
Brazil	0.577	6	70
Colombia	0.565	7	73
Cuba	0.481	8	81
Chile	0.470	9	83
Dominican Republic	0.430	10	92
Jamaica	0.407	11	94
Argentina	0.407	11	94

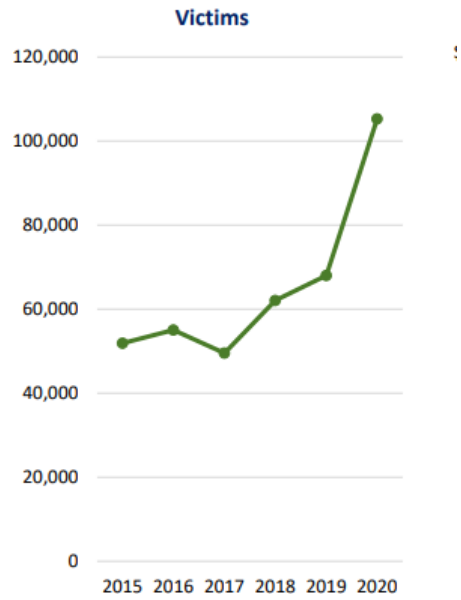
Fuente: La ciberseguridad según la ITU. 2019. Alejandro Barros [en línea] Consulta realizada el 28 de abril de 2021. Disponible en: https://www.alejandrobarros.com/la-ciberseguridad-segun-la-itu/

Al posicionamiento del país en materia de ciberseguridad, se suma la situación de pandemia presentada a nivel mundial a partir de marzo del año 2019, donde la mayoría de empresas y entidades asumieron forzosamente un modelo de trabajo en casa.

Para el caso de las entidades de orden público, esta situación generó un replanteamiento de procesos y modalidad de operación, donde el uso de plataformas online y herramientas de videoconferencia se hicieron indispensables. A pesar de que poco a poco se está retornando hacia una normalidad, la modalidad de trabajo en entidades públicas cambió de forma definitiva, y actualmente apunta hacia un modelo dual donde el teletrabajo será utilizado por al menos el 40% de los empleados, de acuerdo a un estudio realizado por Gamma Ingenieros en 2020. [11]

Esta reforma al modelo de trabajo, origina un crecimiento considerable de las víctimas de cibercrimenes y los delitos informáticos reportados. IC3 (Internet Crime Complaint Center) genera anualmente un reporte del número de víctimas de ciberdelitos reportados, la ilustración 3 muestra que para el año 2019 y 2020 se produjo un crecimiento que duplica la tendencia en años anteriores.

Ilustración 3. Registro crecimiento de victimas de cibercrimenes reportados



Fuente. IC3. Internet Crime Report. 2020. Disponible en https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf

En consecuencia, la necesidad de implementar soluciones en seguridad ha incrementado, en la medida que han incrementado los riesgos y posibles vulnerabilidades sobre los sistemas y activos de información de las entidades públicas. A partir de esta situación es posible concluir que la identificación de

[11] VARGAS RUBIO, Paola Andrea. La demanda de los servicios de ciberseguridad se incrementó 40% a nivel nacional. La Republica. 2020.

vulnerabilidades mediante el uso de pruebas de intrusión y testing sobre los sistemas, nunca fue más necesaria.

Entonces, al interior de las entidades públicas colombianas se refleja la necesidad de contar con profesionales en ciberseguridad con conocimientos en Hacking que determinen estrategias y planes de acción que atiendan las necesidades e intereses de la empresa, al mismo tiempo que promueven el cumplimiento de los objetivos organizacionales.

Actualmente las entidades públicas en Colombia son autónomas para la definición de la necesidad de contratar profesionales en materia de ciberseguridad, esto adicional a los cargos de planta que sean definidos para tal fin.

En este orden de ideas, la rigurosidad y determinación de esquemas de ciberseguridad está directamente relacionada con profesionales capacitados, los cuales deben ser reconocidos como “necesarios” por los directivos que aprueban la contratación en cada entidad pública.

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

A nivel técnico es preciso enmarcar el desarrollo de la presente investigación, centrándose principalmente en las funciones atribuidas a un profesional en hacking dentro de una entidad pública colombiana, a partir de lo cual sea posible analizar como la ejecución efectiva de estas funciones implica una ventaja significativa al desarrollo y misionalidad de cualquier institución gubernamental.

En primer lugar, es importante reconocer que el hacking no es una actividad ilegal siempre y cuando se haga bajo el permiso del dueño del sistema y sea con fines de mejora a nivel de ciberseguridad. Un profesional en hacking está en la capacidad de emitir un diagnóstico efectivo a nivel empresarial, a partir del cual puede diseñar e implementar estrategias de prevención y gestión de incidentes que fortalezcan la capacidad de la organización de sobreponerse a las indiscutibles amenazas cibernéticas a las que se está expuesto en el mundo digital y el ciberespacio. Este conjunto de políticas y directrices que rigen la ciberseguridad al interior de una organización se conoce como Sistema de Gestión de la Seguridad de la Información (SGSI).

Todos los días, los ciberdelicuentes o piratas informáticos están en la constante búsqueda de nuevos mecanismos para la vulneración de sistemas de información. El campo de acción de un hacker, se define como una constante batalla entre WHITE HACKERS y BLACK HACKERS en las cuales se pretende identificar vulnerabilidades y posibles formas de atacarlas, con el fin de tomar acciones frente a estos hallazgos.

Es importante reconocer que un ciberataque es todo aquel conjunto de pasos ejecutados con el fin de hurtar, dañar o alterar de forma abusiva la data o el funcionamiento de sistemas de información. Es posible reconocer diferentes tipos de ataques, los cuales pueden ser prevenidos mediante el estudio riguroso del estado actual de la compañía y la implementación de un SGSI.

IC3 (Internet Crime Complaint Center) consolida anualmente los datos de ciberdelitos reportados y los clasifica de acuerdo a su naturaleza, de esta forma es posible reconocer aquellas modalidades y ataques que ocurren con mayor frecuencia sobre los usuarios y organizaciones, como se muestra en la Tabla2. Adicionalmente es posible percibir el comportamiento del incremento de cada uno de estos ciberdelitos en el transcurso del tiempo (2018,2019,2020)

Tabla 2. Comparación tipos de cibercrimenes reportados.

Crime Type	2020	2019	2018
Advanced Fee	3,008	4,038	3,988
BEC/EAC	3,530	3,792	3,174
Charity	105	72	114
Civil Matter	170	150	130
Confidence Fraud/Romance	6,817	5,871	5,492
Corporate Data Breach	285	133	311
Credit Card Fraud	3,195	2,716	2,841
Crimes Against Children	58	31	42
Denial of Service/TDos	52	40	48
Employment	1,867	1,670	1,873
Extortion	23,100	12,242	13,600
Gambling	16	28	19
Government Impersonation	4,159	4,038	2,983
Hacktivist	5	2	15
Health Care Related	243	72	77
IPR/Copyright and Counterfeit	552	287	260
Identity Theft	7,581	2,744	2,644
Investment	1,062	612	583
Lottery/Sweepstakes/Inheritance	3,774	2,764	2,607
Malware/Scareware/Virus	287	622	813
Misrepresentation	4,735	768	718
Non-Payment/Non-Delivery	14,534	7,731	7,328
Other	3,259	3,340	2,610
Overpayment	2,196	2,913	3,005
Personal Data Breach	6,121	6,725	10,439
Phishing/Vishing/Smishing/Pharming	7,353	5,383	5,368
Ransomware	365	337	276
Re-shipping	114	141	118
Real Estate/Rental	1,882	1,754	1,539
Spoofing	7,279	6,260	2,497
Tech Support	9,429	6,781	6,731
Terrorism/Threats of Violence	1,699	1,941	2,217

Fuente. IC3. Internet Crime Report. 2020. Disponible en https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf

Con el ánimo de contextualizar y reconocer más oportunamente las conductas asociadas a los ciberdelitos, se procede a definir de forma simple y precisa algunos conceptos necesarios:

Malware. Software malicioso que tras su ejecución desencadena una serie de daños a la data del equipo asociado, o bien permite el acceso del atacante a información confidencial almacenada.

Ransomware. Tipo de malware el cual pretende inhabilitar el uso de un sistema o restringir el acceso a la data de un usuario, de modo que el atacante pasa a tener control sobre los activos de información. En consecuencia, el atacante extorsiona a la víctima mediante el secuestro de la información.

Spyware. Un tipo de malware cuyo objetivo es actuar de manera silenciosa mientras provee a los atacantes de información sensible sin que el usuario se dé cuenta. Entre los spyware es posible reconocer sistemas de cámara espía o KEYLOGGERS (software que almacena como texto todas las pulsaciones que el usuario hace en el teclado)

Phishing. Conducta fraudulenta asociada al engaño de usuarios mediante interfaces falsas, medios de comunicación directos y suplantación de identidad, como mecanismo para manipular a la víctima y que está suministre información privada o bien ejecute alguna acción beneficiosa para el atacante.

Ciberterrorismo. Es la manipulación de medios digitales de comunicación y publicación de contenido, para promover el miedo colectivo y el pánico general en una población específica.

Denegación de Servicio (DoS). Forma de ataque donde la máquina o servicio objetivo son desactivados o deshabilitados. Se busca entorpecer el correcto funcionamiento de un sistema con el fin de explotar otra vulnerabilidad o afectar a los usuarios o dueños del servicio.

Suplantación de identidad (spoofing). Conducta fraudulenta donde le atacante se apropia de la identidad digital de un individuo con el fin de efectuar operaciones nocivas para el sistema o hurto, de forma incógnita. Puede darse mediante la simulación, clonación o hurto de credenciales o identificadores digitales.

Virus informático. Es un sistema informático malicioso, que se instala sobre un objetivo sin previa autorización y genera una alteración de su funcionamiento o de la data que este almacena. Es un tipo de malware diseñado para dañar la integridad de un equipo o sistema.

4.6 MARCO LEGAL

Con el fin de definir un marco legal relacionado a la presente investigación se hace necesario citar las leyes, decretos y normativas mediante las cuales se han regulado los temas de ciberseguridad en Colombia.

CONPES 3854 DE 2016 "POLÍTICA NACIONAL DE SEGURIDAD DIGITAL". Este documento plantea la estrategia nacional y consideraciones relacionadas a la seguridad digital, incluyendo la gestión de riesgos como elemento principal. Es un documento publicado por MinTIC, MinDefensa, Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación. El plan de acción relacionado a esta política, es planteado para ejecutarse en los años 2016 al 2019 con una inversión total de 85.070 millones de pesos. Se estimó que para el 2020, la implementación de esta política iba a impactar de forma positiva la economía colombiana y la generación de empleos.[12]

CONPES 3701 DE 2011"LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y DEFENSA". Este documento busca plantear una estrategia nacional para mejorar la capacidad del Estado colombiano de responder oportunamente frente a ciberamenazas. Se analizan las debilidades existentes mediante una revisión de antecedentes nacionales e internacionales. [13]

Se definen recomendaciones específicas para entidades directa o indirectamente relacionadas al campo de ciberseguridad. Y se realiza una necesidad de financiamiento proyectada de forma anual hasta el 2014. Esta proyección se evidencia mediante la tabla 3 cuyos valores mantienen un promedio de 4.107.111.082 COP

Tabla 3. Proyección necesidad de financiamiento realizada en 2011

2011	2012	2013	2014
$ 1.428.444.328	$ 5.400.000.000	$ 5.000.000.000	$ 4.600.000.000

Fuente. Documento CONPES 3701 del 14 de julio de 2011 [sitio web] Consulta realizada el 27 de abril de 2021. Disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

[12] DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES 3854. Bogotá, Colombia. 2016

[13] DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES 3701. Bogotá, Colombia. 2011

LEY 1581 DE 2012 "PROTECCIÓN DE DATOS PERSONALES"

En esta ley se desarrolla el derecho constitucional que tienen todas las personas a conocer y actualizar información sobre ellas que se haya consolidado en archivos y bases de datos.

La ley define aquellos datos considerados como sensibles, es decir que afectan la intimidad del titular y que su uso indebido puede generar discriminación. Adicionalmente se puntualizan los procedimientos y las condiciones para que exista legalidad en el tratamiento de datos personales. Finalmente se enlistan los mecanismos de control y sanciones ocasionadas a partir de incumplimientos relacionados a esta ley. [14]

LEY 1273 DE 2009 "PROTECCIÓN DE LA INFORMACIÓN Y LOS DATOS"

En esta ley se tipifican a detalle los delitos informáticos y las sanciones que implican en el territorio colombiano. Los atentados son clasificados en dos grupos: atentados contra la integridad, confidencialidad y disponibilidad de los datos en sistemas de información; atentados informáticos y otras infracciones.

Esta ley permite reconocer las conductas delictivas y fraudulentas asociadas a entornos cibernéticos, así como aquellas situaciones que implican una agravación punitiva a este tipo de delito. [15]

LEY 1928 DE 2018 "APROBACIÓN CONVENIO SOBRE CIBERDELINCUENCIA"
Mediante esta ley interna se adopta para el estado colombiano el contenido del convenio sobre ciberdelincuencia celebrad en Budapest el 23 de noviembre de 2001.

Este convenio es el primer tratado internacional que busca elaborar una estrategia que contrarreste los cibercrimenes mediante la armonización de leyes concretas entre naciones. Se tratan con especial relevancia los delitos informáticos relacionados a derechos de autor, pornografía infantil, delitos de odio y violación de seguridad en redes.[16]

DECRETO 1008 DE 2018 "POLÍTICA DE GOBIERNO DIGITAL"

Mediante este decreto se especifican los lineamientos generales de la política de gobierno digital, coherente a la estrategia de gobierno en línea, mediante lo cual se pretende el aprovechamiento de las tecnologías de la información y la comunicación

[14] CONGRESO DE COLOMBIA. Ley Estatutaria 1581 de 2012. Colombia. 2012
[15] CONGRESO DE COLOMBIA. Ley Estatutaria 1273 de 2009. Colombia. 2009
[16] CONGRESO DE COLOMBIA. Ley Estatutaria 1928 de 2018. Colombia. 2018

para la generación de un estado competitivo e innovador que generen valor público en un entorno de confianza digital

Las normas y leyes referenciadas se relacionan con la presente investigación ya que suministran una visión de la ciberseguridad como materia de discusión y regulación en el estado colombiano. Es posible reconocer un esfuerzo del gobierno por promover la aplicación de estrategias de ciberseguridad, desde la regulación y análisis de las entidades competentes. [17]

[17] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1008 de 2018. Colombia. 2018

5 DESARROLLO DE LOS OBJETIVOS

5.1 NECESIDADES EN CIBERSEGURIDAD A NIVEL ORGANIZACIONAL EN ENTIDADES DE ORDEN PÚBLICO EN COLOMBIA, CON BASE AL ANÁLISIS DE LOS ANTECEDENTES RELACIONADOS A ATAQUES INFORMÁTICOS CON EL FIN DE RECONOCER LA EXISTENCIA DE ASPECTOS MEJORABLES.

5.1.1 ¿Por qué es necesario preocuparse por la ciberseguridad en las entidades públicas colombianas? En primer lugar, con el ánimo de reconocer la necesidad de las entidades estatales colombianas de robustecer su infraestructura de ciberseguridad, se describe un panorama general de activos de información y sistemas que deben ser protegidos.

5.1.1.1 Información que se gestiona al interior de las entidades públicas colombianas. La data que se gestiona al interior de las entidades públicas en Colombia requiere una especial atención en esta investigación, debido a que parte de estos datos son clasificados como sensibles o reservados, por lo que se justifica la necesidad de implementar estrategias en ciberseguridad que garanticen su disponibilidad, confidencialidad e integridad.

Es importante reconocer que actualmente en Colombia se adopta una ley de transparencia y acceso a la información pública, mediante la cual toda empresa estatal y organismo autónomo está en la obligación de publicar en canales digitales destinados para tal fin, un reporte periódico financiero y administrativo, con el fin de hacer público el acceso a estos datos, promoviendo un principio de honestidad en la ejecución y operación de las entidades. Este hecho implica que información de ejecución de las entidades públicas, como por ejemplo estados financieros, son datos que dejan de considerarse como reservados o confidenciales. [18]

En primera instancia, y común a todas las entidades del sector público, se tiene la información personal y de contacto de sus trabajadores, tanto contratistas como empleados de planta. A nivel de individuo, es considerado como dato sensible a toda información que afecte la intimidad de la persona y puedan conllevar discriminación o riesgos al titular. En este sentido, aplican a esta descripción los datos de contacto, residencia, orientación política, sexualidad, origen racial o étnico, convicciones religiosas, información clínica, afiliaciones sindicales, entre otros.

En segundo lugar, es posible destacar data considerada como sensible o reservada, directamente relacionada al sector y operatividad de las entidades públicas. Para esta descripción aplica información generada o consolidada al interior de una

[18] CONGRESO DE COLOMBIA. Ley Estatutaria 1712 de 2014. Colombia. 2018

entidad estatal, la cual varía de acuerdo a la funcionalidad que cumple la organización[19]. Algunos ejemplos de este tipo de información se consolidan en la Ilustración 4.

Ilustración 4. Tipos de data sensible gestionada en entidades de orden público en Colombia de acuerdo al sector

Sector de Operación	Ejemplo de data sensible relacionada
Arte y Cultura	Datos de poblaciones discriminadas
Vivienda y Territorio	Datos de residencia
Medio Ambiente	Procesos legales para la protección ambiental
Tecnologías de la Información	Datos de patentes e ideas de innovación
Educación	Datos de poblaciones vulnerables
Salud y protección social	Diagnósticos e historias clínicas
Defensa	Estrategias de defensa nacional
Relaciones exteriores	Procesos jurídicos internacionales
Agricultura y desarrollo rural	Datos de patentes y poblaciones vulnerables.

Fuente. Elaboración propia

5.1.1.2 Desarrollo de las funciones asignadas a las entidades públicas colombianas. Adicional a la información que se gestiona, las entidades públicas en Colombia cumplen con una misión específica designada por Ley y que contribuye al desarrollo de un proceso considerado como necesario o útil para la sostenibilidad de la Nación.

De la anterior afirmación es posible concluir que la interrupción inesperada o el entorpecimiento de los procedimientos asociados a la operatividad de las organizaciones públicas, son eventos que repercuten directamente contra los objetivos de desarrollo y progreso nacional. Así mismo, está implícita una pérdida de recursos presupuestales asignados, los cuales no son aprovechados satisfactoriamente si la operatividad de la organización se ve interrumpida.

[19]DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Instructivo de la política para el tratamiento de datos personales.

Lo anterior, sumado al hecho de que todas las entidades gubernamentales en Colombia poseen sistemas de información internos y portales web oficiales, resalta la importancia de proteger estos activos contra posibles intrusiones, alteraciones no autorizadas o ataques que atenten contra su correcto funcionamiento. Entre los sistemas de información y herramientas software que se utilizan al interior de las entidades gubernamentales colombianas, vale la pena destacar las siguientes:

- **PORTALES WEB**
  Las páginas web de las entidades gubernamentales son el medio de presentación oficial y publicación de contenido institucional. Mediante estos espacios web las entidades públicas y organismos de control informan a detalle los datos organizaciones, metas alcanzadas, índices de progreso, datos de contacto y atención al público, publicaciones relacionadas a la ley de transparencia, organización interna, directivos, etc.

  Un ataque que inhabilite el contenido de los portales web estatales, implica un atentado contra la imagen de las entidades y contra su capacidad para publicar e informar su progreso.

- **SISTEMAS PARA LA GESTIÓN DE PERSONAL Y TRÁMITES INTERNOS**
  Se hace referencia a aquellos sistemas de información adquiridos o desarrollados por las entidades estatales colombianas, a través de los cuales gestionan y registran procesos internos los cuales pueden ser el registro histórico de personal, gestión de viáticos, gestión documental, inventario de recursos e infraestructura, entre otros.

  Un ciberataque a estos sistemas implica una afectación indirecta a la misionalidad, en el sentido que se entorpecen los procedimientos de operación generales a todas las entidades públicas.

- **SIIF NACIÓN**
  El sistema integrado de información financiera, es el aplicativo web integral mediante el cual se administran y registran las operaciones financieras realizadas con los recursos de la nación. Esta plataforma online es utilizada por todas las entidades estatales en Colombia.

  Un ataque que inhabilite el SIIF NACIÓN implica una afectación general de la operación pública financiera. Además, vale la pena mencionar, que el acceso no autorizado a este entorno es un riesgo considerable en vista de la posibilidad de realizar operaciones financieras y transacciones con recursos públicos asignados. [20]

[20] CONTADURÍA GENERAL DE LA NACIÓN. Preguntas frecuentes SIIF y SPGR [sitio web] Consulta realizada el 12 de mayo de 2021. Disponible en https://www.contaduria.gov.co/preguntas-acerca-del-siif-y-spgr

- **SECOP**
  EL sistema electrónico para la contratación pública, es la plataforma oficial mediante la cual se gestiona y registra el proceso contractual de entidades públicas en Colombia. Este aplicativo web es utilizado por todas las entidades estatales de forma continua y rigurosa, con el fin de oficializar los procesos de contratación pública y demás subprocesos asociados.

  Un ataque que inhabilite esta plataforma implica una detención abrupta del proceso de contratación pública, el cual requiere la ejecución de operaciones diarias comprendidas en un esquema de vigencias y términos de vencimiento de tiempos que pueden acarrear sanciones o pérdidas económicas.[21]

- **MUISCA**
  Modelo único de ingresos, servicios y control automatizado, es la plataforma administrada por la DIAN, donde se promueve el cumplimiento de los objetivos de la entidad, y se relacionan de forma integral los procesos de la misma, generando optimización del proceso de recaudo.

  Un ciberataque a esta plataforma implica una afectación a los procesos relacionados a impuestos y aduanas nacionales, lo cual se traduce en importantes consecuencias sobre la economía nacional. [22]

- **SIRI**
  El sistema de registro de sanciones y causas de inhabilidad, es la herramienta web administrada por la procuraduría general de la nación mediante la cual se gestionan procesos relacionados a sanciones penales, disciplinarias, de responsabilidad fiscal y violaciones en las relaciones contractuales.

  Un ciberataque dirigido a esta plataforma, no solo entorpece los procesos sancionatorios e investigaciones ejecutadas por la procuraduría, sino que además implica un riesgo de hurto de datos por la calidad de información confidencial relacionada a los casos que se gestionan desde el aplicativo. [23]

---

[21] COLOMBIACOMPRA. ¿Qué es SECOP? [sitio web] Consulta realizada el 21 de mayo de 2021. Disponible en https://colombiacompra.gov.co/secop/secop-i

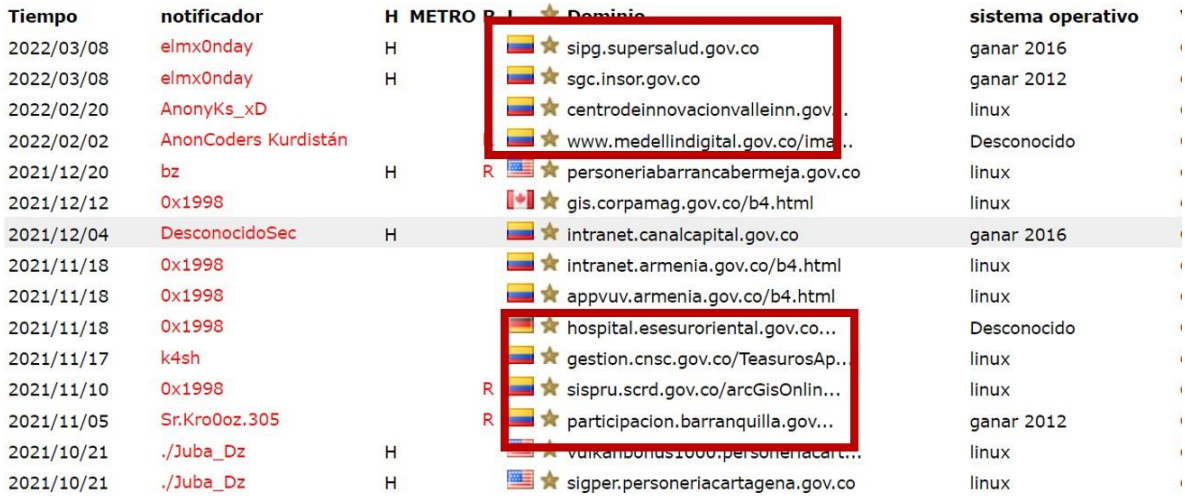
[22] MOLINA Pedro Antonio. El muisca es mucho más que un sistema informático. LEGIS. Revista 127.Colombia. 2005.

[23] PROCURADURÍA GENERAL DE LA NACIÓN. Sistema de registro de sanciones y causas de inhabilidad. [sitio web] Consulta realizada el 5 de junio de 2021. Disponible en https://www.procuraduria.gov.co/portal/Siri.page#:~:text=Sistema%20de%20Informacion%20de%20Registro%20de%20Sanciones%20y%20Causas%20de%20Inhabilidad%20%2D%20SIRI,-Introducci%C3%B3n%20%2F%20Certificado%20de

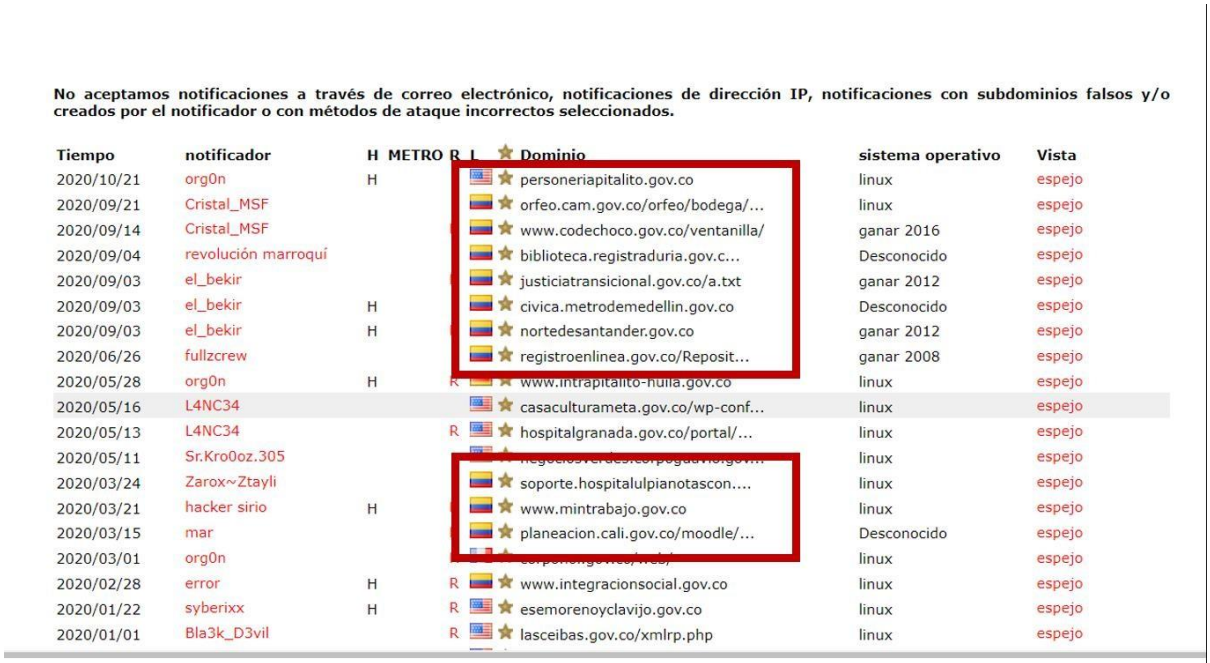
5.1.1.3 Riesgo de ciberataques efectuados contra entidades estatales colombianas. De acuerdo a la información presentada en los ítems anteriores, es posible reconocer que preservar la seguridad informática en el sector público en Colombia, implica proteger los intereses colectivos de la Nación, así como la integridad de los ciudadanos. Es evidente que las entidades públicas en Colombia almacenan y gestionan una gran cantidad de información que puede ser objetivo de ciberataques con consecuencias perjudiciales en una mayor o menor escala.

Así mismo, es importante reconocer que la implementación efectiva de esquemas de ciberseguridad que garanticen la protección de los datos y sistemas de información, es un proceso continuo en el tiempo, el cual implica el estudio constante de las nuevas amenazas informáticas que se registran todos los días, y de las posibles metodologías o estrategias que permitan contrarrestarlas. El riesgo a sufrir un ciberataque permanece constante en el tiempo, a la espera de reconocer un vacío que permita ejecutar acciones nocivas contra una entidad, población o individuo; es deber de las entidades estatales, dotarse de profesionales capaces de mitigar este riesgo.

Ilustración 5. Resultado búsqueda de ciberataques contra sitios web con dominio gov.co



Tiempo	notificador	H	METRO	R	Dominio	sistema operativo
2022/03/08	elmx0nday	H			sipg.supersalud.gov.co	ganar 2016
2022/03/08	elmx0nday	H			sgc.insor.gov.co	ganar 2012
2022/02/20	AnonyKs_xD				centrodeinnovacionvalleinn.gov...	linux
2022/02/02	AnonCoders Kurdistán				www.medellindigital.gov.co/ima...	Desconocido
2021/12/20	bz	H		R	personeriabarrancabermeja.gov.co	linux
2021/12/12	0x1998				gis.corpamag.gov.co/b4.html	linux
2021/12/04	DesconocidoSec	H			intranet.canalcapital.gov.co	ganar 2016
2021/11/18	0x1998				intranet.armenia.gov.co/b4.html	linux
2021/11/18	0x1998				appvuv.armenia.gov.co/b4.html	linux
2021/11/18	0x1998				hospital.esesuroriental.gov.co...	Desconocido
2021/11/17	k4sh				gestion.cnsc.gov.co/TeasurosAp...	linux
2021/11/10	0x1998			R	sispru.scrd.gov.co/arcGisOnlin...	linux
2021/11/05	Sr.Kro0oz.305			R	participacion.barranquilla.gov...	ganar 2012
2021/10/21	./Juba_Dz	H			vulkanbonus1000.personeriacart...	linux
2021/10/21	./Juba_Dz	H			sigper.personeriacartagena.gov.co	linux



No aceptamos notificaciones a través de correo electrónico, notificaciones de dirección IP, notificaciones con subdominios falsos y/o creados por el notificador o con métodos de ataque incorrectos seleccionados.

Tiempo	notificador	H	METRO	R	L	Dominio	sistema operativo	Vista
2020/10/21	org0n	H				personeriapitalito.gov.co	linux	espejo
2020/09/21	Cristal_MSF					orfeo.cam.gov.co/orfeo/bodega/...	linux	espejo
2020/09/14	Cristal_MSF					www.codechoco.gov.co/ventanilla/	ganar 2016	espejo
2020/09/04	revolución marroquí					biblioteca.registraduria.gov.c...	Desconocido	espejo
2020/09/03	el_bekir					justiciatransicional.gov.co/a.txt	ganar 2012	espejo
2020/09/03	el_bekir	H				civica.metrodemedellin.gov.co	Desconocido	espejo
2020/09/03	el_bekir	H				nortedesantander.gov.co	ganar 2012	espejo
2020/06/26	fullzcrew					registroenlinea.gov.co/Reposit...	ganar 2008	espejo
2020/05/28	org0n	H		R		www.intrapitalito-huila.gov.co	linux	espejo
2020/05/16	L4NC34					casaculturameta.gov.co/wp-conf...	linux	espejo
2020/05/13	L4NC34			R		hospitalgranada.gov.co/portal/...	linux	espejo
2020/05/11	Sr.Kro0oz.305					[redacted]	linux	espejo
2020/03/24	Zarox~Ztayli					soporte.hospitalulpianotascon....	linux	espejo
2020/03/21	hacker sirio	H				www.mintrabajo.gov.co	linux	espejo
2020/03/15	mar					planeacion.cali.gov.co/moodle/...	Desconocido	espejo
2020/03/01	org0n					[redacted]	linux	espejo
2020/02/28	error	H		R		www.integracionsocial.gov.co	linux	espejo
2020/01/22	syberixx	H		R		esemorenoyclavijo.gov.co	linux	espejo
2020/01/01	Bla3k_D3vil			R		lasceibas.gov.co/xmlrp.php	linux	espejo

Fuente. Archivo ZONE-H [en línea] Consulta realizada el 7 de abril de 2022. Disponible en https://www.zone-h.org/archive/filter=1/published=0/special=1/domain=gov.co/fulltext=1/page=1

Vale la pena mencionar ciberataques registrados que permiten sentar un precedente y reafirmar la problemática que se ha venido enunciando. El sitio web ZONE-H, el cual es un archivo digital que registra notificaciones de sitios web afectados a nivel mundial, permite reconocer ataques asociados a ubicaciones identificadas por el dominio oficial del estado colombiano GOV.CO, como se puede evidenciar en la ilustración 5.

Dentro de las entidades afectadas es posible reconocer algunos casos del sector salud como Superintendencia de Salud, Hospital Granada, entre otros. Así mismo, vemos entidades de orden administrativo como Registraduría Nacional, Ministerio de Trabajo, Personería, Función pública.

El registro de estos ataques demuestra una constante amenaza contra diferentes sectores y diferentes tipos de instituciones públicas. Se entiende que los ataques se dan de forma dirigida, en momentos puntuales en el tiempo con el fin de sabotear eventos importantes o afectar una población específica. Este tipo de conductas asociadas a ciberataques resalta la necesidad de fortalecer los planes de ciberseguridad implementados hasta la fecha.

Adicional a ataques de alteración de sitios web, también se tiene registro de ciberataques asociados a otro tipo de conductas criminales, como son denegación de servicio, inhabilitación de sistemas informáticos internos, corrupción de información, suplantación de identidad, entre otros.

En este orden de ideas es posible reconocer casos relevantes de ciberataques a entidades públicas colombianas que reafirman el riesgo existente y permiten dimensionar los efectos negativos a los cuales están expuestos los activos de información:

Como primer ejemplo se tiene el ciberataque reportado contra el INVIMA a principios del año 2022, donde se produjo una afectación sobre la plataforma donde se prestan servicios a la ciudadanía, además del envío de correos malintencionados con información falsa a nombre de la institución. Este tipo de situación refleja una intención terrorista que además afecta la salud pública colombiana debido a las características de la entidad afectada. [24]

Como segundo caso es importante mencionar los varios ataques reportados a las plataformas de la Registraduría Nacional, las cuales son numerosos y constantes, especialmente en temporadas de elecciones o consultas nacionales. El ciberataque más reciente registrado tuvo lugar en marzo de 2022 durante las elecciones de congreso y cámara de representantes; los ataques tipo DoS buscaban inhabilitar la plataforma web Infovotantes con el ánimo de entorpecer el proceso de votación y obstaculizar el sufragio a los ciudadanos. Este tipo de conductas demuestran que los ciberdelincuentes actúan no solo con fines lucrativos, sino que además tienen intereses políticos y buscan el sabotaje en contra de eventos públicos de alta importancia nacional.[25]

Finalmente, se menciona el caso del importante ciberataque que sufrió el Departamento Administrativo Nacional de Estadísticas (DANE) el pasado 9 de noviembre de 2021, sobre el cual se reportaron intrusiones, suplantación de identidad e intento de hurto de la información. El DANE es una entidad con alto valor a nivel de data ya que almacena un gran volumen de información sensible y reservada, asociada a reportes nacionales a nivel económico, social, demográfico y cartográfico. El incidente obligó a la entidad a inhabilitar su página web y programas internos, además de solicitar a la ciudadanía que se ignorará cualquier comunicación institucional por correo electrónico o llamada. [26]

---

[24] EL ESPECTADOR. Invima fue víctima de ciberataque, estos son los trámites que no entrarán en pausa. Redacción salud. 18 de febrero de 2022

[25] REVISTA SEMANA. Atención: Registraduría confirmó grave ataque cibernético a su página web en medio de elecciones. Elecciones 2022. 13 de marzo de 2022

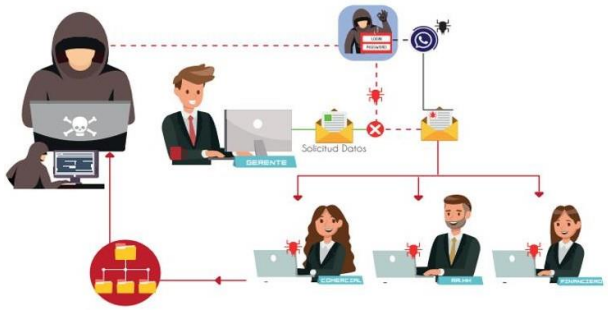
[26] EL HERALDO. Ciberataque contra el Dane borró bases de datos con información confidencial. Javier Mendoza. 11 noviembre de 2022

Si bien sea hecho frente a los ciberataques mencionados desde el centro cibernético de la policía nacional, es importante robustecer las estrategias y capacidad de las entidades públicas de tomar acciones frente a situaciones específicas a nivel de ciberseguridad. El registro histórico de incidentes nos permite afirmar que las entidades seguirán siendo blanco de ciberataques, y que estos buscan hacer daño valiéndose de distintos métodos y con diferentes objetivos de ataque. Es deber del gobierno nacional reconocer y solventar la necesidad en materia de ciberseguridad que afecta la institucionalidad en el sector público.

El hecho de ignorar la necesidad en mención, puede acarrear consecuencias significativas y perjudiciales para el estado colombiano. Con base en el análisis desarrollado, los ciberataques más propensos a ejecutarse contra el sector público colombiano son:

- **Campañas de phishing**
  Acto mediante el cual, a partir del uso de información de contacto adquirida de forma no autorizada, se realiza una ejecución organizada de ingeniería social en la cual se busca la obtención de datos personales de las víctimas para realizar transacciones no autorizadas o extorsión. A continuación, se muestra sobre la ilustración 5 la operación del ciberataque en mención y sus componentes

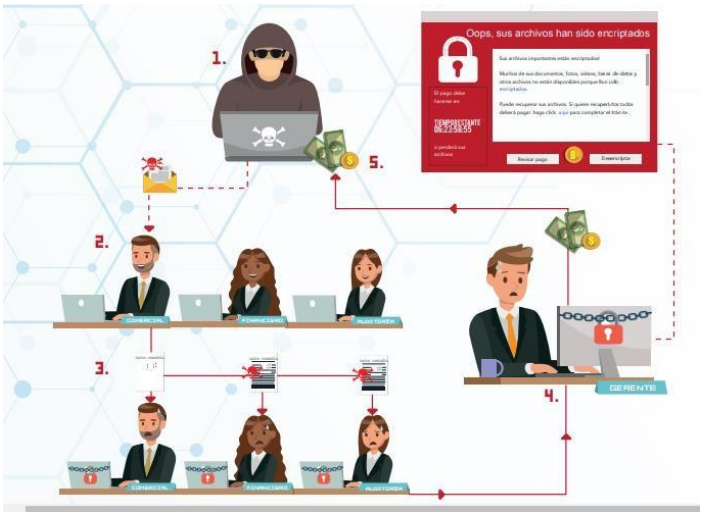
Ilustración 6. Operación ataque phishing



Fuente. Documento Tendencias Cibercrimen Colombia 2019-2020 [en línea] Consulta realizada el 01 de mayo de 2021. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

- **Infección con Ransomware**
  Acto mediante el cual se busca comprometer un sistema o equipo mediante la ejecución de código malicioso que permite al atacante tomar control sobre la data o el sistema para posteriormente extorsionar al propietario. A continuación, se muestra sobre la ilustración 6 la operación del ciberataque en mención y sus componentes.

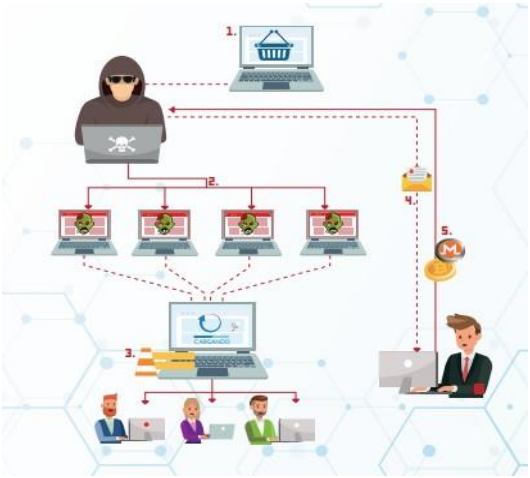
Ilustración 7. Operación ataque ransomware



Fuente. Documento Tendencias Cibercrimen Colombia 2019-2020 [en línea] Consulta realizada el 01 de mayo de 2021. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

- **Ataques de denegación de servicio DDoS:** Acto mediante el cual se busca inhabilitar un servidor o sistema con el fin de que este no cumpla la función para la cual fue creado. Usualmente los ciberatacantes reconocen el objetivo y utilizan software o botnets para la simulación de solicitudes que saturan el servidor y originan la incapacitación del sistema. A continuación, se muestra sobre la ilustración 7 la operación del ciberataque en mención y sus componentes

Ilustración 8. Operación ataque DoS



Fuente. Documento Tendencias Cibercrimen Colombia 2019-2020 [en línea] Consulta realizada el 01 de mayo de 2021. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

De los ataques mencionados, es posible identificar como factor común la necesidad del atacante de acceder y establecer una conexión con el sistema objetivo. En este sentido, el hacking es un proceso necesario para el reconocimiento y planificación asertiva de un ataque informático. De esta forma se reconoce que un profesional con conocimientos en hacking y técnicas de intrusión, orientado a fortalecer la ciberseguridad de una entidad, es el recurso humano ideal para la mitigación de riesgos y creación de planes de respuesta a amenazas en el ciberespacio.

Entonces, como aspectos mejorables que permiten directamente disminuir la posibilidad de sufrir altos impactos a razón de un ciberataque efectivo en las entidades de orden público, es posible reconocer:

- Infraestructura: Muchas de las entidades públicas en Colombia no destinan demasiados recursos a su infraestructura, sino que se destinan a asuntos misionales. Sin embargo, los sistemas deben mantenerse actualizados y buscar el uso de tecnologías recientes, ya que el uso de plataformas y dispositivos obsoletos implica una brecha de ciberseguridad.

- Personal profesional en ciberseguridad: Muchas de las entidades públicas en Colombia solo poseen personal de TI para soporte y temas de apoyo. Sin embargo, el contar con profesionales en ciberseguridad permite acatar recomendaciones asertivas e implementar metodologías eficientes para la protección de la data y los activos de cualquier entidad pública.

- Creación de planes de contingencia: Muchas entidades de orden público no están preparadas para responder de forma eficiente a posibles ataques informáticos y los efectos que estos lleguen a producir. El gobierno colombiano debería exigir documentos de planeación donde se consideren escenarios críticos en materia de ciberseguridad y la mejor forma de hacerles frente.

5.2 IMPORTANCIA DEL HACKING A NIVEL ORGANIZACIONAL EN ENTIDADES DE ORDEN PÚBLICO EN COLOMBIA MEDIANTE UNA REVISIÓN EN FUENTES BIBLIOGRÁFICAS ESPECIALIZADAS PARA DISTINGUIR LAS VENTAJAS QUE IMPLICA EL PROCESO EN CUANTO A LA CREACIÓN DE UN ESQUEMA DE CIBERSEGURIDAD

5.2.1 ¿Qué ventajas implica la inclusión de procesos de hacking ético en los esquemas de ciberseguridad del sector público en Colombia? De acuerdo a los datos suministrados y a las consideraciones técnicas en materia de ciberseguridad, es posible reconocer que el hacking es un proceso complejo que requiere la aplicación de conocimientos informáticos avanzados para una correcta ejecución.

Con base en esta premisa, se determina que la forma efectiva de prevenir y contrarrestar el hacking ejecutado con fines maliciosos, es contar con profesionales en la capacidad de recrear los ciberataques, identificar vulnerabilidades y proponer mecanismos de ciberdefensa. En este orden de ideas, la práctica conocida como HACKING ÉTICO es parte fundamental de la solución a problemas de ciberseguridad en cualquier tipo de organización.

Para reconocer las ventajas de contratar servicios de hacking ético en entidades gubernamentales de Colombia es necesario consolidar las funciones que puede desempeñar un “hacker” en una entidad estatal.

5.2.1.1 Prevenir eventos desastrosos para la entidad. En primera instancia, un “hacker” ético permite contrarrestar los intentos de causar perjuicios a la entidad o a los intereses nacionales por medio de ciberataques. La primera ventaja implícita en la contratación de profesionales en hacking es la ejecución de procesos propios de la definición de “hacker” ético.

La principal función de este tipo de profesionales TI es la de evaluar el esquema de seguridad organizacional con el fin de generar un plan de seguridad que se ajuste a las necesidades de la empresa y permita proteger los activos de posibles ciberataques. La prevención de ataques informáticos, así como la generación de respuestas oportunas, evita catástrofes empresariales que, en mayor o menor medida, atentan contra la sostenibilidad y progreso de la organización. [27]

Al centrarse en entidades estatales de Colombia, es posible afirmar que la contratación de profesionales en hacking protege los intereses de la nación y su

[27] INTEGRAITBLOG. Hackers necesarios para la seguridad de la información [sitio web] Consulta realizada el 15 de octubre de 2021. Disponible en https://integrait.com.mx/blog/seguridad-de-la-informacion-por-que-es-necesario-un-hacker/#:~:text=La%20importancia%20de%20los%20hackers%20dentro%20de%20la%20estrategia&text=Tienen%20la%20capacidad%20de%20conocer,salir%20airosos%20de%20un%20ataque.

operatividad. Lo anterior, es una necesidad contundente que ha sido expuesta en la última década, donde el gobierno y las entidades estatales se han convertido en el segundo objetivo de preferencia para los ciberatacantes, siendo el primer puesto para las entidades financieras.

5.2.1.2 Garantizar los principios básicos de la información digital. La segunda ventaja implícita en el ejercicio de las funciones de un "hacker" ético es la preservación de los tres pilares básicos de la seguridad de la información: Integridad, confidencialidad y disponibilidad.[28] A continuación, se presentan las definiciones puntuales descritas por la empresa Redtrust (Compañía española para que brinda soluciones asociadas a certificados digitales) consolidadas mediante un infograma relacionado en la ilustración 8.

Ilustración 9. Principios básicos de la información digital

Fuente. REDTRUST a keyfactor Company. 2020 [en línea] Consulta realizada el 26 de Abril de 2021. Disponible en: https://redtrust.com/

Un profesional en hacking, mediante la prevención de ataques y la definición de estrategias que orienten el uso de las tecnologías de la información hacia prácticas que promuevan la seguridad de la información, garantizan integralmente los principios básicos mencionados.

En este orden de ideas, el ejercicio del hacking ético fortalece la capacidad de la entidad estatal de salvaguardar la data de forma correcta, de modo se agrega un

[28] UNIR REVISTA. Principios de la seguridad Informática [sitio web] Consulta realizada el 24 de mayo de 2021. Disponible en https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/

carácter confiable a los ojos de los trabajadores y usuarios. Específicamente para las entidades estatales colombianas, garantizar los principios de seguridad para la data que se administra, implica proteger la integridad de la ciudadanía en general.

5.2.1.3 Ahorro de dinero mediante aplicación de técnicas efectivas Otra ventaja significativa que vale la pena mencionar, es la optimización de recursos económicos destinados a la adquisición de herramientas que actúen en el esquema de ciberseguridad de la Nación.

Contar con un equipo de profesionales en hacking, implica tener la capacidad de evaluar asertivamente que herramientas software y hardware deben ser adquiridas o desarrolladas para la necesidad específica de la empresa. Si bien el mercado está lleno de herramientas (gratuitas o por licencia) para cumplir este fin, es relativamente sencillo elegir de forma errónea, o bien, no reconocer la forma de sacar el mayor provecho a la utilidad de los activos para la ciberseguridad.

Esta capacidad de seleccionar y aplicar de forma asertiva las herramientas TI relacionadas a la ciberseguridad, se traduce en ahorro de recursos invertidos para tal fin. La orientación y capacidad de los profesionales en hacking para recomendar e implementar recursos que favorezcan los esquemas de defensa, es una ventaja contundente que adicionalmente favorece a las entidades estatales colombianas a nivel de inversión.

5.2.1.4 Mantenimiento de infraestructura TI actualizada. Es importante reconocer que el ejercicio de un "hacker" a nivel empresarial, es un proceso integral desde el punto de vista tecnológico. Lo anterior, significa que además de las estrategias puntuales de ciberdefensa, un equipo de hackers éticos está encargado de velar por que se cumplan condiciones de infraestructura TI consideradas como óptimas, que contribuyan al esquema de ciberseguridad implementado.[29]

Las condiciones de infraestructura TI pueden ser resumidas como:

- Contar con los recursos TI necesarios para las estrategias implementadas:
  Hace referencia a la propia adquisición de los recursos y herramientas TI necesarias para los procesos que se requieren ejecutar.

- Contar con la capacidad de realizar mantenimientos preventivos o reparaciones que garanticen el buen funcionamiento de los recursos:
  Hace referencia a la capacidad del área TI para realizar mantenimientos periódicos o solventar problemas de reparación de los recursos informáticos,

[29] OSI. La importancia de las actualizaciones de seguridad [sitio web] Consulta realizada el 8 de agosto de 2021. Disponible en https://www.osi.es/es/actualizaciones-de-seguridad

con el fin de que estos funcionen de manera correcta y su utilidad sea prolongada en el tiempo.

- Contar con plataformas y licencias actualizadas:
  Hace referencia al monitoreo constante de actualizaciones y nuevas tecnologías, las cuales son evaluadas con el fin de garantizar que la empresa cuente con plataformas y licencias beneficiosas que den un valor añadido a la estrategia TI.

En consecuencia, es evidente que el ejercicio de prevención realizado sobre la infraestructura TI de una entidad estatal, garantiza una vigilancia constante relacionada a la actualización de plataformas y herramientas, lo cual promueve el progreso y desarrollo de la organización, directamente relacionado al desarrollo tecnológico del estado.

5.2.1.5 Aumento de la cultura de ciberseguridad en la población organizacional. Finalmente, se destaca la preocupación de un profesional en hacking, por disminuir las probabilidades de ataques informáticos efectuados exitosamente sobre la entidad estatal.

Esta preocupación se ve reflejada en la definición de un plan para la promoción y consolidación de una cultura de ciberseguridad sobre la población organizacional. Es decir, el profesional en hacking está en la capacidad de generar campañas de concientización y aprendizaje, a través de las cuales se capacite a los demás trabajadores de la entidad para la identificación y mitigación de riesgos de ataques informáticos.

El ejercicio de reconocimiento de vulnerabilidades por parte de un profesional en hacking, siempre va a considerar la capacidad de todos los trabajadores de la empresa para reconocer y notificar intentos de ciberataques.

De esta forma, otra ventaja significativa al momento de contratar un profesional en hacking, es que directamente se está promoviendo la adopción de conocimiento en ciberseguridad entre todos los miembros de la entidad estatal. Una cultura de ciberseguridad implica conocimiento útil para cualquier individuo del mundo moderno, tanto a nivel profesional como a nivel personal. Lo anterior sugiere un aporte a la formación de los colombianos vinculados a entidades estatales, quienes a su vez está en capacidad de trasmitir el conocimiento adquirido.

5.3 PROPONER RECOMENDACIONES QUE PERMITAN FORTALECER LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES DE ORDEN PÚBLICO EN COLOMBIA CON BASE A LINEAMIENTOS Y DIRECTRICES RELACIONADOS CON EL ÁREA RESALTANDO LA NECESIDAD DE CONTAR CON MÁS PROFESIONALES EXPERTOS EN CIBERSEGURIDAD

5.3.1 ¿Cómo se puede mejorar el esquema de ciberseguridad en entidades de orden público en Colombia? Posterior a identificar las ventajas de incluir procesos de hacking ético al interior de las entidades públicas en Colombia, es posible afirmar que, si existe la necesidad de robustecer los esquemas de ciberseguridad a partir del reconocimiento oportuno de necesidades organizacionales, identificación de activos de información y generación de estrategias para prevención y respuesta de incidentes.

De acuerdo a esta necesidad es importante reconocer y consolidar cuales recomendaciones son asertivas y otorgan un valor añadido para la gestión TI en entidades públicas colombianas.

5.3.1.1 Recomendaciones relacionadas a infraestructura TI. En primer lugar, se hace mención a recomendaciones relacionadas a la infraestructura TI recomendada para las entidades. Es importante mencionar que la capacidad adquisitiva que posee una entidad pública colombiana, depende del presupuesto asignado por el Ministerio de Hacienda y crédito público.

Las condiciones de infraestructura son entendidas como el conjunto de recursos tecnológicos (hardware y software) con los que cuenta una organización; así mismo al hablar de infraestructura se hace referencia a la forma en que están dispuestos estos recursos y las conexiones existentes entre ellos. La infraestructura TI en su conjunto, es el elemento que garantiza que los profesionales TI puedan proveer de forma óptima los servicios y recursos que requieren los usuarios de la organización.

En materia de ciberseguridad, es posible identificar elementos TI importantes que cumplen un papel de agente de seguridad, desempeñando tareas de seguimiento, supervisión y monitoreo sobre los recursos de la entidad. La forma en que se disponen los agentes de seguridad, así como la gestión adecuada de los mismos, asegura la integrad de los usuarios y dispositivos de la red corporativa.

En este orden de ideas, es posible consolidar las siguientes recomendaciones, orientadas a las necesidades de las entidades públicas colombianas, y a los activos de información que estas poseen:

Implementar sistema de Control físico de acceso y seguridad perimetral

Inicialmente se hace mención al aseguramiento físico de los espacios que hacen parte de la entidad. En Colombia, las entidades de orden público son espacios accesibles, normalmente con atención a los ciudadanos, por lo tanto, es importante asegurar y controlar el acceso físico de personal a las instalaciones.

- **Sistema de control de acceso externo.** Toda entidad de orden público en Colombia debe contar con un sistema de control de acceso que permita la autenticación de usuarios al momento de ingresar a las instalaciones, ya sea mediante tarjetas de acceso o datos biométricos. Así mismo, el sistema debe almacenar un registro de ingresos y salidas tanto de usuarios autorizados como de visitantes autorizados.

  Este tipo de sistemas implementan soluciones hardware que controlan los accesos físicos a las instalaciones (torniquetes de acceso, puertas inteligentes, registradoras, etc) las cuales a su vez envían los datos registrados a un software centralizado el cual almacena un histórico de eventos. Estos sistemas permiten al personal de seguridad controlar el acceso peatonal y/o vehicular, sobre las instalaciones mediante la verificación de identidad y bloqueo de personas no autorizadas. Se sugiere su implementación en entradas principales y alternativas de toda entidad gubernamental y sedes correspondientes. Se muestra un ejemplo implementado en la ilustración 9.

Ilustración 10. Dispositivos hardware para control de acceso

Fuente. MANDUA. Sistemas de control de acceso vehicular y parking. [sitio web] Consulta realizada el 25 de noviembre de 2021. Disponible en https://www.mandua.com.py/sistemas-de-control-de-acceso-vehicular-y-de-parking-n657

- **Sistemas de control de acceso interno.** Toda entidad de orden público en Colombia cuenta con activos de información críticos para los intereses de la

organización, alojados en las mismas instalaciones. Entre los activos más importantes se encuentran documentos legales y archivos de la entidad, los cuales son almacenados de forma física de acuerdo a la política de Gestión Documental publicada por la Función pública.

En este orden de ideas, es importante disponer de un sistema de control de acceso que restringa el acceso de personal a zonas especialmente sensible que almacenen activos críticos. Los permisos de acceso a estos espacios deben ser supervisados por el área administrativa de cada entidad, y deben ser debidamente documentados con el respectivo flujo de aprobación.

Entre los espacios más comunes para implementar controles de acceso se encuentran cuartos de archivo, datacenter, salas de videoconferencia, puestos de trabajo de jefes de área y cuartos de monitoreo.

- **Seguridad perimetral.** Toda entidad de orden público en Colombia debe poseer un sistema de seguridad perimetral, que por lo general incluye una red integrada de cámaras y alarmas que se mantiene en constante monitoreo.

  Estos sistemas son usualmente administrados por el cuerpo de seguridad contratado, y permiten una supervisión constante de las áreas internas y externas de la entidad, con una función de alerta contra intrusos. Los dispositivos en mención remiten los datos a una central de monitoreo que almacena un registro de eventos y muestra las imágenes de las cámaras en tiempo real.

Implementar un Sistema Firewall

Para todo esquema de ciberseguridad es indispensable la implementación de un sistema firewall. En el caso de las entidades públicas colombianas, se considera relevante la disposición de un dispositivo firewall para la protección de la red, y de un firewall definido por software para la protección individual de los dispositivos de la organización.

Un firewall es una agente de seguridad que se encarga del filtrado de tráfico y detección de actividades sospechosas, mediante la ejecución de políticas de seguridad y controles definidos previamente por el administrador del sistema.

- **Firewall Físico** Para la protección de la red corporativa de una entidad pública en Colombia, se sugiere la implementación de un firewall físico dispuesto entre el dispositivo frontera que brinda acceso a internet, y la red interna de la organización.

Las políticas configuradas sobre este dispositivo deben incluir listas de control donde se especifiquen aplicaciones y servicios confiables, y así mismo se descarte el tráfico y solicitudes realizadas desde orígenes desconocidos. Deben configurarse funciones de alerta donde se identifiquen comportamiento sospechosos o intentos de intrusión sobre la red interna.

El uso de un dispositivo de nueva generación permite obtener servicios adicionales ya incluidos y configurables desde el mismo recurso, como por ejemplo sistemas IDS que permitan generar alertas y acciones de respuesta frente a intrusiones efectivas. Se muestra un ejemplo de referencia hardware en la ilustración 10.

Ilustración 11. Fotografía firewall CISCO última generación ASA -SERIE 5500 -X

Fuente. CISCO. Firewalls de última generación. [sitio web] Consulta realizada el 28 de noviembre de 2021. Disponible en https://www.cisco.com/c/es_es/products/security/asa-5500-series-next-generation-firewalls/index.html

- **Firewall Definido Por Software.** Un sistema firewall definido por software es altamente recomendable, y se requiere que este activo en cado uno de los dispositivos finales habilitados dentro de la entidad, esto permite el control sobre las acciones de los usuarios generando bloqueos de instalaciones, descargas, navegación y acceso a terminales.

  Un sistema firewall activo en cada dispositivo restringe el campo de acción de un atacante que tenga acceso al recurso, así mismo, centraliza el control sobre los recursos al requerir una autorización o autenticación de administrador para ejecutar ciertas acciones sobre la red.

- **Firewall Respaldo (Opcional).** La implementación de un segundo firewall es una medida opcional que permite dar un valor añadido a la seguridad de la red en una entidad. Esta implementación añade un segundo filtro lo cual dificulta las acciones intrusivas y genera un respaldo al firewall principal en caso de que

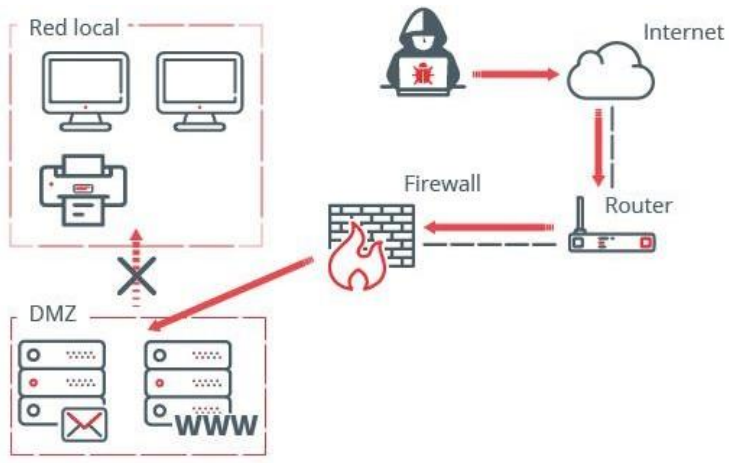
este se sature o presente una falla. Es altamente recomendable y debe considerarse de acuerdo al presupuesto designado para adquisición de recursos TI.

Implementar una DMZ

En informática es común encontrar el termino DMZ o zona desmilitarizada. Este concepto es un elemento de seguridad por lo general asociado a la implementación de un firewall. Una DMZ es un elemento de ciberseguridad que permite proteger la red corporativa mediante la disposición de recursos TI en una sección monitoreada de la red, sin acceso a los recursos relevantes de la red interna.

La implementación de una DMZ es altamente recomendada para entidades públicas en Colombia, ya que permite hacer frente a los ataques DoS que comúnmente tienen lugar, en contra de los sitios web y aplicaciones sobre la nube. Una DMZ es definida desde el enrutador que comunica con la red externa, o desde el dispositivo firewall. Se muestra gráficamente la disposición de una DMZ en la red en la ilustración 11.

Ilustración 12. Ejemplo diagrama de red con DMZ implementada



Fuente. INCIBE. Qué es una DMZ y cómo puede ayudar a proteger tu empresa. [sitios web] Consulta realizada el 1 de diciembre de 2021. Disponible en https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Una DMZ permitirá limitar el alcance de los ataques y proteger la integridad de la red corporativa y sus usuarios. Se sugiere definir DMZ con conexiones habilitadas desde internet, pero deshabilitadas desde la DMZ hacia la red interna. Es importante mencionar que la DMZ y los recursos que se habiliten en ella, debe permanecer en constante vigilancia por parte del cuerpo de seguridad, ya que es una zona propensa a recibir ataques.

Implementar una arquitectura de VLANs

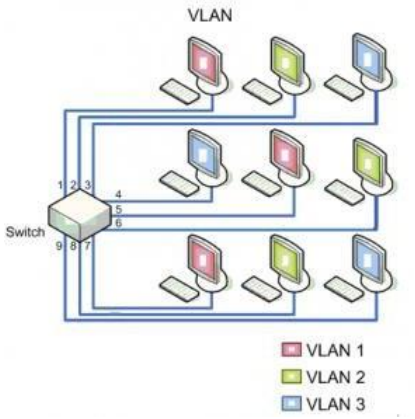
Se sugiere a las entidades públicas la implementación de un esquema de redes LAN virtualizadas (VLAN) las cuales permitan organizar el trabajo de los usuarios de la entidad según las necesidades de las áreas y grupos de trabajo.

Las VLAN son elementos útiles configurados desde el enrutador, los cuales permiten segmentar la red interna, y proveer de diferentes permisos y accesos a los usuarios de cada segmento. Adicional al valor añadido que brinda el uso de VLAN al esquema de seguridad, se obtiene beneficios adicionales como facilidad al momento de hacer escalar la red, y la optimización de servicios.

Toda entidad pública colombiana, posee un organigrama que especifica las áreas que conforman a la entidad, si bien esta organización varia, por lo general se mantienen elementos comunes sobre los cuales se basa la estructura de toda entidad de orden público en el país. Esta estructura involucra dependencias o áreas con funciones diferenciadas, por lo tanto, es altamente recomendable restringir las acciones de los usuarios de cada área de acuerdo a sus funciones.

Se recomienda implementar una estructura de VLAN donde se asigne una subred a cada área de la entidad, de esta forma los usuarios serán aislados, así como los recursos tecnológicos y servicios a los que tiene acceso, de esta forma se reduce la posibilidad de que un ataque que comprometa un recurso, termine por afectar a todos los usuarios de la red corporativa. En la ilustración 12 se muestra gráficamente un ejemplo de distribución de VLANs sobre una red interna.

Ilustración 13. Ejemplo distribución de usuarios por VLAN



Fuente. INTERNET PASO A PASO. Diseño de VLANs y direccionamiento IP. [sitio web] Consulta realizada el 1 de diciembre de 2021. Disponible en https://internetpasoapaso.com/diseno-vlans-direccionamiento-ip/

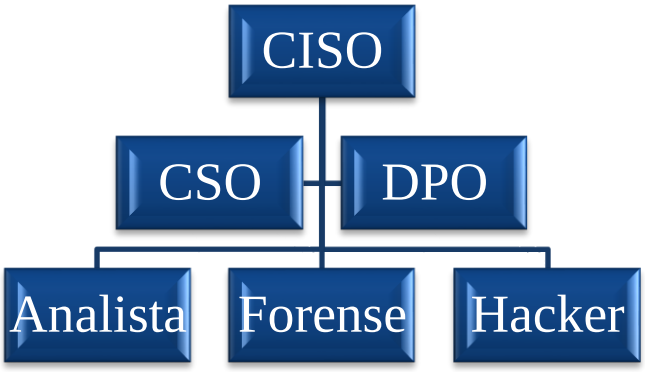
5.3.1.2 Recomendaciones relacionadas a perfiles profesionales. Adicional a las recomendaciones de infraestructura, es importante reconocer a la entidad de contar con profesionales Ti que estén en la capacidad de gestionar los recursos TI que provee la entidad, identificar vulnerabilidades e implementar soluciones que mejoren la gestión de ciberseguridad en una entidad.

Es importante mencionar que las recomendaciones relacionadas a perfiles profesionales útiles para entidades públicas colombianas, se centran en profesionales enfocados en ciberseguridad, es decir son perfiles adicionales a los que comúnmente conforman las demás áreas de una oficina de tecnologías (desarrolladores, ingenieros de soporte, técnicos, ingenieros de bases de datos, etc).

A continuación, se consolidan los perfiles relevantes considerados como útiles y necesarios para la gestión de ciberseguridad en entidades de orden público en Colombia. Es importante reconocer que el conocimiento asociado a hacking es relevante para cualquiera de los roles, debido a que la identificación de riesgos y actividad sospechosa sobre los recursos de una entidad, es una responsabilidad de todo colaborador que forme parte del área de ciberseguridad.

Los roles mencionados cumplen con una jerarquía sobre la cual se designan supervisiones y organización interna del grupo de ciberseguridad[30], esta organización se muestra en la Ilustración 13.

Ilustración 14. Jerarquía sugerida grupo de ciberseguridad



Fuente. Elaboración propia

CISO (Chief Information Security Officer)

[30] ARSYSBLOG. Estos son los principales roles en la ciberseguridad. [sitio web] Consulta realizada el 02 de diciembre de 2021. Disponible en https://www.arsys.es/blog/principales-roles-ciberseguridad/

En primer lugar, se encuentra el rol principal en materia de ciberseguridad a nivel organizacional. El CISO es director de ciberseguridad, y es el máximo responsable de hacer efectiva la estrategia de ciberseguridad que está implementada sobre la organización. Tiene a su cargo a los demás profesionales que conforman el área de ciberseguridad, y es responsable de coordinar el trabajo de cada uno en pro del cumplimiento de los objetivos de la entidad. [31]

Es un cargo que requiere ejecutar operaciones administrativas y prácticas, encaminadas a consolidar e implementar un Plan Director de Ciberseguridad (documento que consolida los activos de información y políticas de seguridad definidas para la entidad).

El CISO es el agente principal del equipo de ciberseguridad, encargado de la toma de decisiones y la supervisión de procesos, mantiene una estrecha comunicación con altos directivos de la entidad con el fin de alinear toda acción de ciberseguridad con los intereses organizacionales.

El aspirante a CISO debe ser un profesional en ingeniería de sistemas o afines con postgrado orientado a administración y gestión de proyectos, preferiblemente con dos certificaciones relacionadas a ciberseguridad como pueden ser:

- CEH. Hacker ético certificado. Otorgado por EC-COUNCIL
- CISSP: *Certified Security Systems Security Professional. Otorgada por ICS*
- CISM: *Certified Information Security Manager. Otorgada por ISACA*

CSO (Chief Security Officer)

Se sugiere también contar con un oficial en ciberseguridad CSO el cual es otro cargo directivo orientado a la toma de decisiones técnicas asociadas a la seguridad físicas y lógica de la entidad.

El CSO, además del conocimiento en materia de ciberseguridad debe poseer una visión de negocio y la capacidad de reconocer escenarios favorables para los intereses económicos de la entidad.

El CSO se encarga de la creación de políticas de seguridad en los distintos campos de ciberseguridad de la organización. Así mismo tiene la responsabilidad de velar por la mejora del modelo de negocio de la entidad y el cumplimiento de la

[31] INCIBE. CISO, CDO y ahora DPD: las siglas de la seguridad, los datos y la privacidad. [sitio web] España. 2018. [Consulta realizada el 9 de diciembre de 2021] Disponible en https://www.incibe.es/protege-tu-empresa/blog/ciso-cdo-y-ahora-dpd-las-siglas-seguridad-los-datos-y-privacidad

normatividad asociada. Para el caso de entidades públicas de Colombia se debe supervisar el cumplimiento de funciones asignadas por el estado, y el cumplimiento de leyes de transparencia y directrices emitidas por entes de control. [32]

El aspirante a CSO debe ser ingeniero de sistemas o afines, preferiblemente con posgrado en administración o finanzas. Debe tener experiencia en el sector público y estar relacionado con el objeto social de la entidad.

En organizaciones de menor dimensión como entidades adscritas o sedes alternas, el CSO puede ser un cargo desempeñado por el mismo CISO.

DPO (Data protection officer)

Se sugiere contar con un oficial para la protección de datos DPO, el cual es un rol responsable de reconocer los riesgos y medidas asociadas al esquema de ciberseguridad implementado sobre la entidad.

El DPO se encarga de velar por el cumplimiento de la normativa de protección de datos, manteniendo una coherencia con las funciones atribuidas a la entidad. Este agente de ciberseguridad supervisa el cumplimiento de políticas de ciberseguridad en la entidad, coopera con entes de control para verificar el cumplimiento de la norma en todos los procesos, y coordina toda operación relacionada a controles implementados sobre riesgos identificados.

El DPO está estrechamente relacionado a la supervisión del cumplimiento de la 1581 DE 2012 SOBRE LA PROTECCIÓN DE LOS DATOS PERSONALES EN COLOMBIA. El aspirante debe ser un profesional en ingeniería de sistemas o afines, preferiblemente con postgrado en ciberseguridad y con experiencia en el sector público.

Informático forense, Analista de seguridad, hacker

Estos roles son adicionales al esquema de directivos en ciberseguridad y están orientados al conocimiento práctico útil para la entidad.

Un informático forense es aquella persona con conocimiento para preservar, almacenar, recuperar y administrar la información y los sistemas de almacenamiento con los que cuenta la entidad. Actualmente las entidades en Colombia apuntan a una trasformación digital, donde los documentos y soportes se convertirán en archivos digitales que deben ser almacenados de forma eficiente. De

[32] IT DIGITAL SECURITY. CISO y CSO: ¿tienes clara la diferencia de roles? [sitio web] España. 2018. [Consulta realizada el 10 de diciembre de 2021] Disponible en https://www.itdigitalsecurity.es/actualidad/2018/08/ciso-y-cso-tienes-clara-la-diferencia-de-roles

igual forma, los conocimientos forenses permiten proveer de evidencias confiables a la entidad, para cualquier proceso disciplinario o investigación. [33]

Un hacker es aquella persona con la capacidad de auditar sistemas de información y elementos de seguridad con el fin de reconocer vulnerabilidades y proveer soluciones que las solventen. Se requiere conocimiento específico en áreas de hacking e intrusión.

Un analista de seguridad es aquella persona con la capacidad de cuantificar procesos de gestión de riesgos y controles, con el fin de proveer documentación útil para la toma de decisiones que favorezcan el esquema de seguridad.

El aspirante a estos cargos, o a un cargo integral que incluya estas aptitudes, debe ser un técnico o profesional en sistemas o afines, el cual debe demostrar el conocimiento práctico suficiente mediante una prueba teórico práctica donde se evalúen procesos de testing sobre los elementos específicos con los que cuenta la entidad.

5.3.1.3 Recomendaciones específicas relacionadas a lineamientos y directivas del gobierno colombiano. Posterior a evaluar condiciones de infraestructura y perfiles profesionales consideras como óptimas, es importante enmarcar una serie de recomendaciones asociadas a directrices que aplican específicamente para entidades de orden público en Colombia.

Para lograr este fin, se reconoce al Ministerio de las Tecnologías de Información y la Comunicación (MINTIC) como la máxima entidad gubernamental en Colombia en materia de telecomunicaciones, la cual se encarga de diseñar, adoptar y promover políticas y proyectos de tecnología. Desde sus funciones el MINTIC promueve el proyecto de gobierno digital sobre el cual se generan diferentes documentos, normas y directrices que deben ser evaluados y acogidos por todas las entidades públicas del país.

También se reconoce al Departamento Administrativo de la Función Pública (DAFP), como la entidad transversal encargada de la mejora continua de la gestión de servidores públicos y entidades estatales. En este orden de ideas, el DAFP emite y regular directrices con el ánimo de mejorar la gestión pública en Colombia, y constantemente supervisa y actualiza la implementación de dichas estrategias.

---

[33] WORLDSCHORALSHIPFORUM. ¿Qué hace un analista informático forense? Información profesional, salarios, conjunto de habilidades. [sitio web] Colombia. 2021. [Consulta realizada el 5 de diciembre de 2021] Disponible en https://worldscholarshipforum.com/es/forensic-computer-analyst/#:~:text=Los%20analistas%20forenses%20inform%C3%A1ticos%20combinan,y%20tambi%C3%A9n%20de%20recuperar%20pruebas.

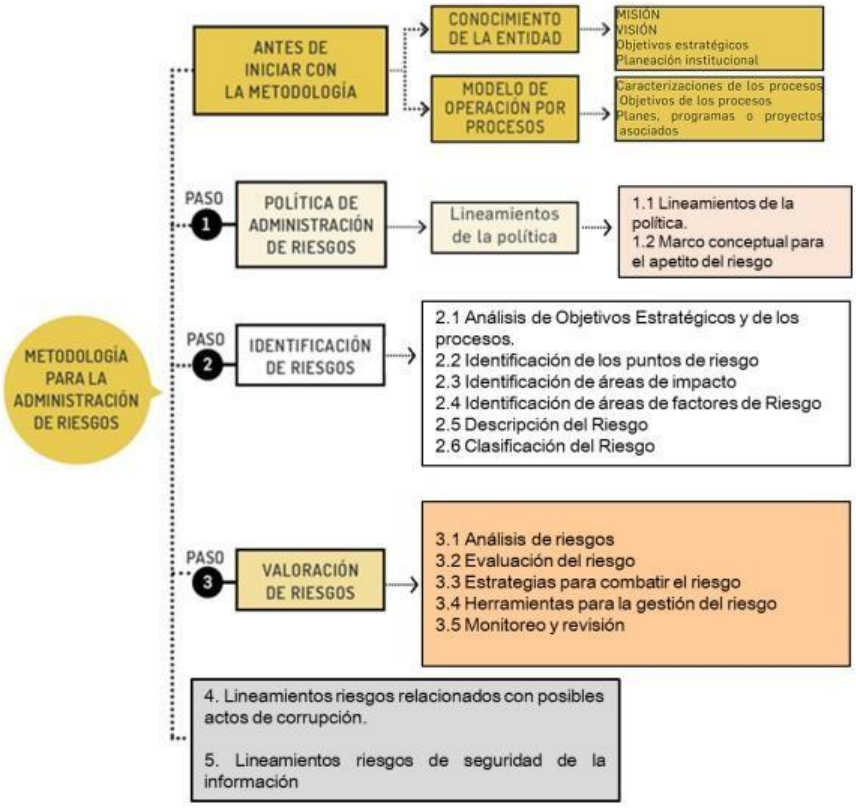
Con relación a los lineamientos establecidos por MINTIC y el DAFP, asociados a recursos TI y ciberseguridad, se recomienda a las entidades públicas colombianas:

- Generar un plan de gestión de riesgos e implementación de controles con base a la Guía para la administración de riesgo y diseño de controles.

La guía mencionada es un documento publicado por MINTIC en su quinta versión, en el año 2020. Este documento consolida un manual para la gestión de riesgos e implementación de controles asociados a la seguridad de la información en entidades públicas colombianas.

Los lineamientos mencionados son formulados en coherencia con las políticas de transparencia gubernamentales, y permiten la formulación de estrategias efectivas de acuerdo a una identificación eficaz de las necesidades de cada entidad. Se sugiere una metodología basada en la norma NTC ISO31000 numeral 2.4.

Ilustración 15. Infografía de metodología de Gestión de riesgo propuesta en la guía



Fuente. MINTIC. Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. Diciembre 2020.

Al revisar al detalle la metodología sugerida el documento, mostrada en la ilustración 15, es posible reconocer un protagonismo para los procesos asociados a identificación, valoración y mitigación de riesgos. Lo anterior permite afirmar que la guía en mención le apuesta a la formulación de estrategias preventivas en materia de ciberseguridad, basadas en un estudio previo de reconocimiento de necesidades y activos de una institución.

Así mismo es posible reconocer un factor comúnmente presente en estrategias del gobierno colombiano, y es la formulación de indicadores anticorrupción los cuales permiten asociar riesgos específicos que tiene que ver con posibles manipulaciones y fraude en la ejecución de un proceso. Este hecho realza la importancia, no solo de formular estrategias efectivas en materia de ciberseguridad, sino también de ejecutarlas en el marco de la transparencia y supervisión nacional.

- Evaluar las recomendaciones y modelos del MSPI de acuerdo a una identificación oportuna de amenazas.

  El modelo de Seguridad y Privacidad de la Información (MSPI) es un conjunto de guías e instructivos que consolida lineamientos técnicos y administrativos basados en buenas prácticas, que buscan orientar a las entidades públicas colombianas a una correcta gestión de la información. [34]

  Se recomienda que toda entidad pública en Colombia elaboré un Sistema de Gestión de Seguridad de la Información robusto, basado en los aspectos enmarcados en las 21 guías publicadas que conforman el MSPI. Esto incluye consideraciones en cuanto a pruebas de efectividad, roles y responsabilidades, gestión y clasificación de activos, gestión de riesgos, gestión de controles, seguridad en la nube, planes de capacitación y sensibilización, protocolo IPv4 e IPv6, gestión de incidentes, lineamientos para áreas financiera, etc.

  Es importante reconocer que los lineamientos del MSPI son actualizados regularmente, es responsabilidad de las entidades actualizar su SGSI con el fin de adoptar conductas modernas y confiables.

- Adoptar políticas de implementación y gestión avaladas por el MIPG en materia de TI

  El Modelo Integrado de Planeación y Gestión es un conjunto de lineamientos publicados por Función Pública, mediante el cual se promueve que todas las entidades de orden público en Colombia, desde el apoyo de cada una de sus

[34] MINTIC. ¿Qué es el MSPI?. Gobierno Digital. [sitio web] consulta realizada el 7 de abril de 2022. Disponible en https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

áreas, implemente políticas puntuales que garanticen la calidad en la ejecución de procesos.[35]

Es de gran importancia que las políticas que se adopten en materia de TI tengan coherencia con las políticas del MIPG que busca implementar cada entidad. Para ello se recomienda un análisis completo del SGSI y demás lineamientos en materia de TI, donde se verifique el cumplimiento de los estándares de calidad de la entidad.

Es importante reconocer que los lineamientos del MIPG están alineados con el MSPI publicado por MINTIC. Sin embargo, esta recomendación sugiere un análisis más integral, en colaboración con las demás áreas que forman la estructura organizacional de una entidad.

[35] FUNCIÓN PÚBLICA. MIPG. [sitio web] Consultado el 7 de Abril de 2022. Disponible en https://www.funcionpublica.gov.co/web/mipg

6. CONCLUSIONES

El análisis presentado sobre la situación de las entidades gubernamentales en Colombia, en materia de ciberseguridad, permite reconocer la necesidad de robustecer los sistemas y soluciones TI implementados, con el ánimo de asegurar la data y los recursos que se gestionan.

La necesidad descrita se justifica mediante el reconocimiento de una gran cantidad de data sensible gestionada y almacenada de forma digital al interior de las entidades de orden público colombianas, lo cual representa un activo valioso de información cuya protección debe ser priorizada. De la misma manera, se resalta la misionalidad de las entidades públicas como un interés de la nación y por ende, de los ciudadanos, ya que su operación contribuye a: procesos de administración pública, gestión de recursos públicos, procesos de justicia, proyectos productivos, desarrollo rural, desarrollo TI, proyectos de arte y cultura, desarrollo vial, procesos de reparación a víctimas de la violencia, entre otros.

A partir del reconocimiento de esta justificación, se analizan los beneficios que conlleva la inclusión de procesos asociados a hacking y ciberseguridad en la gestión de este tipo de entidades. Se identifica como ventaja principal la prevención de eventos desastrosos que afecten la misionalidad y los recursos, que al final son recursos financiados por los colombianos. De igual forma se reconoce una ventaja asociada al progreso de la nación mediante la implementación de tecnologías actualizadas y sistemas eficientes que además de salvaguardar la data permiten mejorar el rendimiento mediante la automatización de procesos.

De esta forma es posible enmarcar la importancia de contar con profesionales capacitados, organizados mediante roles ordenados, que identifiquen las necesidades de una entidad gubernamental, que justifiquen desde la teoría y los resultados la adquisición de recursos TI actualizados, que provean soluciones acordes a la necesidad y a los objetivos institucionales, y finalmente que gestionen métodos de seguimiento y control sobre los mecanismos de seguridad implementados.

En este orden de ideas, se reconoce el “hacking” como un concepto fundamental y transversal a la gestión de ciberseguridad que se lleva a cabo en una entidad de orden público en Colombia. Su relevancia se justifica en el hecho de que la capacidad de auditar ambientes informáticos, reconocer vulnerabilidades y riesgos, e implementar planes de mitigación y respuesta, son aptitudes asociadas a este campo de conocimiento, y sobre las cuales se fundamenta la implementación de un esquema de ciberseguridad eficiente.

7. RECOMENDACIONES

- Las entidades de orden público en Colombia requieren la incorporación de un grupo de ciberseguridad competente para garantizar los intereses de estado mediante el cumplimiento de las funciones de la entidad.

- La data que se gestiona al interior de las entidades públicas en Colombia por lo general involucra información sensible asociada a datos de ciudadanos o procesos de interés nacional.

- El progreso global asociada al uso de las tecnologías de la información y la comunicación, presiona a las entidades gubernamentales de Colombia a proveerse de recursos y profesionales que permitan afrontar la trasformación de procesos de la forma más segura posible.

- Robustecer los esquemas de ciberseguridad en una entidad pública colombiana, permite salvaguardar los intereses del estado, y por lo tanto los intereses de los ciudadanos.

- El registro histórico de ciberataques a entidades de orden público en Colombia permite reconocer una tendencia a atacar sitios web y herramientas gubernamentales, por lo general con motivaciones políticas o de protesta social.

- El conocimiento en hacking e intrusión es transversal a todos los procesos de ciberseguridad, debido a que los atacantes pueden utilizar cualquier vector del sistema para lograr una acción maliciosa.

- La infraestructura TI en entidades públicas colombianas debe ser aprovechada y redefinida de acuerdo a las necesidades organizacionales y a la disponibilidad de recursos.

- Los sistemas FIREWALL y DMZ son elementos esenciales de ciberseguridad, de fácil implementación, que favorecen el control y la gestión de riesgos al interior de una red corporativa.

- Definir los roles de CISO, CSO y DPO garantiza una jerarquía de directivos en materia de ciberseguridad que promueven la definición y el cumplimiento de un plan director el cual es favorable para cualquier organización.

- Las oficinas de tecnologías definidas al interior de entidades públicas en Colombia no pueden carecer de un grupo de ciberseguridad, debido a que siempre existen activos críticos que deben ser protegidos desde la gestión TI.

BIBLIOGRAFÍA

RUEDA QUINTERO Jeniffer. Impacto de la técnica de ataque de phishing en Colombia durante los últimos cinco años. UNAD. 2020 pp 15-80

ARSYS BLOG. Estos son los principales roles en la ciberseguridad. [sitio web] Consulta realizada el 02 de diciembre de 2021. Disponible en https://www.arsys.es/blog/principales-roles-ciberseguridad/

BELCIC, Iván. ¿Qué es exactamente el phishing? [sitio web]. Avast. Colombia. Consulta realizada el 20 de febrero de 2020. Disponible en https://www.avast.com/es-es/c-phishing

BELTRÁN BÁEZ A, CARRILLO CARRASCAL S. El acceso abusivo a sistemas informáticos en el ordenamiento jurídico colombiano: problemáticas y propuesta para su superación. Doctoral dissertation, Universidad del Rosario. 2017.

CANO JJ. Estudio de la evolución de la Seguridad de la Información en Colombia: 2000-2018. Revista Ibérica de Sistemas e Tecnologías de Informação. 2020. pp 470-483.

CASTRILLÓN DE LA OZ Fabio José. ¿Cuáles son los riesgos que tienen las empresas sobre la información contable y financiera con los hackers?. Universidad Cooperativa de Colombia. 2019

CASTRO BOLAÑOS Duvan, ROJAS MORA Ángela. Riesgos, amenazas y vulnerabilidades de los sistemas de información geográfica. Trabajo de grado. Universidad Católica de Colombia. 2013.pp 25-26

Castro Cubillos, S. M. White hat: hacking ético. Bachelor's thesis, Universidad Piloto de Colombia. 2017

COLOMBIA COMPRA. ¿Qué es SECOP? [sitio web] Consulta realizada el 21 de mayo de 2021. Disponible en https://colombiacompra.gov.co/secop/secop-i

CONGRESO DE COLOMBIA. Ley Estatutaria 1273 de 2009. 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. Colombia. 2009

CONGRESO DE COLOMBIA. Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales Colombia. 2012

CONGRESO DE COLOMBIA. Ley Estatutaria 1712 de 2014. Por medio del cual se

crea la ley de transparencia y del derecho de acceso a la información pública nacional. Colombia. 2018

CONGRESO DE COLOMBIA. Ley Estatutaria 1928 de 2018. por medio de la cual se aprueba el «convenio sobre la ciberdellncuencia», adoptado el 23 de noviembre de 2001, en budapest. Colombia. 2018

CONTADURÍA GENERAL DE LA NACIÓN. Preguntas frecuentes SIIF y SPGR [sitio web] Consulta realizada el 12 de mayo de 2021. Disponible en https://www.contaduria.gov.co/preguntas-acerca-del-siif-y-spgr

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Instructivo de la política para el tratamiento de datos personales. 2016. Pp 4-31

DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES 3701. Bogotá, Colombia. 2011

DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES 3854. Bogotá, Colombia. 2016

OSPINA DÍAZ Milton Ricardo. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Criminalidad. 2020. pp 199-217.

FISCALIA GENERAL DE LA NACIÓN. Datos abiertos de la Fiscalía General de la Nación. [en línea]. [Consultado: 05 de mayo de 2021]. Disponible en https://www.fiscalia.gov.co/colombia/gestion/estadisticas/

FUNCIÓN PÚBLICA. Glosario [sitio web] Colombia. Consulta realizada el 5 de noviembre de 2021. Disponible en https://www.funcionpublica.gov.co/glosario/-/wiki/Glosario+2/Entidad+Estatal

GACHARNÁ Federico.” hacker” ético vs. delincuente informático: Una mirada en el contexto colombiano. Universidad Minuto de Dios. 2009. pp 46-49.

GACHARNÁ Federico. El estigma hacker, entre lo bueno y lo malo. Universidad Minuto de Dios. 2011. pp 24-27.

GONZÁLEZ SOLARTE Nancy Adriana. Casos de estudio de cibercrimen en Colombia. UNAD. 2020. PP 23 - 44

HOYOS BUIRON Víctor Antonio. ¿Qué tal esta Colombia en cuestión de ciberseguridad? UMNG. 2015. Pp 1 – 19

INCIBE. CISO, CDO y ahora DPD: las siglas de la seguridad, los datos y la privacidad. [sitio web] España. 2018. [Consulta realizada el 9 de diciembre de 2021]

Disponible en https://www.incibe.es/protege-tu-empresa/blog/ciso-cdo-y-ahora-dpd-las-siglas-seguridad-los-datos-y-privacidad

INTEGRAITBLOG. Hackers necesarios para la seguridad de la información [sitio web] Consulta realizada el 15 de octubre de 2021. Disponible en https://integrait.com.mx/blog/seguridad-de-la-informacion-por-que-es-necesario-un-hacker/#:~:text=La%20importancia%20de%20los%20hackers%20dentro%20de%20la%20estrategia&text=Tienen%20la%20capacidad%20de%20conocer,salir%20airosos%20de%20un%20ataque.

IONOS. Ethical hacking: solucionar fallos de seguridad y prevenir la cibercriminalidad [sitio web] Ionos digital guide. 2020. Consulta realizada el 2 de diciembre de 2021. Disponible en https://www.ionos.es/digitalguide/servidores/seguridad/que-es-el-ethical-hacking/

ISOTOOLS. Norma ISO 27001:2013. [sitio web]. Consulta realizada el 5 de mayo de 2021. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

IT DIGITAL SECURITY. CISO y CSO: ¿tienes clara la diferencia de roles? [sitio web] España. 2018. [Consulta realizada el 10 de diciembre de 2021] Disponible en https://www.itdigitalsecurity.es/actualidad/2018/08/ciso-y-cso-tienes-clara-la-diferencia-de-roles

KASPERSKY. ¿Qué es la ciberseguridad? [sitio web]. Colombia. Consulta realizada el 28 de junio de 2021. Disponible en https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

LA ENCICLOPEDIA - RED CULTURAL DEL BANCO DE LA RÉPUBLICA. Estructura del Estado Colombiano. [sitio web]. Colombia. Consulta realizada el 12 de noviembre del 2021. Disponible en https://enciclopedia.banrepcultural.org/index.php/Estructura_del_Estado_colombiano#:~:text=El%20Estado%20colombiano%20est%C3%A1%20organizado,ejecutiva%20y%20la%20rama%20judicial.

MARTÍNEZ LÓPEZ Leidy Paola. El Cibercrimen en Colombia. UMNG. 2018. pp 1 - 19

MEDINA ROJAS Edwin Ferney. Hacking Ético: Una herramienta para la seguridad informática. Universidad Piloto de Colombia. Tesis. 2015. Pp 1 – 8

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1008 de 2018. **"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el**

capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" Colombia. 2018

MINTIC. Índice de información clasificada y reservada [sitio web] Colombia. Consulta realizada el 2 de septiembre del 2021. Disponible en https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135889:Indice-de-informacion-clasificada-y-reservada

MOLINA Pedro Antonio. El muisca es mucho más que un sistema informático. LEGIS. Revista 127.Colombia. 2005.

MONSALVE MENDEZ, Jaime Yesid. Ciberseguridad: principales amenazas en Colombia (ingeniería social, Phishing y Dos). (2018) pp 1-9.

OLMEDO Jorge Isaguirre. Análisis de los ciberataques realizados en América Latina. INNOVA Research Journal. 2018. pp172-181.

OSI. La importancia de las actualizaciones de seguridad [sitio web] Consulta realizada el 8 de agosto de 2021. Disponible en https://www.osi.es/es/actualizaciones-de-seguridad

PÉREZ PÉREZ Yuly. Importancia de la ciberseguridad en Colombia. Universidad Piloto de Colombia. Tesis. 2017. pp 1 – 9

POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias Cibercrimen Colombia 2019-2020 [en línea].2020 [Consultado: 03 de mayo de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

PROCURADURÍA GENERAL DE LA NACIÓN. Sistema de registro de sanciones y causas de inhabilidad. [sitio web] Consulta realizada el 5 de junio de 2021. Disponible en https://www.procuraduria.gov.co/portal/Siri.page#:~:text=Sistema%20de%20Informacion%20de%20Registro%20de%20Sanciones%20y%20Causas%20de%20Inhabilidad%20%2D%20SIRI,-Introducci%C3%B3n%20%2F%20Certificado%20de

RICHARDSON, Ronny; NORTH, Max M. Ransomware: Evolution, mitigation and prevention. International Management Review, (2017) pp 3-9.

SILVA CASTRO Larry Andrés. Análisis comparativo de las principales técnicas de hacking empresarial. Universidad Tecnológica de Pereira. 2011. PP 1 - 8

TAMAYO John Freddy. Usuarios y hackers, un riesgo en la transmisión de datos

financieros en Colombia. I+D REVISTA DE INVESTIGACIONES. 2013. PP 89-98.

OWASP. Ingeniería Social. [sitio web]. 2016. Consulta realizada el 1 de mayo de 2021. Disponible en: https://owasp.org/www.pdf-archive/02_INGENIER%C3%8DA_SOCIAL.pd

TROCHEZ Isabel Cristina. Revisión de la clasificación, categorías, métodos y efectos de la ciberdelincuencia en Colombia en la última década. Universidad Santiago de Cali. 2020. Pp 1 – 9

UNIR REVISTA. Principios de la seguridad Informática [sitio web] Consulta realizada el 24 de mayo de 2021. Disponible en https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/

VARGAS RUBIO, Paola Andrea. La demanda de los servicios de ciberseguridad se incrementó 40% a nivel nacional. La Republica. 2020.

VARÓN OLARTE Giovanny Fabián. Ciberterrorismo: De latente a evidente amenaza para las entidades públicas en Colombia. Universidad Piloto de Colombia. 2012. Pp 1 – 8

VIDAL LONDOÑO Jesús Hernán. Una nueva experiencia en seguridad hacking ético. UMNG. Trabajo de grado. 2017. pp 1 - 25

VILLAMIL BELTRÁN Wilmar Fabián. Gestión de riesgos en entidades del gobierno en Colombia. Universidad Piloto de Colombia. 2019. Pp 1 - 8

VILLANUEVA MÉNDEZ Julio César. La ciberdefensa en Colombia. Universidad Piloto de Colombia. 2015. Pp 1 - 9

WILHELM Thomas. Professional penetration testing: Creating and learning in a hacking lab. Newnes. ELSEVIER EDITORIAL. 2013 pp 11 – 35

WORLDSCHORALSHIPFORUM. ¿Qué hace un analista informático forense? Información profesional, salarios, conjunto de habilidades. [sitio web] Colombia. 2021. [Consulta realizada el 5 de diciembre de 2021] Disponible en https://worldscholarshipforum.com/es/forensic-computer-analyst/#:~:text=Los%20analistas%20forenses%20inform%C3%A1ticos%20combinan,y%20tambi%C3%A9n%20de%20recuperar%20pruebas.

Estructura del documento para la estructura del Resumen Analítica Especializado -RAE

Fecha de Realización:	22/03/2021
Programa:	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Línea de Investigación:	Infraestructura Tecnológica y Seguridad en redes
Título:	LA IMPORTANCIA DEL HACKING EN LA CIBERSEGURIDAD A NIVEL ORGANIZACIONAL EN ENTIDADES DE ORDEN PUBLICO EN COLOMBIA.
Autor(es):	ROZO DÍAZ JUAN FELIPE
Palabras Claves:	Hacking, White hacker, Vulnerabilidades, Pentesting, Intrusión.
Descripción:	La presente investigación enmarca de forma teórica las capacidades de un profesional en ciberseguridad orientado al hacking y la intrusión, con el fin de reconocer la importancia de contar con este tipo de perfiles en el equipo de TI de una entidad pública en Colombia. El desarrollo de la investigación se hace mediante una contextualización al mundo del hacking y un repaso histórico por la evolución que ha tenido el gobierno colombiano en la implementación de la ciberseguridad dentro de sus políticas públicas. Después se busca reconocer las vulnerabilidades y posibles consecuencias que puede traer para el gobierno colombiano el hecho de ignorar el riesgo a sufrir ciberataques en las organizaciones de gobierno. Finalmente se especifican características recomendadas de perfiles profesionales e infraestructura TI, las cuales buscan otorgar una guía para las entidades estatales de Colombia, mediante la cual puedan reconocer sus necesidades y el papel de la ciberseguridad con base a factores como el sector, el tamaño y la vigencia proyectada de la organización.

Fuentes bibliográficas destacadas:

Beltrán Báez, A., & Carrillo Carrascal, S. (2017). El acceso abusivo a sistemas informáticos en el ordenamiento jurídico colombiano: problemáticas y propuesta para su superación (Doctoral dissertation, Universidad del Rosario).

Cano, J. J., & Almanza, A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000-2018. Revista Ibérica de Sistemas e Tecnologias de Informação, (E27), 470-483.

Castrillón de la Hoz, F. J., & López Torregrosa, J. E. (2019). ¿Cuáles son los riesgos que tienen las empresas sobre la información contable y financiera con los hackers?

Castro Cubillos, S. M. (2017). White hat: hacking ético (Bachelor's thesis, Universidad Piloto de Colombia).

Díaz, M. R. O., & Rangel, P. E. S. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Criminalidad, 62(2), 199-217.

Gacharná G., F. (2009). Hacker ético vs. delincuente informático: Una mirada en el contexto colombiano. INVENTUM, 4(6), 46-49. https://doi.org/10.26620/uniminuto.inventum.4.6.2009.46-49

Contenido del documento:	La monografía presentada inicia con el planteamiento de la problemática seleccionada y la definición de objetivos asociados. Posteriormente se enmarca el conocimiento mediante una revisión teórica e histórica de incidentes de ciberseguridad en entidades de orden público en Colombia. Después se presenta el desarrollo de cada uno de los tres objetivos específicos, donde se consolidan las necesidades en ciberseguridad de las entidades públicas colombianas, las ventajas de la inclusión de profesionales TI especialistas en este campo y recomendaciones en cuanto a infraestructura y perfiles profesionales para un grupo de ciberseguridad. Finalmente se detallan las conclusiones y recomendaciones obtenidas a partir del análisis desarrollado, así como las referencias bibliográficas consultadas en el proceso.
Conceptos adquiridos :	A partir del desarrollo de la presente investigación se adquieren conocimientos útiles en materia de ciberseguridad, enmarcados en su aplicación y análisis sobre el sector público colombiano y la gestión de seguridad informática en las entidades de esta índole.

	Se fortalecen conocimientos asociados a normatividad, legislación, estructura y regulaciones relacionadas a entidades públicas en Colombia. Se fortalecen conocimientos asociados a infraestructura TI seguras, pruebas de intrusión, tipos de ciberataques, medidas de prevención y mitigación de riesgos de ciberseguridad, entre otros conceptos asociados a seguridad de la información orientada al sector publico colombiano. Finalmente, es importante mencionar que se adquiere capacidad crítica de análisis partir de la cual es posible evaluar el panorama de ciberseguridad del gobierno colombiano, promoviendo así la propuesta de reformas para las políticas de ciberseguridad orientadas a un mejoramiento de gestión de recursos y respuesta a incidentes.
Conclusiones:	El análisis presentado sobre la situación de las entidades gubernamentales en Colombia, en materia de ciberseguridad, permite reconocer la necesidad de robustecer los sistemas y soluciones TI implementados, con el ánimo de asegurar la data y los recursos que se gestionan. La necesidad descrita se justifica mediante el reconocimiento de una gran cantidad de data sensible gestionada y almacenada de forma digital al interior de las entidades de orden público colombianas, lo cual representa un activo valioso de información cuya protección debe ser priorizada. De la misma manera, se resalta la misionalidad de las entidades públicas como un interés de la nación y por ende, de los ciudadanos, ya que su operación contribuye a: procesos de administración pública, gestión de recursos públicos, procesos de justicia, proyectos productivos, desarrollo rural, desarrollo TI, proyectos de arte y cultura, desarrollo vial, procesos de reparación a víctimas de la violencia, entre otros.