POSICIONAMIENTO DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES PÚBLICAS DE COLOMBIA

Valenzuela Buitrago, Juan Carlos.
Juanc9010@hotmail.com
Universidad Piloto de Colombia

***Resumen*—** El país se encuentra en medio de un proceso de digitalización y transformación digital que está impactando en igual medida a todos los actores de la sociedad colombiana (Ciudadanía, Empresas Privadas y Públicas), bien sea para el consumo de servicios o la provisión de estos, en este sentido, el uso de la tecnología como canal para obtener o brindar servicios se ha vuelto un aliado fundamental para ello.

En el caso específico del sector público, se ha incrementado exponencialmente el uso de la tecnología para la prestación de servicios y trámites para los ciudadanos, sin una proyección alineada con la gestión de la seguridad de la información, es decir, se trabajó primero en brindar los servicios sin primero fortalecer internamente a las entidades en temas de seguridad informática y seguridad de la información, haciendo que estos temas pasaran a un segundo plano.

El presente documento busca detallar cual es el rol del Oficial de Seguridad de la Información y que funciones cumple dentro de las entidades públicas, para luego mostrar cómo ha ido evolucionando a través de los últimos años el índice de adopción de este rol, teniendo como base estudios realizados por distintos entes como el Ministerio de Tecnologías de la Información y las Comunicaciones y la OEA (Organización de Estados Americanos)

Así mismo el documento demostrará las estrategias que el Gobierno de Colombia ha desarrollado o se encuentra desarrollando en los últimos años para dar impulso a la adopción de este rol de "Responsable de Seguridad Digital" en el sector público.

***Abstract*—** The country is passing through a process of digital transformation that is having an impact on all the stakeholders of the Colombian society (Public and Private Entities and Citizens) in the same way for the provision of services or the use of them, in this way, the use of Information Technologies as a mean for provide or consume the services, is becoming an strategical ally.

In the case of the public sector, the use of IT has increased exponentially to provide services for the citizens, without a proper projection aligned with Information Security, in other words, the sector only worried about to launch digital services without strengthen internally about IT Security or Information Security, letting this subjects in second plain.

This document will give details about what is the CISO (Chief Information Security Officer), which are the main responsibilities and show how the adoption index in this role has evolved in the last years, taking as base some investigations made by the Ministry of Information and Communications Technology and OAS (Organization of American States).

Likewise, the document will show the strategies that the Government of Colombia has developed or are being implemented in the last few years to give an impulse to the adoption of this role of "Chief Information Security Officer" in the public sector.

***Índice de Términos*—**Oficial de Seguridad, Sistema de Gestión de Seguridad de la Información, Política de Seguridad Digital, Modelo Integrado de Planeación y Gestión.

I. INTRODUCCIÓN

La intención de los últimos años de gobierno en cuanto a las TIC (Tecnologías de la Información y las Comunicaciones), ha sido que todas las entidades públicas inicien un proceso de digitalización, con un único objetivo, brindar más y mejores servicios a los ciudadanos a través de internet desde la comodidad de sus hogares, para que no existan más filas en las oficinas de las entidades públicas, sino que, al contrario, los sistemas de información y los trámites estén a la orden de las exigencias que tiene la población colombiana, empleando para ello las TIC.

El inconveniente con esto es que se han focalizado los esfuerzos en implementación de servicios de una

manera desmedida, sin tener en cuenta, otros factores que se encuentran enmarcados en la Estrategia de Gobierno En Línea (ahora Gobierno Digital) y que debían desarrollarse paralelamente al aprovisionamiento de nuevos servicios, para fortalecer el BackOffice (Interior) de las entidades públicas como, por ejemplo: Interoperabilidad, Arquitectura de TI y Seguridad de la Información.

Este último, busca que todas las entidades implementen los lineamientos para establecer y mantener un sistema de gestión de seguridad de la información, que garantice no solo la protección de la información que las entidades tienen en su poder, sino que los servicios que se presten a través del entorno digital se presten de una manera segura y adecuada, dando así, confianza al ciudadano en su interacción con el Estado a través de estos canales.

Este componente ha enfrentado diversas dificultades, entre las cuáles se destaca la ausencia del Rol del "Oficial de Seguridad de la Información", quien es el líder en la implementación de este componente en una entidad y en muchos casos su ausencia, es la causa principal por la que estos lineamientos no se implementan o se llevan a cabo actualmente o de manera deficiente en las entidades públicas.

Pero ¿Qué es y que labores desempeña un oficial de seguridad de la información en una entidad?

II. EL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN Y SUS FUNCIONES

El oficial de seguridad de la información nace oficialmente en el año de 1994, cuando el gigante financiero Citigroup (en ese entonces Citi Corp. Inc.) sufrió una serie de ciberataques por parte de un ciberdelincuente ruso llamado Vladimir Levin, por esta razón el banco creó la primer Oficina Ejecutiva de Ciberseguridad y contrató a Steve Katz para liderarla [1].

Es un rol que constantemente se encuentra evolucionando, dadas las condiciones en las que este se desenvuelve dentro de una entidad, inicialmente, se designaba a una persona de TI para que administrara los dispositivos de seguridad en las entidades y con ello se percibía como suficiente el esfuerzo que una entidad realizaba para protegerse en el entorno digital.

Sin embargo, al ver que la seguridad de los datos y de la información no solamente se limitaba al uso de la tecnología, sino que, por el contrario, trascendía a cualquier proceso de una entidad, se empezó a requerir de un ROL con una perspectiva y visión más amplios, que guiara a toda la organización hacia la debida protección de toda la información, sin importar si está física o digitalmente almacenada en algún medio.

Según la revista FORBES, el mantener la Seguridad de la Información bajo un terreno plenamente tecnológico (o dependiendo de la Oficina de Tecnología), hace que esta se aísle de los problemas que pueda enfrentar el negocio y de la toma de decisiones a un nivel transversal, por ejemplo, los equipos de seguridad no tienen visibilidad sobre la planificación o toma de decisiones en áreas como Recursos Humanos o las áreas de I+D (Investigación y Desarrollo) y solo se acude a la seguridad cuando los problemas o riesgos están latentes o se materializan los incidentes [2].

Con base a lo anterior y evidenciando la evolución que han tenido el Rol del Oficial de Seguridad, se han definido unas responsabilidades muy específicas, sin embargo, estas pueden variar según el nivel de robustez o de necesidades que tenga la entidad, la SANS Institute [3] ilustra las siguientes responsabilidades:

- Balancear las necesidades de seguridad con los planes estratégicos del negocio, identificando factores de riesgo y determinar soluciones para mitigar.

- Supervisar la selección, despliegue y mantenimiento de las soluciones de seguridad de la entidad.

- Actuar como el representante de la organización respecto a las solicitudes hechas por clientes, terceros y el público en general relacionado con la estrategia de seguridad de la entidad.

- Actuar como el representante de la organización relacionado al cumplimiento de la ley o situaciones donde sea necesaria la investigación de fuentes de ataques a la red o algún robo de información por parte de empleados.

- Planificar y probar respuestas a las brechas de seguridad incluyendo la posibilidad de discutir los resultados con clientes, socios o el público en general.

A nivel técnico, la CNBC [4], relaciona una recopilación de actividades qué según la industria, la academia y otros expertos en el área de la ciberseguridad, deben ser realizado por el Oficial de Seguridad de la Información:

- Operaciones de Seguridad
- Riesgos de Ciberseguridad y ciberinteligencia.
- Prevención de perdida de información.
- Arquitecturas de Seguridad.
- Gestión de accesos.

III. ESTADO ACTUAL DE ADOPCIÓN DEL ROL DE OFICIAL EN EL PAÍS:

El Gobierno nacional, a través de diferentes estudios ha buscado medir en los últimos años varias características relacionadas con la seguridad digital como la cultura, la apropiación, los recursos o el personal requerido para ejecutar las tareas de seguridad, donde se ha preguntado también sobre la adopción o designación del Rol de "Oficial de Seguridad" en las entidades públicas.

A continuación, se presentarán algunos resultados de los estudios más significativos hasta la fecha:

A. Año 2016 – Infografía Sigma Dos

Con base a un Sondeo efectuado en 2016 en el que participaron más de 1266 entidades públicas (casi el 93% de todas las entidades), el 21% de las entidades públicas en general, argumentó que contaban con un funcionario o Rol de Oficial de Seguridad dentro de su entidad, dejando así un 79% de entidades sin ningún tipo de representante o funcionario dedicado a estas labores de seguridad.

Fig 1. Infografía Apropiación en Seguridad de la Información, MinTIC 2016 **[5]**.

B. Año 2017 – Estudio de Impacto de los Incidentes de Seguridad Digital en Colombia

Durante el año 2017, el Ministerio TIC, la OEA (Organización de Estados Americanos) y el BID (Banco Interamericano del Desarrollo), llevaron a cabo el "*Estudio de Impacto de los Incidentes de Seguridad Digital en Colombia*", con el objetivo de "tener una visión completa de los ataques que sufren tanto el sector público como el privado, así como su nivel de preparación para defenderse de dichos ataques.

En la Sección 2 de este documento, se encuentra el análisis focalizado hacia el sector público. Dentro de esta sección se encontró la siguiente pregunta relacionada con el Oficial de Seguridad de la Información o un área con estas funciones en las entidades públicas: **"¿Tiene su entidad un área, cargo (s) o rol(es) dedicado (s) a la seguridad digital (seguridad digital y/o de seguridad de la información)? [**6**]"**

Donde la respuesta fue "*Entre las entidades públicas, solo el **33% a nivel nacional** y el **10% y 17% a nivel municipal y departamental**, respectivamente, tienen un área dedicada a la seguridad digital dentro de su organización. Se observó que existe una tendencia general a transferir la responsabilidad de la respuesta a incidentes y la seguridad digital bajo las funciones generales de los departamentos de tecnología de la información*". En la siguiente gráfica se puede evidenciar las estadísticas previamente indicadas:

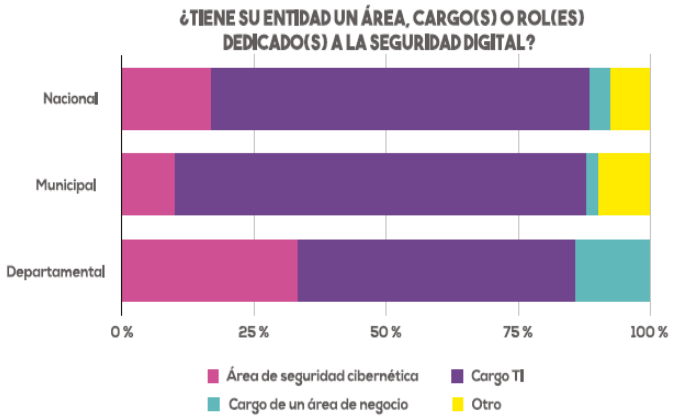

Fig 2. ¿Tiene su Entidad un Área, Cargo o rol dedicado a la seguridad digital? Estudio de Impacto Económico de los Incidentes Digitales en Colombia en 2017 **[6]**.

El estudio también precisó que el 52% a nivel nacional, el 78% a nivel municipal y el 72% a nivel departamental abordan la cuestión de la seguridad digital bajo el Departamento de Tecnología de la Información. Solamente un porcentaje muy pequeño de los entrevistados abordó esto bajo las áreas de negocio generales de las entidades u otras áreas.

Si se comparan los dos datos de las investigaciones en los últimos años se obtienen las siguientes variaciones:

TABLA I. COMPARATIVO ADOPCIÓN OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

ENTIDADES	AÑO 2016	AÑO 2017	VARIACIÓN
NACIONALES	25%	33%	**+8%**
TERRITORIALES	20%	17%	**-3%**

La diferencia al año 2017 respecto a este rol entre entidades nacionales y entidades territoriales se ha hecho mucho mayor con una diferencia de casi el **16%** en la adopción de esta posición.

Existen varias causas para estos resultados, las cuales se indicarán en la siguiente sección.

IV. CAUSAS DEL BAJO ÍNDICE DE OFICIALES DE SEGURIDAD EN LAS ENTIDADES PÚBLICAS

Con base a los resultados previamente ilustrado, en el entorno actual del país se pueden identificar varias debilidades o causas que justifican estos índices, que han dificultado el posicionamiento tanto de las políticas de seguridad digital como el Rol del Oficial de Seguridad, dichas causas se han analizado y se han dividido en dos ámbitos, Legal e Institucional:

A. Debilidades A Nivel Legal Y Normativo

La legislación actual que tiene alguna relación con seguridad de la información (O Seguridad Digital) como por ejemplo la estrategia de gobierno digital (Decreto 1008 de 2018) o el CONPES 3854 (11 de abril de 2016), tienen unas limitantes bastantes grandes cómo, por ejemplo:

1. Se indica que toda la estrategia de gobierno digital debe estar liderada por la Oficina de TI, como el componente transversal de seguridad de la información se encuentra inmerso en la estrategia, se asume que este componente también debe ser asumido por la oficina de TI, anulando la independencia que este Rol debe tener dentro de una entidad.

2. El CONPES 3854, tiene muy buenas intenciones en la consolidación de un entorno digital seguro, sin embargo, no plantea soluciones directas y concretas para aumentar el presupuesto para seguridad digital en las entidades, ni tampoco para la designación de un responsable de seguridad digital en cada

entidad (indica que deben definirse estos roles, pero no define directamente como hacerlo ni con qué recursos).

3. La seguridad digital tiene mucha importancia mediática (se habla mucho en conferencias, charlas, foros etc…) pero no se ha considerado aún como una política de Estado dada la importancia que tiene actualmente y que tendrá a futuro (una vez todas las entidades públicas y también privadas lleguen a un grado de digitalización casi completo y todo se haga a través del entorno digital los riesgos serán mucho mayores).

4. No existen herramientas o lineamientos a nivel legal que obliguen al nombramiento de un oficial de seguridad o "Responsable de Seguridad" en las entidades públicas, una ventaja que si tiene la posición de CIO (Chief Information Officer) a través del decreto 415 de 2016.

Estas debilidades en el marco legal, a su vez no han permitido que las debilidades a nivel institucional que enfrentan las entidades puedan superarse, es decir, las políticas a la fecha no han surtido los resultados esperados, por lo menos en lo que al Oficial de Seguridad concierne.

B. Debilidades A Nivel Institucional

Las entidades públicas aún no priorizan las temáticas de gobierno digital (algunas ni siquiera cuentan con una oficina de tecnología), ni con un CIO o Jefe de Oficina de TI incumpliendo inclusive con normativas como el Decreto 415 de 2016, que hace obligatorio el nombramiento del CIO, entonces se infiere que si no existe ni siquiera un cargo relacionado con el liderazgo a nivel de tecnologías de la información, la adopción de un rol relacionado con la seguridad de la información será mucho menor.

También se observan debilidades a nivel económico en las entidades públicas, el Estudio de Impacto económico indicó que "*la inversión en las entidades públicas, la estimación de la mediana del presupuesto asignado a la seguridad digital en relación con el presupuesto de inversión fue aproximadamente 0,05% del total de las inversiones en 2016, es decir, cuando se asignó presupuesto a la seguridad digital, este presupuesto* ***no llegó a 1% de las ventas o inversiones de las organizaciones en 2016****. Además, se verificó que, en promedio simple, la mayor parte del presupuesto fue asignado para plataformas y medios tecnológicos, mientras la generación de capacidades recibió la menor cantidad de recursos tanto en las organizaciones públicas como en las privadas*" [7], en conclusión, las entidades públicas no invierten en seguridad (tanto en componentes tecnológicos enfocados a la seguridad ni tampoco para la generación de capacidades en seguridad de la información).

Finalmente, también se identifica que las personas que son designadas como "Oficiales de Seguridad" son comúnmente trabajadores por prestación de servicios (OPS), ya que no es posible designarlos dentro de la nómina de una entidad, al ser un cargo que no existe legalmente en el organigrama de las entidades públicas ni está aprobado por el Departamento Administrativo de la Función Pública (DAFP), esto a su vez causa una alta rotación del personal encargado de la seguridad en las entidades, llevando a implementaciones deficientes de los sistemas de gestión, retrasos e inestabilidad para la entidad.

V. ESTRATEGIAS Y ACCIONES DESARROLLADAS POR EL GOBIERNO PARA POSICIONAR AL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta lo visto en las infografías previamente ilustradas, el Ministerio de Tecnologías de la Información y las Comunicaciones ha desarrollado estrategias para impulsar el posicionamiento de este rol en las

entidades públicas, como complemente a lo ya impulsado a través del CONPES 3854.

A. MIPG (Modelo Integrado de Planeación y Gestión v2)

El Modelo Integrado de Planeación y Gestión (MIPG), "*es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto 1499 de 2017"* [8]. Dentro de este Modelo se manejan varias dimensiones y políticas dentro de las cuáles se destaca la "Política de Seguridad Digital".

Esta política se encuentra consignada en la sección **3.2.1.4** del MIPG y menciona lo siguiente respecto al rol del Oficial de Seguridad: "*…en el Comité Institucional de Gestión y Desempeño se deben articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política. Para ello, se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área que haga parte de la Alta Dirección. Para las entidades cabeza de sector, el Responsable de Seguridad Digital será el enlace sectorial*".

Lo anterior da a conocer de manera directa a todas las entidades públicas de la existencia y la importancia de este Rol y su ubicación en un área estratégica.

Así hace al responsable de seguridad, parte activa de los sistemas de gestión de las entidades, en especial del Sistema de Gestión de Seguridad de la Información (MSPI).

B. Guía para la Administración de Riesgos de Gestión, Corrupción y Seguridad Digital

De manera articulada entre el Ministerio de Tecnologías de la Información y las Comunicaciones, la Función Pública y la Secretaría de Transparencia de la Presidencia de la República, en agosto de 2018 se expiden la primera versión de la "*Guía para la Administración de Riesgos de Gestión, Corrupción y Seguridad Digital*", en la que se relaciona la tipología de riesgos de seguridad digital que deben ser tenida en cuenta en el proceso de gestión y administración de las entidades de la rama ejecutiva y todas las entidades públicas en general.

Así, las entidades públicas emplearán una única metodología para gestionar todo tipo de riesgos en su entidad, adicionando el enfoque de seguridad digital y su análisis basado en activos, a su vez dando fuerza al responsable de seguridad digital en la entidad, que debería tener las siguientes responsabilidades, según el Anexo 4 de esta guía [9]:

- Definir el procedimiento para la Identificación y Valoración de Activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa (líderes de procesos) en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

Así, las actividades de gestión de riesgos de seguridad adquieren un significado transversal en las entidades en acompañamiento constante del Oficial de Seguridad.

C. Posicionamiento en el Manual de Gobierno Digital

En la sección 1.6 del nuevo manual de gobierno digital denominada "¿Quiénes ejecutan la política?", se habla de varios roles que hacen parte importante de la implementación de la estrategia, dentro de los cuáles se destaca el "Responsable de Seguridad Digital", aquí se menciona que "…*se debe designar un Responsable de Seguridad de la Información que a su vez responderá por la Seguridad Digital en la entidad, el cual debe pertenecer a un área que haga parte del direccionamiento estratégico o Alta Dirección"*[10].

En el manual se destacan algunas de las principales características o responsabilidades que debe cumplir este rol de seguridad:

- Se debe apoyar fundamentalmente en el CIO de la entidad para mitigar los riesgos asociados a la tecnología (Seguridad Informática o Ciberseguridad), también se debe apoyar en otras áreas que permitan mitigar otros tipos de riesgos de seguridad de la información, Ej. Recursos Físicos, Talento Humano entre otras.

- Debe apoyar a los líderes de los procesos o áreas de la entidad, con el objetivo de implementar adecuadamente los lineamientos, esto incluye la identificación de los activos y los riesgos derivados en estos.

- Cumplir con lo designado en la guía de roles y responsabilidades (Guía #6) del Modelo de Seguridad y Privacidad de la Información.

Finalmente, para consolidar este rol a nivel institucional, el manual hace la siguiente sugerencia a todas las entidades: *"…Para lograr un adecuado balance entre funcionalidad y seguridad, se recomienda que el elemento transversal de seguridad de la información opere de manera independiente a la Oficina de T.I. En este caso, la entidad puede decidir si considera ubicar esta iniciativa en un área como planeación, gestión de riesgos, procesos o cualquier área que tenga alcance transversal en la entidad o crear una nueva área dedicada a la seguridad de la información"*.

D. Generación de Capacidades

Otra de las iniciativas que se ha ido desarrollando en los últimos años ha sido las convocatorias para financiar la realización de cursos, certificaciones y diplomados en temas relacionados con Gestión de Tecnologías de Información y Seguridad de la Información.

El Ministerio TIC, argumenta que "…*teniendo en cuenta los resultados del FURAG (Formulario Único del Avance de la Gestión) de las mediciones correspondientes a las vigencias 2016 y 2017 y por otro lado el resultado de los sondeos de mercados realizados durante la vigencia 2017 evidenciaron la necesidad de fortalecer las competencias de los líderes de gestión TI y líderes de Seguridad de la Información de las diferentes Entidades, sus equipos de trabajo; toda vez que en la medida en que las Entidades cuenten con profesionales debidamente capacitados en los temas de TI y Seguridad de la información, se optimizará el uso de los recursos tecnológicos y se minimizará el riesgo de daños y/o perdida de información, sistemas y equipos por uso inadecuado*"[11].

Es decir, que con base a los resultados y mediciones realizadas (ilustradas previamente en este artículo) se ha considerado necesario fortalecer los conocimientos en este campo a los funcionarios y servidores públicos que ejercen estas labores. A 2018, se han llevado a cabo un total de 5

convocatorias a través de convenios con ICETEX, dejando un total de 529 funcionarios capacitados y certificados a través de modelos de condonación, es decir, que, si se cumplen los requisitos y se aprueban los cursos, los funcionarios no deben pagar por el beneficio recibido.

Teniendo en cuenta todas las estrategias anteriores y que la Política de Seguridad Digital (CONPES 3854) está en plena fase de implementación, se espera que estos niveles de adopción del Oficial de Seguridad aumenten, permitiendo proporcionalmente mejoras en los niveles de seguridad en las entidades públicas.

Como se observa a lo largo del artículo, queda un largo camino para poder consolidar este rol dentro del sector público y poder así aumentar los índices de seguridad de la información en las entidades públicas.

VI. CONCLUSIONES

El Oficial de Seguridad de la Información es un Rol que aún está en proceso de adopción por parte de la Alta Dirección de las entidades públicas.

Una de las causas por las cuales no existe el responsable de seguridad en una entidad pública es la falta de presupuesto, dado que se requiere de una persona con unas capacidades específicas, tanto estratégicas, como técnicas, que puedan guiar adecuadamente la implementación del SGSI, como los objetivos institucionales a través de la seguridad de la información, además no solamente se requiere de presupuesto para mantener una persona con este perfil, sino que también el Sistema de Gestión de Seguridad en sí mismo, necesita de inversión en controles para mitigación de riesgos de tipo tecnológico (Firewalls, IPS, Antivirus, Cifrado, Soluciones en la Nube ETC…) y tampoco existe presupuesto para estas temáticas.

Muchas entidades desconocen cuales son las funciones que debe cumplir el Oficial de Seguridad de la Información, por lo que deciden no prestar atención al tema.

Debería articularse una iniciativa entre el Ministerio de Tecnologías de la Información (Líder de la política de seguridad digital – CONPES 3854) y el Departamento Administrativo de la Función Pública), para la creación y definición oficial del rol de “Oficial de Seguridad Digital” en todas las entidades públicas, esto facilitará continuidad en el tiempo de esta iniciativa y permitirá tener un responsable directo respecto a la seguridad digital.

La seguridad digital debería considerarse como una política de Estado y no solamente como una política de gobierno, para que las estrategias pueden implementarse con los recursos y personal suficientes (Oficiales de Seguridad en todas las entidades públicas), para poder garantizar la privacidad y la integridad de los datos y la continuidad de los servicios en las entidades públicas.

REFERENCIAS

[1] CNBC. Here's what cybersecurity professionals at companies actually do, and why they're so vital. [Online]. Disponible: https://www.cnbc.com/2018/07/20/what-is-ciso-chief-information-security-officer.html

[2] FORBES. Why It's Worth Divorcing Information Security From IT. (2015). [Online]. Disponible: https://www.forbes.com/sites/frontline/2015/06/22/why-its-worth-divorcing-information-security-from-it/#f61e5f742a33

[3] SANS Institute. Mixing Technology and Business: The Roles and Responsibilities of the Chief Information Security Officer (2003). [Online]. Disponible: https://www.sans.org/reading-room/whitepapers/assurance/mixing-technology-business-roles-responsibilities-chief-information-security-officer-1044

[4] CNBC. Here's what cybersecurity professionals at companies actually do, and why they're so vital. [Online]. Disponible: https://www.cnbc.com/2018/07/20/what-is-ciso-chief-information-security-officer.html

[5] Infografía Apropiación en Seguridad de la Información, Gloria Gallego Sigma 2 Proyecto MinTIC 2016.
[6] Organización de los Estados Americanos (OEA); Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC); Banco Interamericano de Desarrollo (BID). Impacto de los incidentes de seguridad digital en Colombia 2017. Pag 78-79. [Online]. Disponible: https://publications.iadb.org/handle/11319/8552?locale-attribute=es
[7] Organización de los Estados Americanos (OEA); Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC); Banco Interamericano de Desarrollo (BID). Impacto de los incidentes de seguridad digital en Colombia 2017. Pag 17. [Online].
[8] Departamento Administrativo de Función Pública. Modelo Integrado de Planeación y Gestión v2 (2018). Pág. 10 [Online]. Disponible: http://www.funcionpublica.gov.co/documents/28587410/34112007/Manual+Operativo+MIPG.pdf/ce5461b4-97b7-be3b-b243-781bbd1575f3
[9] Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Departamento Administrativo de Función Pública. Guía de Administración de Riesgos de Gestión Corrupción y Seguridad Digital, Anexo 4, Pag. 10 http://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b
[10] Ministerio de Tecnologías de la Información y las Comunicaciones. Manual de Gobierno Digital. Pag 19-20 (2018). [Online]. Disponible: http://estrategia.gobiernoenlinea.gov.co/623/articles-7929_recurso_1.pdf
[11] ICETEX. Quinta convocatoria para financiar cursos, certificaciones y diplomados en gestión TI y seguridad de la información (2018) [Online]. Disponible: https://portal.icetex.gov.co/Portal/docs/default-source/alianzas-y-fondos/fondos/texto-convocatoria/texto-de-convocatoria-5-convocatoria.pdf?sfvrsn=6

Autor

Juan Carlos Valenzuela Buitrago, Ingeniero En Telecomunicaciones, estudiante de la Especialización en Seguridad Informática.