Propuesta metodológica para la implementación de un marco de referencia Framework de ciberseguridad en el Icfes

John Carlos Angarita Quiroga

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

Ministerio de Defensa Nacional

Comando General de las Fuerzas Militares

Escuela Superior de Guerra

General Rafael Reyes Prieto

Propuesta metodológica para la implementación de un marco de referencia (*framework*) de ciberseguridad en el Icfes

Estudiante:

John Carlos Angarita Quiroga

Identificación:

79.610.700

Maestría en Ciberseguridad y Ciberdefensa

Trabajo de grado

Bogotá, D.C. - Colombia

Octubre de 2020

Ministerio de Defensa Nacional

Comando General de las Fuerzas Militares

Escuela Superior de Guerra

General Rafael Reyes Prieto

Propuesta metodológica para la implementación de un marco de referencia (*framework*) de ciberseguridad en el Icfes

Director

Doctor Carlos Castañeda Marroquín

Maestría en Ciberseguridad y Ciberdefensa

Trabajo de grado

Bogotá, D.C. - Colombia

Octubre de 2020

Nota de aceptación:

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

"Otra característica de la naturaleza humana, quizás la que más nos hace humanos, es nuestra capacidad de hacer lo antinatural, de trascender y, por lo tanto, de transformar nuestra naturaleza".

Dr. M. Scott Peck

AGRADECIMIENTOS

Agradezco al Ministerio de Tecnologías de la Información y las Comunicaciones y a la Escuela Superior de Guerra (Esdeg), por la oportunidad brindada para ser parte de este selecto grupo de la Maestría en Ciberseguridad y Ciberdefensa.

Agradezco a mi entidad, a mis jefes y compañeros de trabajo, por permitirme llevar a cabo este proceso profesional que, sin su apoyo, no hubiera sido posible.

Agradezco a cada uno de mis compañeros de la maestría por darme un pedacito de su conocimiento, el cual es, sin lugar a dudas, amplio por su experiencia y trayectoria profesional.

Agradezco especialmente al doctor Carlos Castañeda Marroquín por su entrega como tutor de esta monografía. Gracias a sus consejos y presiones se logró el objetivo planteado con excelentes resultados para mi vida tanto personal como profesional.

Gracias a todos mis allegados. Dios los bendiga grandemente.

DEDICATORIA

Esta monografía la quiero dedicar ante todo a mi Padre celestial, quien cada día me lleva a ocupar lugares de privilegio, me renueva las fuerzas y me concede sus bendiciones sobreabundantes.

Segundo, a mi amada familia. Mi queridísima esposita, quien es mi ayuda idónea y apoyo incondicional. A mis queridos hijos, Paulita, Sarita y Davidcito, quienes con sus consejos y apoyo permitieron que en el seno de mi hogar pudiera avanzar en este logro profesional. A mis padres y hermanos, que comparten cada bendición que el Señor me da.

A ellos, que me permitieron quitarles un poco de su tiempo para lograr este sueño.

Los amo con todo mi corazón; son mi motor diario para levantarme cada día y ser un mejor esposo, mejor padre, mejor hijo, mejor hermano… mejor cristiano.

AUTORIZACIÓN

El doctor Carlos Castañeda Marroquín, tutor principal, investigador y docente de la Escuela Superior de Guerra. Departamento de Ciberseguridad y Ciberdefensa.

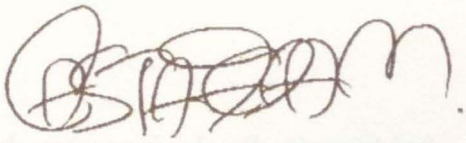
AUTORIZA:

La presentación de la monografía de maestría titulada:

Propuesta metodológica para la implementación de un marco de referencia (*framework*) de ciberseguridad en el Icfes.

Realizada por el ingeniero John Carlos Angarita Quiroga, y que cumple con los requisitos exigidos por la Escuela Superior de Guerra.

Firma:



Carlos Castañeda Marroquín, Ph.D.

RESUMEN EJECUTIVO

El tratamiento de los riesgos cibernéticos en las organizaciones, la resiliencia cibernética y la capacidad de identificación y reacción ante un ciberataque se han convertido en un factor clave para la seguridad de la información en cualquier entidad pública de Colombia. Las entidades se han vuelto cada día más dependientes de la tecnología, y la globalización de sus portafolios de servicio ha llevado al uso inminente del ciberespacio y la inclusión de nuevas prácticas de conectividad. Sin embargo, aunque se cuenta con estándares y mejores prácticas internacionales que pretenden generar lineamientos para mejorar la ciberseguridad, los mismos se enfocan en la plataforma tecnológica y los procesos a implementar; por lo cual, la presente monografía se propone recomendar la implementación de un *framework* –en adelante marco de referencia– de ciberseguridad en el Icfes que propenda a mejorar su nivel de seguridad en la información de los servicios ofrecidos por el instituto; mediante el fortalecimiento del nivel de concientización de los colaboradores a través de campañas soportadas en técnicas psicológicas que conlleven a la adopción de nuevas medidas para generar un cambio de comportamiento y disminuir el nivel del riesgo cibernético.

Palabras claves: *Ciberseguridad, Ciberriesgo, Marco de referencia de ciberseguridad, Cambio de comportamiento, Ciberseguridad organizacional, Seguridad de la información*

ABSTRACT

The treatment of cyber risks in organizations, cyber resilience and the capacity to identify and react to a cyber-attack, has become a key factor for Information Security in any Public Agency in Colombia. Agencies have become increasingly dependent on technology and the globalization of their service portfolios has led to the imminent use of cyberspace and the inclusion of new connectivity practices. However, although there are international standards and best practices that aim to generate guidelines to improve cyber security, they focus on the technological platform and processes to be implemented; therefore, this monograph aims to provide recommendations for the implementation of a cybersecurity framework in the Icfes to improve its level of information security of the services offered by the Institute, by strengthening the level of awareness of the collaborators through campaigns supported by psychological techniques that lead to the adoption of new measures to generate a change in behavior and decrease the level of cyber risk.

Keywords: *Cybersecurity, Cyberrisk, Implementation framework of Cybersecurity, Behavior change, Organizational Cybersecurity, Information Security*

CONTENIDO

ABREVIATURAS

ACIS - Asociación Colombiana de Ingenieros de Sistemas.

APK - Siglas en inglés de Android Application Package (paquete de aplicaciones para Android).

BID - Banco Interamericano de Desarrollo.

CCOC - Comando Conjunto Cibernético.

CEO - Siglas en inglés de Chief Executive Officer (líder o director ejecutivo).

CIO - Siglas en inglés de Chief Information Officer (líder o director de la gestión estratégica de tecnologías de información).

CISA – Siglas en inglés de Cybersecurity and Infrastructure Security Agency (Agencia de Ciberseguridad e Infraestructura).

CNSS - Siglas en inglés de Committee on National Security Systems (Comité de Sistemas de Seguridad Nacional).

Colcert – Grupo de respuesta a emergencias cibernéticas de Colombia.

CSIRT - Siglas en inglés de Computer Security Incident Response Team (equipo de respuesta ante incidencias de seguridad informática).

CSRC - Siglas en inglés de Computer Security Resource Center (Centro de Recursos de Seguridad Computacional).

CTF - Siglas en inglés de Capture the Flag (capture la bandera).

DAFP - Departamento Administrativo de la Función Pública de Colombia.

Enisa - Siglas en inglés de European Union Agency for Cybersecurity (Agencia Europea de Seguridad de las Redes y la Información).

EY - Consultora Ernst & Young.

Icfes - Instituto Colombiano para la Evaluación de la Educación en Colombia.

ISO/IEC - Siglas en inglés de International Organization for Standardization / International Electrotechnical Commission (Organización Internacional de Normalización / Comisión Electrotécnica Internacional).

ITU - Siglas en inglés de International Telecommunication Union (Unión Internacional de Telecomunicaciones).

Mintic – Ministerio de las Tecnologías de la Información y las Comunicaciones.

MSPI - Modelo de seguridad y privacidad de la información propuesto por Mintic.

NICSS - Siglas en inglés de National Initiative for Cybersecurity Careers and Studies (Iniciativa nacional para las carreras y estudios de ciberseguridad).

NIST – Siglas en inglés de National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología).

OEA – Organización de Estados Americanos.

ONU – Organización de Naciones Unidas.

OWASP – Siglas en inglés de Open Web Application Security Project (Proyecto abierto de seguridad de aplicaciones web)

PHVA – Ciclo planear, hacer, verificar y actuar. También conocido como ciclo Deming.

SGSI - Sistema de Gestión de Seguridad de la Información.

TAR - Teoría de la acción razonada.

TCP - Teoría del comportamiento planeado.

TI – Tecnologías de la información.

TIC – Tecnologías de la Información y las Comunicaciones.

UE – Unión Europea.

LISTA DE FIGURAS

LISTA DE TABLAS

CAPÍTULO 1

INTRODUCCIÓN

En el ámbito de la ciberseguridad, cada día las entidades se enfrentan al aumento de riesgos cibernéticos y amenazas emergentes relacionadas con ciberataques terroristas (ciberterrorismo), cuyo objetivo principal involucra personas e infraestructuras tecnológicas, lo que incrementa la vulnerabilidad del gobierno corporativo y conlleva grandes cambios en el normal funcionamiento de las organizaciones (Martínez, 2019).

En la era digital, la gestión de la seguridad de la información y la ciberseguridad requiere en todos los sentidos un contexto adecuadamente definido para la consecución de los objetivos deseados.

Sin embargo, como es bien sabido y sufrido por la gran mayoría de sus gestores, esta estabilidad es, en el mejor caso, muy relativa. La necesidad de los responsables informáticos (CIO) para adaptarse a los cambios de visión de los responsables del negocio (CEO), provocados por nuevos modelos de negocio asociados normalmente a la propia irrupción de nuevas tecnologías, es el día a día en las empresas (Salvador, 2015).

El reporte de la consultora Ernst & Young, que llevó a cabo una encuesta a 1.400 líderes de riesgo y seguridad cibernética de algunas de las organizaciones más grandes del planeta, reflejó que el 80 % de las juntas directivas no hacen de la ciberseguridad un tema estratégico para sus compañías (Dinero, 2019).

Ahora bien, hablando de ciberseguridad y ataques a la información y las comunicaciones, no es fácil predecir lo que pasará, puesto este se mueve en un espacio permanentemente cambiante y que evoluciona muy rápido; muchos especialistas y empresas de seguridad del sector son capaces de vislumbrar lo que puede estar por venir, analizando las amenazas y tendencias en ciberseguridad (Gómez-Merelo, 2020).

Sin embargo, el uso de tecnología en línea ofrece una oportunidad para la *e-inclusión*, pero también se arriesga a una nueva brecha digital, debido a la falta de acceso en los países de bajo ingreso, ya sea por carencia de dispositivos o de ancho de banda y velocidad (ONU, 2018).

Según el informe realizado por el Banco Interamericano de Desarrollo (BID) en conjunto con la Organización de Estados Americanos (OEA) en América Latina, evidencia que diversos países de la región son vulnerables a ataques cibernéticos que pueden llegar a ser devastadores si se llegan a materializar.

Cuatro de cada cinco países no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica. Dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética. La gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos (BID, 2016).

No obstante, las organizaciones han mejorado su nivel de implementación de sistemas de seguridad de la información y ciberseguridad, dadas las nuevas estrategias generadas a nivel internacional y los marcos de cooperación entre las diferentes naciones, lo cual

minimiza la exposición al riesgo cibernético desde el punto de vista de plataforma tecnológica y de procesos. (BID-OEA, 2020)

Sin embargo, el conocimiento al respecto y la forma en que las entidades llevan a cabo el proceso de concientización a los colaboradores, han dejado de lado la adopción e interiorización verdadera de la gestión del riesgo de ciberseguridad en la vida profesional y cotidiana de los mismos, lo cual conlleva a que se generen brechas de ciberseguridad y seguridad de la información que les facilitan a los ciberdelincuentes el ingreso a las plataformas tecnológicas, elevando por ésta causa el riesgo cibernético. (Martínez, 2019)

Es por esto, que diferentes organizaciones internacionales, tales como el Centro de Ciberdelincuencia de Cambridge del Laboratorio de Informática de la Universidad de Cambridge, el Instituto de Estudios de Justicia Criminal de la Universidad de Portsmouth, Consejo de Investigaciones Científicas e Industriales, el Centro de Capacidad de Seguridad Cibernética Mundial de la Universidad de Oxford, la Universidad de Fort Hare, la Universidad Metropolitana Nelson Mandela y la Universidad de Pretoria, se han dedicado a la investigación de la eficacia de campañas de sensibilización sobre la ciberseguridad, tratando de identificar los factores que pueden conducir al fracaso de las mismas para modificar el comportamiento de los consumidores y los empleados en materia de ciberseguridad y seguridad de la información (https://www.cl.cam.ac.uk, https://www.port.ac.uk/, http://researchspace.csir.co.za/).

Por lo cual, el recurso humano se sigue caracterizando por ser el más vulnerable y, por tanto, el más difícil de controlar en la cadena de la ciberseguridad y la seguridad de la información.

> Por esto, cuando las organizaciones se ocupan del factor humano, el procedimiento para ubicar al personal con el nivel adecuado de compromiso con las políticas de la tecnología de la información (TI) debe contener una evaluación del comportamiento en materia de seguridad de los miembros individuales de personal. Varios estudios han sugerido que cuando se mide el nivel de cumplimiento y aceptación de la políticas y controles de seguridad establecidos entre los miembros del personal de una organización, se puede anticipar el éxito de esas políticas (Alotaibi et al., 2015).

En una encuesta del Centro de Investigaciones Pew se menciona que "la generalidad de los entrevistados pudo responder correctamente a menos de la mitad de las preguntas en una prueba de conocimiento sobre temas y conceptos de seguridad cibernética" (PewResearchCenter, 2017).

Es así como el objetivo general de esta monografía es:

Plantear una propuesta metodológica para la implementación de un marco de referencia de ciberseguridad en el Instituto, mediante el fortalecimiento del programa de concientización, basado en el cambio de comportamiento del usuario en el Icfes, teniendo en cuenta que el enfoque de la monografía no sólo es un marco de referencia como lo plantean las mejores prácticas, sino que se encauza en el programa de concientización, que pretende alinear los esfuerzos con las investigaciones mencionadas anteriormente, que conlleven a la generación de un verdadero cambio de comportamiento para mejorar el nivel del riesgo cibernético en el Instituto.

Con lo cual se pretende aportar al Instituto Colombiano para la Evaluación de la Educación (Icfes), de manera contundente, con el objeto de minimizar la exposición de la organización al ciberriesgo, teniendo en cuenta que "la concientización es uno de los factores primordiales que constituye la cultura de seguridad de la información en una entidad" (M. A. Alnatheer, 2012).

Hasta el momento, en el Icfes se ha tratado de seguir los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante la adopción del Modelo de seguridad y privacidad de la información (MSPI), pero hace falta fortalecer el componente de concientización en ciberseguridad, incluyendo metodologías de cambio de comportamiento, que permita generar mayor conocimiento y conciencia por parte de los colaboradores en esta materia (Peña & Segura, 2014).

Como parte fundamental de la campaña por implementar, se debe tener en cuenta el cambio de comportamiento, o conducta, que debe darse en los colaboradores para mejorar el nivel del ciberriesgo.

Dado que la conducta es un fenómeno observable e identificable, las respuestas internas están mediadas por la conducta observable y ésta puede ser modificada. El aprendizaje puede ser descrito en términos de la relación entre eventos observables, esto es, la relación entre estímulo y respuesta (Arancibia et al., 2008).

"El objetivo clave del programa de concientización sobre seguridad es reducir los riesgos a los que se enfrentan estos objetivos en un nivel aceptable, tanto para las raras

"amenazas persistentes avanzadas" dirigidas directamente, como para las amenazas mucho más comunes" (Robinson, 2019).

Lo anterior lleva a proponer la siguiente pregunta de investigación para la presente monografía:

¿Cómo establecer y disminuir el nivel de ciberriesgo al cual se enfrenta la plataforma tecnológica que soporta los servicios esenciales del Icfes?

Para esto, se definen los siguientes objetivos específicos, que pretenden dar respuesta a la pregunta anterior y atender el objeto general de la monografía:

1. Establecer el estado del arte de la conciencia en ciberseguridad en los contextos internacional y colombiano.
2. Identificar el marco normativo en Colombia, en materia de ciberseguridad.
3. Determinar el nivel de conocimiento y conciencia, en materia de ciberseguridad, que poseen los colaboradores del Icfes.
4. Proponer un instrumento para la implementación del marco de referencia de ciberseguridad en el Icfes, enfocado al componente de concientización en la materia.

CAPÍTULO 2

METODOLOGÍA

La presente monografía se lleva a cabo partiendo de la hipótesis: "La ciberseguridad en el Icfes se incrementa en la medida en que los colaboradores aumentan sus capacidades de detección y de actuación frente a la materialización del ciberriesgo, y se implementan controles administrativos, operativos y tecnológicos".

Este trabajo plantea el diseño de una propuesta metodológica para la implementación de un marco de referencia de ciberseguridad basado en el cambio de comportamiento de los usuarios mediante la adopción de un programa de concientización soportado en técnicas psicológicas, para lo cual se aborda el estudio con un enfoque cualitativo, que es el más adecuado en el marco del proyecto, el cual brinda las proposiciones necesarias que permiten hacer las recomendaciones para el planteamiento metodológico.

El tipo de investigación por desarrollar es mixto y está compuesto por los diseños de investigación exploratoria, descriptiva, explicativa y proyectiva. En el tercer y cuarto capítulo y en la investigación exploratoria, se busca establecer el estado del arte que permita identificar la aproximación al nivel de concientización en ciberseguridad en las entidades internacionales y en Colombia, e identificar el marco normativo vigente en el país en materia de ciberseguridad, lo que permite atender los dos primeros objetivos específicos.

En el nivel descriptivo, en el quinto capítulo se pretende descubrir la brecha del grado de concientización de los colaboradores del Icfes, mediante la aplicación de una encuesta, atendiendo el tercer objetivo específico. En la fase explicativa se busca dar respuesta a la

pregunta de investigación y corroborar la hipótesis planteada. Esta última, de acuerdo con el enfoque de estudio abordado (cualitativo), puede ser afinada con base en los resultados (Hernández Sampieri et al., 2014), lo que permitirá desarrollar el diseño de la monografía en el nivel de investigación proyectiva en el sexto capítulo, mediante el planteamiento de la propuesta metodológica para la implementación del marco de referencia de ciberseguridad en el Icfes, basado en el componente de concientización requerido en la materia, atendiendo el último objetivo específico.

Por último, en el séptimo capítulo se relacionarán las conclusiones y los logros obtenidos de la monografía, producto del proceso de investigación y la aplicación del prototipo planteado.

El método de investigación por desarrollar en el proyecto será el deductivo, dado que se pretende determinar el resultado del proceso de investigación para plantear las premisas y establecer y disminuir el nivel de ciberriesgo al cual se enfrenta la plataforma tecnológica que respalda los servicios esenciales del Icfes.

CAPÍTULO 3

ESTADO DEL ARTE

Por su naturaleza, la ciberseguridad es un componente esencial de la gestión integral del riesgo en las organizaciones, la cual se mantiene en constante evolución (Kassicieh et al., 2015), lo que hace que sus amenazas creativas e innovadoras se pongan en el radar público para descubrir nuevas formas de contrarrestarlas y así minimizar el riesgo digital al cual se exponen la entidades hoy en día. Sin embargo, a pesar del gran esfuerzo e interés de las organizaciones para atender la ciberseguridad, "parece ser que hay una falta de comprensión dentro de la comunidad de seguridad en cuanto a lo que es realmente la ciberseguridad", así como "lagunas y debilidades dentro de la industria y la práctica" (Mark Evans et al., 2012).

1. Definiciones de ciberseguridad

1.1. NIST

Según el National Institute of Standards and Technology (NIST) (NIST-CSRC, 2020), la ciberseguridad se define como "la capacidad de proteger o defender el uso del ciberespacio de los ataques cibernéticos".

1.2. Instituto de Tecnología de Massachusetts

El Instituto de Tecnología de Massachusetts, MIT por sus siglas en inglés, en su documento de 2011 "El futuro de la red eléctrica" define: "La ciberseguridad se refiere a todos los enfoques adoptados para proteger los datos, los sistemas y las redes de ataques

deliberados, así como de compromisos accidentales que van desde la preparación hasta la recuperación" (MIT, 2015).

1.3. NICSS

La National Initiative for Cybersecurity Careers and Studies, Iniciativa nacional para las carreras y estudios de ciberseguridad, NICSS por sus siglas en inglés, página oficial de la Agencia de Ciberseguridad e Infraestructura, CISA por sus siglas en inglés, define la ciberseguridad como:

> La actividad o el proceso, la capacidad o habilidad, o el estado por el cual los sistemas de información y comunicaciones y la información contenida en ellos se protegen o defienden contra el daño, el uso o la modificación no autorizados, o la explotación.
>
> Definición ampliada: Estrategia, política y normas relativas a la seguridad y las operaciones en el ciberespacio, que abarcan toda la gama de políticas y actividades de reducción de amenazas, reducción de la vulnerabilidad, disuasión, participación internacional, respuesta a incidentes, resistencia y recuperación, incluidas las operaciones de redes informáticas, garantía de la información, aplicación de la ley, diplomacia, misiones militares y de inteligencia, en la medida en que se relacionan con la seguridad y la estabilidad de la infraestructura mundial de información y comunicaciones (NICSS, 2020).

1.4. Conpes 3701 de 2011

En el documento Conpes 3701 del 14 de julio del 2011, en el que se establecen los lineamientos de política para ciberseguridad y ciberdefensa, se define la ciberseguridad como "Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus

ciudadanos, ante amenazas o incidentes de naturaleza cibernética" (Ministerio de Tecnologías de la Información y las Comunicaciones et al., 2011).

1.5. Doctor Jeimy José Cano

Por otra parte, el doctor Jeimy José Cano, en su blog IT-Insecurity menciona que la ciberseguridad en las organizaciones "es una realidad que prepara a la organización para comprender un escenario de amenazas digitales propias del ecosistema donde opera y establece un conjunto de nuevas prácticas de defensa y anticipación antes desconocidas y poco nombradas" (Cano, 2015).

Así mismo, menciona:

> El concepto de ciberseguridad, como realidad complementaria de la ciberdefensa, materializa el concepto de defensa nacional digital en un conjunto de variables claves acertadamente definidas por la International Telecommunication Union (ITU), en las cuales se hace necesario el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación en el contexto de una realidad digital y de información instantánea (Cano, 2011).

1.6. ISO/IEC 27032

La norma ISO/IEC 27032 (British Standards Institution, 2012), sobre tecnología de la información, técnicas de seguridad y directrices para la seguridad cibernética, define la ciberseguridad como:

> La preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

Nota 1. Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la fiabilidad también pueden estar implicadas.

Nota 2. Adaptado de la definición de seguridad de la información en ISO/IEC 27000:2009.

1.7. Otros autores

La ciberseguridad se define como:

Prevención del daño, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicación por cable y comunicación electrónica, incluida la información contenida en ellas, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio (Kissel, 2009; CNSS, 2005).

La prevención de daños, el uso no autorizado, la explotación y, en caso necesario, la restauración de los sistemas electrónicos de información y comunicaciones, así como de la información que contienen, a fin de reforzar la confidencialidad, la integridad y la disponibilidad de esos sistemas (Hogan & Newton, 2015).

"El proceso de protección de la información mediante la prevención, detección y respuesta a los ataques" (Stouffer et al., 2019).

2. Estado empresarial

Las organizaciones podrían, y deberían, hacer un mayor esfuerzo en materia de capacitación y sensibilización, y en la documentación de los riesgos y adopción de controles técnicos de buenas prácticas para protegerse mejor.

Con base en la encuesta realizada por el Departamento de Digital, Cultura, Medios de Comunicación y Deporte, en asocio con la Universidad de Portsmouth, de Inglaterra, a 1519 empresas de negocios del Reino Unido:

> Una quinta parte de las empresas (20 %) han tenido algún personal que ha asistido a la formación interna o externa en materia de ciberseguridad en los últimos 12 meses. Además, una de cada diez empresas (10 %) informan sobre brechas en las habilidades cibernéticas, no estando de acuerdo en que las personas que se ocupan de la ciberseguridad en su organización tengan las habilidades y conocimientos adecuados para hacer el trabajo de forma efectiva (University of Portsmouth, 2018).

Sin embargo, haría falta un lineamiento claro y definido con respecto a las estrategias en cuanto a la forma de construir sistemas de información para evitar los riesgos de ciberseguridad a escala no solo institucional sino global, dado que la escasez de investigación fundamental con visión de futuro conduce a una comprensión deficiente de la tecnología de ciberseguridad. Esto resulta en la producción continua de sistemas de TI defectuosos y vulnerables (Landau & Stytz, 2005).

2.1. La transformación y la brecha digital

La transformación digital pública requiere herramientas que mejoren la calidad de vida de los ciudadanos y generen valor público; en el Manual de Política de Gobierno Digital se definen los lineamientos, estándares y acciones para que las entidades públicas implementen esta política, y así mejoren su funcionamiento a través del uso de las TIC (Mintic, 2018).

La transición hacia la sociedad de la información constituye un verdadero desafío para los países en vías de desarrollo, particularmente dada la creciente brecha digital con los países desarrollados, que los hace cada vez más vulnerables a la reducción de la productividad y la capacidad económica. "El ritmo de la transformación tecnológica y económica mundial exige una acción urgente para convertir la actual brecha digital en oportunidades digitales para todos" (Sukaina Al-Nasrawi, 2015).

El concepto de brecha digital puede explicarse desde dos perspectivas:

> La brecha que existe entre los países que tienen pleno acceso a la información de la investigación electrónica y los que no lo tienen; y la diferencia en la alfabetización y aptitud en internet entre los ciudadanos de los países desarrollados y los de los países subdesarrollados (Sam Brooks, 2013).

2.2. Ejercicios de ciberataques

El 4 de noviembre de 2010 se llevó a cabo el primer simulacro de ciberataque cibernético a escala europea, con el objetivo de mejorar la seguridad de los estados frente a los ataques a las redes electrónicas. El objetivo del ejercicio fue hacer frente a las acciones de piratas informáticos en un intento simulado de paralizar en varios estados miembros de la UE servicios en línea de importancia crítica (Joyanes et al., 2011).

Con el propósito de avanzar en la preparación ante un ciberataque, el Ministerio de Defensa de Colombia, con el apoyo de la Organización de los Estados Americanos (OEA), desarrolló el 20 y 21 de septiembre de 2012 un ejercicio de gestión de crisis de seguridad cibernética en la Universidad de los Andes de Bogotá, que tuvo como objetivo reforzar las

capacidades del Estado colombiano en la prevención, detección y mitigación de los efectos de un ataque cibernético de gran escala en el país (*El Tiempo*, 2012).

> Con lo anterior, y con los eventos recientes sobre fuga de información, las noticias de atacantes informáticos doblegando protocolos y tecnologías de seguridad, las fallas de seguridad que se han presentado tanto en el sector público como en el sector privado, son argumentos suficientes para evidenciar que Colombia se encuentra en un nuevo escenario de riesgos y amenazas, donde la información se convierte en un arma estratégica y táctica, que cuestiona la gobernabilidad de una organización o la de una nación (Cano, 2011).

2.3. La seguridad y la protección de la información

Según ACIS (2012), "la figura opcional de la seguridad de la información comienza a desvanecerse y a tomar relevancia estratégica, ahora en un escenario donde la información es la "moneda fundamental" para generar, proponer y desarrollar posiciones privilegiadas de personas, empresas y naciones".

La protección de la información es una función del departamento de tecnologías de la información, compartida con todos los que trabajan en una organización. Los colaboradores toman decisiones que influyen de manera esencial en la seguridad o falta de seguridad de los datos de la organización; por ejemplo, hacer clic en un enlace malicioso de un sitio web de suplantación de identidad o *phising*, abrir un archivo adjunto de un correo electrónico malicioso, divulgar información confidencial a un ingeniero social o permitir el acceso de personal no autorizado a áreas restringidas, puede tener consecuencias negativas graves (Coventry et al., 2014).

2.4. La cultura y las personas en la ciberseguridad

El recurso humano es un factor clave en el programa de seguridad de la información de una organización y esto es especialmente cierto si los empleados desconocen los riesgos que ello puede acarrear. "Las infracciones pueden producirse con mucha rapidez debido a las grandes velocidades de la red y al fácil acceso a los datos, incluso a través de dispositivos móviles o aplicaciones de internet en la nube" (Kim, 2018).

La cultura ha influido en la formación de muchas medidas de seguridad, como la política de seguridad nacional, la ética de la información, la capacitación en seguridad y las cuestiones de privacidad. "La cultura de la seguridad abarca medidas sociales, culturales y éticas para mejorar el comportamiento relevante en materia de seguridad de los miembros de la organización y se considera una subcultura de la cultura de la organización" (NACD & ISA, 2016).

Uno de los principales beneficios de la creación de una cultura de seguridad de la información es la protección de los activos de la organización, en la que se producirá una "interacción directa con los activos de información y, por tanto, se minimizarán las amenazas que el comportamiento de los usuarios plantea a la protección de los activos de información"(Alnatheer et al., 2012). La importancia de crear una cultura de seguridad dentro de los entornos de las organizaciones surge del hecho de que la dimensión humana en la seguridad de la información se considera de alto riesgo. Por lo tanto, la creación de una cultura de seguridad de la información es fundamental para una gestión eficaz de la seguridad de la información.

(Dhillon, 1999) define la cultura de seguridad como: "La totalidad de los atributos humanos tales como comportamientos, actitudes y valores que contribuyen a la protección de todo tipo de información en una organización determinada".

Von (2000) pide la creación de una cultura de seguridad dentro de la organización: "Inculcando los aspectos de la seguridad de la información para cada empleado como una forma natural de realizar su trabajo".

De acuerdo con el informe del Banco Interamericano de Desarrollo:

> Si se le va a sacar la mayor ventaja posible a la llamada cuarta revolución industrial, se tiene que crear una infraestructura digital no solo moderna y robusta sino también segura. Proteger a los ciudadanos del cibercrimen no es una opción simple: es un elemento clave para el desarrollo (BID, 2016).

Según (Alnatheer, 2012), muchos estudios han demostrado que se requiere una cultura de seguridad de la información para que ésta sea efectiva. Lo que hace que la cultura de la seguridad de la información sea un reto es la complejidad de definir y comprender tanto el elemento "seguridad" como el elemento "cultura". "Cuantificar la seguridad de la información es un reto, la cultura de seguridad refleja los valores y creencias de la seguridad de la información compartidos por todos los miembros a todos los niveles de una organización" (Alnatheer, 2012).

2.5. La resiliencia y la concientización en la ciberseguridad

Como en cualquier estrategia de ciberseguridad, la resiliencia descansa en gran parte en el factor humano. En este caso, principalmente en la capacidad ejecutiva, el liderazgo y la concientización.

Como principio de seguridad, la concientización del personal de la organización es un aspecto de suma importancia. Pero para alcanzar un nivel adecuado de resiliencia se necesita algo más que crear conciencia, es indispensable el compromiso real del personal. Si, por un lado, en los últimos años se ha puesto de moda la necesidad de fidelización de los clientes en cuanto al mercadeo, por otro se ha abandonado la fidelización del personal en las organizaciones.

Al abandonar el compromiso de la organización con los trabajadores, éstos abandonan el compromiso con la organización y se convierte en una relación de carácter utilitarista a corto plazo y en ambos sentidos. Los resultados son aún peores cuando la falta de fidelización se produce en el nivel directivo. Para crear este compromiso mutuo, la organización ha de ofrecer una carrera profesional a sus trabajadores, más aún, un plan de vida, una seguridad, un sentimiento de grupo, en algunos casos un ideal, y proporcionar una serie de valores añadidos que vayan más allá del estímulo económico directo (Carrasco, 2015).

Diversos autores han puesto en conocimiento y con especial énfasis que cualquier proceso de entendimiento y construcción de la sociedad de la información debe hacerse sobre una activa participación social de la población, la cual se desarrolla en el actual escenario mundial con el uso intensivo de las herramientas informáticas. Sin embargo, para un desarrollo socialmente integrado, tales usos requieren un proceso de alfabetización digital (Gros & Contreras, 2006).

2.6. Gestión de la seguridad en el ciberespacio

Para llevar un control de mayor seguridad en el ciberespacio, existen normativas que regulan y ayudan a mejorar este tipo de problemas. Son las normas ISO/IEC 27032:2012-Tecnologías de la información - Técnicas de seguridad - Directrices de ciberseguridad; la ISO/IEC 27001:2013 - Tecnología de la información - Técnicas de seguridad - Requisitos para los sistemas de gestión de la seguridad de la información; y las que aportan a la mitigación de riesgos, como la ISO/IEC 31000-Gestión del riesgo - Directrices y la ISO/IEC 27005 - Gestión de riesgos de seguridad de la información (Zambrano & Zambrano, 2019).

La ISO 27001 es una herramienta de gestión estratégica que conduce a lograr la protección de la información, bien en un contexto en el cual la empresa pretenda alcanzar una certificación, o bien que solo pretenda incorporar buenas prácticas de seguridad de la información, no solo en sus procesos internos sino también en sus procesos externos" (Velasco, 2006).

El anexo A de la Norma NTC/ISO/IEC 27001 (Icontec, 2006), contempla diez objetivos de control, a saber:

1. Política de seguridad de la información
2. Organización de la seguridad de la información
3. Gestión de activos
4. Seguridad de recursos humanos
5. Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones
7. Control de acceso

8. Adquisición, desarrollo y mantenimiento de sistemas de información
9. Gestión de incidentes de la seguridad de la información
10. Cumplimiento

"Estos dominios están compuestos por un conjunto de subdominios y sus correspondientes controles, los cuales han de ser abordados adoptando un modelo PHVA (planificar, actuar, verificar y actuar)" (Velasco, 2006).

Según la norma ISO/IEC 27032:2012 (British Standards Institution, 2012), "la seguridad cibernética se refiere a las medidas que las partes interesadas deberían adoptar para establecer y mantener la seguridad en el ciberespacio.

La ciberseguridad se basa en la seguridad de la información, la seguridad de las aplicaciones, la seguridad de las redes y la seguridad de internet como elementos fundamentales".

3. Gestión del riesgo

El aumento de riesgos y amenazas no tradicionales, especialmente el terrorismo internacional y los ciberataques, han tenido como objetivos principales tanto a los individuos como a las infraestructuras, incrementando la vulnerabilidad del Estado y produciendo graves perturbaciones en el normal funcionamiento de la sociedad. Durante los últimos años se ha producido un crecimiento del número de ataques dirigidos específicamente a aquellos sectores o infraestructuras que proporcionan "servicios esenciales", de importancia vital para el desarrollo de la vida de los ciudadanos y sus

actividades diarias, así como para la continuidad de las funciones del Estado (Miranzo & Río, 2014).

Entre los riesgos emergentes de seguridad de la información de la mayoría de los países se encuentra la protección de las personas y las infraestructuras críticas, especialmente en los dominios de ciberseguridad organizacional de aquellas entidades que afectan masivamente a la población. "Los gobiernos se están concientizando alrededor de estas amenazas, elaborando legislaciones nacionales o mejorando las que ya tienen para potenciar la colaboración entre agencias gubernamentales, empresas y ciudadanos" (Talbot et al. 2010).

3.1. Modelo nacional de gestión de riesgos de seguridad digital

En este mismo sentido, el Ministerio de las TIC (Mintic), en busca de fortalecer los lineamientos definidos en el documento Conpes 3854, crea el "Modelo nacional de gestión de riesgos de seguridad digital".

En este modelo, los gestores de los sistemas de información, comunicaciones o servicios informáticos, entre otros que tengan relación con la información del país, son actores principales que deben ser conscientes de los riesgos presentes en el entorno digital y de las medidas correctivas que deben implementarse para fortalecer la seguridad de la información en cada una de las entidades. Esto contribuye con el desarrollo social, económico y ambiental del país (Gobierno_de_Colombia, 2018).

3.2. Guía de orientación para la gestión de riesgos de seguridad digital

De acuerdo con lo anterior, y como extensión del "Modelo nacional de gestión de riesgos de seguridad digital", se establece la "Guía de orientación para la gestión de riesgos de seguridad digital en el Gobierno nacional, territoriales y sector público", dentro de la cual

se encuentra el anexo 4, "Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas".

El objetivo principal de este anexo es:

> Orientar a todas las entidades del Gobierno nacional, territoriales y sector público en la implementación de la gestión de riesgos de seguridad digital basada en la definición metodológica del "Modelo nacional de gestión de riesgos de seguridad digital" para, entre otros aspectos, incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en cada entidad pública. (MinTIC, 2018).

3.3. Guía para la administración del riesgo y el diseño de controles en entidades públicas

Sumado a esto, en octubre de 2018 el Departamento Administrativo de la Función Pública crea la guía para la administración del riesgo y el diseño de controles en entidades públicas con el fin de "entregar a los ciudadanos lo mejor de la gestión para producir cambios en las condiciones de vida, mayor valor público en términos de bienestar y prosperidad general, y fortalecer la lucha contra la corrupción" (DAFP, 2018).

3.4. ISO 31000

Por otra parte, la Norma de gestión del riesgo - Directrices está dirigida a:

> Las personas que crean y protegen el valor en las organizaciones gestionando riesgos, tomando decisiones, estableciendo y logrando objetivos y mejorando el desempeño.

> Las organizaciones de todos los tipos y tamaños se enfrentan a factores e influencias externas e internas que hacen incierto si lograrán sus objetivos (ISO_31000, 2018).

Allí menciona que la gestión del riesgo es:

> Iterativa y asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas. La gestión del riesgo es parte de la gobernanza y el liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión.

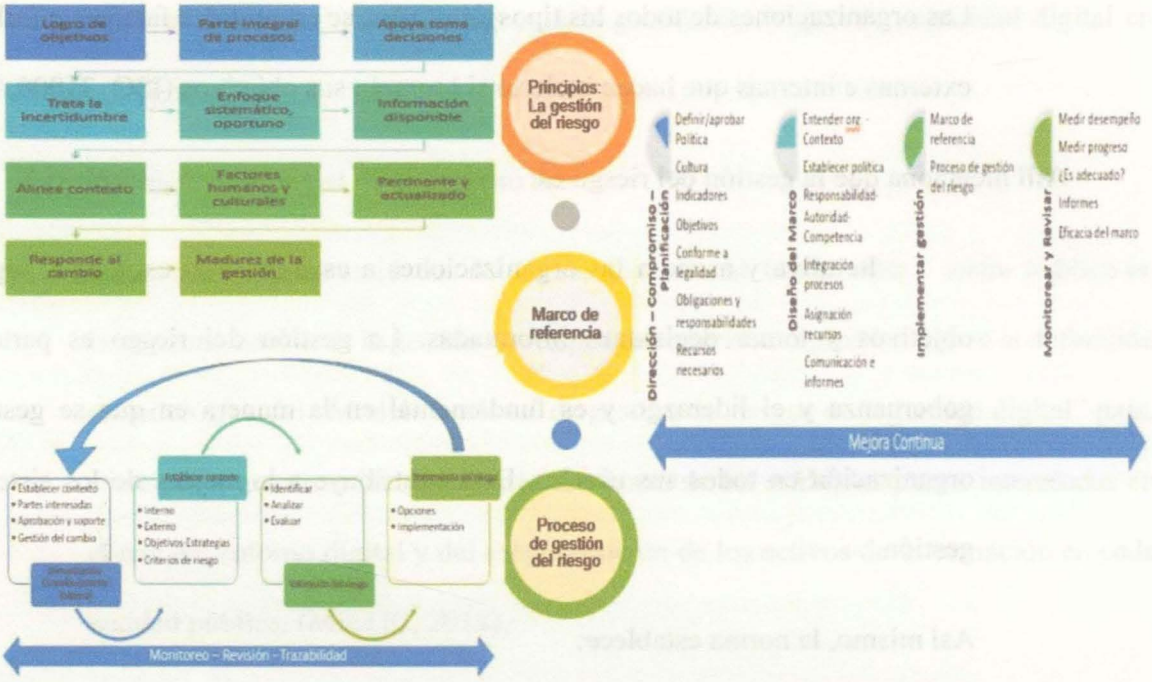
Así mismo, la norma establece:

> La gestión del riesgo es parte de todas las actividades asociadas con la organización e incluye la interacción con las partes interesadas. La gestión del riesgo considera los contextos externo e interno de la organización, incluidos el comportamiento humano y los factores culturales.

La gestión del riesgo está basada en los principios, el marco de referencia y el proceso descritos en este documento, conforme se muestra en la figura 1.

Figura 1

Gestión del riesgo según la ISO 31000



3.5. ISO 27005

Así mismo, en la Norma de tecnologías de la información - Técnicas de seguridad - Gestión de riesgos para la seguridad de la información (ISO_27005, 2018) se ofrecen directrices para la gestión de los riesgos para la seguridad de la información.

Este documento apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñado para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y terminologías descritos en la ISO/IEC 27001 y en la ISO/IEC 27002 es importante para una completa comprensión de este documento.

Este documento es aplicable a todos los tipos de organizaciones que tienen la intención de gestionar los riesgos que pueden comprometer la seguridad de la información de la organización (Bacca Urbina, 2016).

4. Teorías que respaldan el cambio de comportamiento

Muchas de las personas en las organizaciones no cumplen con las políticas de seguridad, algunas por desconocimiento de los riesgos a los cuales se enfrentan o por desconocimiento del comportamiento de seguridad adecuado que deben seguir, pero otras simplemente porque son indiferentes a las consecuencias que puede acarrear dicho incumplimiento, aun conociendo los riesgos a los cuales se enfrentan o el adecuado comportamiento (Cano J. , 2015).

El objetivo debe ser influenciar en la adopción de comportamientos adecuados en materia de seguridad de la información sobre las personas que tienen acceso a ella por medio de los sistemas de la entidad, lo cual puede ser un primer gran desafío. "Se debe lograr que las personas entiendan y reconozcan la relevancia de la información, que comprendan la forma de asegurarla y estén dispuestas a llevar a cabo lo determinado en las políticas de seguridad" (Bada & Sasse, 2014).

En el comportamiento intervienen multitud de factores personales, sociales y contextuales, según (Eufic, 2014):

La mayoría pertenecen a uno de estos tres niveles:

- Personal o individual: creencias, conocimientos, actitudes, habilidades, genética.
- Social: interacción con otras personas, tales como amigos, familiares y miembros de la comunidad.

- Contextual: el ámbito en el que se desarrolla la vida de las personas, por ejemplo, la escuela, el lugar de trabajo o los comercios y servicios locales, así como otros aspectos más amplios como la economía (los precios, por ejemplo) y la tecnología.

Existen algunas teorías que persiguen el cambio de comportamiento; sin embargo, para que esto ocurra debe haber un cambio de actitudes e intenciones en las personas. Algunas de las teorías con mayor relevancia que tratan con el cambio de comportamiento son:

4.1. Teoría de la acción razonada (TAR)

El modelo propuesto por Fishbein y Ajzen (1975) es muy completo y permite obtener mayor seguridad en la medición de los factores determinantes de la conducta. Factores que suelen ser identificados por la psicología social simplemente dentro de la categoría actitud, pero que en esta teoría aparecen discriminados. Se toman en cuenta tanto factores individuales como grupales, siendo ésta una de las principales ventajas técnicas. Otra ventaja consiste en abordar el contexto en el que tienen lugar los factores con la suficiente flexibilidad para permitir distinguirlos y medir su ocurrencia (Rodríguez, 2007).

4.2. Teoría del comportamiento planeado (TCP)

De acuerdo con la TCP:

El antecedente inmediato de cualquier comportamiento es la intención de ejecutarlo. Conceptualmente, la TCP propone que la intención conductual está

> determinada por tres factores independientes: la actitud personal, la norma subjetiva o la norma social percibida y el control conductual percibido (García Díaz, 2005).

Según (Montaño, 1992), el TCP también postula que:

> El control percibido es un determinante independiente de la intención de la conducta, junto con la actitud hacia la conducta y la norma subjetiva. Manteniendo constante la actitud y la norma subjetiva, la percepción de una persona de la facilidad o dificultad del desempeño conductual afectará su intención conductual. El peso relativo de estos tres factores en la determinación de las intenciones debe variar según las diferentes conductas y poblaciones.

Pocos estudios han puesto en práctica el control percibido utilizando las medidas subyacentes de las creencias de control y poder percibido; en cambio, los investigadores han utilizado sobre todo la medida directa del control percibido.

> Tanto la TRA como la TPB suponen que el mejor predictor de una conducta es la intención conductual, que a su vez está determinada por la actitud hacia la conducta y las percepciones sociales normativas con respecto a ella. El TPB es una extensión del TRA e incluye un constructo adicional: el control percibido sobre el desempeño de la conducta (Montaño, 1992).

4.3. Teoría de la autoeficacia

No se trata simplemente de cuán capaz es alguien, sino de cuán capaz se considera que es.

Las personas con diferentes niveles de autoeficacia perciben el mundo de manera diferente; los individuos con un alto sentido de autoeficacia son generalmente de la opinión que tienen el control absoluto sobre sus vidas, que sus acciones y decisiones personales dan forma a sus vidas. A diferencia de los individuos con un bajo sentido de autoeficacia, que sienten que sus vidas no dependen de ellos. Nuestras creencias sobre la autoeficacia afectan la manera en que pensamos y, por supuesto, afectan nuestras reacciones emocionales (Bandura, 1977).

4.4. Teoría de la autodeterminación

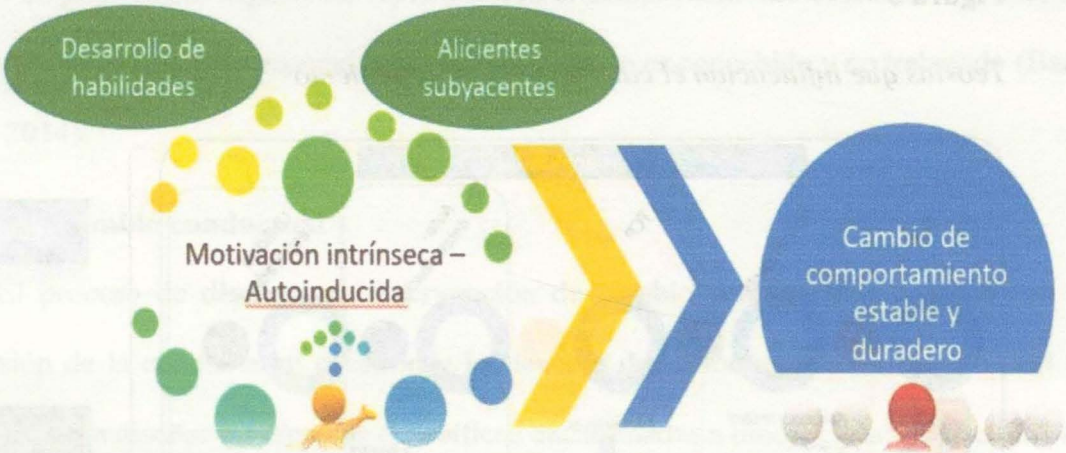
Combinar el desarrollo de habilidades con una motivación y un aliciente subyacentes e intrínsecos es esencial para lograr un cambio duradero. La motivación intrínseca no surge de la presión externa, proveniente de las recompensas y la aprobación o el castigo, la censura del entorno y los profesionales. Es propia de cada individuo y deriva del interés o disfrute que cada uno encuentra en la actividad propiamente dicha. Esta es la base de la teoría de la autodeterminación. A diferencia de las recompensas o los incentivos, la motivación autoinducida se considera estable y duradera. La persona debe sentir que la conducta en cuestión es agradable o compatible con su «concepto de sí misma», sus valores o sus metas vitales. Este sentimiento

puede estimularse analizando los motivos por los que se debe perseverar o cómo encaja la nueva conducta en los objetivos globales. Las personas necesitan percibir que eligen y se responsabilizan de sus acciones para sentirse capaces de conseguir sus metas y ser merecedoras de la comprensión, los cuidados y el reconocimiento de los demás (Eufic, 2014).

En la siguiente figura se plasman los aspectos generales de la teoría (figura 2).

Figura 2

Teoría de la autodeterminación



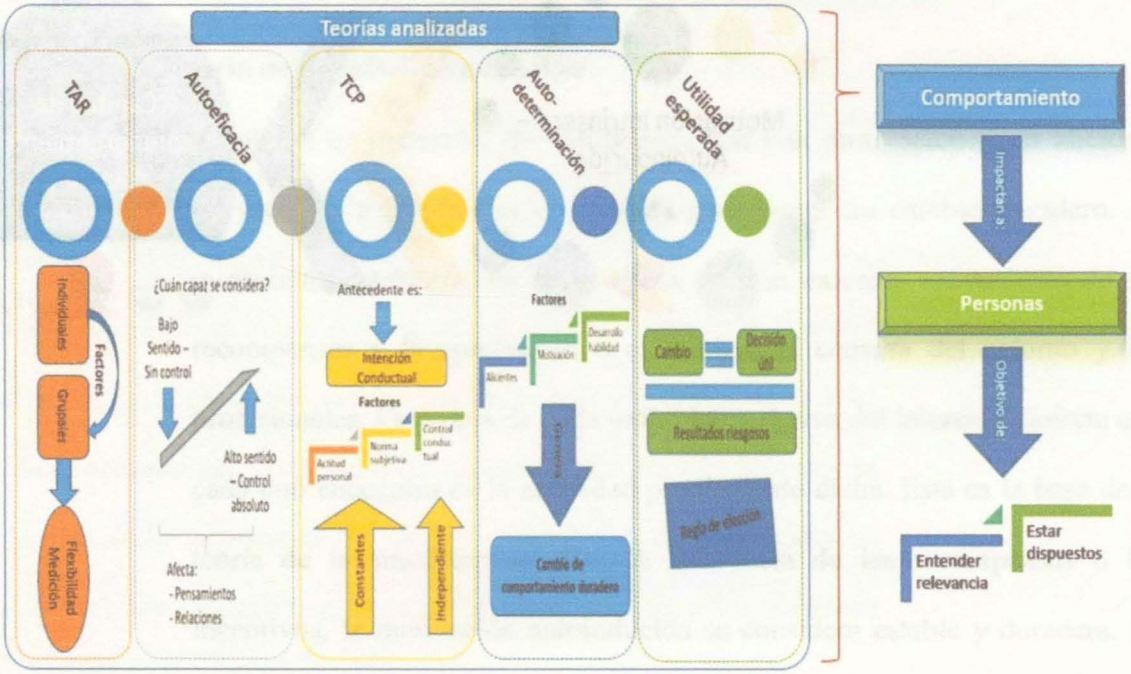
4.5. Teoría de la utilidad esperada

De acuerdo con el enfoque de la utilidad esperada, el cambio de comportamiento puede explicarse porque los individuos lo perciben como una decisión "útil". Ante resultados riesgosos, un responsable de la toma de decisiones podría utilizar el criterio del valor esperado como regla de elección: las inversiones de mayor valor esperado son simplemente las preferidas (Bernoulli, 1954).

En la siguiente figura se plasma cómo las teorías anteriormente descritas influyen en el cambio de comportamiento (figura 3).

Figura 3

Teorías que influencian el cambio de comportamiento



5. Fundamentos teóricos del cambio de comportamiento

Para lograr el cambio deseado en el comportamiento, primero se debe lograr un cambio en las actitudes y en las intenciones, que es un factor clave en la preparación mental que requiere una persona. Lo anterior puede estar fundamentado en los modelos existentes, tales como la teoría de la acción razonada, la teoría de la conducta planificada, la teoría de la motivación personal o la autodeterminación.

Es necesario pasar de la toma de conciencia a los comportamientos tangibles. Las entidades necesitan asegurar sus activos de información, lo cual se realiza mediante el desarrollo de políticas de seguridad, especificando el comportamiento deseado. Pero esto no siempre obtiene el resultado esperado, el comportamiento es concebido y no trabajado (Bada & Sasse, 2014).

5.1. Cambio conductual

"El proceso de diseñar una intervención de cambio conductual comienza con la comprensión de la conducta en cuestión y la elección del enfoque general, tras lo cual se puede proceder a diseñar las técnicas específicas encaminadas a modificarla" (Eufic, 2014).

El propósito real de una estrategia de seguridad debe ser que la gente esté dispuesta a cambiar. Se deben identificar conductas vitales, conductas de sentido que las personas deseen cambiar antes que las entidades pretendan hacer el cambio e identificar los momentos en los cuales se puede presentar un fracaso en el proceso por seguir para el cumplimiento de los objetivos (Winkler & Manke, 2013).

El modelo de comportamiento de Fogg muestra que tres elementos deben converger en el mismo momento para que ocurra un comportamiento: motivación, habilidad y una alerta. Cuando no se produce un comportamiento, falta al menos uno de esos tres elementos (Fogg, 2009).

Así mismo, en la orientación conductual, la contribución de los psicólogos ha sido decisiva en el proceso del cambio conductual, "ya que en su seno se han desarrollado las conceptualizaciones fundamentales que basan el proceso emocional en el propio proceso de aprendizaje. Las aportaciones más importantes se centran en el estudio del miedo y la ansiedad" (Fernández-Abascal et al., 2013).

Sin embargo, para realizar efectivamente el cambio, se deben encontrar realmente las fuentes de influencia actuales, ya sean conscientes o inconscientes, personales, ambientales o sociales, que les impiden a las personas adoptar comportamientos vitales (Kerry-Patterson, 2012).

Teniendo en cuenta lo anterior, nos podemos apoyar en las diferentes formas y estudios que existen actualmente para entender y tratar de cambiar el comportamiento de las personas, tales como:

> La neurociencia, que se interesa por el conocimiento de los mecanismos cerebrales, hormonas y neurotransmisores implicados en la emoción; por su parte, la psicología evolutiva se centra en el desarrollo delimitando los cambios emocionales que se producen a lo largo de la vida de una persona; y la psicología cognitiva, que acentúa la importancia de la relación entre emoción y cognición (Fernández, 1995).

5.2. Conciencia y formación

La conciencia, la educación y la formación en materia de seguridad no se pueden limitar a "arreglar" la seguridad (Coventry et al., 2014). Muchos de los problemas a los que se enfrentan los profesionales de seguridad de la información podrían ser resueltos, o al menos aliviados, si las personas actuaran de una manera diferente. Por ejemplo, si no hubieran hecho clic en el enlace que venía en el correo electrónico, no descargaran *software* o películas gratuitas, escogieran contraseñas largas o un poco más complejas, se negaran a caer en las artimañas de las personas que se dedican a la persecución.

> Cuando los usuarios se sienten tentados por un buen negocio en línea, no se centran en las advertencias de seguridad, sino que buscan señales para confiar en la fiabilidad de un sitio. La educación del usuario debe enfocarse en desafiar y corregir los conceptos erróneos que guían el comportamiento actual (Kirlappos & Sasse, 2014).

De acuerdo con los informes del Proyecto Abierto de Seguridad de Aplicaciones Web, Owasp por sus siglas en inglés, la inyección SQL[1] se ha venido encontrando entre los diez mejores por más de una década, y se sigue presentando como una de las técnicas favoritas por los atacantes (Owasp, 2017).

5.3. La persuasión como herramienta

La persuasión es una herramienta de comunicación útil para transformar ideas, creencias, actitudes y, en el mejor de los casos, comportamientos. Las técnicas de

[1] Inyección SQL: Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización. Fuente: Owasp Top 10 2017. Riesgos en seguridad de aplicaciones.

persuasión se dividen en dos grupos: las racionales y las emocionales. Algunas técnicas racionales son la argumentación, la lógica, la retórica, el método científico y la evidencia; y entre las técnicas emocionales se encuentran la publicidad, la fe, la imaginación, la propaganda, la seducción (López-Rúa, 2015).

La persuasión verbal puede ser una herramienta poderosa y conveniente, pero si las conductas no están cambiando, incluso cuando se cuenta con evidencias, los profesionales de seguridad deben usar otras herramientas en sus arsenales (Robinson, 2019).

La persuasión, según Fogg (2005), "es un intento de cambiar actitudes, o comportamientos, o ambos sin usar coacción o engaño".

Un mensaje persuasivo debe tener cuatro características: "En primer lugar, debe atraer la atención, en segundo lugar, debe ser comprendido, en tercer lugar, debe estar relacionado con un asunto digno de ser procesado y, en cuarto lugar, su contenido debe ser almacenado y recuperado fácilmente de la memoria" (Bada & Sasse, 2014).

Sin embargo, las conferencias e intentos de persuasión verbal no han logrado tener el efecto requerido. "La concientización en seguridad requiere antecedentes y experiencias y no estrategias de una sola fuente, dado que rara vez son la respuesta a problemas complejos" (Kerry-Patterson, 2012).

5.4. Las motivaciones y emociones

Las motivaciones personales involucran los sentimientos asociados con una acción; las motivaciones sociales provienen de la presión de los compañeros y las interacciones con otros grupos; las motivaciones medioambientales pueden ser

difíciles de distinguir, ya sea que vengan del entorno físico o la forma en que una organización premia o castiga las actividades (Kerry-Patterson, 2012).

Los estudios realizados en humanos confirman la participación de la amígdala en la adquisición del miedo condicionado y en los procesos de aprendizaje emocional implícito. La amígdala desempeña también un papel relevante en la evaluación afectiva de estímulos relacionados con la amenaza y el peligro y actúa como un sistema muy rápido que alerta y permite responder de forma rápida y eficaz ante cualquier amenaza (Fernández-Abascal et al., 2013).

"El marketing sensorial sitúa las experiencias y los sentimientos vividos y experimentados por los consumidores en el centro del proceso. Lo que mueve a los seres humanos es la emoción, no la razón" (López-Rúa, 2015).

5.5. Las áreas del cerebro

Básicamente, hay unas áreas dentro del cerebro que se asocian a los estímulos del *marketing*, y otras que participan en el sistema nervioso junto con los sentidos, y así estimulan zonas del organismo del ser humano que pueden propender a escoger una marca, un producto o servicio sobre otro, o a realizar una acción determinada (Naranjo, 2015).

Según (Naranjo, 2015), dichas áreas se dividen en:

- Lóbulo parietal: Integra información sensorial desde distintos lugares del cuerpo, tiene el conocimiento numérico y sus relaciones, y manipulación de objetos. En este lóbulo se integran sensaciones, lectura, lenguaje e inteligencia.

- Lóbulo occipital: Básicamente es el lugar donde se procesan los estímulos visuales, allí se integra la función visual.
- Lóbulo temporal: Aquí residen las funciones de memoria, especialmente el almacenamiento de palabras y nombres de objetos. En este lóbulo se integran, entre otros la visión, el discurso, el comportamiento, la memoria y la escucha.
- Lóbulo frontal: En él se encuentran los controles de impulsos, juicio, socialización, comportamiento sexual y la espontaneidad. Este importante lóbulo genera toda la coordinación, control y ejecución de la conducta.

Figura 4

Centros nerviosos del cerebro

Nota: Tomado de *Academo, Revista de Investigación en Ciencias Sociales y Humanidades* (2015)

5.6. La estrategia de influencia y las conductas vitales

Una de las lecciones más importantes que enseñan las estrategias de influencia es que para lograr un cambio positivo, los profesionales de la concientización sobre seguridad deben centrarse no en la visión global de lo que quieren conseguir, sino en lo que la gente debe hacer. "Deben identificar las conductas que desean cambiar antes de empezar a intentar cambiarlas. Los estrategas de la influencia llaman a estas claves de éxito "comportamientos vitales"" (Robinson, 2019).

Tan importante como identificar las conductas vitales que las personas deben promulgar es determinar los momentos cruciales en los que es más probable que fracasen en el cumplimiento de estas metas (Kerry-Patterson, 2012).

> Las mentes conscientes e inconscientes a menudo están en desacuerdo cuando se trata del comportamiento de las personas. La mente inconsciente está siguiendo patrones establecidos para la acción rápida, basados en miles de tácticas de supervivencia y evolución. En muchos casos, las personas tendrán que superar estos patrones para formar nuevos hábitos (Hogan, 2004).

5.7. La imagen heroica en el cambio de comportamiento

Si los profesionales de la concientización sobre seguridad pueden utilizar la imagen heroica que han creado para sus usuarios como protectores de datos y de la privacidad, e inspirarlos para que se comprometan a un pequeño acto –como prometer la instalación de un gestor de contraseñas seguro o activar la autenticación de dos factores–, entonces tienen el potencial de conseguir compromisos más grandes. "A medida que los usuarios empiezan a

pensar en sí mismos como personas conscientes de la seguridad, empiezan a actuar de acuerdo con esta imagen" (Robinson, 2019).

En muchos casos, estos cambios de comportamiento pueden conducir a cambios de actitud: Si quiere que la gente diga que sí, "haga que haga algo" (Hogan, 2004). Cambiar la emoción asociada con una actividad es una manera poderosa de motivar este cambio de comportamiento (Kerry-Patterson, 2012).

En situaciones en las que la gente no está segura de cómo actuar, es mucho más probable que busque "pruebas sociales"; la tendencia es suponer que una respuesta es correcta si muchas personas se comportan de esa manera (Cialdini, 2009).

Los mensajes mixtos, ya sea entre las palabras y el lenguaje corporal o en otras señales, tienden a hacer que las personas se sientan incómodas y las inclinen firmemente hacia el campo del "no" (Hogan, 2004).

5.8. Líderes de influencia

Los líderes de seguridad de la información deberían ser líderes de influencia. Según Kerry Patterson (2012), "Los líderes de influencia se derivan de cuatro percepciones:

1. Son conocedores, siguen aprendiendo.
2. Tienen los mejores intereses de los demás en el corazón.
3. Son generosos con su tiempo y bien conectados.
4. Dicen lo que piensan directamente".

Para influenciar en las personas es necesario identificar el contexto, tal como se lleva a cabo la gestión de los riesgos de acuerdo con las mejores prácticas. "Una historia bien

contada, llena de detalles vívidos, puede ayudar a establecer el contexto de por qué los usuarios deben cambiar el comportamiento de una manera que recuerden, con un contexto emocional completo" (Robinson, 2019).

Aunque la experiencia personal es la herramienta más persuasiva, la experiencia vicaria, utilizando historias vivas, puede ser especialmente útil cuando los oyentes desconfían de la experiencia o motivos del expositor; "al identificarse con los personajes de la historia, los propios oyentes se convierten en participantes" (Kerry-Patterson, 2012).

El aprendizaje es un proceso a través del cual se logra que un comportamiento –respuesta– que antes ocurría tras un evento determinado -estímulo– ocurra tras otro evento distinto (Arancibia et al., 2008).

Un programa de seguridad puede ser efectivo si el material transmitido es interesante y actualizado, una presentación en que la persona perciba en forma general y que aplique a cualquier miembro de las organizaciones (Wilson & Hash, 2003).

6. Conclusiones de la cultura cibernética y el cambio de comportamiento

Para ir adelante de los ciberdelincuentes, es necesario cambiar la forma en que se hacen las cosas. Los líderes de ciberseguridad y seguridad de la información en las empresas deben identificar y reconocer las amenazas, las vulnerabilidades, los riesgos y asegurarse de que su plataforma tecnológica, y en sí la organización, esté apropiadamente preparada y protegida ante la materialización de cualquier riesgo identificado.

Dejar la ciberseguridad solamente a cargo del departamento de tecnología es una infracción al adecuado deber, dado que no solo es con plataforma tecnológica con la que se

va a reaccionar ante los posibles ataques, sino con el apoyo de los colaboradores que entienden, asimilan y reaccionan de forma adecuada ante dichas amenazas.

La cultura de la seguridad abarca las medidas sociales, culturales y éticas para mejorar el comportamiento en materia de seguridad de los miembros de una organización. Se concentra en un pequeño aspecto de los valores y comportamientos humanos, y no cubre todos los valores, normas y creencias humanas básicas que influyen en la cultura organizacional (Alnatheer, 2012).

Por lo anterior, en lugar de inundar a los usuarios con información relacionada con la seguridad de la información, o con la creación de multitudinarias políticas de ciberseguridad y seguridad, es indispensable considerar cómo los usuarios toman decisiones, tanto en los procesos del negocio como en los asuntos personales, y adaptar nuevas soluciones de seguridad basadas en su comportamiento (Kirlappos & Sasse, 2014).

Si los profesionales de la ciberseguridad y seguridad de la información pueden anticiparse a estos momentos y proporcionarles a las personas herramientas para tratarlos con antelación o utilizar factores personales, sociales y medioambientales para proporcionar una motivación suficiente en estos momentos claves, aumentarán las probabilidades de que sus usuarios tengan éxito (Robinson, 2019).

Por lo anterior, el propósito principal de toda entidad en materia de conciencia de ciberseguridad y seguridad de la información debe ser el cambio de comportamiento de sus colaboradores (Winkler & Manke, 2013).

Según Ki-Aries y Faily (2017) mencionan que:

La responsabilidad, la confianza, la comunicación y la cooperación son las cuatro piedras angulares de una cultura de seguridad atractiva. Utilizar un enfoque que motive y capacite a los empleados para desempeñar un papel activo en la seguridad es esencial para lograr la concientización y los comportamientos positivos.

7. Campañas de concientización en ciberseguridad

7.1. Tipos de Campañas

Es importante implementar campañas de concientización y capacitación en ciberseguridad y seguridad de la información, las cuales deben contar con el apoyo de un líder de influencia en la entidad, quien no solo de palabra sino en persona debe apoyar y hablar a los asistentes dando a conocer la visión general del programa y la trayectoria del líder de seguridad que lo guiará (Robinson, 2019). Así demostrará su total respaldo.

Según Bada y Sasse (2014), la mayoría de las campañas de concientización no se enfocan en el aseguramiento del factor humano. El estudio de ISF del 2014 menciona las siguientes razones:

1. Las soluciones no están alineadas con los riesgos del negocio.
2. No se miden ni el progreso ni el valor.
3. Se hacen suposiciones incorrectas sobre las personas y sus motivaciones.
4. Se establecen expectativas poco realistas.
5. No se utilizan las habilidades correctas.
6. La conciencia es solo ruido de fondo.

A pesar de la presencia de los mejores programas de sensibilización en materia de seguridad de la información, existen obstáculos para la ejecución satisfactoria de las actividades de sensibilización. Estos obstáculos comunes son, según Qudaih et al. (2014):

1. La implementación de nuevas tecnologías.
2. Una talla única para todos.
3. Demasiada información.
4. Falta de organización.
5. Falta de seguimiento.
6. No se explica el porqué.

Para mejorar las defensas del usuario es necesario dar un paso más. "Siempre que un instrumento detecte el uso no autorizado de símbolos de confianza, debe presentar a los usuarios información sobre lo que ha fallado, aumentando su conciencia del problema y de los posibles riesgos a los que se enfrentan" (Kirlappos & Sasse, 2014). Esto se debe hacer en el navegador cuando visitan los sitios que llevan esos sellos, de modo que los usuarios no necesiten descargar e instalar *software* adicional para estar protegidos. Además, si una herramienta de seguridad identifica un riesgo, debe generar mensajes visuales llamativos, asegurándose de que los usuarios entienden la naturaleza del problema y el significado de los mensajes que se les entregan.

Al considerar la investigación de trabajos semejantes, a pesar de la gran cantidad de enfoques de sensibilización en materia de seguridad, muchos se centran en temas de sensibilización relacionados con el cumplimiento de las normas. Muy pocos, sin embargo, consideran realmente los factores humanos pertinentes específicos de las empresas que

identifican las necesidades reales de concientización sobre la seguridad de las personas que interactúan con el proceso y la tecnología para apoyar los objetivos empresariales. Ninguno ofrece un método consistente de Human Computer Interface (HCI) para integrar los factores humanos en la conciencia de seguridad utilizando personas (Ki-Aries & Faily, 2017).

7.2. Impactos generados

"Se evidencia una debilidad en la difusión, concientización, generación de una cultura de prevención y acción segura en ciberseguridad, dirigida tanto al sector público como al privado, así como a la sociedad civil" (Ministerio de Interior y de Justicia et al., 2011).

Una formación integrada debe contener la experiencia en el marco y la seguridad, también el apoyo en materia de seguridad percibido, la carga de información, el método de notificación preferido y mucho más. "Las personas conocen las respuestas a las preguntas de la campaña de concientización o sensibilización, pero no actúan en consecuencia con las acciones de su vida real" (Wilson & Hash, 2003).

La concientización no es entrenamiento. El propósito de las presentaciones de sensibilización es simplemente centrar la atención en la seguridad. Las presentaciones de concientización tienen por objeto permitir que las personas reconozcan los problemas de seguridad de TI y respondan en consecuencia (Wilson & Hash, 2003).

Coventry et al. (2014) aseguran que "es esencial que las prácticas de seguridad y privacidad se diseñen en un sistema desde el principio. Un sistema difícil de usar llevará finalmente a los usuarios a cometer errores".

La sensibilización y la modificación de los comportamientos en materia de seguridad pueden ser un reto, ya que el público debe estar comprometido con la realidad de las

amenazas y comprender el proceso de identificación y tratamiento de las cuestiones o preocupaciones, y luego debe estar motivado para aplicar comportamientos positivos, modificar las percepciones de riesgo (Roper, 2006), así como adoptar comportamientos arraigados, con el apoyo de temas pertinentes que no requieran demasiada información (ENISA, 2006).

Los aspectos identificados por Bada, Sasse y Nurse (2014) determinaron que los programas orientados a la sensibilización y el cumplimiento se abordan a menudo como ejercicios de seleccionar la respuesta correcta y no siempre conducen a los comportamientos deseados. Algunos enfoques se basan en "la invocación del miedo para modificar los comportamientos, o dan lugar a una falta de motivación y de capacidad para satisfacer expectativas poco realistas" que pueden derivarse de sistemas y políticas de seguridad mal diseñados (Bada, Sasse & Nurse, 2014).

Se deben tener en cuenta las diferencias culturales en las percepciones de los riesgos cuando se incorporen conductas positivas en materia de seguridad con apoyo, conocimiento y conciencia (Bada, Sasse & Nurse, 2014)(Bada, Sasse, & Bada, M., Sasse, A., Nurse, 2014).

7.3. Campañas de concientización en Colombia

En Colombia no se evidencia desarrollo y continuidad en campañas de concientización o sensibilización en ciberseguridad apoyadas por las empresas públicas y del mismo Gobierno nacional; lo anterior, teniendo en cuenta las campañas identificadas que ha venido desarrollando el Gobierno colombiano, dentro de las cuales se encuentran las que se relacionan a continuación.

7.3.1. Mintic – En TIC Confío

Esta campaña, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, es una estrategia para enseñarle a la ciudadanía, especialmente a niños, niñas y adolescentes entre los 12 y los 18 años, el uso responsable de las TIC (Mintic, 2019).

Dentro del mencionado portal se han venido desarrollando campañas de sensibilización en la materia, como las siguientes:

- La importancia de hablar, de forma lúdica, con niños, niñas y adolescentes sobre ciberseguridad y los cuidados que se deben tener en la red:
  - Aprende seguridad en la red.
  - *Cyberscouts* y *Hackers* vs. Cybercrook de Incibe.
  - Juegos de ciberseguridad *online* de Mozilla.
  - *Be Internet Awesome* de Google.
  - *SecuKid*, es una de las referencias en juegos de ciberseguridad para niños.
- Conozca cómo se gestiona la ciberseguridad en el país con el Facebook Live de En TIC Confío.
- Cómo prevenir los riesgos en el entorno digital: Diez recomendaciones en el Día del Internet Seguro.
- ¡Ten cuidado con las modalidades de Phishing! Consejos para protegerse ante los delitos de *phishing* y, dentro de esta práctica fraudulenta, las modalidades del *Vishing* y el *Smishing*.

7.3.2. Policía Nacional

En el portal de la Policía Nacional de Colombia (Ponal, 2020) existen campañas específicas de acuerdo con los incidentes que se vayan presentando. Allí mismo se encuentra:

- El chat del CAI virtual.
- Un servicio para verificación de archivos y URL sospechosas al servicio de los ciudadanos.
- El servicio de ciberincidentes, que permite visualizar en tiempo real los incidentes informáticos que afectan la ciberseguridad nacional.
- Mural del Cibercrimen, que contiene publicaciones sobre las modalidades empleadas por los ciberdelincuentes.
- Por último, las recomendaciones en ciberseguridad, en las que se encuentran boletines, guías, informes e infografías sobre el tema.

7.3.3. CAI Virtual

Dentro del portal del CAI Virtual, (CAI_Virtual, 2020), se puede evidenciar más información relacionada con la ciberseguridad. Incluye aspectos informativos relacionados con temas tales como:

- Ciudadanía y familia
- Banca
- Educación
- Gobierno
- Industrial
- Comercio electrónico

- Pymes
- Café de expertos

7.3.4. CSIRT Colombia

En el portal del Computer Security Incident Response Team (CSIRT) Colombia (CSIRT, 2020), se encuentra información que ayuda a la ciudadanía a la protección de la ciberseguridad tanto a escala personal como organizacional. En dicho portal hay opciones tales como:

- Sandbox, que le brinda a la ciudadanía la opción para cargar archivos que posiblemente se encuentren infectados, con el objeto de analizarlos y así evitar contagios o vulneraciones.
- APK es una opción que permite cargar aplicaciones desarrolladas para dispositivos móviles con el objeto de validarlas e identificar posible *software* malicioso en ellas.
- CTF permite ingresar al juego conocido a escala internacional como "Capture the Flag" o "Capture la bandera".
- Adicionalmente, en este portal se encuentran boletines informativos que ayudan a las entidades a estar alerta ante posibles ataques cibernéticos.

7.3.5. Colcert

En el portal de Colcert (2020), que es del Grupo de Respuesta a Emergencias Cibernéticas de Colombia, organismo coordinador en el ámbito nacional en aspectos de ciberseguridad y ciberdefensa, se encuentran opciones tales como:

- Boletines de seguridad cibernética.
- Incidentes de ciberseguridad.

En la semana del 1 al 8 de marzo de 2020 se hizo énfasis en los mensajes que estaban circulando en redes sociales en relación con el incidente mundial de coronavirus (Covid-19), los cuales tenían como finalidad infectar los dispositivos electrónicos de los ciudadanos.

7.3.6. Presidencia de la República

Desde junio de 2017, el Gobierno de Colombia, liderado por la Presidencia de la República, comenzó una campaña de prevención cibernética. Aspectos como qué es y cómo prevenir un ataque cibernético, entre otros, se pueden consultar en el portal especiales.presidencia.gov.co, al que se puede ingresar con este enlace corto: https://t.co/JkbAdohMwt (Presidencia, 2017).

Lamentablemente, la información registrada allí, al parecer, no ha sido actualizada desde la fecha en mención, dado que se han presentado diferentes ataques cibernéticos en los últimos años que han requerido atención especial por parte de las empresas o ciudadanía en general. De ahí que en el portal se siga registrando información tal como el ataque de WannaCry.

> WannaCry Ransomware 2017 fue el peor ataque que se haya hecho antes. WannaCry Ransomware es un tipo de *software* malicioso que bloquea el acceso de los usuarios a archivos o sistemas, reteniendo archivos o dispositivos enteros mediante la codificación hasta que la víctima paga un rescate a cambio de una clave de descifrado, que le permite al usuario acceder a los archivos o sistemas codificados por el programa (Mohurle & Patil, 2017).

7.4. Conclusiones de campañas de concientización

En general, y con la información que se presenta en las campañas antes mencionadas, se puede identificar que no existe una línea clara de campañas para la sensibilización o capacitación en ciberseguridad a escala gubernamental para las entidades públicas. Por lo anterior, cada entidad realiza sus mejores esfuerzos para llevar a cabo campañas que conduzcan a minimizar el riesgo ante posibles ataques cibernéticos. Sin embargo, al día de hoy se sigue observando y escuchando la frase "El recurso humano es el eslabón más débil en la cadena de la seguridad" (Kim, 2018).

> Los programas de sensibilización tienen más probabilidades de éxito cuando reciben un apoyo de alto nivel y de toda la empresa que se compromete con la sensibilización, el compromiso y la cooperación hacia una cultura de la seguridad, utilizando un proceso de diseño creativo participativo adaptado a las necesidades de la empresa. La sensibilización debe comunicarse por diversos medios pertinentes a la empresa, su gente y su cultura, y la mejor manera de reforzarla es mediante un programa continuo de 90 días (Winkler, 2012).

Sin embargo, ninguna de las campañas anteriormente expuestas incluye el aspecto fundamental de identificación de las necesidades y generación de cambio del comportamiento, que permite que realmente se evidencie una mejora en el tratamiento de los riesgos de las entidades o de la ciudadanía en general.

"Se debe aplicar una sensibilización que involucre a las personas a escala personal, lo que puede motivar y habilitar a los empleados para que desempeñen un papel activo en la seguridad de la información" (Ki-Aries & Faily, 2017).

Ahora bien, muchas organizaciones fundamentan sus campañas de concientización con el mecanismo de apelación al miedo.

> Se ha demostrado que las apelaciones al miedo por sí solas no proporcionan una garantía efectiva o adecuada, según su definición, y las organizaciones no deberían depender de este mecanismo. El mensaje podría ser malinterpretado, olvidado o incluso ignorado en función de las percepciones, las relaciones y la influencia social (Evans et al., 2012).

Por lo anterior, se incrementa la importancia de realizar un ajuste sustancial en las campañas de concientización que involucre un verdadero cambio de comportamiento de los colaboradores de las entidades públicas, y se observe una real disminución de los incidentes de ciberseguridad en las plataformas tecnológicas de las organizaciones.

CAPÍTULO 4

NORMATIVA COLOMBIANA

1. Conpes 3701 de 2011

En Colombia, el Gobierno ha enfocado los esfuerzos a generar la normativa necesaria que permita dar una dirección clara en el tema de seguridad digital, para lo cual publicó en 2011 el Conpes 3701, un documento que buscaba:

> Generar lineamientos de política en ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normativa del país en torno al tema (Ministerio de Interior y de Justicia et al., 2011).

2. Conpes 3854 de 2016

Con el apoyo internacional y los cambios continuos del entorno digital en Colombia, el Gobierno, mediante el Conpes 3854 de 2016, actualizó el documento antes mencionado, el cual tiene como objetivo:

> Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país (Mintic et al., 2016).

3. Decreto 1008 de 2018

Adicionalmente, el Gobierno nacional, mediante el Ministerio de Tecnologías de la Información y las Comunicaciones, el 4 de junio de 2018 expidió el Decreto 1008, el "cual establece 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", en el cual se definen, para las entidades del estado, los habilitadores transversales: seguridad de la información, arquitectura de TI y servicios ciudadanos digitales.

4. Leyes en materia de seguridad digital y ciberseguridad en Colombia

Así mismo, el Gobierno nacional ha definido e implementado una serie de leyes y regulaciones que pretenden cobijar y dar un marco normativo al Estado colombiano en materia de seguridad digital y ciberseguridad. En la siguiente tabla (tabla 1) se condensan algunas de ellas de manera cronológica.

Tabla 1

Resumen del marco normativo colombiano en materia de ciberseguridad

Normativa	Descripción
Ley 527 de 1999	Se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Carta iberoamericana de 2007	Se definen los principios de administración electrónica en los países de la comunidad Iberoamericana.
Ley 1341 de 2009	Se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones (TIC).
Ley 1437 de 2011	Se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. - Capítulo IV - Utilización de medios electrónicos en el procedimiento administrativo.
Ley 1581 de 2012	Se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1413 de 2017	Se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales
Ley 1928 del 2018	Se aprueba el «Convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest

5. Conclusiones del marco normativo en Colombia

Al analizar las normas, leyes y regulaciones expedidas en Colombia, se identifica en ellas la mención a los temas de capacitación, concientización y cultura en seguridad cibernética, como se puede observar en los siguientes apartados:

En el Conpes 3701 se menciona que "se evidencia una debilidad en la difusión, concientización, generación de una cultura de prevención y acción segura en ciberseguridad,

dirigida tanto al sector público como al privado, así como a la sociedad civil" (Ministerio de Interior y de Justicia et al., 2011).

En el Conpes 3854 se menciona:

> Garantizar que los programas, proyectos y campañas de concientización y sensibilización, así como las capacitaciones que adelanten las diferentes entidades, se diseñen a partir de los lineamientos y orientaciones que emita la Comisión Nacional Digital y de Información Estatal, o de quien haga sus veces, con el fin de evitar la duplicación de esfuerzos y garantizar la eficiencia en el manejo de los recursos (Justicia et al., 2016).

En la Ley 1437 de 2001, se hace mención a la "previsión de la demanda y ejecución de planes de capacitación en el nuevo sistema a los jueces, magistrados y demás servidores judiciales".

En la Ley 1712 de 2014, se establece:

> Conforme al principio de planeación, las entidades públicas deberán efectuar las provisiones de recursos financieros, físicos y de capacitación del talento humano para avanzar en la implementación de los mecanismos previstos en la ley para asegurar la máxima publicidad de la información y de las actuaciones de las autoridades.

Sin embargo, en estas leyes no se especifica cómo desarrollar este aspecto fundamental dentro de un programa de ciberseguridad en las organizaciones públicas. Un cambio de comportamiento de los colaboradores de las entidades ante la asimilación y

apropiación de la forma de gestionar los riesgos cibernéticos a los cuales se enfrentan cada día mejora la posición de ciberseguridad de la organización (Arancibia et al., 2008).

Es fundamental que el Gobierno y cada entidad del Estado, en lugar de concentrarse tanto en la expedición de más normativa en materia de ciberseguridad, y las organizaciones en el cumplimiento de dichas normas o mejores prácticas, cambien la forma de llevar a cabo las campañas de concientización que les dirigen a sus colaboradores, con el objetivo de incluir en ellas metodologías de cambio de comportamiento que lleven a una verdadera disminución de incidentes cibernéticos y una mejor gestión del riesgo de ciberseguridad.

CAPÍTULO 5

ESTADO ACTUAL

1. Gestión del riesgo

La metodología para la identificación, evaluación y gestión de riesgos de los sistemas de gestión vigentes del Icfes se basa en la NTC-ISO 31000, la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del Departamento Administrativo de la Función Pública (DAFP), principalmente en lo dispuesto en el Anexo 4 - Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas del Ministerio de Tecnología de la Información y las comunicaciones, la cual se encuentra definida en el política de gestión de riesgos de la entidad PDE-PT001 (Icfes, 2019).

En el informe de riesgo de gestión con corte a 2019[2], el Icfes identificó:

Tabla 2

Identificación Riesgo-Causa-Control

Riesgos	Causas	Controles
50	106	115

Tabla 3

Clasificación de riesgos

[2] Infografía del informe de riesgos de gestión 2019 (Icfes)

	Riesgos			
	50			
	Extremo	**Alto**	**Moderado**	**Bajo**
Inherente	5	22	11	12
Residual	1	11	20	18

- Del total de los riesgos, los impactos generados de cara a seguridad de la información, de acuerdo con lo identificado por la primera línea de defensa (Líderes de procesos con sus equipos de apoyo), se tienen:
  - Afectación de la imagen
  - Indisponibilidad de servicios tecnológicos misionales
  - Pérdida de información clasificada
  - Interrupción de las operaciones de la entidad

Con base en lo anterior, se observa la necesidad de mantener y fortalecer la gestión de seguridad de la información en el instituto, mediante estrategias que lleven a disminuir los riesgos de seguridad de la información, teniendo en cuenta que no solo deben ser aspectos enfocados en la implementación de plataforma tecnológica, sino en el fortalecimiento de la política de concientización por medio de campañas dirigidas a los colaboradores, que permitan minimizar los impactos identificados por la primera línea de defensa ante la materialización de cualquier riesgo que afecte la confidencialidad, integridad o disponibilidad de la información.

2. Estado actual de concientización

Como parte de la campaña de concientización, el instituto llevó a cabo una serie de actividades que propenden a minimizar los riesgos identificados en el numeral anterior. En dicha campaña se incluyó la encuesta diseñada y desarrollada por el maestrando para el

personal de la entidad, con el objeto de identificar las necesidades de la entidad y de los colaboradores y medir el nivel de conciencia en ciberseguridad y seguridad de la información, atendiendo el tercer objetivo de la monografía.

El diseño de ésta encuesta, fue pensada en determinar el estado actual del Icfes, con el objetivo de respaldar con datos el nivel de inmadurez con el cual cuenta el instituto respecto a la concientización en ciberseguridad y sus campañas implementadas.

2.1. Encuesta para determinar el nivel de concientización

El Icfes contrata a personal contratista que hace parte del proyecto de Seguridad de la Información a cargo de la Dirección de Tecnología y la Subdirección de Información, quienes tienen el rol de líderes de seguridad de la información en conjunto con la Dirección y la Subdirección mencionada; con dicho personal se lleva a cabo toda la implementación del sistema de gestión de seguridad de la información, incluyendo las campañas de concientización requeridas.

El maestrando, como parte de dicho equipo de trabajo, y con el objeto de identificar el nivel de conciencia que el personal del Icfes tiene respecto a la seguridad de la información y la ciberseguridad, e identificar las necesidades que se tienen en la materia y que sirva como insumo para enfocar la campaña de concientización a ejecutar, elaboró la siguiente encuesta, la cual se incluyó como parte del programa de concientización[3]. Esta actividad consistió en el envío de un formulario con diez preguntas de diferentes características, teniendo en cuenta el objetivo requerido como parte de la monografía y lo esperado por los mismos líderes.

[3] Plan de concientización de seguridad de la información. Icfes.

Las preguntas realizadas a los colaboradores fueron las siguientes, las cuales tenían estructura de varias opciones con única respuesta.

1. ¿Sabes quiénes son los Súper I?

   Sí/No

2. ¿Sabes dónde está publicada la política de seguridad de la información?

   Sí/No

3. Los pilares de seguridad de la información son:

   a) -Confidencialidad, imparcialidad e integridad

   b) -Integridad, reciprocidad y disponibilidad

   c) -Integridad, confidencialidad y disponibilidad

   d) -No sé

4. ¿Cuál de las siguientes opciones consideras que es *phishing*?

   a) Suplantación por correo electrónico

   b) Correos enviados a un gran número de destinatarios con fines publicitarios

   c) No sé

5. ¿Sabes para qué sirve la combinación de las teclas Windows + L?

   a) Para imprimir

   b) Para bloquear el computador

   c) Para borrar información permanentemente.

   d) No sé

6. ¿Cómo se clasificaría un documento con información como nombres, documentos, teléfonos y direcciones electrónicas de los inscritos a una prueba de Saber Pro?

   a) Información pública

b) Información pública clasificada

c) Información pública de uso interno

d) Información pública reservada

e) No sé

7. ¿Quién es el propietario de los datos personales que se almacenan en el Icfes?

a) El Gobierno de Colombia

b) El Ministerio de Educación Nacional

c) El titular de la información

d) El Icfes

e) No sé

8. ¿Sabes qué debe tener una contraseña?

LETRAS MAYÚSCULAS

Letras minúsculas

Números (1234567890)

Caracteres especiales (%&$"#-+)

Todas las anteriores

No sé

9. ¿Sabes por qué medio debes reportar un correo sospechoso?

a) Orfeo

b) Mesa de ayuda

c) Daruma

d) Línea Nacional Gratuita 01 8000 519 535

e) No sé

10. ¿Sabes por qué es importante portar el carné?

a) Prevenir que personas ajenas a la entidad pasen inadvertidas

b) Identificarnos fácilmente en caso de una emergencia

c) Hacer uso de los recursos dados por la institución

d) Todas las anteriores

e) No sé

2.2. Resultados de la encuesta de conocimiento y concientización

Como resultado de la encuesta realizada a los colaboradores del instituto dentro de la campaña de concientización, se obtuvo lo siguiente:

La estadística permite analizar que de las 20 áreas que conforman el Icfes, 18 áreas (90 %) se vieron representadas por 65 colaboradores que participaron en la actividad; se resalta la alta participación de los colaboradores de las áreas de Subdirección de la Información (15,4 %), Subdirección de Desarrollo y Aplicaciones (13,8 %), la Oficina de Control Interno y la Subdirección de Producción de Instrumentos (10,8 %).

Las respuestas a las preguntas más relevantes se detallan a continuación:

- ¿Sabes quiénes son los Súper I?

63 colaboradores (96,9 %) conocen los personajes de los Súper I, es decir que la recordación e imagen de estos personajes está presente y que las campañas usando su imagen han servido para ser reconocidos como parte del sistema de seguridad de la información.

- ¿Sabes dónde está publicada la política de seguridad de la información?

El 70,8 % conoce que las políticas se ubican en el sistema de gestión Daruma, lo que significa que la mayoría de los colaboradores no solo lo usan, sino que saben que en él se

ubica la documentación asociada al sistema de seguridad de la información. El restante 29,2 % dijo que podría encontrase en la página web o el correo electrónico.

- Los pilares de seguridad de la información son:

El 89,2 % de los colaboradores conocen los pilares de la información, lo que significa que los conceptos de confidencialidad, integridad y disponibilidad forman parte del lenguaje común y se asocia con seguridad de la información. Tan solo el 7,7 % aún no reconoce estos términos.

- ¿Cuál de las siguientes opciones consideras que es *phishing*?

El 84,6 % reconoce el concepto asociado a suplantación, lo que significa que las campañas realizadas en el Icfes han permitido que los colaboradores conozcan el significado de esta modalidad de estafa. Sin embargo, el 15,4 % de los colaboradores desconocen este concepto tan fundamental para la ciberseguridad, dado que el mayor número de ataques se presentan por ésta modalidad de engaño.

- ¿Cómo se clasificaría un documento con información de nombres, documentos, teléfonos y direcciones electrónicas de los inscritos a una prueba de Saber Pro?

En esta pregunta se evidenció el bajo conocimiento que tienen los colaboradores sobre cómo se clasifica la información según la ley, ya que solo el 26,2 % logró asociar los tipos de datos preguntados como información pública clasificada; el 73,8 % restante seleccionó las opciones incorrectas, lo que significa que se debe reforzar la divulgación de este tema con todos los colaboradores del Icfes.

- ¿Quién es el propietario de los datos personales que se almacenan en el Icfes?

El 52,3 % de los colaboradores reconocen que los datos personales son propiedad del titular de la información; sin embargo, el 47,7 % desconoce la respuesta, lo que significa que, a pesar de que la mayoría tiene claros los conceptos propios de la ley de protección de datos personales, aún muchos colaboradores lo desconocen. Se debe reforzar este aspecto.

- ¿Sabes qué debe tener una contraseña?

El 98,5 % de los colaboradores saben cómo se debe estructurar una buena contraseña, lo que significa que las campañas realizadas en este sentido han generado el resultado esperado.

- ¿Sabes por qué medio debes reportar un correo sospechoso?

El 90,7 % de los colaboradores saben que los incidentes asociados a correos sospechosos se deben reportar por medio de la mesa de ayuda, lo que significa que han adoptado la buena práctica tanto de identificar correos considerados anómalos como de reportarlos correctamente. Sin embargo, el 9,3 % aún no tiene claro por qué medio se deben reportar, aspecto que es importante y necesario fortalecer para mejorar el nivel del riesgo cibernético al cual se encuentra expuesto el Instituto.

2.3. Aspectos relevantes identificados en la campaña

Los siguientes son los aspectos relevantes identificados en la campaña realizada en el Icfes:

- Se requiere fortalecimiento en la capacitación brindada como parte de la gestión de TI y el sistema de gestión de seguridad de la información (SGSI) a los colaboradores, de modo que mejore su conocimiento ante la adopción de una postura adecuada para la atención de incidentes de seguridad de la información.

- Existen dificultades para establecer responsabilidades sobre la propiedad y custodia de los datos. Las responsabilidades ya identificadas no están centralizadas y se dificulta identificar a los custodios de los datos.
- No existe conciencia y cultura dentro del instituto sobre la importancia del control, la calidad y la responsabilidad sobre la información.
- No existen mecanismos de transmisión del conocimiento acerca de los procedimientos y requisitos para acceder a la información, lo cual dificulta el desarrollo de actividades y funciones, así como la incorporación de nuevos funcionarios en la cultura de gestión responsable de la información.
- Se debe continuar con las campañas de sensibilización y divulgación del SGSI, ya que los resultados obtenidos en la encuesta de conocimiento demuestran que éstas son una buena opción para llegarles a los colaboradores.
- Se debe reforzar lo correspondiente a temas legales, específicamente la Ley de Protección de Datos Personales y la Ley de Transparencia (clasificación de la información), ya que los resultados obtenidos en estas temáticas evidencian el bajo conocimiento de los colaboradores al respecto.

3. Conclusiones del estado actual de concientización

Con base en los resultados obtenidos en las actividades realizadas como parte de la campaña de concientización en el Icfes, se identifican aspectos tales como:

- Se debe incluir la ciberseguridad como dominio principal en el SGSI, dado que a la fecha hace falta fortalecer este aspecto en el instituto, mediante la adopción de

políticas y mejores prácticas que lleven a la gestión adecuada del ciberriesgo y sus componentes adicionales.

- Las campañas realizadas en el instituto, aunque han tenido resultados positivos, requieren una reingeniería en su planeación, dado que han sido actividades que comúnmente se llevan a cabo en las organizaciones y no trascienden a la mejora en la gestión de los riesgos de ciberseguridad y seguridad de la información.
- En las campañas de sensibilización no se identifican las necesidades de los colaboradores y de la misma entidad, sino que se realizan actividades que, desde el punto de vista del conocimiento de los líderes de seguridad de la información, se deberían ejecutar para propender a la confidencialidad, integridad y disponibilidad. Lo anterior no significa que lo ejecutado hasta el momento sea errado; quiere decir que, incluyendo el aspecto mencionado, es posible obtener mejores resultados en la materia.
- Es importante incluir en las campañas la aplicación de los modelos de cambio de comportamiento que generen en los colaboradores un mayor nivel de apropiación con la gestión del ciberriesgo y la adecuada actuación frente a la materialización de un incidente de ciberseguridad y seguridad de la información.
- El cambio de mentalidad para la atención del ciberriesgo debe empezar por los mismos líderes de seguridad de la información, teniendo en cuenta que es necesario dejar de ver a los usuarios como niños pequeños a quienes se les debe hacer todo para evitar la vulneración de la plataforma tecnológica o la fuga de información del instituto, o como áreas separadas y únicos responsables ante la materialización de un riesgo cibernético. Se debe

empezar a trabajar como un equipo para que en conjunto se blinde tanto a los usuarios como a la entidad.

CAPÍTULO 6

PLANTEAMIENTO DEL MARCO DE REFERENCIA

1. Enfoque – Marco de referencia que debe tener la organización

Propuesta metodológica para la implementación de un marco de referencia de ciberseguridad en el Icfes, mediante el fortalecimiento del programa de concientización basado en el cambio de comportamiento del usuario.

Teniendo en cuenta que el Icfes ha venido desarrollando e implementando un Sistema de Gestión de Seguridad de la Información (SGSI) con base en buenas prácticas dadas desde el MinTiC y alineadas con la norma internacional ISO 27001 y con base en el resultado de la encuesta realizada a los colaboradores del Icfes, y su correspondiente análisis; se identifica la necesidad de fortalecer el sistema mediante la propuesta metodológica del marco de referencia, cumpliendo así el cuarto objetivo de la presente monografía, de modo que contribuya a mejorar el nivel del riesgo de ciberseguridad y seguridad de la información.

Dicho marco de referencia cuenta con diferentes aspectos que permiten mejorar el nivel de resiliencia cibernética, pero su eje principal se centra en brindar un enfoque especial en aspectos como la capacitación y la concientización mediante campañas que permitan obtener un cambio de comportamiento de los involucrados en el sistema a través de técnicas psicológicas que lo soportan, para ofrecer un servicio de gran calidad a los ciudadanos y mejorar la gestión de la información. Aspecto que es considerado por el maestrando de suma importancia para obtener un nivel adecuado del ciberriesgo, con base en lo evidenciado en el capítulo tercero.

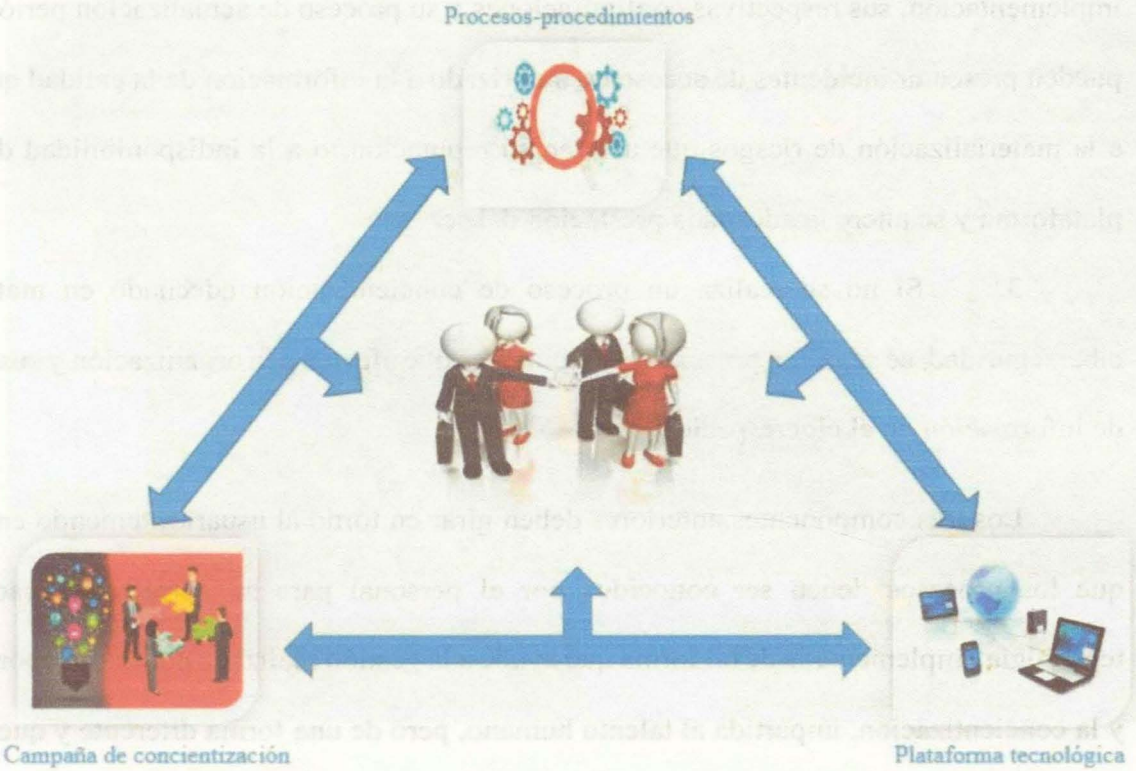
Teniendo en cuenta lo anterior, se plantea el presente marco de referencia alineándose con el marco de seguridad cibernética del NIST, las normas ISO 27001 (Requisitos para los Sistemas de gestión de la seguridad de la información), ISO 27005 (gestión de riesgos de seguridad de la información), ISO 31000 (gestión de riesgos), e ISO 27032 (directrices para ciberseguridad).

En la actualidad, los aspectos de seguridad de la información y ciberseguridad son preocupaciones de toda organización, más cuando se encuentran de por medio aspectos normativos o aquellos que puedan poner en riesgo a la entidad o su reputación. Como se puede observar, un gran número de accesos no autorizados a la información de las entidades siguen siendo atribuidos al recurso humano, ya sea de forma intencional o accidental. Por lo anterior, las entidades no pueden depender solamente de la plataforma tecnológica para el aseguramiento de sus datos y la reducción de los riesgos de ciberseguridad y seguridad de la información, lo cual es el actuar común de las organizaciones; sino que necesitan una mayor consideración de las personas y su integración con la tecnología y los procesos de negocio.

Por lo anterior, se plantea que es esencial contar con el siguiente marco de ciberseguridad, el cual está basado en el principio denominado "Triángulo de la ciberseguridad usuario-centrista", que se compone de la integración de los procesos, la tecnología y la concientización, con un componente central que es el talento humano. Dicho principio se detalla a continuación (figura 5).

Figura 5

Triángulo de la ciberseguridad usuario-centrista



El desbalance de este triángulo puede propiciar brechas de seguridad que afectarían considerablemente la exposición de los riesgos cibernéticos de las entidades, por las siguientes razones:

1. Si no se cuenta con los procesos y procedimientos de ciberseguridad claramente definidos, publicados y documentados en forma entendible y aplicable por los usuarios, se puede incurrir en vulnerabilidades por desconocimiento ante un incidente que afecte los pilares de la seguridad (integridad, confidencialidad y disponibilidad).

2. Si no se tiene la plataforma tecnológica de seguridad adecuadamente implementada (entiéndase por plataforma la integración del *hardware* y el *software*), la cual es respaldada por los procesos y procedimientos en donde se deben detallar la forma de su

implementación, sus respectivas configuraciones y su proceso de actualización periódica, se pueden presentar incidentes de acceso no autorizado a la información de la entidad que lleve a la materialización de riesgos que afecten su reputación, o a la indisponibilidad de dicha plataforma y se altere la adecuada prestación del servicio

3. Si no se realiza un proceso de concientización adecuado en materia de ciberseguridad, se seguirán presentando incidentes que afecten a la organización y sus activos de información en el ciberespacio.

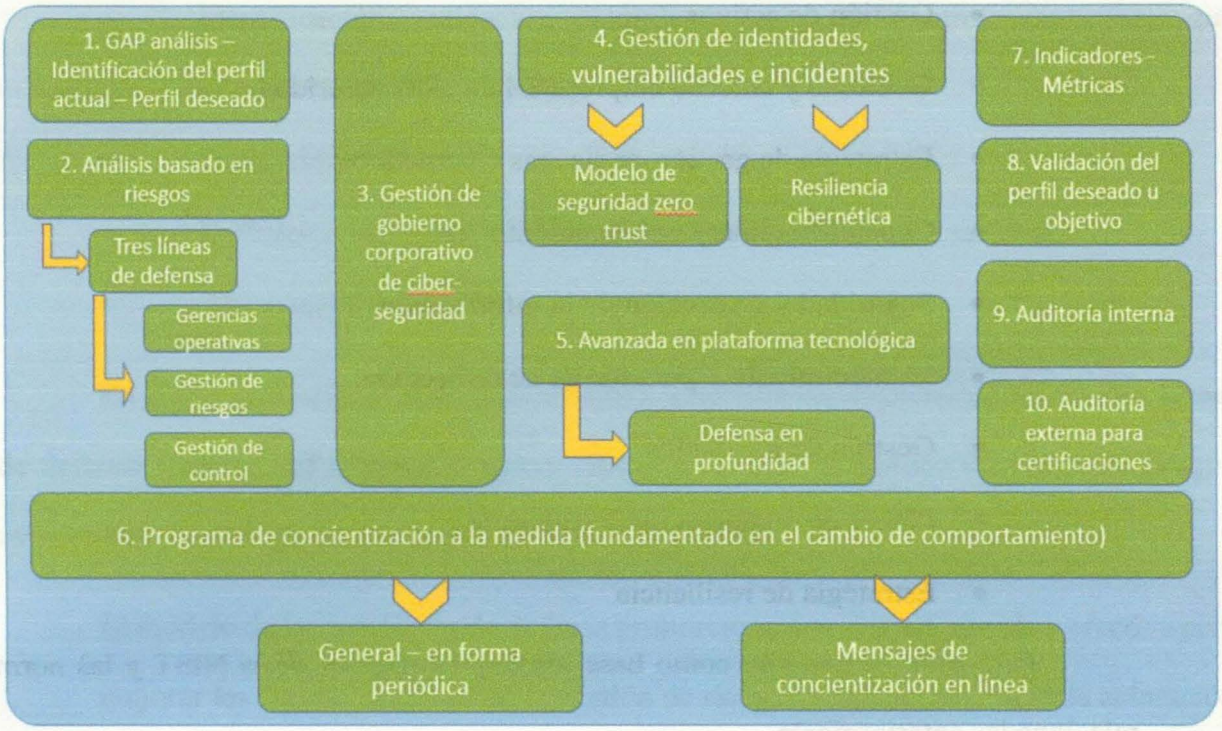
Los tres componentes anteriores deben girar en torno al usuario, teniendo en cuenta que los procesos deben ser conocidos por el personal para su correcta aplicación; la tecnología, implementada de tal forma que ayude a la gestión realizada por los colaboradores; y la concientización, impartida al talento humano, pero de una forma diferente y que lleve a un cambio de comportamiento que permita identificar, asimilar, interiorizar y aplicar los objetivos de aseguramiento que pretende obtener la organización en materia de ciberseguridad.

Por esto, partiendo del principio antes mencionado, se plantea el siguiente marco de ciberseguridad por implementarse en el Icfes, que podría ser extensible a cualquier otra entidad del Estado que requiera mejorar su nivel de madurez en este aspecto.

El marco de referencia planteado en la presente monografía está conformado por las fases que se pueden observar en la siguiente figura 6.

Figura 6

Propuesta de marco de referencia de ciberseguridad



La figura 6 muestra de manera gráfica el marco de ciberseguridad planteado en la presente monografía, el cual contiene los componentes por ser validados e implementados de acuerdo con lo especificado a continuación; en donde, el componente de concientización es el eje principal del presente trabajo, con el que se pretende generar una reducción considerable en el nivel del riesgo cibernético, atendiendo el objetivo general de la monografía, dando respuesta a la pregunta de investigación y corroborando la hipótesis planteada.

1.1. Identificación del perfil actual y deseado en la entidad - GAP Análisis

Identificación de necesidades de la entidad en materia de ciberseguridad y seguridad de la información por medio de encuestas, grupos de discusión, grupos focales, que permitan identificar el estado actual y el deseado u objetivo en aspectos tales como:

- Gestión de activos
- Gobierno y entorno empresarial de ciberseguridad
- Estrategia de gestión de riesgos cibernéticos
- Concientización y entrenamiento
- Seguridad y protección de la información
- Mantenimiento y plataforma de protección
- Gestión de incidentes
- Planes de recuperación y respuesta
- Estrategia de resiliencia

Para esto, se tomarán como base los requerimientos de la NIST y las normas ISO relacionadas anteriormente.

1.2. Análisis basado en riesgos

Actualización del proceso de gestión de riesgos, alineándolo con los requerimientos del marco de seguridad de la NIST, la ISO 27005 y la ISO 31000, identificando, desarrollando y aplicando los siguientes componentes:

- Identificación del contexto
- Identificación de los activos cibernéticos
- Clasificación de los activos cibernéticos
- Identificación de los riesgos asociados a los activos y que impacten la confidencialidad, integridad y disponibilidad.
- Identificación de vulnerabilidades aplicables a los activos cibernéticos en el ciberespacio.

- Identificación, validación o implementación de controles aplicables que minimicen la materialización del riesgo.
- Definición del plan de tratamiento de riesgos.
- Definición del apetito de riesgo de ciberseguridad en la entidad.
- Aprobación del apetito de riesgo por la alta dirección.

En dicho procedimiento se debe incluir e implementar el concepto de las tres líneas de defensa (Institute of Internal Auditors (IIA), 2013) y la definición y gestión de riesgos emergentes y estratégicos que impactan la ciberseguridad.

El modelo de las tres líneas de defensa proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados.

- Primera línea de defensa:

Como primera línea de defensa, las gerencias operativas son propietarias de los riesgos y los gestionan. Estas gerencias también son responsables de la implementación de acciones correctivas para hacer frente a deficiencias de proceso y control.

- Segunda línea de defensa

Una función de gestión de riesgos (o comité) que facilita y monitorea la implementación de prácticas efectivas de gestión de riesgos por parte de la gerencia operativa y que asiste a los propietarios del riesgo en la definición del objetivo de

exposición al riesgo y en la presentación adecuada de información relacionada con riesgos a toda la organización.

Una función de cumplimiento para monitorear diversos riesgos específicos tales como el incumplimiento de leyes y regulaciones aplicables.

Una función de contraloría que monitorea riesgos financieros y la emisión de la información financiera.

- Tercera línea de defensa

Los auditores internos proporcionan a los organismos de gobierno corporativo y a la alta dirección un aseguramiento comprensivo basado en el más alto nivel de independencia y objetividad dentro de la organización.

Este alto nivel de independencia no está disponible en la segunda línea de defensa. Los auditores internos proveen aseguramiento sobre la efectividad del gobierno corporativo, la gestión de riesgos y el control interno, incluyendo la manera en que la primera y segunda líneas de defensa alcanzan sus objetivos de gestión de riesgos y control.

Los procesos de riesgo y control deben ser estructurados de acuerdo con el modelo de las tres líneas de defensa.

1.3. Gestión de gobierno corporativo de ciberseguridad

Con éste se pretende regular y normar las políticas de ciberseguridad y seguridad de la información tendientes a brindar el norte o la ruta de los colaboradores en los diferentes ambientes relacionados. Para esto, aparte se toman como base las buenas prácticas generadas

a partir de las ISO 27001, 27002, 27032, 27017, 27018, 27005, 31000, etc., y se deben llevar a cabo las siguientes actividades:

- Identificación y apropiación del perfil de la entidad con base en la clasificación del marco de seguridad de la NIST.
- Actualización de la declaración de conformidad.
- Actualización de la información general relacionada con:

1..1. El contexto y alcance de la organización, incluyendo los aspectos de ciberseguridad (gestión de activos, gestión de riesgos, gobierno, gestión de identidades, capacitación y entrenamiento, seguridad de datos, protección de la información, etc.).

1..2. La política del sistema de ciberseguridad y seguridad de la información, incluyendo lo relacionado con la gestión del riesgo cibernético, gestión con terceros, contacto con nuevas autoridades y grupos de interés, continuidad de la seguridad, que debe ser aprobada por la alta dirección.

1..3. Identificación de nuevos procesos y procedimientos para gestionar el riesgo cibernético.

1..4. Actualización de los roles y responsabilidades.

1..5. Actualización de las partes cibernéticas interesadas.

1..6. Obtener aprobación de la dirección respecto del nuevo proceso.

1.4. Gestión de identidades, vulnerabilidades e incidentes

Partiendo de la identificación de los activos de información cibernéticos, se debe incluir el monitoreo de éstos, así como la gestión de accesos y actualización del perímetro de

seguridad física. Dentro de la gestión de accesos se debe tener en cuenta el modelo de seguridad Zero Trust.

Zero Trust, está redefiniendo la forma en que vemos la ciberseguridad: atrás quedaron los días de la IT centralizada y los perímetros físicos; los usuarios, empleados y socios de una entidad ahora se conectan desde múltiples lugares.

Los tres pilares sobre los cuales se construye esta estrategia son:

- **Acceso seguro** con base en variables contextuales propias del usuario y no solo en su dirección IP.
- **Menores privilegios** que limitan el alcance del acceso a los recursos que el usuario necesita. El resto de la red permanece invisible e inaccesible.
- **Visibilidad para los analistas de seguridad** sobre las solicitudes de acceso realizadas desde todos los puntos de la red. Esto permite tomar mejores decisiones más rápidamente.

Esta arquitectura proporciona una hoja de ruta a largo plazo para una red flexible, escalable y extensible que incorpore seguridad por defecto. Para empezar con Zero Trust, Forrester Research (Kindervag, 2010) recomienda:

- **Cambiar la forma de pensar sobre la confianza**. Desafiar y romper el paradigma de confianza existente. Ya no se debe aceptar y adoptar el "Confía, pero verifica".
- **Romper con el modelo de red jerárquica de tres niveles**. Si estuviera diseñando la red desde cero y no supiera sobre este modelo de tres niveles, ¿diseñaría su red de esa manera? Busque subredes o entornos de laboratorio en los que pueda empezar a probar e implementar de forma incremental las ideas de arquitectura de Zero Trust.

- **Organice reuniones periódicas con sus homólogos en la red**. Empiece a socializar el concepto de red de Zero Trust con sus compañeros de red. Inicie un grupo de trabajo multifuncional de "Cero confianza" para hacer una lluvia de ideas y una pizarra de usos tanto inmediatos como a largo plazo de la arquitectura de red de "Cero confianza".
- **Incluir los requisitos de arquitectura de Zero Trust en cada RFP de red o seguridad.** En una economía de mercado altamente competitiva, los esfuerzos de gestión de proveedores y de abastecimiento pueden impulsar el desarrollo de productos.

Así mismo, es necesario tener bien identificado el plan de recuperación ante ataques cibernéticos, o el plan de resiliencia cibernética. Teniendo en cuenta que la organización puede ser un objetivo claro de ataques cibernéticos, dicho plan debe estar claramente definido y dado a conocer por los interesados con el propósito de minimizar cualquier impacto que pueda llegar a causar a la información, los activos cibernéticos o la disponibilidad de los servicios ofrecidos por la entidad.

1.5. Avanzada en plataforma tecnológica – Defensa en profundidad

Implementar una plataforma tecnológica adecuada que controle y contribuya a mejorar los niveles de seguridad perimetral, minimizando el riesgo de contagio o intrusión de manera no deseada, con base en el resultado del análisis de los riesgos cibernéticos. Apoyándose en dispositivos tales como DLP, WAF, Firewalls, SIEM, Suite de antivirus (incluyendo antispam y filtrado de contenido para reducir el riesgo de caer en campañas tipo *phishing* o instalación de *malware* por el ingreso a páginas

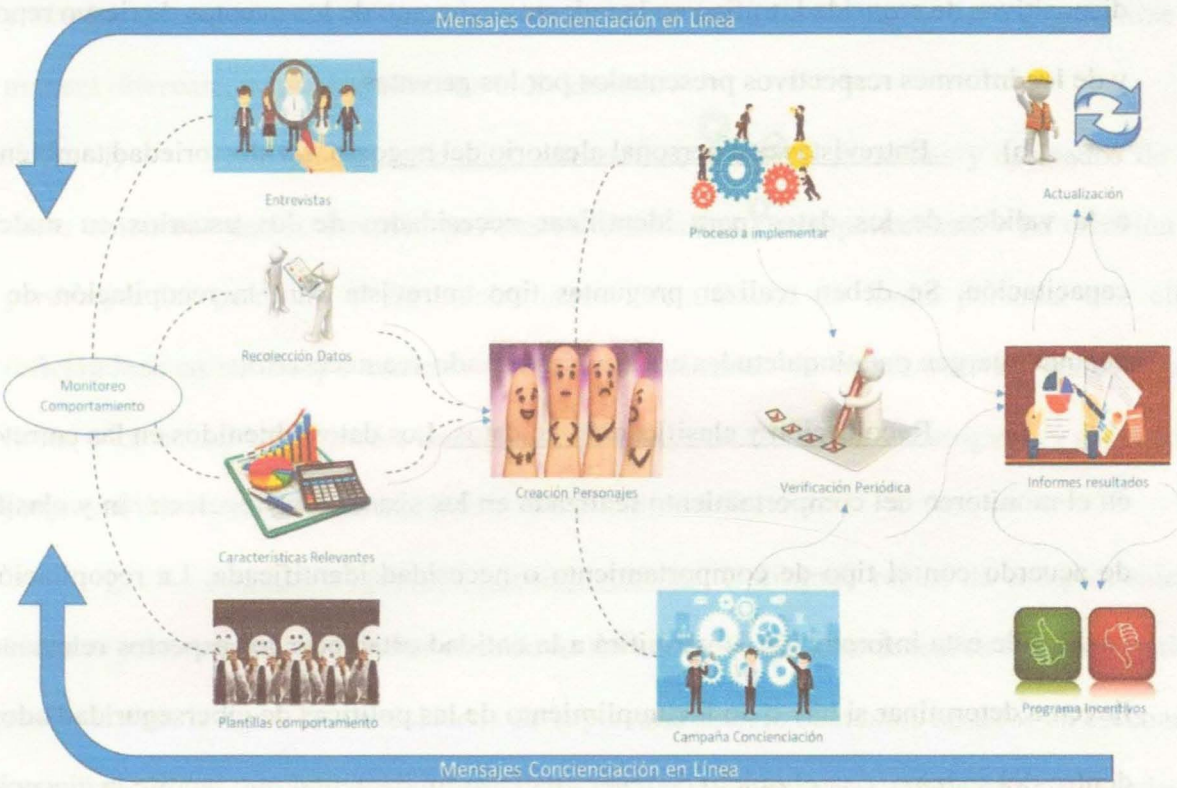
de dudosa reputación). Lo anterior, generando una estrategia de seguridad basada en múltiples capas de defensa o defensa en profundidad para asegurar el acceso autorizado a la información (https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_73/rzaj4/rzaj40a0internetsecurity.htm).

1.6. Programa de concientización a la medida

El programa de concientización a la medida parte de identificar las necesidades tanto de la entidad como de los colaboradores en materia de ciberseguridad, con el objeto de implementar campañas de concientización alineadas con dichos requerimientos, de modo que permita minimizar el riesgo cibernético al cual se encuentra expuesto el instituto, de acuerdo con lo identificado en el análisis basado en riesgos. Dicho programa se enfoca en la adopción de estrategias que lleven al cambio de comportamiento de los empleados y la oportuna gestión de conciencia. El programa, bandera fundamental del presente marco de referencia, se puede observar en forma gráfica en la figura 7.

Figura 7

Programa de concientización a la medida



El programa consta de dos componentes esenciales, a saber:

1.6.1. Programa periódico para generar cambio de comportamiento

El programa periódico se diferencia de las campañas que en forma común se realizan en las entidades, dado que parte de identificar las necesidades en materia de ciberseguridad en el instituto, para generar una campaña de concientización a la medida, que incluya la estrategia de cambio de comportamiento con el fin de disminuir de una forma clara y sencilla el riesgo cibernético. Las fases que componen este programa se detallan a continuación.

a) Monitoreo del comportamiento, información que se obtendrá del aplicativo encargado de correlacionar los eventos SIEM o de logs de los aplicativos tales como directorio activo, correo electrónico, aplicaciones core del negocio, proxy, registro de

dispositivos de seguridad, tráfico en la red, etc., así como de los eventos de riesgo reportados y de los informes respectivos presentados por los gerentes.

b) Entrevistas con personal aleatorio del negocio. La aleatoriedad también ayuda a la validez de los datos para identificar necesidades de los usuarios en materia de capacitación. Se deben realizar preguntas tipo entrevista para la recopilación de datos, dejando margen para inquietudes adicionales cuando sea necesario.

c) Recolección y clasificación de datos. Los datos obtenidos en las entrevistas y en el monitoreo del comportamiento realizado en los sistemas se recolectarán y clasificarán de acuerdo con el tipo de comportamiento o necesidad identificada. La recopilación y el análisis de esta información le permitirá a la entidad establecer los aspectos relevantes que lleven a determinar si hay o no incumplimiento de las políticas de ciberseguridad adoptadas dentro del sistema, con el objeto de tener una base fundamental que facilite la ejecución del plan según las necesidades allí identificadas.

d) Identificación de características relevantes. Agrupamiento de características por grupos de comportamientos identificados en la información recolectada. Identificar aspectos tales como habilidades de los usuarios, actividades realizadas, motivaciones, opiniones del colaborador sobre la ciberseguridad y la seguridad, incumplimiento de políticas en forma reiterada, etc.

e) Identificación de plantillas del comportamiento de los usuarios (usuarios típicos, cambiantes, modernos, atípicos, etc.). Una alternativa para consolidar la información y la clasificación de la misma puede ser a través del diagrama multicapa de radar de (Christiernin, 2010), quien menciona que el diseño multicapa (MLD) separa la interfaz gráfica de usuario de las aplicaciones en varias capas, basadas en las capacidades, habilidades

y niveles de experiencia de los usuarios. La disposición de las capas debe organizarse de manera diferente, según los usuarios individuales.

f) Creación de personajes, alineados con dichas plantillas y derivados de los datos obtenidos de los usuarios por sus características y comportamiento. La creación de personajes les permitirá a los colaboradores identificarse de forma personal con ellos, reflejándose en su comportamiento y acciones realizadas. El objetivo de los personajes es llevar a los usuarios a entender los aspectos por mejorar de una forma amigable y sin sentirse juzgados, pero tomando conciencia.

g) Analizar el proceso por implementar. Utilizando reglas de comportamiento simples y coherentes, se pueden considerar los comportamientos deseados con expectativas realistas para integrar las necesidades de la persona usando contextos basados en escenarios y analizando los riesgos y las necesidades de la entidad con respecto al ámbito particular de las personas, para identificar ajustes requeridos.

Las diferencias en las percepciones de los riesgos y los conjuntos de aptitudes aplicables que se requieren para adoptar el aprendizaje, determinan las estrategias para abordar la identificación del comportamiento del recurso humano tales como la ingeniería social. Para ello, se puede apoyar el proceso en estrategias de cambios de comportamiento como la programación neurolingüística (PNL).

> El modelo de estilos de aprendizaje de la programación neurolingüística (PNL) toma en cuenta el criterio neurolingüístico, el que considera que la vía de ingreso de información al cerebro (ojo, oído, cuerpo) resulta fundamental en las preferencias de quien aprende o enseña. Concretamente, el ser humano tiene tres grandes sistemas para representar mentalmente la información:

visual, auditivo y cinestésico (VAC). (López Bravo, Romo Aliste, & López Real, 2006).

Así mismo, existen juegos tales como Ctrl-Alt-Hack que está diseñado para ayudar a mejorar la conciencia de seguridad en entornos de grupo (Denning, 2013).

h) Ejecución de la campaña de concientización con los personajes creados, transmitiendo por diferentes canales de la entidad e incorporando la marca para brindarle una mayor personalización. Incluir otros estilos requeridos para abordar elementos adicionales de emociones, valores, impresiones y expectativas que conduzcan a un contenido y un contexto de diseño relevantes.

Se deben adoptar métodos de diseño participativos como juegos, pruebas, videoclips cortos o breves resúmenes de temas incluidos en las reuniones de equipos de trabajo.

Adicional, para la ejecución de la campaña se debe tener en cuenta la disponibilidad de personal y á planificar y aplicar la entrega de contenidos y métodos de comunicación adaptados.

i) Verificación periódica del resultado de la campaña para valorar el cambio obtenido o los ajustes requeridos para mejorar y llegar al objetivo planeado. Se pueden realizar ajustes a los personajes con nuevas versiones, ajustes en carteles, artículos novedosos o promocionales o herramientas de desarrollo basadas en la web; o generar nuevos folletos, secciones de noticias en curso, alertas en línea y en los medios de comunicación social, encuestas o foros. Todo lo que se realice debe estar adaptado al contexto real de la entidad.

Es importante llevar a cabo una retroalimentación para determinar la eficacia, los beneficios, los inconvenientes y las mejoras del ciclo de sensibilización. Los parámetros de

evaluación pueden ser modificados, pero siempre deben medir la eficacia del ciclo de concientización.

j) Presentación de informes sobre los problemas identificados, llevando a cabo el análisis de las causas fundamentales, como las tendencias en el servicio de asistencia técnica, el restablecimiento de las contraseñas, las verificaciones técnicas en los equipos y en la red, las campañas internas de suplantación de identidad (*phishing*) o de ingeniería social, etc.

k) Comprender y acordar las actualizaciones o modificaciones necesarias de las políticas, los procedimientos o el proceso de concientización. Considerar la incorporación de nuevas tecnologías o amenazas en las revisiones posteriores del ciclo, asegurándose de que se mantenga actualizada frente a los requerimientos del negocio y de las personas.

l) Programa de incentivo y retroalimentación. Con el resultado obtenido en la campaña de concientización y el monitoreo constante del comportamiento, definir con la alta dirección el programa de incentivo para persuadir a los usuarios a que cumplan, o sigan cumpliendo si ya lo está haciendo. Así mismo, definir las consecuencias del incumplimiento a la política de ciberseguridad y seguridad de la información.

Adicionalmente, se debe realizar una retroalimentación a los colaboradores con respecto al resultado general obtenido, resaltando los aspectos positivos y los avances logrados y reconociendo a los colaboradores que fueron premiados por su comportamiento adecuado.

m) Volver a ejecutar el proceso desde el inicio, cada 60 o 90 días, dependiendo de los resultados y la dinámica de la entidad.

1.6.2. Mensajes de concientización en línea

Con base en el monitoreo de los registros de auditoría de la plataforma por medio del SIEM, se deben configurar mensajes persuasivos de concientización a los colaboradores con respecto al uso adecuado de los permisos otorgados y el riesgo que se genera por la exposición de la información de la entidad. Por ejemplo, si un colaborador trata de ingresar a una página no autorizada, la cual se encuentra bloqueada por el sistema de navegación, se le debe mostrar, a parte del mensaje común de bloqueo, la política que está infringiendo y el riesgo que representa tanto para él mismo como para la entidad el hecho de no adoptarla.

Dependiendo del sistema que genera la alerta en el SIEM, se configura en el mensaje la política respectiva que puede estar incumpliendo y el mensaje que la alta dirección quiere hacerles llegar a los colaboradores para propiciar un cambio de comportamiento constante y en cada incumplimiento registrado.

1.7. Validación del perfil deseado u objetivo

Considerando el perfil actual, los nuevos objetivos del negocio con su respectivo alcance cibernético y los aspectos identificados por los actores, tales como la auditoría. Teniendo en cuenta lo definido en la fase de identificación de necesidades, validar si el perfil objetivo se ha cumplido o qué tan distante se está de cumplirlo, para llevar a cabo las mejoras que amerite el proceso en pro de obtener y lograr el perfil deseado.

1.8. Indicadores de gestión

Con el objeto de medir la eficacia y eficiencia de la implementación del marco de referencia y el nivel de madurez obtenido.

Elevar la eficacia y eficiencia constituye un gran reto al cual deben enfrentarse en la actualidad los sistemas empresariales debido a las exigencias cada vez más elevadas de los clientes. Para alcanzar estos objetivos es necesario que los directivos utilicen herramientas que les permitan diagnosticar los niveles de desempeño de la organización y, en función de los resultados, definir las estrategias a seguir (Oliva, 2018).

Con base en lo anterior, la manera más eficaz de mejorar los resultados generales y particulares de la entidad es midiendo y controlando la correcta implementación del sistema mediante los indicadores de gestión (Salgueiro, 2001).

1.9. Realizar procesos de auditoría interna y externa

En forma regular, incluyendo la validación del proceso de gestión de riesgos y controles aplicados.

El desarrollo de la auditoría incide de forma directa en la eficacia del sistema de gestión de la organización y su mejora; dicho sistema puede estar conformado por diversos estándares. Su integración en diferentes dimensiones (documentación, procesos y recursos humanos) confluye en un sistema integrado de gestión (SIG) (Escobar et al., 2016).

2. ¿Qué están haciendo mal las organizaciones en ciberseguridad?

Las entidades destinan muchos esfuerzos en materia de ciberseguridad, enfocándose en robustecer la plataforma tecnológica que asegura el perímetro tanto interno como externo, realizando diferentes pruebas de penetración y análisis de vulnerabilidades; sin embargo, no

se han obtenido los resultados esperados, ya que los incidentes se siguen presentando y se mantiene la tendencia de la debilidad en el talento humano.

En el estudio patrocinado por el Reino Unido (PWC, 2015) se identificó un aumento en los niveles de concientización sobre ciberseguridad y seguridad de la información brindados por las organizaciones, en comparación con el año anterior, aunque también se habían incrementado las incidencias relacionadas con el personal. La encuesta mostró que el 72 % de las grandes organizaciones le brindan una formación continua de concientización sobre la ciberseguridad y seguridad de la información al personal, en comparación con el 68 % del año anterior. "Esto pone de relieve que el simple hecho de transmitir información estándar sobre seguridad a los empleados de una organización no es un medio eficaz para garantizar la seguridad cibernética en relación con la seguridad humana" (Mark Evans et al., 2012).

Por lo anterior, se debe entender que "Una política es típicamente un documento que describe los requisitos o normas específicas que deben cumplirse. En el ámbito de la seguridad de la información/red, las políticas suelen ser específicas para cada punto y cubren una sola área" (SANS, 2020).

Una política de seguridad de la información se divide en dos categorías principales:

"Política de seguridad de alto nivel y política de seguridad de nivel inferior" (Baskerville, 2002). El hecho de contar con una política de ese tipo no garantiza que los colaboradores adopten el comportamiento requerido; es posible que no se comporten como se espera debido a la falta de comprensión del contenido de la política (Alotaibi et al., 2015).

De acuerdo con las campañas realizadas en el Icfes, se podría decir que la entidad considera que contar con una política de seguridad y sus respectivas políticas de nivel

inferior, y capacitar a los colaboradores para su cumplimiento, es suficiente como programa de concientización. Un programa de concientización y sensibilización debería utilizar normas de comportamiento sencillas y coherentes para los colaboradores, que ofrezcan una mayor percepción de control y una mejor aceptación de los comportamientos sugeridos. "Se deben tener en cuenta las diferencias culturales en las percepciones de los riesgos cuando se incorporen conductas positivas en materia de seguridad con apoyo, conocimientos y concientización" (Bada, Sasse & Nurse, 2014).

El contenido de la sensibilización debe ser atractivo, apropiado y continuo, con una gama de temas pertinentes que sean específicos, aplicables, factibles, y que proporcionen retroalimentación para ayudar a mantener la voluntad de cambio de las personas (Bada, Sasse & Nurse, 2014).

3. ¿Qué se espera obtener con este enfoque?

La medición del nivel de conciencia es más complicada, dado que los cuestionarios pueden indicar un nivel de conocimiento, sin implicar niveles de motivación para mejorar los comportamientos (Bada, Sasse & Nurse, 2014).

Con el marco de referencia de ciberseguridad expuesto, que se basa en un componente de cambio de comportamiento del recurso humano para lograr un resultado que se alinee con los objetivos de la alta dirección, se busca disminuir los riesgos cibernéticos generados por el talento humano, tales como:

- Pérdida de información clasificada
- Indisponibilidad de los servicios tecnológicos misionales

Dado que, en algunos casos, los objetivos de sensibilización en materia de seguridad se identifican y comunican claramente, "en el plano cultural, las personas no sienten la necesidad de consultar las orientaciones sobre seguridad interna, ya que los usuarios no creen tener preocupaciones en materia de seguridad" (Ki-Aries & Faily, 2017).

Por lo anterior, se plantea que, como parte del marco de referencia por implementar, se cambie este paradigma –que es muy común en las campañas de concientización, no solamente de ciberseguridad– y se inicie con un proceso de identificación de las verdaderas necesidades de la entidad y las personas en la materia, teniendo en cuenta los comportamientos identificados por medio de los aplicativos y las estrategias que ha diseñado la organización, para finalmente tener claras las acciones que lleven a un cambio de comportamiento de los colaboradores en su forma de percibir la seguridad y de asimilarla a su entorno, en pro del beneficio propio y de la misma organización.

> Un programa de seguridad cibernética consiste en las diversas iniciativas e infraestructuras establecidas para lograr la preparación y la capacidad de recuperación en materia de seguridad cibernética, mientras que las políticas de seguridad cibernética son la codificación por parte de una organización de las prácticas destinadas a mejorar la seguridad cibernética en una lista de directrices o principios" (Kassicieh et al., 2015).

Sin embargo, los esfuerzos para capacitar a los colaboradores de una organización y mantenerlos al tanto de los riesgos de la ciberseguridad durante sus tareas diarias también son una parte esencial de la ciberseguridad eficaz (Anderson, 2013).

4. Prototipo para aplicar como parte de la monografía

Con el objeto de llevar a la práctica el componente esencial de concientización del marco de referencia planteado en la presente monografía, se determina aplicar el siguiente prototipo, para el cual la teoría base será la de autodeterminación, teniendo en cuenta que el propósito es llevar a que los colaboradores se sientan agradados y en compatibilidad con el nuevo comportamiento que se quiere adoptar en sus vidas en el plano de la ciberseguridad, lo que contribuye a un cambio de comportamiento duradero y estable.

"Los seres humanos pueden ser proactivos y comprometidos o, alternativamente, pasivos y alienados, en gran medida como una función de las condiciones sociales en las cuales ellos se desarrollan y funcionan" (Deci & Ryan, 2000).

"Cambiar comportamientos puede ser un desafío, especialmente cuando se quiere transformar varias cosas al mismo tiempo. Esto no debe ser como una resolución sino como una evolución" (Eufic, 2014).

4.1. Definición de la muestra para la prueba del prototipo

Para la selección de la muestra, se tomaron los siguientes aspectos, teniendo en cuenta lo planteado por Hernández Sampieri et al. (2014):

a) La población por tener en cuenta, como parte del prototipo planteado, estará conformada por los colaboradores del Icfes en la ciudad de Bogotá.

b) La unidad de análisis por tomar en el prototipo planteado será el universo de personas que participaron en la encuesta presentada en el capítulo anterior (60 colaboradores aproximadamente). Lo anterior, dado que han sido los colaboradores que han podido ser parte de la estrategia de concientización llevada a cabo por el instituto.

c) La muestra por tomar para el prototipo en mención será no probabilística, teniendo en cuenta que serán aquellos colaboradores que participaron en la encuesta y que, de acuerdo con lo observado por el liderazgo de seguridad de la información, consideren fundamentales para aplicar el prototipo del proyecto.

4.2. Aplicación del prototipo

Para la ejecución del prototipo se llevaron a cabo las siguientes actividades:

1. Se definieron diez personas con el apoyo de los líderes de seguridad de la información, que corresponde aproximadamente a un 15 % de la unidad de análisis, a quienes se les dio el contexto del proyecto en forma general, y se les aplicó una encuesta de diez preguntas para determinar su nivel de conocimiento y compromiso con la ciberseguridad y la seguridad de la información, previo a la ejecución del prototipo. Dicha actividad se ejecutó en un tiempo aproximado de 20 minutos.

Para la definición de las personas requeridas, se tomaron aquellos colaboradores que participaron en las encuestas de conocimiento y campañas realizadas y que, de acuerdo con lo observado por el liderazgo de seguridad de la información, consideraron fundamentales para aplicar el prototipo del proyecto, teniendo en cuenta aspectos tales como:

1. Personas que se han identificado en incumplimiento de políticas.
2. Personas identificadas que requieren un cambio de comportamiento frente a la ciberseguridad y la seguridad de la información.
3. Personas en las que se ha identificado que, aunque cumplen las políticas, pueden ser apáticas al tema de ciberseguridad y seguridad de la información.

2. Se dividió el grupo de las diez personas seleccionadas en dos, con el objetivo de llevar a cabo las siguientes sesiones de máximo 20 minutos con cada uno de ellos, así:

a) Primer grupo, aplicación de técnica 1-Switch. Es una de las más utilizadas por la programación neurolingüística y es muy útil en cualquier momento que se desea cambiar de comportamientos o sentimientos no deseados.

Este método puede lograr cambios personales importantes en un lapso de tiempo bastante breve.

> Esta técnica de desarrollo personal no recurre a concepciones filosóficas, religiosas o espirituales, sino que los resultados los obtiene de una forma práctica y concreta. Su eficacia se debe al propio espíritu humano, que es capaz de transformar cualquier mecanismo por complicado que este sea (Redford, 2014).

Lo anterior les permite a las personas generar un cambio de comportamiento mediante la estimulación de la creatividad, que se ubica en la parte derecha del cerebro, lóbulo occipital, donde se interpreta la visión; lóbulo temporal, donde se integran la memoria, la escucha y el comportamiento; y el lóbulo frontal, desde donde se coordina, controla y ejecuta la conducta. El proceso enseñado debe ser aplicado a diario por cada una de las personas del grupo, hasta generar realmente un cambio en la conducta.

b) Segundo grupo, aplicación de técnica 2–Videos de concientización y charla magistral para que queden en el recuerdo dichas historias o mensajes, e incentivar a seguir un patrón teniendo en cuenta a una persona que consideren que aportaría al ejercicio del cambio, estimulando también la parte derecha del cerebro, el lóbulo parietal, donde se integran las sensaciones; el lóbulo occipital, donde se interpretan la visión y la función visual; el lóbulo temporal, donde se integran el comportamiento y la memoria, pretendiendo que

recuerde lo aprendido y aplique en pro de mejorar la ciberseguridad y seguridad de la información.

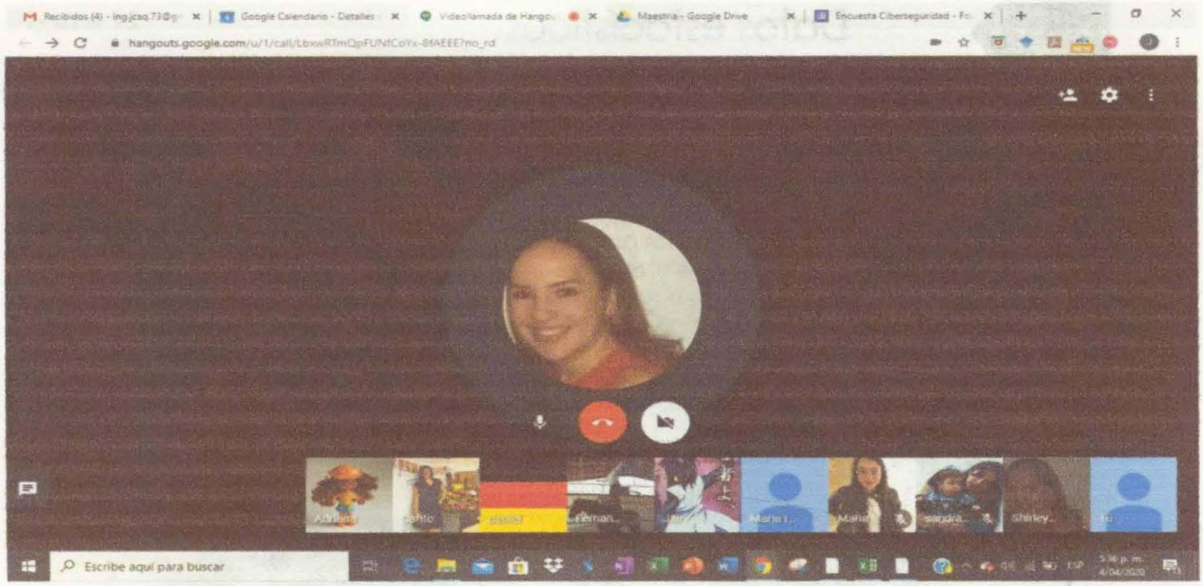
A las personas de cada grupo se les solicitó que evitaran hablar con las de los otros equipos con respecto a lo que se llevó a cabo en la sesión grupal; lo anterior, teniendo en cuenta que el éxito de este prototipo estará en esta parte, dado que si cada uno se concentra en realizar el ejercicio sin que influya en él lo que los otros equipos tomaron, se podría determinar mejor su eficacia y eficiencia.

En esta primera sesión se invirtió un tiempo aproximado de una hora, que para los colaboradores representó aproximadamente unos 40 minutos (20 minutos de la charla general y 20 minutos de la sesión con cada grupo).

Esta sesión se realizó aprovechando la plataforma de conferencias virtuales Meet de Google, a la cual se unieron los participantes seleccionados para la aplicación del prototipo. Así mismo, se diligenció la encuesta en forma virtual por medio de la plataforma de formularios de Google.

Figura 8

Evidencia de la primera sesión del prototipo



Nota: Tomado de la plataforma Google Meet (2020)

Para la aplicación del prototipo, el ejercicio se apoyó en el uso de videos tanto para la explicación de la técnica *switch*, que permite generar cambio de comportamiento, como para crear conciencia. Se utilizaron los siguientes videos:

- https://www.youtube.com/watch?v=VELH_ZHIRhw
- https://www.youtube.com/watch?v=j-tFoYNHi1w&feature=youtu.be
- https://www.youtube.com/watch?v=NHlTtqmjy5k

Así mismo, algunas de las diapositivas con las que se realizó el proceso de concientización fueron:

Figura 9

Presentación de concientización. Datos estadísticos

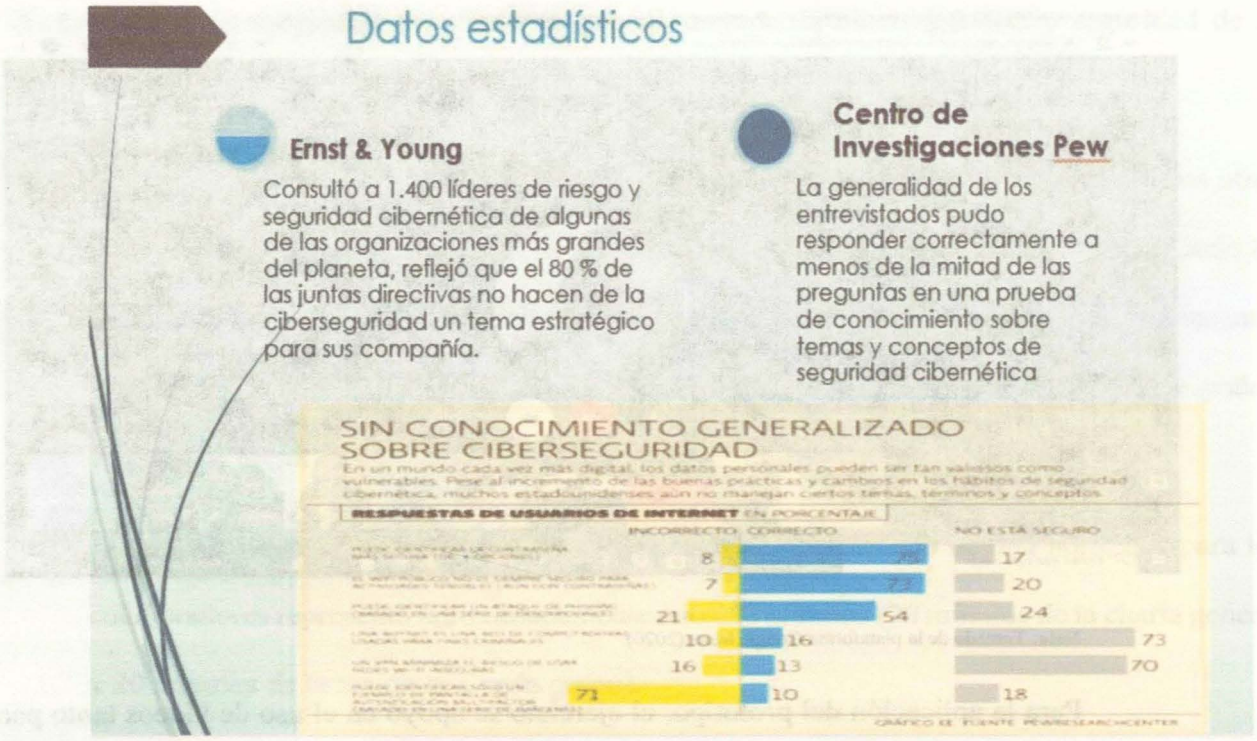


Figura 10

Presentación de concientización. Aspectos generales

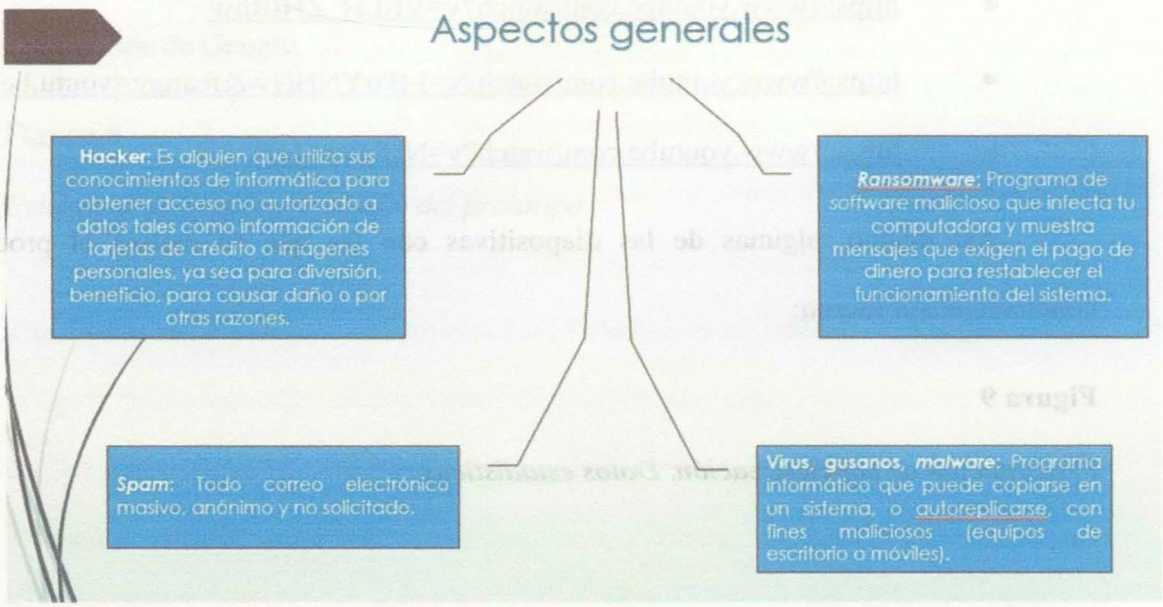


Figura 11

Presentación de concientización. Algunas técnicas más comunes

Figura 12

Presentación de concientización. Buenas prácticas

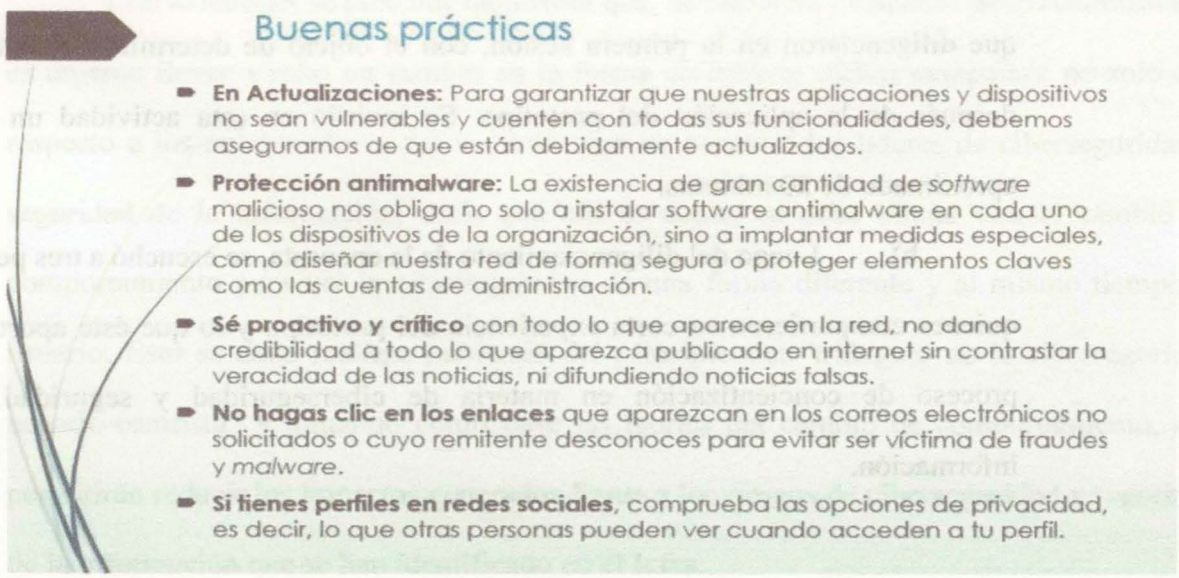
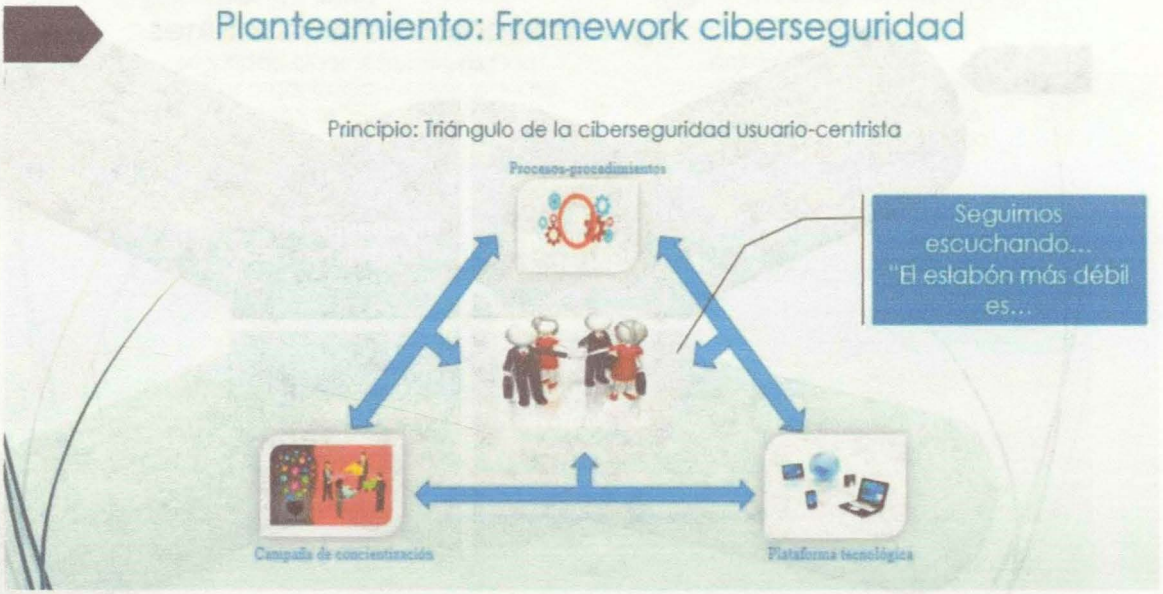


Figura 13

Presentación de concientización. Planteamiento: Framework ciberseguridad



3. Al cabo de tres días, se efectuó una segunda sesión para realizar las siguientes actividades con las mismas diez personas:

a) Se recordó la generalidad del proyecto y se aplicó la misma encuesta que diligenciaron en la primera sesión, con el objeto de determinar el antes y el después de la aplicación del prototipo. Se invirtió en esta actividad un tiempo aproximado de 20 minutos.

b) Luego del diligenciamiento de la encuesta, se escuchó a tres personas, quienes compartieron su corta experiencia del prototipo y lo que éste aportó en el proceso de concientización en materia de ciberseguridad y seguridad de la información.

El objetivo de esta actividad es que las personas del primer grupo aporten más aspectos positivos que las del segundo grupo. En esta segunda parte se invirtió un tiempo aproximado de 40 minutos, dado que se escucharon atentamente los testimonios que cada persona voluntariamente realizó.

En esta segunda sesión, que se llevó a cabo en la plataforma de conferencias virtuales Zoom, se invirtió un tiempo aproximado de una hora. Se cuenta con el audio respectivo de la sesión, dado que, por tener una cuenta no paga, no se acceder al video. Al igual que en la primera sesión, se diligenció la encuesta virtual por medio de la plataforma de formularios de Google.

4. Se consolidó la información obtenida antes y después de la aplicación del prototipo, con el objeto de comparar las respuestas con las encuestas y los testimonios que se recibieron por parte de los colaboradores. Producto de dicha consolidación, se obtuvo el resultado del trabajo de campo de la aplicación del prototipo planteado.

Con lo anterior se pretende demostrar que, de cara a las campañas de concientización, es urgente llevar a cabo un cambio en la forma de realizar dichas campañas; no solo con respecto a los colaboradores del instituto sino en cuanto a los líderes de ciberseguridad y seguridad de la información, dado que allí es donde se debe iniciar con el cambio de comportamiento para ver la ciberseguridad de una forma diferente y al mismo tiempo al usuario. Esto se debe realizar partiendo del principio del "triángulo de la ciberseguridad usuario-centrista" y tomando como base las teorías del cambio de comportamiento, que permitirán reducir los impactos generados frente a los riesgos de ciberseguridad y seguridad de la información que se han identificado en el Icfes.

4.3. Encuesta aplicada

Los colaboradores respondieron la siguiente encuesta en las dos sesiones realizadas:

Tabla 4

Encuesta aplicada a los colaboradores

Id	Pregunta
1	¿Sabes si la entidad tiene implementado un sistema de gestión de la seguridad de la información (SGSI), en el cual se incluye la ciberseguridad?
2	¿De acuerdo a las campañas de seguridad que has recibido en la Entidad, es una buena práctica utilizar la misma contraseña para acceder a varios servicios o aplicativos?
3	Para el siguiente planteamiento: Tengo que inventar una nueva clave para mi usuario de red. He decidido tomar el nombre de mi gata que es mi adoración junto con el día de mi cumpleaños, quedando de la siguiente manera: Chinis21. ¿Consideras que es una contraseña segura?
4	De acuerdo con tu conocimiento, ¿qué tipo de persona crees que son los *hacekrs* ?
5	De acuerdo con tu conocimiento, ¿qué consideras que es el *ransomware* ?
6	He recibido un mensaje al correo personal en donde me solicitan colaboración con una ONG que se dedica a la investigación del nivel de estudios en los colombianos para plantear nuevas estrategias, para lo cual me piden facilitar cierta información de la entidad. A dicha información tengo acceso por mi rol y considero que me quedaría fácil ayudar con este proceso de investigación.
7	Al llegar a la oficina, después de un delicioso almuerzo, encuentro a Juan, mi compañero de trabajo con quien he tenido una relación de amistad muy buena y hemos laborado juntos por más de 10 años, haciendo copia de la información de los proyectos que él administra en la entidad a su USB personal. Al consultarle qué está haciendo, me informa que es una copia de seguridad que él genera todos los jueves para llevársela a la casa y tenerla allí por cualquier inconveniente que se pueda presentar en el equipo.
8	Durante varios meses he tenido inconvenientes con el líder de seguridad de la información porque en varias ocasiones he dejado mi computador sin bloqueo cuando me desplazo a media mañana a tomar un pequeño descanso. En cada situación presentada me han dejado mensajes molestos para que bloquee mi sesión antes de ausentarme del puesto y estos mensajes han sido vistos por mi jefe.
9	Al ingresar a un sitio en internet, del cual requiero una información urgente para culminar con el requerimiento de mi jefe, me aparece un mensaje que dice que debo instalar primero un ayudante que permitirá visualizar mejor dicha información. Procedo a instalarlo y descargo la información requerida. Al cabo de unas horas, termino el informe para mi Jefe y se lo remito por correo, cumpliendo así con mi compromiso. Al día siguiente, al ingresar al equipo de la Entidad me aparece un mensaje que me impide acceder a la información y que debo proceder a realizar un pago para obtenerla de nuevo.
10	¿Qué tanto confía usted en las campañas de concientización en seguridad de la información? ¿Ha sido retroalimentado de los resultados obtenidos y le ha generado nuevos conocimientos para ser aplicados a su labor?

Adicionalmente, se solicitó a los colaboradores ofrecer la siguiente información:

Tabla 5

Preguntas adicionales

Id	Pregunta
1	Por favor, selecciona el rango del año en el que naciste: a. Entre 1946 y 1964 (Generación Baby Boomers) b. Entre 1965 y 1979 (Generación X) c. Entre 1965 y 1979 (Generación Y) d. A partir del 2000 (Generación Z)
2	Por favor, selecciona el género al cual perteneces: a. Femenino b. Masculino c. Otro
3	Por favor, selecciona tu nivel de escolaridad: a. Secundaria b. Pregrado c. Especialización d. Maestría e. Doctorado

4.4. Resultados del prototipo

Una vez aplicado el prototipo en los colaboradores seleccionados, se obtuvieron los siguientes resultados:

De las preguntas de información general se tienen los siguientes datos:

Figura 14

Clasificación por generaciones

Figura 15

Clasificación por género

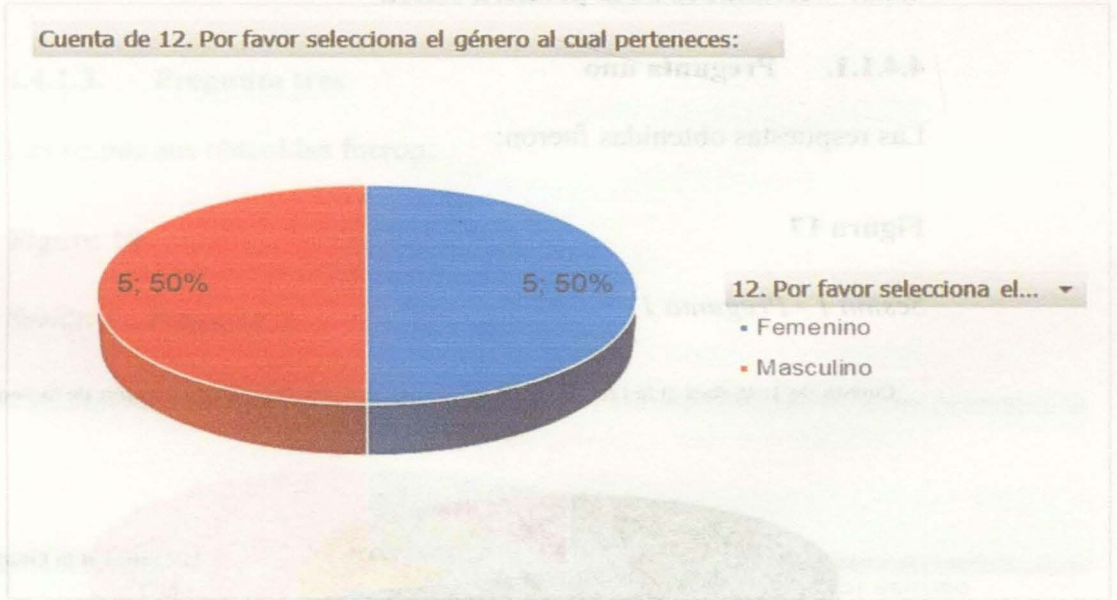
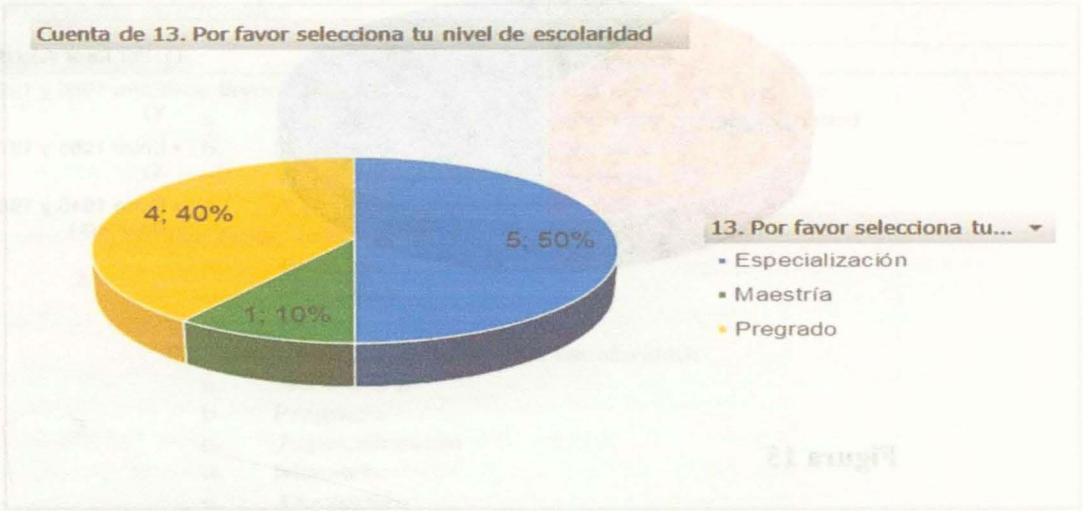


Figura 16

Clasificación por nivel de escolaridad



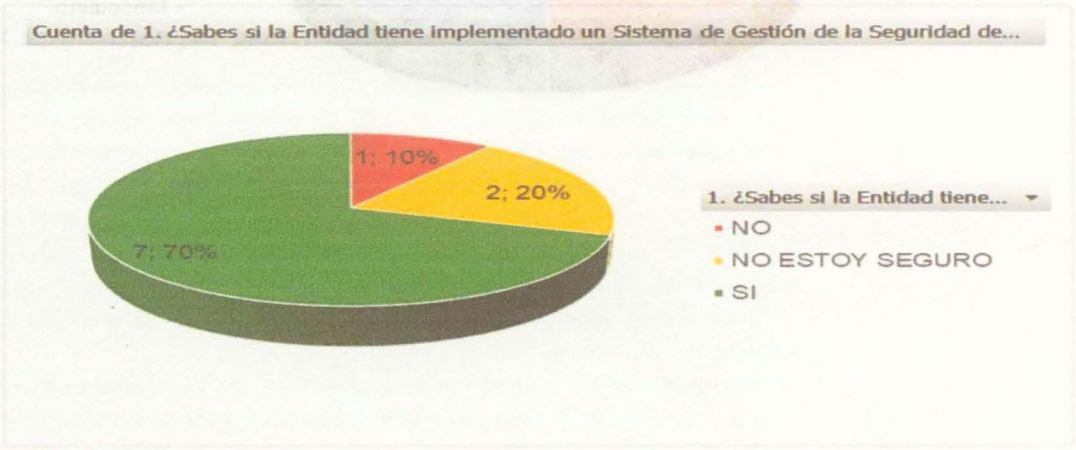
4.4.1. Resultados de la primera sesión

4.4.1.1. Pregunta uno

Las respuestas obtenidas fueron:

Figura 17

Sesión 1 - Pregunta 1

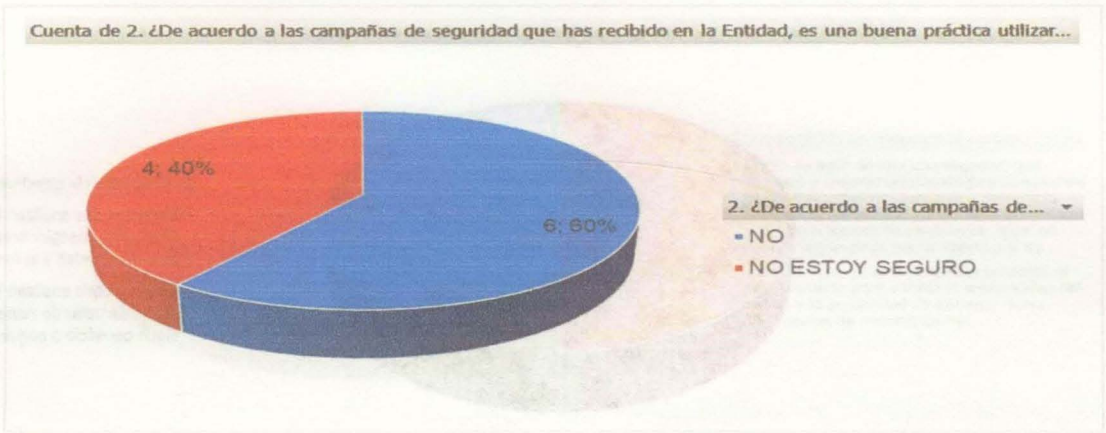


4.4.1.2. Pregunta dos

Las respuestas obtenidas fueron:

Figura 18

Sesión 1 - Pregunta 2



4.4.1.3. Pregunta tres

Las respuestas obtenidas fueron:

Figura 19

Sesión 1 - Pregunta 3

4.4.1.4. Pregunta cuatro

Las respuestas obtenidas fueron:

Figura 20

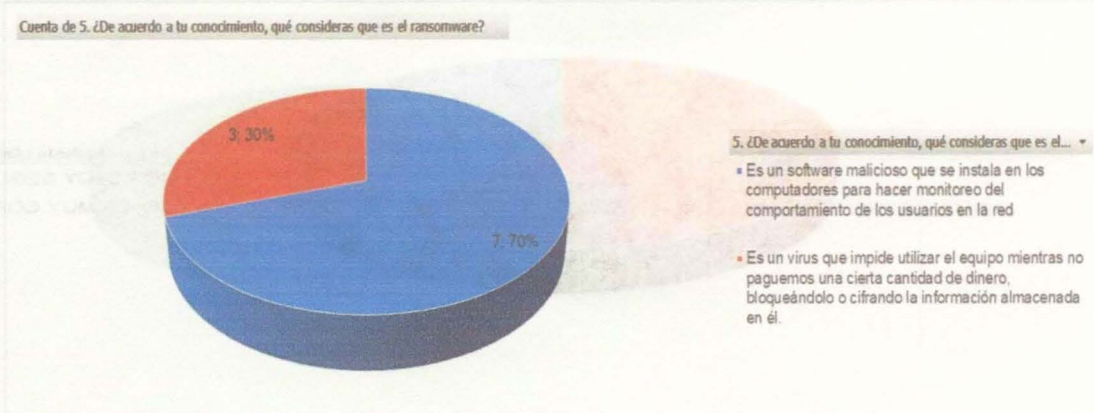
Sesión 1 - Pregunta 4

4.4.1.5. Pregunta cinco

Las respuestas obtenidas fueron:

Figura 21

Sesión 1 - Pregunta 5

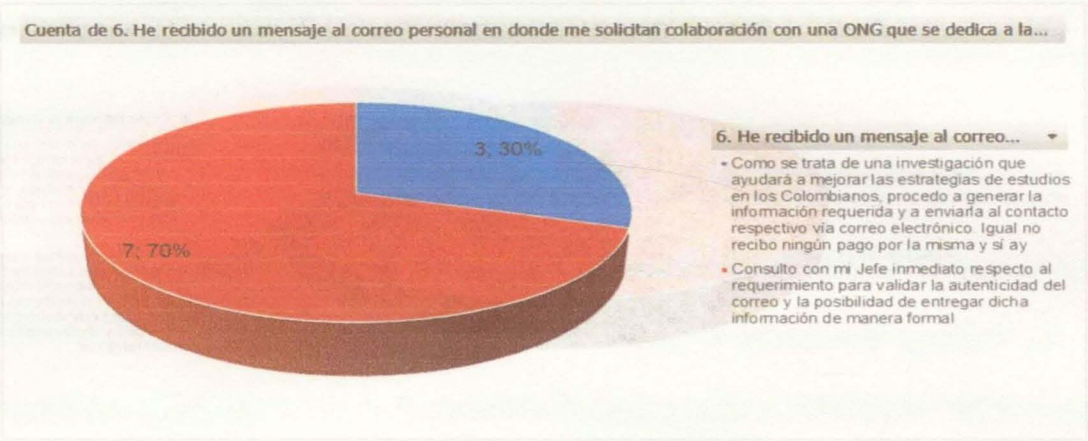


4.4.1.6. Pregunta seis

Las respuestas obtenidas fueron:

Figura 22

Sesión 1 - Pregunta 6

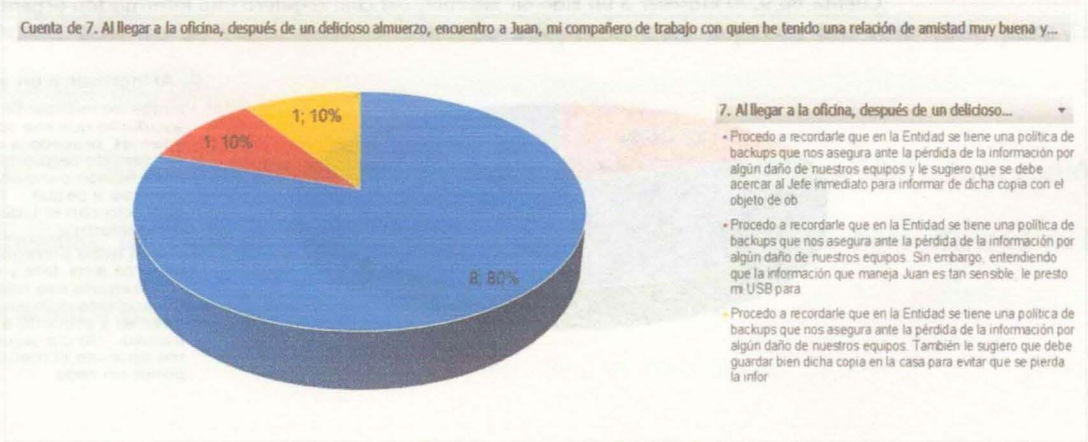


4.4.1.7. Pregunta siete

Las respuestas obtenidas fueron:

Figura 23

Sesión 1 - Pregunta 7

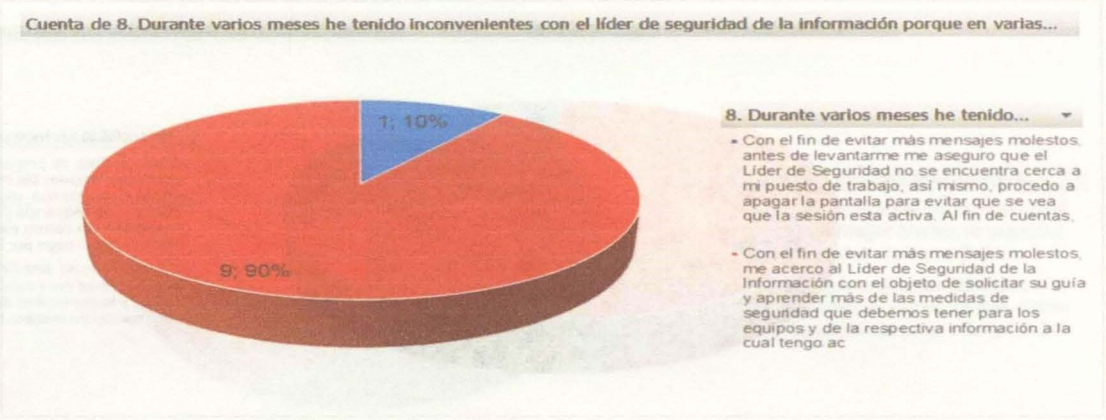


4.4.1.8. Pregunta ocho

Las respuestas obtenidas fueron:

Figura 24

Sesión 1 - Pregunta 8

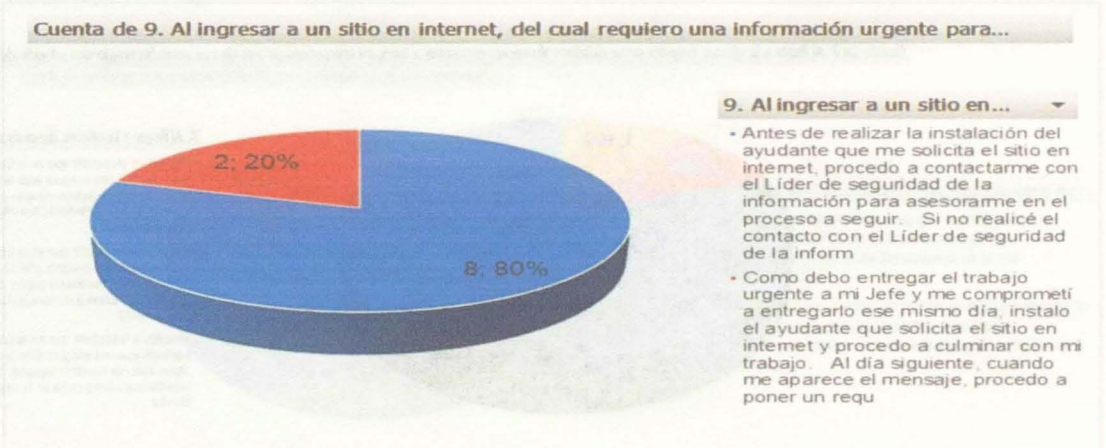


4.4.1.9. Pregunta nueve

Las respuestas obtenidas fueron:

Figura 25

Sesión 1 - Pregunta 9



4.4.1.10. Pregunta diez

Las respuestas obtenidas fueron:

Figura 26

Sesión 1 - Pregunta 10

4.4.2. Análisis de resultados y conclusiones de la primera sesión

Con base en los resultados obtenidos en la aplicación de la encuesta en la primera sesión del prototipo, se puede concluir que:

a) Prácticamente el 30 % de los encuestados afirman que la entidad no cuenta con un programa de ciberseguridad, o por lo menos en el programa de seguridad de la información aún no se tiene adecuadamente adoptado este aspecto tan relevante para las organizaciones hoy en día.

b) Se requiere reforzar en los colaboradores aspectos de seguridad para la gestión de contraseñas, teniendo en cuenta que el 40 % de los encuestados no tiene claridad en la identificación o gestión de una contraseña segura.

c) Así mismo, es necesario reforzar los conocimientos en ciberseguridad, de tal forma que los colaboradores tengan la capacidad de diferenciar el objetivo que persiguen inescrupulosos en su labor diaria.

Lo anterior, dado que:

- Un 50 % de los encuestados tienen claridad de las funciones de un *hacker* (en el contexto de un usuario con conocimientos básicos de seguridad).
- Un 30 % tiene dudas en la identificación de la función de un *ransomware*, aspectos que hoy en día son de vital importancia para las entidades.

d) Igualmente, se requiere un cambio en la forma de analizar e interiorizar aspectos que pueden ser fundamentales para ayudar a la entidad a minimizar el riesgo de ciberseguridad al cual se encuentra expuesto el Icfes. Lo anterior, teniendo en cuenta que:

- Un 30 % de los encuestados podrían ser víctimas en campañas de ingeniería social, entregando información vital de la entidad.
- Prácticamente un 20 % de los encuestados podrían permitir la fuga de información dada por colaboradores de la propia entidad, o por el actuar ingenuo de ellos mismos.
- Un 10 % tendría inconvenientes con las prácticas de seguridad de la información aplicadas por el respectivo liderazgo, al no asumir una postura profesional frente al manejo de las sesiones activas en periodos de ausencia de los puestos de trabajo, lo cual podría llevar a una posible fuga de información y afectar al mismo personal que la permite.

- Un 20 % de los encuestados podrían llevar a la entidad a una contaminación por *ransomware*, u otro tipo de *malware*, al tener acciones poco evasivas frente a los mensajes presentados en sitios de internet de dudosa reputación.
- Un 60 % manifiesta no haber recibido retroalimentación de las campañas de seguridad de la información realizadas por la entidad, lo cual lleva a que las personas sigan actuando de la misma forma, dado que no se les enseñan los aspectos por mejorar, o cambiar, de modo que se asuma una mejor postura frente a los temas relacionados con la ciberseguridad.

e) Como se puede observar, el personal encuestado es un grupo interdisciplinario que tiene un buen nivel de escolaridad, lo cual permite que temas como el de la ciberseguridad tengan buena acogida. Lo anterior se basa en que el 50 % de los encuestados forman parte de la Generación Y o *millenials*, que tienen más arraigo con la tecnología y menos apatía al cambio, pero a la vez son una generación más desprendida de una relación laboral, con bajos niveles de fidelización y motivación por la permanencia en los empleos (Martín, 2014).

f) Sin embargo, se observa que es necesario un cambio de comportamiento que permita mejorar el nivel de actuación de los colaboradores frente al riesgo de ciberseguridad al que se encuentra expuesta la entidad, el cual debe ser parte de las campañas de concientización por implementar por el instituto.

g) Así mismo, se observa la necesidad de fortalecer las campañas de concientización en ciberseguridad con aspectos actualizados que les permita a los colaboradores contar con información actual que ofrezca un mejor apoyo a la gestión

realizada en la entidad, no solo por los líderes de seguridad de la información, sino por todo el personal que es parte del Icfes.

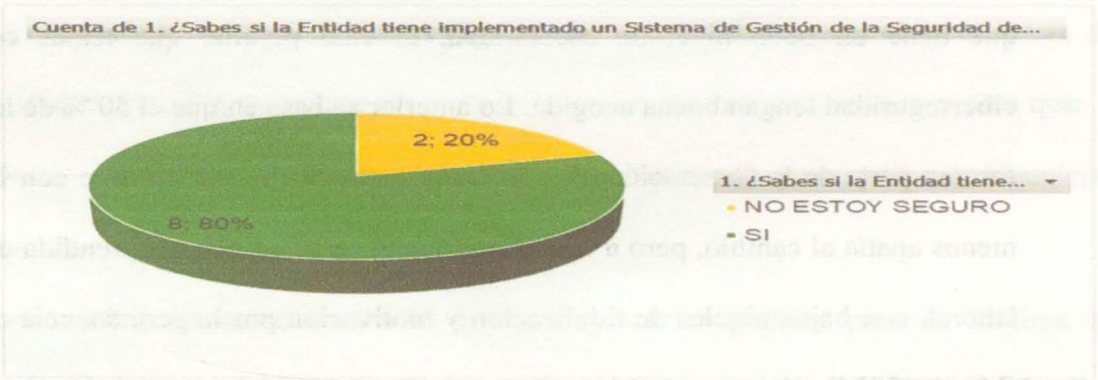
4.4.3. Resultados de la segunda sesión, luego de aplicar la metodología planteada

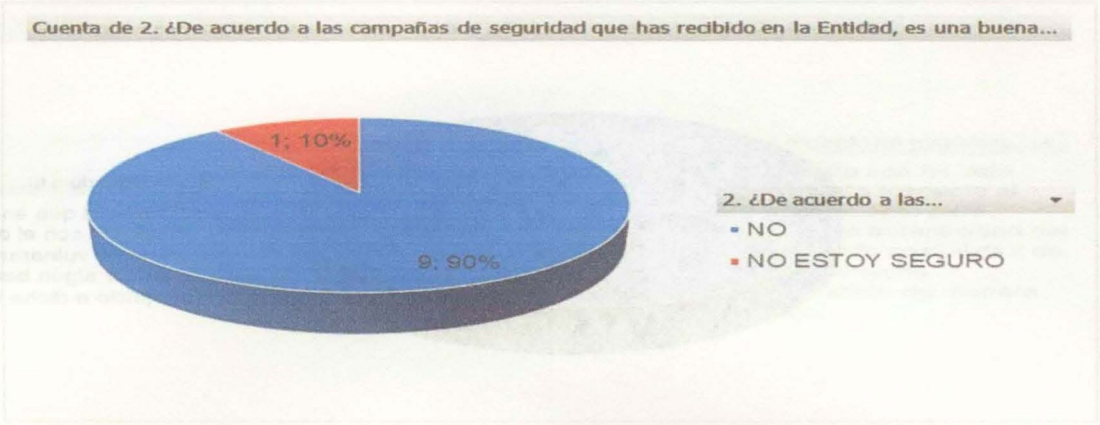
4.4.3.1. Pregunta uno

Las respuestas obtenidas fueron:

Figura 27

Sesión 2 - Pregunta 1





4.4.3.3. Pregunta tres

Las respuestas obtenidas fueron:

Figura 29

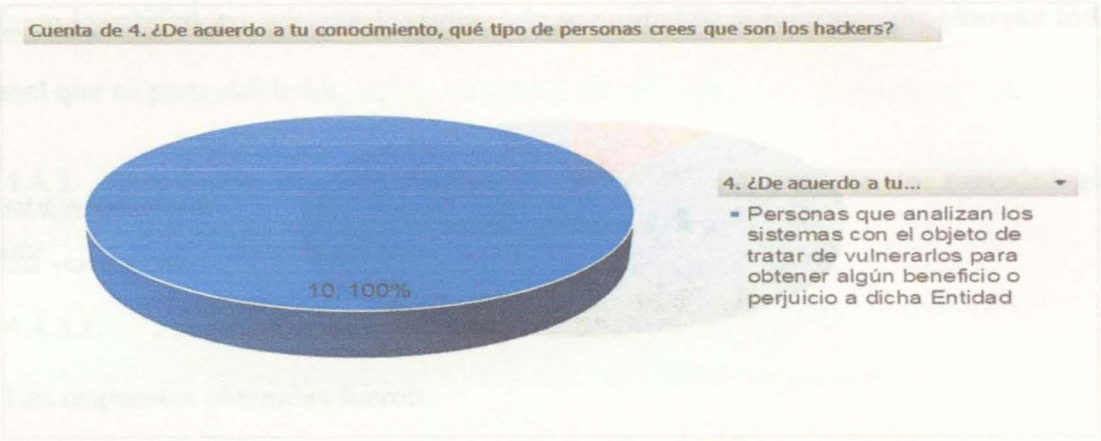
Sesión 2 - Pregunta 3

4.4.3.4. Pregunta cuatro

Las respuestas obtenidas fueron:

Figura 30

Sesión 2 - Pregunta 4

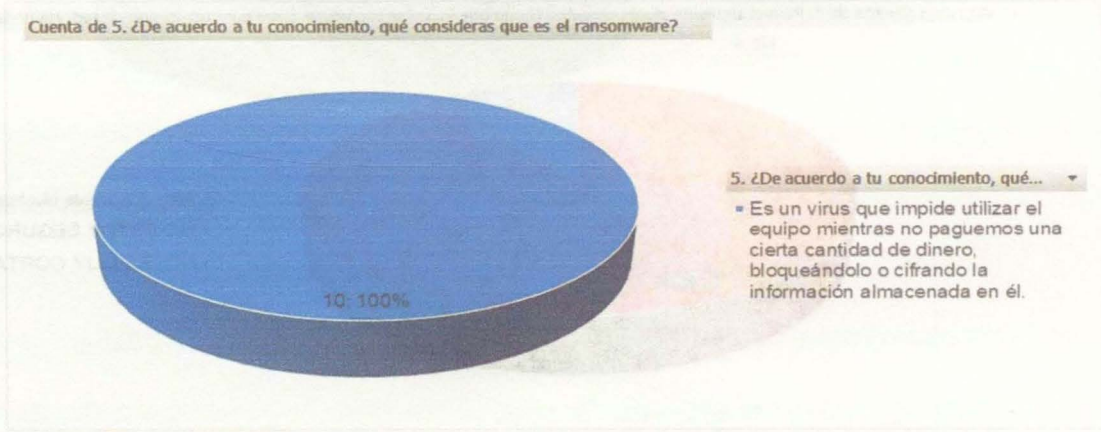


4.4.3.5. Pregunta cinco

Las respuestas obtenidas fueron:

Figura 31

Sesión 2 - Pregunta 5

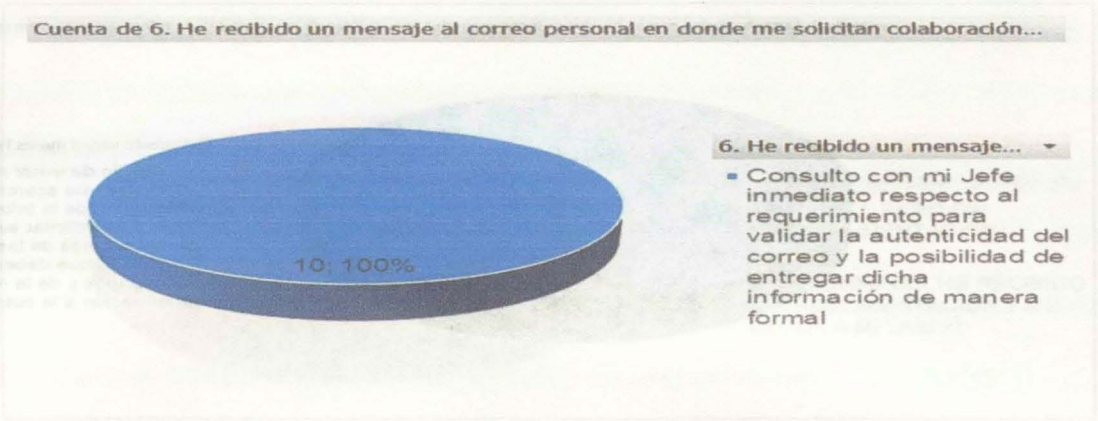


4.4.3.6. Pregunta seis

Las respuestas obtenidas fueron:

Figura 32

Sesión 2 - Pregunta 6



4.4.3.7. Pregunta siete

Las respuestas obtenidas fueron:

Figura 33

Sesión 2 - Pregunta 7

4.4.3.8. Pregunta ocho

Las respuestas obtenidas fueron:

Figura 34

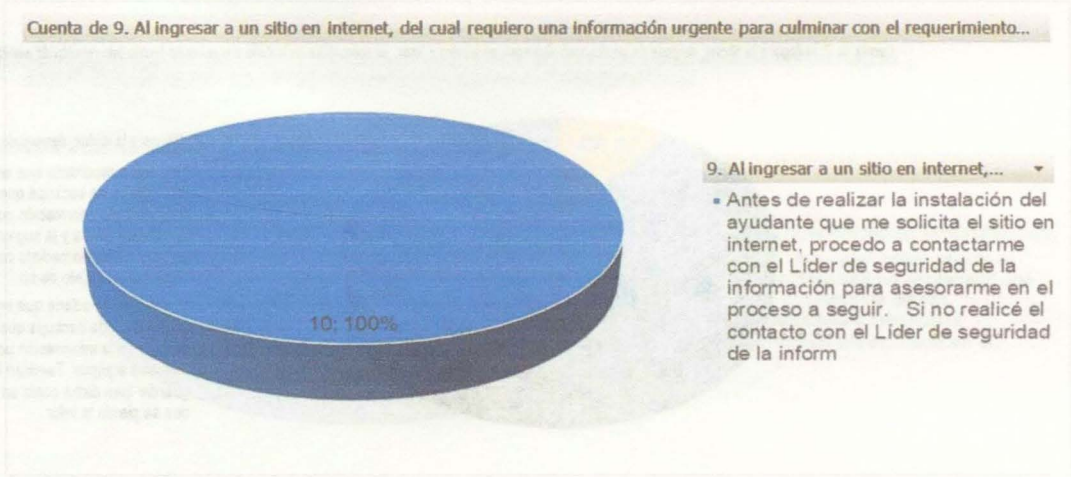
Sesión 2 - Pregunta 8

4.4.3.9. Pregunta nueve

Las respuestas obtenidas fueron:

Figura 35

Sesión 2 - Pregunta 9

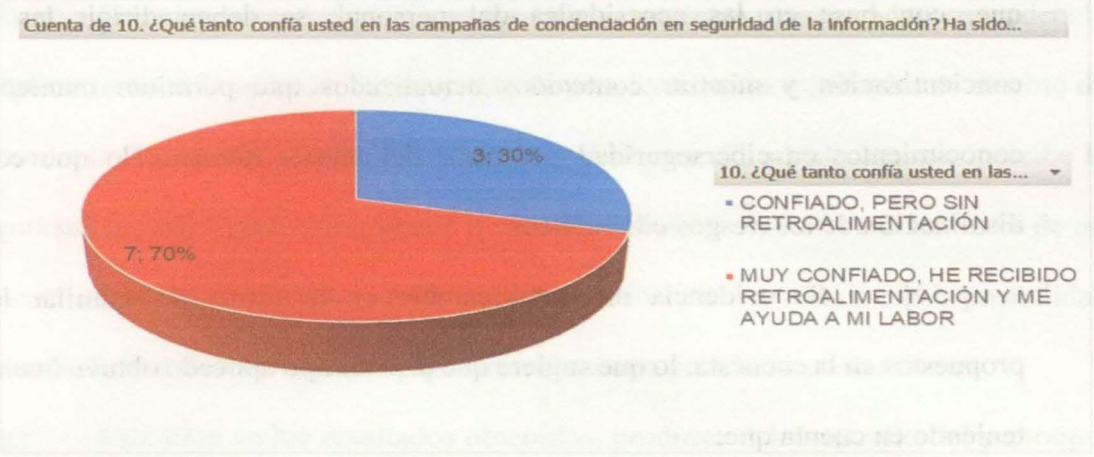


4.4.3.10. Pregunta diez

Las respuestas obtenidas fueron:

Figura 36

Sesión 2 - Pregunta 10



4.4.4. Resultados obtenidos en la aplicación del prototipo

Una vez aplicada la estrategia definida para el prototipo en mención, con el cual se pretendía propiciar un cambio de comportamiento en los colaboradores participantes, y con base en los resultados de la encuesta, se obtienen los resultados relacionados a continuación:

a) Aclarados los conceptos básicos de ciberseguridad, se observa una disminución, a favor, en la pregunta 1. Se considera que lo anterior se presenta dada la explicación de dichos conceptos en la primera sesión, lo cual lleva a que el colaborador aclare dudas con respecto al tema.

b) Así mismo, se observa una disminución del 30 %, a favor, de cara a la gestión de contraseñas, producto de lo explicado en las sesiones de concientización llevadas a cabo.

c) Con respecto a los conocimientos en ciberseguridad, se observa una mejora dado que el personal encuestado logró diferenciar las funciones básicas de un *hacker* y el resultado que un *malware* tipo *ransomware* puede generar para la información de la entidad.

d) Los resultados obtenidos, de acuerdo con lo evidenciado en los puntos anteriores, lleva a reforzar lo evidenciado en el resultado de la primera sesión en cuanto a

que, con base en las necesidades del personal, se deben dirigir las campañas de concientización y mostrar contenidos actualizados que permitan mantener al día los conocimientos en ciberseguridad por parte del talento humano, lo que contribuye a la disminución de los riesgos cibernéticos.

e) Se evidencia un grato cambio en la forma de asimilar los escenarios propuestos en la encuesta, lo que sugiere que el prototipo aplicado obtuvo buenos resultados, teniendo en cuenta que:

- El 100 % de los encuestados adoptaron una medida segura frente a la posibilidad de ser engañados mediante la ingeniería social.
- Se obtiene una mejora del 10 % frente a la posibilidad de permitir fugas de información, producto del actuar de un compañero de labores con quien han compartido por mucho tiempo.
- Se asume una postura bastante profesional, identificando un cambio importante de actuación frente a las relaciones con los líderes de seguridad de la información, de cara a la labor realizada por estos últimos, tendientes al aseguramiento de la información.
- Así mismo, se observa un cambio en la forma de actuar frente a situaciones que conllevan poner en una balanza la seguridad versus el cumplimiento de las funciones.
- Con sorpresa se observa que en la pregunta de retroalimentación recibida en las campañas de seguridad se presenta una disminución del 30 %. Al parecer, lo anterior se debe a la forma en que se realizó el prototipo, con el que se llevó a los colaboradores a entender, o recordar, aspectos fundamentales de la ciberseguridad y se permitió plantear sus puntos de vista o dudas para aclararlas.

f) Con el resultado obtenido en los últimos aspectos mencionados, se evidencia que, al aplicar, o formar parte de las campañas de concientización estrategias de cambio de comportamiento, las personas asumen una postura diferente. El talento humano percibe la ciberseguridad de otra forma, entendiendo que la gestión del riesgo cibernético no es de un área específica, sino que cada uno es parte de dicha gestión y en sus manos está la posibilidad de disminuir el nivel de este tipo de riesgos tan relevantes para las organizaciones.

g) Con base en los resultados obtenidos, producto del desarrollo del prototipo, se observa que es necesario replantear la forma en que se llevan a cabo las actuales campañas de concientización en la entidad. No se debe seguir llevando lo mismo a los colaboradores, sino que se deben plantear de forma diferente dichas campañas, incluyendo nuevos contenidos, actualizados, haciendo partícipes a las personas de la gestión del riesgo cibernético o realizando retroalimentación continua de los resultados obtenidos de cada ejercicio ejecutado en la entidad.

h) Si el ejercicio se organiza en forma más adecuada, desde el punto de vista de:

- Contar con personal experto en el proceso de cambio de comportamiento
- Con mayores actividades por realizar por parte de los colaboradores
- Con un tiempo más amplio al que se tuvo para la aplicación del prototipo

Se obtendrá mejores resultados a los obtenidos en el protocolo aplicado, producto de la presente monografía. Esto se deja a consideración del instituto, con el objeto de lograr mejores niveles en el riesgo residual cibernético.

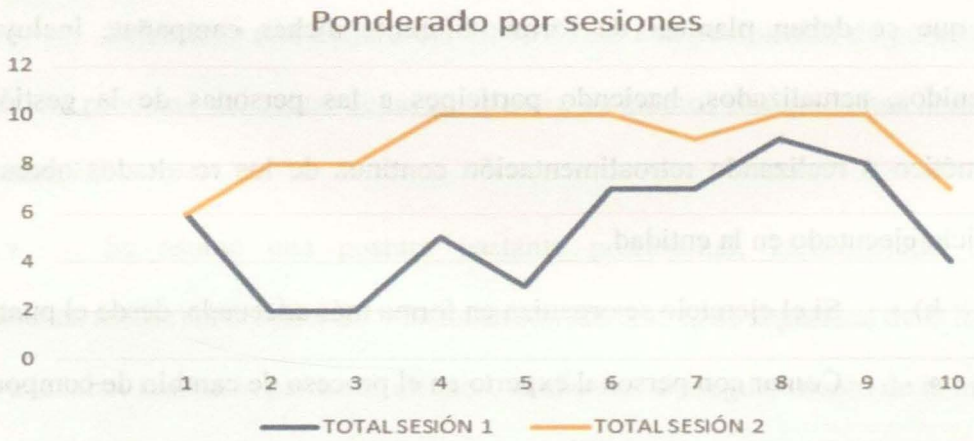
En la figura 37 se observa el consolidado de los resultados obtenidos en las encuestas antes y después del prototipo. Se le asignó un puntaje a cada respuesta de acuerdo con:

- Respuesta asertiva, obtiene un puntaje de uno (1).
- Respuesta neutra, obtiene un puntaje de cero (0).
- Respuesta negativa, obtiene un puntaje de menos uno (-1).

Se evidencia una mejora considerable entre las respuestas de la primera sesión frente a la segunda, principalmente en aquellas que permiten medir un cambio de comportamiento tras la aplicación del protocolo establecido:

Figura 37

Consolidado de respuestas obtenidas por sesión



4.5. Ficha técnica de la encuesta

A continuación, se muestra la ficha técnica de la encuesta aplicada en el desarrollo del prototipo planteado (tabla 6):

Tabla 6

Ficha técnica de la encuesta de concientización en ciberseguridad

Aspecto	Descripción
Nombre del proyecto de investigación	Propuesta metodológica para la implementación de un *framework* de ciberseguridad en el Icfes
Nombre de la encuesta	Encuesta de concientización en ciberseguridad
Objetivos de la encuesta	La presente encuesta pretende identificar el grado de conocimiento, conciencia y apropiación de los colaboradores frente al tema de ciberseguridad. Los datos ingresados serán anónimos y se guardará la reserva respectiva; así mismo, no serán utilizados para un fin diferente del académico.
Población de la muestra	Colaboradores del Icfes en la ciudad de Bogotá
Unidad de análisis	Universo de personas que participaron en la última encuesta de seguridad de la información (60 colaboradores aproximadamente)
Tipo de muestra	No probabilística
Técnica de recolección de datos	Encuesta virtual realizada mediante la plataforma de formularios de Google, anonimizando los datos del encuestado.
Selección de la muestra	El liderazgo de seguridad de la información seleccionó las personas de la muestra con base en los siguientes aspectos definidos: 1. Personas que se han identificado en incumplimiento de políticas 2. Personas identificadas que requieren un cambio de comportamiento frente a la ciberseguridad y seguridad de la información. 3. Personas que se han identificado que, aunque cumplen las políticas, pueden ser apáticas al tema de ciberseguridad y seguridad de la información.
Tamaño de la muestra	Se realizó una encuesta por cada persona de la muestra, para un total de diez (10) encuestas de manera virtual, representando un 15 % aproximadamente de la unidad de análisis. Se realizó a cada persona una encuesta antes de la aplicación del prototipo y otra (con las mismas preguntas) después de la aplicación del prototipo.
Nivel de confianza	95 % (Valor estándar utilizado)
Fecha de realización en campo	Del 4 al 8 de abril de 2020
Persona que realiza la encuesta	Ingeniero John Carlos Angarita Quiroga
Fecha de entrega del informe	12 de abril de 2020

4.6. Costos por tener en cuenta en la implementación del marco de referencia

Para la aplicación de un marco de ciberseguridad en cualquier entidad, se deben tener en cuenta ciertos aspectos que llevan a la organización a realizar una inversión.

Lo primero que se debe hacer, aspecto inicial que se plantea en el presente marco de referencia, es la identificación del estado actual mediante la ejecución de un análisis de brechas. El instituto puede llevarlo a cabo de dos formas:

1. Directamente, con sus especialistas contratados mediante servicios profesionales y con los cuales también se aplican las campañas de concienctización. Este aspecto tiene la ventaja de que no requiere inversión adicional, pero puede tener la desventaja de que, por la falta de experiencia del personal en este tipo de análisis, no se obtengan resultados acertados o el nivel real de la organización, dado que se puede sesgar la calificación.
2. Con personal especializado en la realización de éste tipo de análisis, para lo cual se pueden obtener propuestas desde setenta millones de pesos ($70.000.000), dependiendo la firma consultora y el nivel de profundidad que se solicite.

Se recomienda contratar personal externo especializado en la realización de análisis de brechas, para obtener un resultado más acertado y con una visión externa a la entidad. Producto de dicho análisis, se obtendrán los aspectos por mejorar y se podrá dimensionar el costo asociado a la implementación de los controles requeridos que permita obtener el nivel deseado, u objetivo, que se haya trazado el instituto.

Como segundo aspecto, en cuanto a costos, se deja a consideración la contratación de un especialista en concientización del recurso humano y en la generación de cambios de comportamiento mediante la aplicación de técnicas reconocidas internacionalmente y con resultados demostrados, lo cual formaría parte de la campaña de concientización que se sugiere en el marco de referencia de la presente monografía y que permitirá mejorar el nivel de riesgo cibernético en el instituto.

En promedio, la tarifa de un especialista en este tema es de alrededor de cuatrocientos mil pesos ($400.000) por hora, incluyendo un diagnóstico inicial y sesiones grupales de hasta 20 personas al mismo tiempo. Con base en el diagnóstico, y el alcance que se le quiera dar a estas sesiones, se obtendrá el costo definitivo requerido por el especialista.

Se sugiere, al igual que con el primer aspecto mencionado, contratar personal externo a la entidad que ayude a obtener el resultado deseado y en el tiempo especificado.

Como tercer costo asociado, se encuentra la gestión de vulnerabilidades mediante la ejecución de pruebas de seguridad a la plataforma tecnológica (análisis de vulnerabilidades y *ethical kacking*), en especial aquella que hay en el ciberespacio y la que respalda los activos de información cibernéticos identificados en el análisis basado en riesgos. Para este tipo de ejercicios, se pueden obtener ofertas económicas desde doscientos millones de pesos ($200.000.000), dependiendo de la cantidad de activos por validar y el alcance que se le quiere dar a los análisis. En dicha propuesta se pueden incluir ejercicios de ingeniería social, los cuales ayudan a crear conciencia y serían parte de la campaña de concientización de la entidad.

Los demás aspectos planteados en el marco de referencia se pueden ejecutar con el personal contratista que tiene el Icfes actualmente, no solo en el área de seguridad de la información, sino también con el personal de las demás áreas que formarían parte de la mejora continua del sistema, como son las de Talento Humano, Control Interno, Planeación, etc.

4.7. Gestión del riesgo cibernético esperado

El riesgo cibernético y la gestión de la ciberseguridad son aspectos estrechamente relacionados, en principio, con las tecnologías de la información. Sin embargo, como se observó durante el desarrollo de la presente monografía, es fundamental integrar a la gestión de la ciberseguridad, el dominio de capacitación y concientización apoyados en campañas que les permitan a los colaboradores mejorar el nivel de gestión del riesgo, su conocimiento al respecto y su atención ante la materialización de un incidente que ponga en riesgo la seguridad de la información y los activos cibernéticos.

> Se ha cuestionado el retorno de la inversión (ROI) de la formación en seguridad, afirmando que los controles de seguridad automatizados son más fiables que la formación de las personas. Sin embargo, muchas organizaciones continúan con una parte de entrenamiento o de concientización de sus programas de ciberseguridad, y con razón. Siempre habrá fallas en lo mejor de los controles automatizados y, en última instancia, dependerá de los observadores humanos detectar pequeñas discrepancias o evitar acciones sospechosas. (Kassicieh et al., 2015)

Si los comportamientos de seguridad cibernética van a aumentar, el cumplimiento no debe ser el énfasis. "En lugar de entrenar para el cumplimiento, es importante entrenar desde una perspectiva holística e involucrar activamente a la fuerza de trabajo" (Anderson, 2013).

4.8. Técnica para la aplicación del marco de referencia – módulo de concientización

Con el objeto de tener un fundamento sólido para la aplicación del plan de concientización planteado en la presente monografía y generar un guía que permita correlacionar de una manera práctica la información obtenida, se establece el siguiente modelo.

1. Teniendo en cuenta que "las variables constituyen un elemento básico puesto que éstas se construyen sobre la base de relaciones entre variables referentes a determinadas unidades de observación. Por medio de las variables, caracterizamos los fenómenos que estudiamos" (Cauas, 2005). Se definen las variables independientes y dependientes con base en la hipótesis planteada:

Variable Dependiente:

Necesidad de cambio de comportamiento en ciberseguridad por parte de los colaboradores del Icfes.

Variables Independientes:

- Alerta por tiempo de navegación en horario laboral - al día
- Alerta de navegación restringida con el mismo usuario
- Alerta por conectividad en horario diferente al laboral
- Alerta por conectividad desde IP no autorizadas con usuario de la Entidad

- Alerta por presentar varias sesiones conectadas con el mismo usuario al mismo tiempo y en diferentes dispositivos
- Comportamiento no adecuado identificado por el líder del área
- Comportamiento no adecuado identificado por los líderes de ciberseguridad en encuestas realizadas.

2. Con base en las variables previamente definidas, se establecen los siguientes umbrales de comportamiento:

a) ALTO

b) MEDIO

c) BAJO

3. Para obtener el nivel de comportamiento respectivo con base en los datos obtenidos, se define la siguiente tabla:

Tabla 7

Umbral - Nivel de comportamiento

Variable Independientes	UMBRAL		
	ALTO	MEDIO	BAJO
Alerta por tiempo de navegación en horario laboral - al día	Mayor al 40%	Entre el 20 y 39%	Menor al 20 %
Alerta de navegación restringida con el mismo usuario	Mas de 5 veces	Entre 2 y 3 veces	1 vez
Alerta por conectividad en horario diferente al laboral	Mas de 3 veces a la semana	Dos veces a la semana	1 vez
Alerta por conectividad desde IP no autorizadas con usuario de la Entidad	Mas de 3 veces a la semana	Dos veces a la semana	1 vez
Alerta por presentar varias sesiones conectadas con el mismo usuario al mismo tiempo y en diferentes dispositivos	Mas de 3 veces a la semana	Dos veces a la semana	1 vez
Comportamiento no adecuado identificado por el líder del área	Mas de tres veces en el mismo mes	Dos veces en el mes	1 vez
Comportamiento no adecuado identificado por los líderes de ciberseguridad en encuestas realizadas	Mas de tres veces en el mismo mes	Dos veces en el mes	1 vez

4. Una vez obtenidos los resultados del cruce entre las variables independientes y el umbral respectivo, se define el siguiente marco de actuación al respecto:

a) Umbral Alto: Se debe incluir dentro del plan de concientización, aplicando teorías de cambio de comportamiento. Así mismo, se debe reportar incidente de ciberseguridad.

b) Umbral Medio: Se debe incluir dentro del plan de concientización, reforzando medidas de seguridad definidas en el Sistema. Así mismo, se debe reportar incidente de ciberseguridad.

c) Umbral Bajo: Se debe incluir dentro del plan de concientización, reforzando medidas de seguridad definidas en el Sistema. Incluir en el monitoreo el evento identificado.

CAPÍTULO 7

CONCLUSIONES

1. Conclusiones generales

El objetivo principal de esta monografía fue plantear una propuesta metodológica para la implementación de un marco de referencia de ciberseguridad, basado en el cambio de comportamiento de los usuarios mediante la adopción de un programa de concientización. El componente principal del marco de referencia, que es la campaña de concientización, fue validado satisfactoriamente mediante la implementación de un prototipo realizado en el Icfes.

En los últimos tiempos, cuando la ciberseguridad ha tomado tanta fuerza no solo a escala personal sino empresarial, se pensaría que con el cambio tan significativo que ha sufrido la informática, la frase de que "el eslabón más débil es el recurso humano" debería no aplicar; pero aún se escucha más de lo mismo (M. Alnatheer et al., 2012).

Lo anterior se sigue presentando, debido a que al talento humano no se le ha brindado un adecuado proceso de concientización y se le siguen dando las mismas pautas de hace unas décadas. Esas actividades requieren ser ajustadas y acompañadas con un proceso de fortalecimiento y cambio de comportamiento que permita asumir, de forma diferente, el riesgo cibernético al cual se enfrentan las organizaciones hoy en día.

La transformación de los comportamientos de los individuos respecto de la protección de la información se realiza desde una comprensión de la competencia de gestión segura de la información y sus niveles de dominio, lo que precisa el desarrollo de una intervención educativa en el contexto organizacional que, superando la postura

mecanicista vigente, es capaz de conectar y retar los saberes previos de los individuos, para desconectar la práctica actual y construir nuevas formas de proteger la información con base en la inestabilidad del entorno y los retos y exigencias estratégicas de la organización (Cano, 2017).

A pesar de los esfuerzos que las organizaciones han llevado a cabo por implementar medidas de seguridad y planes de concientización de los empleados, ya sea porque aún no cuentan con un programa formalmente definido, se sigue observando en las encuestas que uno de los aspectos más relevantes es la preocupación por la concientización (53 % de los encuestados), o porque en los incidentes presentados han identificado la necesidad de aumentar la conciencia en sus colaboradores (12 %) de los encuestados (PWC, 2018).

Las personas conocen la importancia de la aplicación de las prácticas, pero no son conscientes de los impactos de no hacerlo cuando corresponde. En este sentido, los entrenamientos previos realizados, según la lectura mecanicista de la educación, no han permitido una evolución sostenida de los comportamientos esperados por las personas frente al reto de proteger la información y entender dicha responsabilidad como algo inherente a sus actuaciones (Cano, 2017).

Por esto, se identifica la necesidad de proponer para su implementación el marco de referencia de ciberseguridad, en el cual se incluye un componente fundamental de concientización y sensibilización, pero de manera diferente a como se lleva a cabo hoy en

día. Un componente que permite la creación de una cultura de ciberseguridad dentro de las entidades que involucre este aspecto como parte natural y fundamental en la forma de llevar a cabo las labores diarias de los colaboradores (Von, 2000). Un componente primordial con el cual los colaboradores de los diferentes niveles organizacionales pueden identificar sus valores y creencias reflejados en la cultura de ciberseguridad adoptada por la propia entidad, que incluya su capacidad de mejorar la reacción frente a las amenazas cibernéticas, para obtener un compromiso mutuo con la adopción de estos nuevos valores en su esencia personal y profesional.

2. Conclusiones con respecto a los objetivos específicos

La presente monografía da respuesta a la pregunta de investigación ¿Cómo establecer y disminuir el nivel de ciberriesgo al cual se enfrenta la plataforma tecnológica que respalda los servicios esenciales del Icfes?, mediante el desarrollo de cada uno de los objetivos específicos planteados.

El primer objetivo era "Establecer el estado del arte de la conciencia en ciberseguridad en el contexto internacional y colombiano", con el cual se ratificó la necesidad de reforzar las campañas de concientización e incluir el componente de cambio de comportamiento, que es fundamental para las organizaciones que pretenden mejorar el nivel del riesgo residual cibernético. En cuanto a esto, (Bada; Sasse, 2014) afirman que "Se debe lograr que las personas entiendan y reconozcan la relevancia de la información, que las mismas comprendan la forma de asegurarla y estén dispuestas a llevar a cabo lo determinado en las políticas de seguridad".

El segundo objetivo era "Identificar el marco normativo en Colombia, en materia de ciberseguridad", en el cual se puede evidenciar el esfuerzo realizado por el Gobierno nacional; sin embargo, también se evidencia la falta de definiciones concretas y lineamientos claros para la implementación de campañas de concientización en las entidades públicas; y aún más, que dichas campañas incluyan aspectos relacionados a cambios de comportamiento en el recurso humano, que conlleven mejorar el nivel de ciberriesgo en la organizaciones.

Por otra parte, el tercer objetivo plantea: "Determinar el nivel de conocimiento y conciencia, en materia de ciberseguridad en el Icfes, que poseen los colaboradores del instituto". Se identificó un buen nivel de concientización de los colaboradores en el Icfes, aunque se evidenció la falta de capacitación y concientización actualizada que brinde un empoderamiento y actuación adecuada frente a las amenazas cibernéticas a las cuales se pueden enfrentar día a día los usuarios del sistema de seguridad de la información en el instituto. Así mismo, se notó la falta de adopción de un marco de ciberseguridad en la entidad, frente a las buenas prácticas internacionales, como dominio principal del SGSI.

Por último, con el fin de atender el cuarto objetivo de la monografía, "Proponer un instrumento para la implementación del marco de referencia de ciberseguridad en el Icfes, enfocado al componente de concientización en la materia", se planteó el marco de referencia de ciberseguridad basado en el cambio de comportamiento de los usuarios mediante la adopción de un programa de concientización, para el cual se ejecutó un prototipo del componente de concientización, incluyendo estrategias de cambio de comportamiento.

El componente de concientización propuesto en la presente monografía es el factor principal del marco de referencia de ciberseguridad, basado en el principio del triángulo de

la ciberseguridad usuario-centrista (procesos-procedimientos, plataforma tecnológica y campaña de concientización), que tiene como base fundamental el cambio de comportamiento en los usuarios del instituto, con el propósito de reducir el impacto de los riesgos de ciberseguridad y seguridad de la información que se han identificado en el Icfes.

La necesidad de implementar dicho componente se basa en los resultados obtenidos en la primera sesión del prototipo, expuesto en el numeral 3.4.6 de la presente monografía, en donde se evidencia que los encuestados manifiestan:

- El 30 %, no tener un programa de ciberseguridad o identificar el componente de ciberseguridad en el SGSI.
- El 40 %, falta de claridad para la gestión de contraseñas seguras.
- El 30 %, deficiencias en la identificación de la función de nuevos ataques cibernéticos, como es el caso de *ransomware*.
- El 20 % podría permitir la fuga de información debido a la incapacidad de detectar comportamientos inadecuados por parte de personal inescrupuloso.
- El 10 % tendría inconvenientes para asumir posturas profesionales frente al actuar de los líderes de seguridad de la información.

Por estas razones, se aplicó la estrategia para el cambio de comportamiento descrita en el mismo capítulo 5, apoyada en la teoría de la autodeterminación.

Con base en la identificación de las necesidades de la entidad y de las personas participantes, se aplicó la estrategia mencionada para generar un cambio de comportamiento. Se logró un cambio sustancial en la forma de analizar y actuar frente a incidentes que se

pueden presentar y que incrementan el riesgo digital, o ciberriesgo, en el evento de materializarse. Esto se encuentra sustentado en el análisis presentado en el numeral 3.4.8 de la segunda sesión del prototipo, en donde:

- Se evidencia un cambio en la forma de asimilar los escenarios planteados en la encuesta, dado que el 100 % adoptó una medida segura frente a posibles engaños de ingeniería social.
- Se observa un cambio en la forma de actuar frente a situaciones que requiere decidir entre cumplimiento o seguridad.
- Se asume una postura profesional diferente frente al actuar de los líderes de seguridad de la información que pretenden mantener dichos niveles en condiciones adecuadas.

A pesar de que el tiempo invertido en la aplicación del prototipo fue muy corto y se tuvo la limitante del aislamiento obligatorio declarado por el Gobierno nacional de Colombia frente a la emergencia sanitaria y económica que se vive actualmente por el Covid-19, se evidencian resultados interesantes en el cambio del comportamiento de los colaboradores participantes. Por esta razón, se vio la necesidad de avanzar en el prototipo apoyándose en las plataformas digitales.

3. Recomendaciones

Por lo anterior, y tomando como base el resultado de la aplicación del prototipo, se identifica que es fundamental en el Icfes acoger una política de concientización fundamentada en las estrategias de cambio de comportamiento, que lleve a los colaboradores,

desde el nivel directivo, a la adopción e interiorización en el día a día de las definiciones dadas dentro del programa de seguridad de la información.

Se debe crear un plan de concientización diferente de lo que se lleva a cabo hoy en día en la entidad, fortaleciendo el plan estratégico de seguridad de la información, de modo que permita incluir la ciberseguridad como actor fundamental y de mayor importancia. Es primordial que los colaboradores del Icfes, partiendo del nivel directivo, entiendan y adopten por sí mismos las medidas que desde el plan de concientización se difunden, basadas en el cambio conductual que se plantea en el presente marco de referencia. Muchas de las violaciones de ciberseguridad y seguridad de la información se pueden evitar si los mismos colaboradores actúan de manera diferente.

4. Trabajos futuros

Dado que el cambio conductual es un proceso que necesita tiempo, para averiguar si una determinada intervención ejerce un efecto duradero en la conducta, la evaluación debe realizarse a largo plazo. Ello implica destinar fondos suficientes a este aspecto. Cuando sea posible, es conveniente emplear ensayos controlados de otros métodos altamente cualificados. Aunque no siempre son factibles, los ensayos controlados aleatorizados se consideran el instrumento más adecuado para realizar dichas evaluaciones (Eufic, 2014).

Se debe propender a la implementación del marco de referencia propuesto en la presente monografía a escala organizacional y establecer la respectiva campaña de concientización en ciberseguridad para todos los colaboradores del Icfes, con el apoyo del área de Talento Humano, teniendo en cuenta que los resultados obtenidos en el prototipo

implementado arrojaron cambios de comportamiento interesantes en tan solo unos pocos días que duró. Para esto, se espera obtener un mejor resultado que contribuya a disminuir el riesgo digital y mejorar el actual plan estratégico de ciberseguridad y seguridad de la información de la entidad.

De igual forma, para trabajos futuros, analizar la implementación del marco de referencia propuesto en la presente monografía, tomando como base las otras estrategias de cambio de comportamiento existentes, con el objeto de validar e identificar la mejor alternativa que permita obtener el resultado deseado por la entidad frente a los objetivos del plan estratégico de ciberseguridad.

Así mismo, implementar programas de capacitación y concientización es primordial. Si el factor humano no está concientizado, y no ha sido capacitado para operar el sistema de gestión de seguridad de la información adecuadamente, la implementación del marco de referencia planteado en la presente monografía será un fracaso y el día a día se ejecutará paralelamente a una ciberseguridad que no estará presente (Rubio Blanco, 2015).

BIBLIOGRAFÍA

ACIS. (Junio de 2012). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Revista Sistemas de Edición ACIS*, 4-5. 0120-5919

Ajzen, I. (1988). *Attitudes, personality, and behaviour*. Dorsey Press.

Alnatheer, M. A. (2012). Understanding and measuring information security culture in developing countries : case of Saudi Arabia. *Computer Systems and Information Technology*, *9*(14), 897-912.

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. *Pacific Asia Conference on Information Systems (PACIS)*, 144.

Alotaibi, M., Furnell, S., & Clarke, N. (2015). Towards dynamic adaption of user's organisational information security behaviour. *Australian Information Security Management Conference*, (28-36). https://doi.org/10.4225/75/57b698e1d9389

Anderson, K. (2013). Can we make security awareness training stickier? (I. Journal, Ed.), (10-15).

Arancibia, V., Herrera, P., & Strasser, K. (2008). En: Capítulo 2. Teorías conductuales del aprendizaje. *Manual de psicología educacional.* Ediciones Universidad Católica de Chile. 978-956-14-0466-3

Bacca U., G. (2016). *Introducción a la seguridad informática.* Grupo Editorial Patria. 978-607-744-471-8.

Bada, M., & Sasse, A. (Julio de 2014). Cyber security awareness campaigns why they fail to change behavior. *Sans Institute*.

Bada, M., Sasse, A., & Nurse, J. (2014). Cyber security awareness campaigns: why they fail to change behavior. *International Conference on Cyber Security for Sustainable Society*, (July), 38. http://www.cs.ox.ac.uk/publications/publication9343-abstract.html%0Ahttp://discovery.ucl.ac.uk/1468954/1/Awareness CampaignsDraftWorkingPaper.pdf.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review. En A. Bandura, *Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review,* (191-215). https://doi.org/10.1037/0033-295X.84.2.191

Baskerville, R. a. (2002). An information security meta-policy for emergent organizations, (15). *Logistics Information Management*. 10.1108/09576050210447019

Bernoulli, D. (1954). Exposition of a New Theory on the Measurement of Risk. *Econométrica*, 22, (23-36). 10.2307/1909829.

BID-OEA. (2020). CIBERSEGURIDAD - RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE. *Reporte Ciberseguridad 2020*.

BID-OEA. (2016). *Observatory of Cybersecurity in America Latina and the Caribbean*. http://www.observatoriociberseguridad.com/: http://www.observatoriociberseguridad.com/graph/countries//selected//0/dimensions/1-2-3-4-5.

British Standards Institution. (2012). BSI Standards Publication Information technology - Security techniques- Guidelines for cybersecurity. *BS ISO/IEC 27032*.

CAI_Virtual. (2020). https://caivirtual.policia.gov.co/.

Cano, J. (13 de diciembre de 2015). *Ciberseguridad empresarial*. http://insecurityit.blogspot.com/2015/09/ciberseguridad-empresarial-primeras.html.

Cano, J. J. (2017). Modelo sistémico para el diagnóstico y desarrollo de una cultura organizacional de seguridad de la información: Una visión desde las competencias genéricas. *Tesis para optar al título de doctor en Educación*, Universidad Santo Tomás, (15).

Cano, J. J. (10 de enero de 2011). *Ciberseguridad y ciberdefensa*. http://insecurityit.blogspot.com/2011/01/ciber-seguridad-y-ciber-defensa-dos.html.

Carl R., D. L. (2006). *Security Education, Awareness and Training: SEAT from Theory to Practice*. Oxford: Elseiver Inc. 978-0-756-7803-8.

Carrasco, L. D. S. (2015). Ciber-Resiliencia. *IEEE.ES Artigo de opinion*, *35*, (1-15). http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf.

Christiernin, L. G. (2010). Guiding the designer: A radar diagram process for applications with multiple layers. *Interacting with Computers*, *22*(2), (107-122). https://doi.org/10.1016/j.intcom.2009.10.003.

Cialdini, R. B. (2009). *Influence : science and practice*. (5.ª ed.). Pymble, NSW.

Cisco. (Febrero de 2018). *Reporte anual de ciberseguridad*. www.cisco.com/go/offices.

Colcert. (2020). http://www.colcert.gov.co/.

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices improve the public's use of cyber. *Project Report. Government Office for Science. Northumbria University*, (1-20).

CSIRT. (2020). https://cc-csirt.policia.gov.co/.

Cauas, D. (2005). Definición de las variables , enfoque y tipo de investigación. *Universidad Nacional Abierta y a Distancia (UNAD)*, 1–11.

http://www.mecanicahn.com/personal/marcosmartinez/seminario1/los_pdf/l-Variables.pdf

DAFP, D. A. de la F. P. (2018). *Guía para la administración del riesgo y el diseño de controles en entidades públicas.*

Deci, E. L., & Ryan, R. M. (2000). La teoría de la autodeterminación y la facilitación de la motivación intrínseca , el desarrollo social y el bienestar. Teoría de la autodeterminación. *American Psychologist*, *55*, (68-78). https://doi.org/10.1037110003-066X.55.1.68.

Denning T, L. A. (2013). Control-alt-hack: the design and evaluation of a card game for computer security awareness and education. *Association for Computing Machinery*, (915-928). 10.1145/2508859.2516753.

Departamento Nacional de Planeación. (2016). Política nacional de seguridad digital. *Conpes 3854*, 91. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ□micos/3854.pdf.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, *7*(4), (171-175). https://doi.org/10.1108/09685229910292664.

Dinero. (6 de enero de 2019). *Ciberseguridad en el 2019 en Colombia.* https://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858.

El Tiempo. (20 de septiembre de 2012). Gobierno de Colombia y OEA realizan simulacro de ataques cibernéticos. https://www.eltiempo.com/archivo/documento/CMS-12240262.

Enisa. (2006). A Users' Guide : How to Raise Information Security Awareness. *European Network and Information Security Agency*, 1, 64.

Escobar, D., Moreno, M., & Cuevas, L. (2016). La calidad de la auditoría en sistemas de gestión. *Ciencias Holguín*, *76*(89), (1027-2127).

Eufic. (Julio de 2014). *Cómo motivar el cambio conductual.* http://www.eufic.org/article/es/expid/Como-motivar-el-cambio-conductual/.

Evans, M., Maglaras, L. A., He, Y., Janicke, H. (Mayo de 2015). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *(*422-437). https://doi.org/10.1002/sec.

Fernández, A. E. (1995). *Manual de motivación y emoción.* Editorial Centro de Estudios Ramón Areces.

Fernández-Abascal, E., García, B., Jiménez, M. D., Martin, M. D., & Francisco, D. (2013). *Psicología de la emoción*, (17-18). Centro de Estudios Ramón Areces S.A. 978-84-8004-908-5.

Fogg, B. (2009). A behavior model for persuasive design. *ACM International Conference Proceeding Series, 350*. https://doi.org/10.1145/1541948.1541999.

Fogg, B. J. (2005). *Tecnologia della persuasione.* Apogeo Education. 9788838787492.

García D., D. M. (2005). *Factores explicativos de la intención de los adolescentes de tener relaciones sexuales: un análisis a partir de la teoría del comportamiento planeado*. Tesis de maestría, *Universidad de los Andes, 12 Suppl 1*(9), (130). https://doi.org/10.1007/978-1-4614-7990-1.

Gobierno_de_Colombia. (2018). *Guía para la orientación de la GRSD en el Gobierno nacional, entes territoriales y sector público.*

Gómez-Merelo, M. S. (2 de agosto de 2020). *La ciberseguridad en 2019.* https://tendencias21.levante-emv.com/seguridad-la-ciberseguridad-en-2019-una-inversion-irreversible_a42.html.

Gros S., B., & Contreras R., D. (2006). La alfabetización digital y el desarrollo de competencias ciudadanas. *Revista Iberoamericana de Educación, 42*(42), (103-126). https://doi.org/10.35362/rie420764.

Hernández S., R., Fernández, C., & Baptista, P. (2014). *Historia de los enfoques cuantitativo, cualitativo y mixto: raíces y momentos decisivos*. (1929), (1-6). https://doi.org/10.1002/pbc.26473.

Hogan, K. (2004). *The science of influence: how to get anyone to say "yes" in 8 minutes or less!* John Wiley & Sons. 9780471670513.

Icfes. (2019). *Plan de tratamiento de riesgos de seguridad y privacidad de la información 2020.* Icfes.

Icontec. (2006). *Norma técnica NTC-ISO/IEC Colombiana 27001.* http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma. NTC-ISO-IEC 27001.pdf.

IIA. (2013). Declaración de posición: Las tres líneas de defensa para una efectiva gestión de riesgos y control. *The Institute of Internal Auditors*, 12.

ISO_27005. (2018). https://www.iso.org/obp/ui#iso:std:iso-iec:27005:ed-3:v1:en.

ISO_31000. (2018). https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

ITU, G. C. (17 de mayo de 2007). https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

Joyanes A. L. et al. (2011). Ciberseguridad. Retos y amenazas a la seguriad nacional en el ciberespacio. *Cuaderno de Estrategia, 149.*

Kassicieh, S., Lipinski, V., & Seazzu, A. F. (Septiembre de 2015). *Human centric cyber security: What are the new trends in data protection?* Portland International

Conference on Management of Engineering and Technology, (1321-1338). https://doi.org/10.1109/PICMET.2015.7273084.

Kerry P., J. G. (2012). *Change anything: the new science of personal success.* Grand Central Publishing. 978-0446573900.

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers and Security, 70,* (663-674). https://doi.org/10.1016/j.cose.2017.08.001.

Kim, L. (2018). Concienciación en materia de ciberseguridad: protección de datos y de pacientes. *Nursing, 35*(1), (62-64). https://doi.org/10.1016/j.nursi.2018.02.017.

Kindervag, J. (2010). Build security into your network's architecture DNA: The Zero Trust Netw. *Forrester*, 27.

Kirlappos, I., & Sasse, M. A. (2014). Surrogate models assisted by neural networks to assess the resilience of networks danilo. *The Manager's Handbook for Business Security*, (121-128). https://doi.org/10.1016/b978-0-12-800062-5.00010-5.

Landau, S., & Stytz, M. (13 de junio de 2005). *https://ieeexplore.ieee.org.* (I. S. Privacy, ed.) 10.1109/MSP.2005.76.

López B., I., Romo A., M., & López R., D. (2006). ¿Eres visual, auditivo o cinestésico?: Estilos de aprendizaje desde el modelo de la programación neurolingüística (PNL). *Revista Iberoamericana de Educación, 38*(2), (6). https://doi.org/10.35362/rie3822664.

López-Rúa, M. D. (2015). *Persuasión a través del marketing.* Universidad del Zulia. 1012-1587.

Martín, E. (2014). La Generación Y latinoamericana en las organizaciones. *Revista Gestión de las Personas y Tecnología, 19,* 16. https://doi.org/0718-5693.

Martínez, N. (2019). *Ciberseguridad y riesgo operacional en las organizaciones.* Tesis de maestría en Gestión de Riesgos Financieros, ICADE Business School, 54.

Méndez Á., C. E. (2012). *Metodología: Diseño y desarrollo del proceso de investigación con énfasis en ciencias empresariales* (4.ª ed.). 978-968-18-7177-2.

Ministerio de Tecnologías de la Información y las Comunicaciones et al. (2011). Lineamientos de política para ciberseguridad y ciberdefensa. *Conpes 3701*, 43. https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

Ministerio de Tecnologías de la Información y las Comunicaciones. (3 de diciembre de 2018). *Política de gobierno digital.* http://estrategia.gobiernoenlinea.gov.co/623/w3-article-81505.html.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). *Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Modelo de gestión de riesgos de seguridad digital (MGRSD)*, 4, (1-38). Viceministerio de

Economía Digital. Dirección de Gobierno Digital.

Ministerio de Tecnologías de la Información y las Comunicaciones. (19 de mayo de 2019). ¿Sabes en qué consiste el Programa En TIC confío del Ministerio de las TIC? https://www.enticconfio.gov.co/Sabes_en_que_consiste_el_Programa_En_TIC_Confio_del_Ministerio_TIC.

Miranzo, M., & Río, C. D. (Mayo de 2014). La protección de infraestructuras críticas. *Unisci Discussion Papers, 35*, (339-352). ISSN 1696-2206.

MIT. (2015). The future of the us electric grid. In *Perspectives on Complex Global Challenges: Education, Energy, Healthcare, and Security Resilience*. https://doi.org/10.1002/9781118984123.ch8

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science (IJARCS), 8*(5), (1938-1940). https://doi.org/http://dx.doi.org/10.26483/ijarcs.v8i5.4021.

Montaño, D. E. (1992). Health Behavior and Health Education: Theory, Research, and Practice. *Annals of Internal Medicine*, *116*(4), 350. https://doi.org/10.7326/0003-4819-116-4-350_1.

NACD & ISA. (2016). Manual de Supervisión de Riesgos Cibernéticos para Juntas Directivas. *¿Por qué un manual de supervisión de riesgos cibernéticos para juntas corporativas?*. https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf

Naranjo, P. (2015). Introducción al neuromarketing. *Academo, Revista de Investigación en Ciencias Sociales y Humanidades*, *2*(2), 7.

NICSS, N. I. (9 de febrero de 2020). *Glosario*. https://niccs.us-cert.gov/glossary

NIST-CSRC. (9 de febrero de 2020). *Glosario*. csrc.nist.gov/glossary/term/.

Oliva, O. M. (2018). *La evaluación del desempeño empresarial basado en indicadores de eficacia y eficiencia.* Universidad de Holguín.

ONU. (2018). *E-Government Survey 2018_Spanish.*

Owasp. (2017). *Top Ten Owasp Org*. https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/.

Peña, J. C., & Segura, L. A. G. (2014). *La importancia del componente educativo en toda estrategia de ciberseguridad*, Centro de estudios estratégicos sobre seguridad y defensa nacional, (5-13).

Pew Research Center. (27 de marzo de 2017). Qué tanto sabes de ciberseguridad. *El Economista*. https://www.eleconomista.com.mx/tecnologia/Que-tanto-sabes-de-ciberseguridad-20170327-0140.html.

Policía Nacional. (2020). *Ciberseguridad.* https://www.policia.gov.co/ciberseguridad.

Presidencia de Colombia. (1 de junio de 2017). *Conciencia cibernética.* http://especiales.presidencia.gov.co/Documents/20170601-ataques-ciberneticos/sin-ciber-ataques.html.

PWC. (2015). *Information Security Breaches Survey.*

PWC. (2018). Strengthening digital society against cyber shocks. *Cybersecurity and Privacy*, (1-22). www.pwc.com/gsiss.

Qudaih, H. A, Bawazir, M. A, Usman, S. H., & Ibrahim, J. (2014). Security awareness in an organization. *Persuasive Technology Contributions Toward Enhance Information Security Awareness in an Organization, 10*(4), (180-186).

Redford, C. (2014). *PNL: Programación neurolingüística: Una guía práctica y sencilla para iniciarse en la programación neurolingüística.* Esenciales Robinbook. 9788499173573.

Robinson, A. (2019). *Information security reading room using influence strategies to improve security awareness.* SANS Institute.

Rodríguez, L. R. (2007). La teoría de acción razonada : Implicaciones para el estudio de las actitudes. *Investigación Educativa Duranguense*, 7, (66-77).

Rubio B., J. A. (2015). *Un marco para el análisis de riesgos en ciberseguridad.* Tesis doctoral, Universidad Rey Juan Carlos, 214. http://www.tdx.cat/handle/10803/456008.

Salgueiro, A. (2001). *Indicadores de gestión y cuadro de mando.* Díaz de Santos S.A. 84-7978-492-X.

Salvador, C. C. (2015). *Arquitecturas distribuidas de gobierno electrónico con ciberseguridad crítica*. Tesis doctoral. Escuela Técnica Superior de Ingenieros Industriales, de Madrid.

Sam B., P. D. (6 de diciembre de 2013). Developing nations. *The Digital Divide and Research Databases*, (270-278).

SANS. (9 de febrero de 2020). *Políticas de seguridad.* https://www.sans.org/security-resources/policies.

Simón, V. M. (1997). *La participación emocional en la toma de decisiones,* (365-376). Psicothema.

Sukaina Al-Nasrawi, S. Z. (2015). *Information society, digital divide, and e-governance in developing countries.* Encyclopedia of Information Science and Technology (3.ª ed.). 10.4018/978-1-4666-5888-2.ch672.

Talbot, E. B., Frincke, D., & Bishop, M. (2010). *Demythifying Cybersecurity* (3.ª ed.), 8ª . IEEE Security & Privacy. 10.1109/MSP.2010.95.

University of Portsmouth. (2018). *Cyber Security Breaches Survey*, (1), (1-58). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf.

Velasco, A. H. (2006). El derecho informático y la gestión de la seguridad de la información. *Revista de Derecho*, 10(1), (59-68). Universidad del Norte. https://doi.org/0121-8697.

Von, S. B. (2000). Information security. The third wave? *Computer & Security*, 1872-6208. I. Elsevier Science Publishing Company.

Wilson, M., & Hash, J. (Octubre de 2003). Building an information technology security awareness and training program. *NIST*, 70. https://doi.org/10.6028.

Winkler, I. (2012). *The habits of highly successful security*. http://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf.

Winkler, I. (22 de julio de 2017). *CSO Online*. https://www.csoonline.com/article/2133408/network-security-the-7-elements-of-a-successful-security-awareness-program.html.

Winkler, I., & Manke, S. (2 de diciembre de 2013). *CSO Magazine*. https://www.csoonline.com/article/2134189/how-to-create-security-awareness-with-incentives.html.

Zambrano, N., & Zambrano, M. (2019). Ciberseguridad y su aplicación en las instituciones de educación superior públicas de Manabí. *Espam*, 199. http://repositorio.espam.edu.ec/bitstream/42000/1032/1/TTMTI3.pdf.