Desarrollo de competencias en gestión de riesgos sobre seguridad digital en la Contraloría General de la República

Guillermo Aristizábal Restrepo

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 FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

"General Rafael Reyes Prieto"
Unión, Proyección, Liderazgo

DESARROLLO DE COMPETENCIAS EN GESTIÓN DE RIESGOS SOBRE SEGURIDAD DIGITAL EN LA CONTRALORÍA GENERAL DE LA REPÚBLICA

ALUMNO: GUILLERMO ARISTIZÁBAL RESTREPO

DIRECTOR: DANIEL FRANCISCO SANTAMARÍA RODRÍGUEZ

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTÁ – COLOMBIA

2020

Página de aceptación del trabajo

A mi padre José Yomar, quien dejó

marcas profundas e indelebles

en mi existencia, a quien extraño

mucho cada día desde su partida.

"soñaba con fundar un día una escuela en la que los jóvenes pudiesen aprender sin hastío y en la que fuesen estimulados a plantear problemas y a discutirlos; una escuela en la que no hubiese que escuchar respuestas no deseadas a cuestiones no planteadas; en la que no hubiera que estudiar solo por aprobar los exámenes" (Popper, 2002)

Agradecimientos

Quiero agradecer en primer lugar a mi esposa Mónica Alexandra y mi a hija Sara, quienes soportaron mis ausencias presentes con paciencia casi estoica, también a mi madre Sara Inés y mi hermana Paula, su apoyo maternal y fraterno se materializaron en invaluables acciones de tipo logístico y operativo.

Gracias a mis profesores Massimo, Steve, Martha, Samuel, Manuel y Jesús Eduardo por demostrarme que la educación es un proceso que no finaliza; y a mis compañeros de clase Edgar Yesid, Marco, Rosangela y Javier quienes siempre me apoyaron durante este proceso.

Finalmente agradezco infinitamente a Daniel Francisco, el tutor de este trabajo de grado, sin su ayuda y guía no lo hubiera logrado.

Resumen

La presente monografía tiene como objetivo desarrollar un modelo para generar competencias laborales en el área de gestión de riesgos digitales, que se ajuste a las necesidades de la Contraloría General de la República. Para esto tiene en cuenta que la disrupción digital que se vive en la actualidad ofrece nuevos retos y oportunidades, pero también plantea amenazas significativas para la actual sociedad del conocimiento y todos sus actores. Los riesgos están relacionados con las aplicaciones y con nuevos procesos, los cuales discrepan con otras necesidades de negocios, cumplimientos regulatorios o requerimientos de seguridad; pero una de las bases fundamentales para contrarrestar esta problemática es contar con personal competente a nivel laboral y con un buen nivel de conciencia situacional, que pueda tomar las decisiones adecuadas e implementar las acciones pertinentes para mejorar los niveles de la ciberseguridad en las organizaciones a través de procesos adecuados de formación y educación. Este trabajo de grado se vale de las últimas teorías del conocimiento como el conectivismo, apoyándose con instrumentos tecnológicos innovadores como son los cursos en línea, masivos y abiertos (MOOC).

Palabras clave: Competencias laborales, educación abierta y a distancia, conectivismo, gestión de riesgos, ciberseguridad, MOOC.

Abstract

The objective of this monograph is to develop a model to generate competencies in the area of the digital risk management, which meets the needs of the Office of the General Comptroller of the Republic. For this, it takes into account that the digital disruption that exists today offers new challenges and opportunities, but also poses significant threats to the current knowledge society and all its actors. The risks are related to the applications and new processes, which disagree with other business needs, regulatory compliance or security requirements; but one of the fundamental bases to counteract this problem is to have competent personnel at work level and with a good standard of situational awareness, who can make the appropriate decisions and implement the pertinent actions to improve the levels of cybersecurity in organizations through of an appropriate training and education processes. This degree work uses the latest theories of knowledge such as connectivism, supported by innovative technological tools such as massive online open courses.

Keywords: Labor competencies, open education, connectivism, risk management, cybersecurity, MOOC.

Tabla de Contenido

Introducción **14**

1 Marco conceptual **21**

1.1 Competencias laborales 21

1.2 Gestión de riesgos 24

1.3 Educación abierta y a distancia 26

1.4 Modelos pedagógicos 29

1.5 Cursos masivos en línea y abiertos - MOOC 34

2 Marco metodológico **38**

3 Análisis de necesidades **41**

3.1 Contexto institucional 41

3.2 Caracterización de la población 50

3.3 Necesidades normativas 56

3.4 Necesidades comparativas 77

3.5 Necesidades sentidas 82

3.6 Competencias para la CGR 93

3.7 Resultados 99

4 Diseño de la mediación pedagógica 102

4.1 Diseño general 103

4.2 Diseño detallado 109

4.3 Recursos TIC 135

5 Conclusiones 139

6 Bibliografía 144

Anexo A 161

Lista de abreviaturas y siglas

ADDIE	Análisis, Diseño, Desarrollo, Implementación y Evaluación
APA	*American Psychological Association* / Asociación Americana de Psicología
BID	Banco Interamericano de Desarrollo
CaaS	*Crime as a Service* / Crimen como servicio
CEF	Centro de Estudios Fiscales
CGR	Contraloría General de la República
CONPES	Consejo Nacional de Política Económica y Social
DAFP	Departamento Administrativo de la Función Pública
DIAC	Dirección de Imprenta Archivo y Correspondencia
DIARI	Dirección de Información, Análisis y Reacción Inmediata
ESDEGUE	Escuela Superior de Guerra
GAF	Gerencia Administrativa y Financiera
GTH	Gerencia de Talento Humano
ICC	*International Chamber of Commerce* / Cámara Internacional de Comercio

I+D+i	Investigación, Desarollo e Innovación
IoE	*Internet of Everything* / Internet de todo
IoT	*Internet of Things* / Internet de las cosas
ITU	*International Telecommunications Union* / Unión Internacional de Telecomunicaciones
LMS	*Learning Management System* / Sistema de gestión de aprendizaje
MEN	Ministerio de Educación Nacional
MinTIC	Ministerio de las Tecnologías de. la Información y las Comunicaciones
MOOC	*Massive Open Online Course* / Curso masivo en línea y abierto
OIT	Organización Internacional del Trabajo
PND	Plan Nacional de Desarrollo
OECD	*Organisation for Economic Co-operation and Development* / Organización para la cooperación y el desarrollo económicos
OSEI	Oficina de Sistemas e Informática
RAE	Real Academia Española
REA	Recursos Educativos Abiertos

SGS	Sistema de Gestión de Seguridad
TIC	Tecnologías de la Información y la Comunicación
UNESCO	*United Nations Educational, Scientific and Cultural Organization* / Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.
USATI	Unidad de Seguridad y Aseguramiento Tecnológico e Informático

Lista de figuras

Figura 1. Ciclo de sobre expectación de e-learning 2019 18

Figura 2. Nivel de Madurez y Capacidad TIC en la CGR 45

Figura 3. Porcentaje de niveles de formación 46

Figura 4. Distribución por sexo y centro de trabajo 50

Figura 5: Distribución por las Gerencias Departamentales 51

Figura 6: Distribución por edad 52

Figura 7: Distribución por grado de nivel jerárquico 53

Figura 8: Distribución por profesión 54

Figura 9: Histogramas por edades de los grupos de análisis 55

Lista de tablas

Tabla 1. Normatividad aplicable a la CGR 57

Tabla 2 Normas relevantes de la familia ISO 27000 78

Tabla 3 Tabulación de la encuesta 83

Tabla 4. Formato de estructuración de un curso virtual 104

Tabla 5 Módulo 1 - Introducción 109

Tabla 6 Módulo 2 - El riesgo digital en nuestra vida diaria 113

Tabla 7 Módulo 3. Gestionando el riesgo digital en nuestro trabajo 117

Tabla 8 Módulo 4. La normatividad sobre el riesgo digital 124

Tabla 9 Módulo 5 Construcción de buenas prácticas 130

Introducción

Actualmente, los distintos actores de la sociedad actual globalizada afrontan la cuarta revolución industrial, la cual ofrece novedosos desafíos e interesantes oportunidades, como también plantea amenazas significativas para la sociedad del conocimiento. Si esta nieva realidad se entiende como la base de una nueva economía, con la consecuente encrucijada para mejorar la calidad de vida, se está creando un caldo de cultivo que propicia escenarios que posibilitan a todas las partes interesadas aprovechar este nuevo entorno y establecer acciones concretas orientadas a mejorar las condiciones de nuestro país.

Sin embargo, aunados a la corrupción y al desgreño administrativo, existen elementos emergentes tales como la fuga de información sensible, la suspensión de la prestación del servicio, la indisponibilidad de la infraestructura crítica, la violación de la privacidad y los datos personales, la afectación de los bienes físicos, las operaciones de sabotaje o espionaje y, peor aún, el daño a la integridad de las personas. Ahora bien, los riesgos de seguridad están relacionados con los componentes de toda organización: personas, procesos y herramientas; la articulación de éstos siempre genera tensiones por necesidades que, en ocasiones, van en contravía unas de otras, tales como: el cumplimiento regulatorio, nuevos requerimientos técnicos, ajustes presupuestales, personal idóneo y capacitado, sostenibilidad de la estrategia a largo plazo, la colaboración efectiva en su ecosistema y la reinvención permanente.

Según el informe de la Organización para la Cooperación y el Desarrollo Económicos (en adelante: OECD) para el manejo de riesgos a nivel digital, las amenazas e incidentes se han incrementado en los últimos años dando lugar a importantes consecuencias económicas y sociales tanto para individuos como para organizaciones públicas y privadas. Un número cada vez mayor de las partes interesadas son conscientes de la necesidad de gestionar mejor los riesgos de seguridad digital para aprovechar los beneficios de la economía digital. (OECD, 2015, pág. 19). También plantea que la gestión de riesgos de seguridad digital requiere primero entender que existe dicho riesgo y adquirir las habilidades adecuadas a través de la educación, la formación, la experiencia o la práctica - para tomar decisiones responsables en este aspecto (OECD, 2015, pág. 42).

Colombia, es uno de los países del cono sur que tiene una de las mejores coberturas a nivel de internet y el porcentaje de ciudadanos que la usan frecuentemente en este milenio han pasado de un 2% en el 2000 (CCIT, 2014) a un 62,3% en 2017, en el 2016 esta cifra fue de 58,1% (DANE, 2019). Este crecimiento demuestra que esta tendencia al tiempo que trae consigo importantes beneficios, lo que implica una mayor dependencia de las tecnologías de información y comunicaciones (en adelante TICs), lo cual trae como consecuencia natural que la probabilidad de que ocurran incidentes de seguridad en el ámbito digital se incremente, así como el nivel de la gravedad de su posible impacto en los sectores de la sociedad de forma directa o indirecta. Las amenazas están presentes en la vida diaria de cada ciudadano y pueden tener implicaciones mucho más graves como lo expresa Jones al analizar una herramienta de mensajería que es usada ampliamente, la cual puede traer consecuencias en la seguridad nacional (Jones Chaljub, 2017).

Usando la acotación de que "toda política pública busca dar solución a una problemática que desestabilice una materia específica dentro de las obligaciones del Estado" (Ardila Castro & Cubides Cárdenas, 2017, pág. 23), el gobierno nacional atendió la necesidad de protección del ciberespacio y la información, al emitir el documento CONPES 3854 en 2016, que evoluciona los lineamientos de la política para la ciberseguridad y la ciberdefensa (DNP, 2011), el cual plantea la política nacional de seguridad digital, estableciendo que el gobierno debe buscar que todas las partes interesadas sean conscientes de su papel con el fin de hacer frente a los riesgos de seguridad digital y concretamente plantea en el desarrollo de su estrategia E.25 "promover en los diferentes niveles de formación comportamientos responsables en el entorno digital" (DNP, 2016, pág. 48).

En consecuencia, la Contraloría General de la República (en adelante, CGR) se involucra de manera decidida y se compromete profundamente para estar acorde a las políticas y planes de ciencia tecnología e innovación, como entidad fiscalizadora superior. La visión del actual Contralor General Carlos Felipe Córdoba Larrarte, quien desde su campaña para aspirar al mayor cargo de control y vigilancia fiscal del país, ha mencionado de forma reiterada la frase "Más tecnología y más ciudadanía", como mecanismo para enfrentar el flagelo de la corrupción, aplica el principio del fraile franciscano Guillermo de Ockham: "En igualdad de condiciones, la explicación más sencilla suele ser la más probable" (Pérez Cárdenas, Rosas Mercado, & Martínez Valdés, 2017). Es una estrategia simple y poderosa que combina dos de los pilares de las organizaciones modernas: las personas y las herramientas tecnológicas, las cuales se apalancan en los procesos estratégicos, misionales y de apoyo de la Entidad bajo su dirección.

Sin embargo, el desarrollo de esa estrategia implica grandes retos en varios frentes, como en el legal donde se logró gestionar el Acto Legislativo 04 de 2019, el cual permite un control preventivo y concomitante a través del uso de las TICs, la participación ciudadana y la articulación de las medidas de control interno; desarrollado por el Decreto 2037 del siete de noviembre de 2019 por el cual se desarrolla la estructura de la entidad y se crea la Dirección de Información, Análisis y Reacción Inmediata (en adelante DIARI). Esta nueva dependencia debe dirigir la identificación, valoración y administración de los riesgos en la seguridad interna y externa, de los servidores, los bienes y la información de la CGR. Otro frente es el administrativo que por medio del desarrollo del Programa de Fortalecimiento Institucional) (DNP, 2015) para mejorar la planeación, ejecución y seguimiento de las acciones de control fiscal, la gestión de la información y, la transparencia y la participación ciudadana. Y el frente de la gestión del conocimiento y del talento humano, el cual presenta una realidad interesante de abordar, ya que casi el 55% de funcionarios son mayores de 50 años y cerca del 63% son profesionales en ciencias sociales como derecho, contaduría pública y la economía, que conforman una población con fortalezas como la experiencia en el control fiscal, pero debilidades en el uso efectivo, eficaz y seguro de las TICs.

Establecido el contexto anterior, se debe resaltar que el dominio de la seguridad es impredecible y requiere de capacidades, habilidades y conocimientos heterogéneos en distintos campos. Dicha diversidad y complejidad hacen que una organización ciento por ciento segura sea una meta casi imposible de lograr, dados los niveles de incertidumbre sobre los riesgos; lo que sí se puede esperar es que los esfuerzos estén bien encaminados con un adecuado enfoque en la gestión de estos, con la restricción de los recursos humanos, financieros, legales y tecnológicos disponibles y la voluntad de la alta dirección.

En línea con lo anterior, el uso de nuevas metodologías y tecnologías en el ámbito de la educación, particularmente el nacimiento y el uso de los *Massive Open Online Course* (en delante MOOC) (García-LLuis Valencia, 2013) se considera como una revolución que tiene mucho potencial en el mundo académico y empresarial (Bouchard, 2011). Por lo tanto, el desarrollo de este tipo de Recursos Educativos Abiertos (en adelante REA) es una alternativa ante el reto de llevar a cabo procesos educativos exitosos a audiencias numerosas y focalizadas, con las ventajas económicas y logísticas que trae consigo el uso de tecnologías y modelos pedagógicos innovadores. Adicionalmente, usando el ciclo de Gartner sobre expectación (*Hype Cycle*), basado en la ley de Amara que plantea que se sobreestima el efecto de la tecnología a corto plazo y se subestima para el largo plazo, el cual es una herramienta que proporciona una representación gráfica de la madurez de la adopción de tecnologías y de cómo son potencialmente relevantes para resolver problemas comerciales reales y explotar nuevas oportunidades (Gartner, s.f.), se puede observar en el de *e-learning* para el 2019 que los MOOC se encuentran finalizando la fase de desilusión para ingresar en la rampa de la iluminación, donde el los procesos de I+D+i tienen un nivel de madurez interesante para ser abordados.

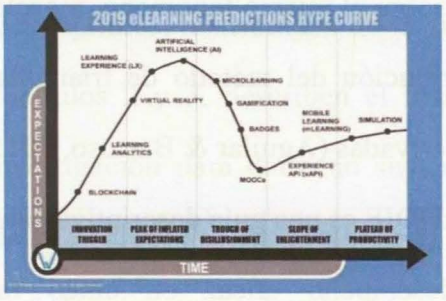

Figura 1. Ciclo de sobre expectación de e-learning 2019

Fuente: https://webcourseworks.com/elearning-predictions-hype-curve

Con esta motivación y teniendo en cuenta lo establecido anteriormente, la pregunta a resolver en esta investigación es: ¿Cómo generar competencias laborales en materia de gestión de riesgos digitales en el personal de la CGR con un uso adecuado de los recursos disponibles?

Con base en los elementos anteriores, se presentan los objetivos del presente trabajo, siendo el objetivo general el de proporcionar a la CGR las herramientas para el desarrollo oportuno y efectivo de competencias en gestión de riesgos sobre seguridad digital en su personal. De este, se derivan los siguientes tres objetivos específicos:

1. Establecer los marcos conceptual y metodológico que guíen la investigación.
2. Realizar un análisis de necesidades en la gestión de riesgo digital al interior de la CGR
3. Diseñar una estrategia de formación que atiendan las necesidades específicas identificadas.

El método general para la elaboración de este proyecto de grado corresponde a la complementariedad metodológica mixta que integra métodos cualitativos y cuantitativos con un enfoque mixto (Hernández, Fernández, & Baptista, 2003), se basa en la recolección de información con diferentes modalidades sobre el mismo fenómeno, mezclando la lógica inductiva y deductiva para su análisis, y la contribución del método de triangulación para validar los resultados y potenciar las conclusiones derivadas (Aguilar & Barroso, 2015). Por otro lado, el marco de diseño instruccional denominado ADDIE es una guía descriptiva para la construcción de herramientas de formación y apoyo al desempeño eficaz en cinco fases: análisis, diseño, desarrollo, implementación y evaluación (Branson, y otros, 1975, pág. 6), provee una metodología de intervención, el cual fue planteado por el comando naval de educación y entrenamiento del ejército

americano; dicho marco es refinado por Galvis en su libro de ingeniería de software educativo, al crear un ciclo retroalimentado para una mejora continua y refinando elementos en las fases de análisis y diseño (Galvis Panqueva, 1992).

En suma, en esta monografía se utilizan los elementos propios de un desarrollo de una estrategia para establecer herramientas que permitan generar competencias laborales en la CGR en el ámbito de la gestión de riesgos digitales, combinando los conceptos de las estrategias propias del enfoque de generación de competencias a través de la formación en línea de un curso abierto masivo en línea, así se le da un marco de elaboración a este trabajo.

Es de acotar que el estilo del documento sigue los lineamientos de formato, estructura e inclusión de referencias determinado por la guía de formato y citación de fuentes (Escuela Superior de Guerra, 2015), la cual adopta el estilo APA por considerarse una de las más difundidas en investigación académica, en su sexta versión (APA, 2010). Las palabras en idiomas diferentes al español se han puesto en cursiva, a excepción de los vocablos aceptados por la Real Academia Española (en adelante RAE).

Este trabajo se divide en seis capítulos, distribuidos de la siguiente manera: el primer capítulo es esta introducción, los capítulos 2 y 3, describen el marco conceptual y el marco metodológico que enmarcan esta investigación para darle un sustento académico y un mejor entendimiento al lector. El análisis de necesidades se desarrolla en el capítulo 4 y el diseño de la estrategia de formación en el capítulo 5. Finalmente se detallan las conclusiones y las referencias bibliográficas.

1 Marco conceptual

1.1 Competencias laborales

El vocablo competencia, desde su perspectiva etimológica asocia su significado inicial al verbo latino *competere*, que significa aspirar, ir al encuentro y el adjetivo competente es aplicado a quien se desenvuelve con eficacia en un determinado dominio (Corominas, 1987). Con anterioridad el término de competencia estuvo asociado a la gestión organizacional para referirse a lo que distingue a una entidad en un mercado, porque lo hace realmente bien y constituye el eje de su ventaja competitiva, fue hasta década de los años setenta que se asocia el mismo término con el comportamiento humano (McClelland, 1973), desde entonces varios autores lo han estudiado.

De esta forma, el concepto de competencia laboral tiene su génesis en la psicología industrial y organizacional desarrollada por autores norteamericanos ente las décadas de 1960 y 1970 (Spencer, 1992). Relacionada con el buen desempeño laboral, Spencer la define como una característica subyacente de un individuo que esta causalmente relacionada a un estándar de efectividad y/o a un desempeño superior en un trabajo o situación. (Spencer & Spencer, 1993, pág. 9). Sin embargo, (Mertens, 1996) es más parco y se refiere a las competencias como sólo algunos aspectos de este acervo de conocimientos y habilidades: aquellos que son necesarios para llegar a ciertos resultados exigidos en una circunstancia determinada. La jefe del Servicio de Políticas de Formación y Desarrollo de Programas de la Organización Internacional del Trabajo (en adelante OIT) en su intervención Seminario Internacional sobre Formación Basada en Competencia Laboral, define la a competencia laboral como la construcción social de aprendizajes significativos y útiles para el desempeño productivo en una situación real de trabajo que se obtiene no sólo a

través de la instrucción, sino también, y en gran medida, mediante el aprendizaje por experiencia en situaciones concretas de trabajo (Ducci, 1996).

Por otra parte, la profesora francesa de psicología del trabajo Claude Levy plantea que las competencias son comportamientos; algunas personas disponen mejor de ellas que otras, incluso son capaces de transformarlas y hacerlas más eficaces y eficientes para una situación dada (Levy-Leboyer, 2003, pág. 3). Mientras que Alles propone una definición sintética de lo que es una competencia laboral: "Competencia hace referencia a las características de personalidad, devenidas en comportamientos, que generan un desempeño exitoso en un puesto de trabajo. Cada puesto de trabajo puede tener diferentes características en empresas y/o mercados diferentes" (Alles, 2013, pág. 6).

La relación entre uso de TIC y las competencias de las personas hay que revisar los tipos de uso que se dan a estas tecnologías y la relación que estos tienen con conceptos y destrezas disciplinarias específicas. Se observa que el provecho que puede sacar una persona del uso de las TIC no solo depende de las oportunidades disponibles sino de cómo interactúa con ellas y su capacidad de usar las oportunidades que abren estas (Cervera & Johnson, 2015, pág. 3). Una vez que un aprendiz tiene las condiciones necesarias de acceso a las TIC, los tipos de usos y los beneficios que obtiene por dicho uso depende de una mezcla de factores, relacionados sobre todo con sus características cognitivas, culturales y sociodemográficas. Esta línea de investigación plantea también la necesidad de atender a la llamada "segunda brecha digital" que se refiere ya no a las diferencias de acceso sino a las diferencias en la capacidad de usar las TIC y beneficiarse de ellas (Necuzzi , 2013, pág. 91).

El Decreto Único Reglamentario del Sector de la Función Pública 1083 de 2015, en su Título 4, establece las competencias laborales comunes a todos los servidores públicos y por nivel jerárquico. Debido a esto, la definición que institucionalmente adopta la CGR en su Resolución Reglamentaria 0067 del 13 de mayo de 2008, la cual usa este trabajo, está alineada con la normatividad mencionada anteriormente:

> "Las competencias laborales se definen como la capacidad de una persona para desempeñar, en diferentes contextos y con base en los requerimientos de calidad y resultados esperados en la Contraloría General de la República, las funciones inherentes a un empleo; capacidad que está determinada por los conocimientos, destrezas, habilidades, actitudes y aptitudes que debe poseer y demostrar el empleado público" (CGR, 2008).

Las actividades de formación y capacitación en la CGR deben estar orientadas a la adquisición de competencias laborales las cuales permiten contar con personal calificado, reducir costos en los procesos de reclutamiento, selección y capacitación de personal, detectar oportunamente las necesidades de capacitación, mejorar la competitividad en la CGR., simplificar la selección de personal con base en los certificados de competencia laboral, coadyuvar al mantenimiento de los sistemas de gestión de calidad y mejorar la administración y control de la capacitación.

1.2 Gestión de riesgos

De acuerdo con el diccionario, riesgo significa "contingencia o proximidad de un daño" (RAE, 2014), tomando en consideración que la CGR es un órgano de control del estado, atiende la siguiente definición del Departamento Administrativo de la Función Pública en la guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP, 2018, pág. 8), de que riesgo es "la posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.", así como detalla el riesgo de seguridad digital en los siguientes términos: "combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas" (DAFP, 2018, pág. 28).

La gestión de riesgos puede abordarse inicialmente desde la Norma Técnica Colombiana NTC ISO 31000 la cual establece principios fundamentales tales como: crear y proteger el valor; estar incorporada en todos los procesos; ser parte del proceso para la toma de decisiones; ser usada para tratar con la incertidumbre; ser estructurada, sistemática, y oportuna; basada en la mejor información disponible; adaptarse a su entorno; considerar factores humanos y culturales; ser transparente, inclusiva, y relevante; dinámica, sensible al cambio, e iterativa y finalmente facilitar la mejora continua de la organización (ICONTEC, 2011).

Por otro lado, el modelo propuesto por la OECD es mucho más específico en abordar la categoría de riesgo de seguridad digital bajo un esquema flexible, holístico y sistemático (OECD,

2015, pág. 36). Evolucionando el concepto de seguridad de la información a la gestión de riesgos de seguridad digital y detallando las actividades clásicas de reducción con la introducción de nuevos conceptos tales como las métricas de seguridad, la innovación y la resiliencia. Los cuatro principios generales de este modelo son: a) conciencia; competencias y empoderamiento; b) responsabilidad; c) derechos humanos y valores fundamentales; y d) cooperación. Los cuales, con considerados por la *International Chamber of Commerce* (en adelante ICC) en su guía de seguridad para los negocios (ICC, 2015), cuando propone que la ciberseguridad empieza por el individuo y que, a diferencia de otros retos empresariales, la gestión de riesgos de ciberseguridad continúa siendo un problema sin fácil solución. Es necesario contar con una atención permanente y consistente por parte de la alta administración, con un manejo tolerante de las malas noticias y finalmente una comunicación clara y disciplinada, puesto que las amenazas están presentes en la vida diaria y pueden tener implicaciones mucho más graves. A la luz de estos lineamientos, dicha guía establece que mejorar la ciberseguridad de una organización es posible a través de un proceso de administración de riesgos con énfasis en la gestión. Debido al constante cambio de la tecnología y de los vectores de amenaza, los sistemas de información de la empresa nunca estarán completos, y nunca estarán completamente seguros. Operar de manera efectiva en un entorno tan cambiante requiere un compromiso con un enfoque de gestión de riesgos a largo plazo y sin un final estático (ICC, 2015, pág. 5), pero sin límites apropiados, se pueden gastar todos los recursos disponibles en un intento de aceptar, mitigar o transferir los distintos tipos de riesgos. Es de especial importancia enfocar la gestión de riesgos de ciberseguridad mediante procedimientos que permitan a las organizaciones establecer conciencia y priorizar los elementos considerados fundamentales para cada una de estas.

1.3 Educación abierta y a distancia

La educación es el proceso por el cual la sociedad transmite a sus miembros los valores, creencias, conocimientos y expresiones simbólicas que hacen posible su desempeño (Bruner, 1997, pág. 22). Esta, es parte fundamental de nuestro crecer como seres sociales, a ella debe dedicársele tiempo para mejorar su efectividad, ya que permite la formación de personas capaces de liderar una nación democrática y con garantías del respeto a los derechos humanos. La estructura y métodos del sistema educativo son muy estables casi desde sus inicios como servicio público, satisfaciendo la necesidad de difundir conocimientos tanto a nivel básico al común de las personas, así como el desarrollo de competencias específicas que les posibilite a estas desempeñarse a nivel laboral de una manera eficaz y eficiente.

Uno de los movimientos más importantes que tuvo lugar a finales del siglo XX desde el punto es la adopción del modelo abierto, conocido generalmente por su nombre en inglés *open*; el cual enfrenta los valores de una cultura dominada e incluso cimentada en el valor de la propiedad intelectual. Así, han surgido apareciendo sucesivas tendencias: *Open Source, Open Standards, Open Access, Open Design, Open Knowledge, Open Data, Open Information,* y por *supuesto Open Education* entre otros. Se trata por tanto de un movimiento social más que de un avance tecnológico, aunque es cierto que para llegar a implementarse es necesaria la utilización de las TIC (Ramírez Montoya & García Peñalvo, 2015)

La idea principal de la educación abierta es ofrecer y compartir de forma gratuita y con acceso abierto recursos, herramientas y prácticas educativas. Esta tipología de enseñanza combina los objetivos educativos tradicionales de compartir y crear, con las posibilidades que ofrecen las

TIC y particularmente internet para difundir conocimiento y conectar a la gente de forma gratuita e inmediata. Es un movimiento que fomenta el espíritu colaborativo, el enfoque centrado en las necesidades de los aprendientes y la personalización del aprendizaje, puesto que no solo significa acceso libre o gratuito, sino libertad de usar, combinar o modificar materiales, produciendo nuevo material (Johnstone & Poulin, 2002).

En la historia de la humanidad se han producido una serie de procesos de cambio, permitiendo que una mayor cantidad de personas tengan acceso recursos educativos y bienes culturales e inmateriales, lo que crea una demanda mayor sobre la accesibilidad a nuevos modelos de enseñanza, sean capaces de trasmitir conocimiento, pero de una forma más flexible. Así, la educación a distancia (en adelante EaD) se comenzó a desarrollar a través del uso de la correspondencia escrita y del telégrafo, posteriormente con los medios masivos de comunicación como la radio y la televisión y en los últimos años aprovechando los recursos multimediales e informáticos como el *e-learning* y la educación móvil.

Los REA fueron originados en el MIT (*Massachussets Institute of Technology*) cuando en 2001 desarrolló el proyecto *Open Course Ware* a través del cual se comenzaron a trabajar y conocer este tipo de elementos educacionales. Estos son herramientas para la enseñanza, el aprendizaje o la investigación que son de dominio público o que son publicados con una licencia abierta que permite, de forma gratuita, la adaptación y la distribución. A través de estos, millones de personas en todo el mundo podrán tener acceso a informaciones que pueden ser utilizadas para el desarrollo social y económico. La educación abierta no es una idea nueva, sino que en muchos países se considera un derecho, y la educación pública garantiza ese derecho a todos los

ciudadanos; por lo tanto, trata de llevar esa idea al ámbito global bajo el principio de que el conocimiento debe ser compartido y llegar a todos los rincones del planeta. como lo plasma la *United Nations Educational, Scientific and Cultural Organization* (en adelante UNESCO) en el *Ljubljana OER Action Plan* del 2017 (UNESCO, 2017).

Los principios en los que se basan este tipo de recursos educativos son los siguientes: a) Las oportunidades de aprender por medio de la educación y el entrenamiento deben existir a lo largo de toda la vida. b) El proceso de aprendizaje debe centrarse en los estudiantes y estructurarse partir de su experiencia para estimularles el pensamiento independiente y crítico. c) La oferta de enseñanza debe ser flexible para que las personas puedan, cada vez más, escoger dónde, cuándo, qué y cómo aprenden, y desarrollar sus procesos a su propio ritmo d) Los conocimientos, aptitudes y la experiencia previos deben ser reconocidos, para que a los aprendices no se les impida el acceso a oportunidades educativas en función de la falta de calificación o idoneidad apropiadas. e) Los estudiantes deben poder acumular créditos desde diferentes contextos de aprendizaje. f) Los proveedores deben generar las condiciones propicias para ofrecer una oportunidad de éxito justa para los aprendientes (Butcher, 2015).

Además de la evolución tecnológica como aspecto disruptivo del cambio, en la actualidad hay un debate abierto sobre cómo deben evolucionar las prácticas de enseñanza para afrontar los desafíos de este siglo, tales como el aprendizaje mediante exploración, estrategias de gamificación, el aprendizaje autorregulado, *microlearning* y colaboración *peer-to-peer* (Revelo-Sánchez, Collazos-Ordoñez, & Jimenez Toledo, 2018); ya que poseen el potencial de cambiar algunos de los pilares en los que se basa la educación . De la misma manera que sectores como la banca,

música, el cine, la prensa y los gobiernos han sido transformados por la acción las TIC, la educación puede verse afectada de forma semejante.

Desde sus inicios la EaD introdujo un cambio significativo que genera ventajas económicas y daba buenos resultados. Los sistemas convencionales de educación requieren una inversión económica importante que, en ciertos casos no es posible realizar. Sin embargo, invertir en educación recursos económicos, humanos y tecnológicos es algo positivo e imperativo para la sociedad en su conjunto general, y para ello hay que extraer la máxima utilidad a dichos esfuerzos. Son múltiples los estudios (Wagner, 1977), (Snowden & Daniel, 1980), (García Aretio , 1998) , (Rabanal, 2017) que confirman el hecho de que el costo de la educación a distancia, que genera fácilmente economía de escala, es muy inferior si se compara con el valor de los sistemas tradicionales.

1.4 Modelos pedagógicos

El aprendizaje es un proceso humano, natural y cultural, a través del cual el hombre le da significado a la realidad en la que vive e interactúa con los demás; posibilitándole al mismo tiempo la conquista del conocimiento, el cambio de su estructura mental y de su medio social (Schunk, 1991).

Una teoría proporciona la explicación general de las observaciones realizadas usando el método científico, estas explican y predicen comportamientos. Una teoría nunca puede establecerse más allá de toda duda y puede ser objeto de modificaciones. En ocasiones una teoría debe desecharse, si durante la prueba no se valida, otras veces pueden tener validez por un tiempo

y de pronto perderla. Por otro lado, un modelo es una representación figurativa de algo que sucede cuando hay un escenario de aprendizaje, se puede ver como una figura mental que nos ayuda a entender las cosas que no podemos ver o explicar directamente (Doring, Demmin, & Gabel, 1990).

Existen tres grandes concepciones clásicas a nivel educativo que corresponden a las corrientes teóricas que surgen desde la psicología en el desarrollo de modelos pedagógicos: el conductismo, el cognitivismo y constructivismo (Nagowah & Nagowah, 2009); convirtiéndose en ejes que orientan las prácticas de enseñanza aprendizaje.

El conductismo se basa en los cambios observables en la conducta del aprendiz. Se enfoca hacia la repetición de patrones de conducta hasta que estos se realizan de manera automática (Skinner, 1974). Su ventaja es que el aprendiz sólo tiene que concentrarse en metas claras y es capaz de responder con rapidez y automáticamente cuando se presenta una situación relacionada a dichas metas, mientras que su falencia radica en que él, puede encontrarse en una situación en la que el estímulo para la respuesta correcta nunca ocurre, por lo tanto, el aprendiz no estaría en capacidad de responder de forma adecuada. Las plataformas LMS y su capacidad interactiva se basan en esta teoría: se insertan materiales de aprendizaje y se observa el avance y la actuación de los aprendientes. Después los datos son analizados y se realizan los cambios necesarios para hacer el aprendizaje más eficaz.

El cognitivismo se enfoca en los procesos que tienen lugar atrás de los cambios de conducta, involucra las asociaciones que se establecen mediante la proximidad con otras personas y la repetición. También reconoce la importancia del reforzamiento, pero resalta su papel como elemento retroalimentador para corrección de respuestas y sobre su función como un motivador

(Vaill, 1996). Su fortaleza radica en que la meta es capacitar al aprendiz para que realice tareas repetitivas y que aseguren consistencia, mientras que su debilidad es que lo aprendido puede no ser la mejor forma de realizar la tarea o la más adecuada para el aprendiz o la situación específica.

El constructivismo se sustenta en la premisa de que cada persona construye su propia perspectiva del mundo que le rodea a través de sus propias experiencias y esquemas mentales desarrollados. Se enfoca en la preparación del que aprende para resolver problemas en condiciones ambiguas (Piaget, 1952). Lo bueno de este modelo el que aprende es capaz de interpretar múltiples realidades, está mejor preparado para enfrentar situaciones de la vida real; pero el pensamiento divergente y la iniciativa personal pueden ser un problema.

No se puede dejar de referir el modelo de Robert Gagné sobre procesamiento de la información que nació en el ámbito militar (Gagné, 1962), que se caracteriza por su línea ecléctica al combinar elementos del conductismo y el cognitivismo.

El conectivismo, intenta solucionar los vacíos que dejan los modelos el anteriores, plantea que el aprendizaje reposa en la diversidad de opiniones, es un proceso de conectar nodos especializados, puede residir en contenedores no humanos, privilegia la competencia de aprender más sobre el conocimiento mismo, requiere de nutrir y mantener conexiones que promueven la continuidad del mismo, el conocimiento preciso y actualizado es la intención de todas las actividades de aprendizaje, reconoce como habilidad el ver conexiones entre conceptos, áreas e ideas y la toma de decisiones es en sí misma un proceso de aprendizaje, el elegir qué aprender y el significado de la información entrante se ve a través de la lente de una realidad cambiante. Si bien

hay una respuesta correcta ahora, puede ser incorrecta mañana a alteraciones en el entorno de la información que afectan la decisión (Siemens, 2004).

Lo anterior parte de la tesis de que el conocimiento está distribuido a través de una red de conexiones y que, por consiguiente, el aprendizaje consiste en la habilidad de construir y recorrer dichas redes (Downes, 2008). No hay una construcción consciente del conocimiento como en las teorías anteriores, sino que las conexiones tienen lugar de forma natural. En este modelo hay tres elementos fundamentales: las redes, los nodos y las conexiones. Una red está formada por dos o más nodos que establecen conexiones para compartir recursos. Los nodos serían las diferentes entidades que actúan como fuentes de información tales como individuos, comunidades, organizaciones, instituciones, que pueden ser de diferente tamaño y fuerza, dependiendo de la concentración de información. Las conexiones que se crean se asocian con el conocimiento y el aprendizaje tiene lugar cuando se forman nuevas redes, se añaden nuevos nodos y se crean conexiones. Se trata de un sistema de aprendizaje en la que no hay un conocimiento que se transfiere de docente a los alumnos, ni donde el aprendizaje tiene lugar en un solo entorno, sino que el conocimiento se distribuye a través de la red y el compromiso de la gente con esta es lo que constituye el aprendizaje (Kop, 2011).

Dado que la información cambia constantemente, su validez y precisión pueden cambiar con el tiempo, dependiendo del descubrimiento de nuevas contribuciones relacionadas con un tema. Por extensión, la comprensión de un tema y la capacidad de aprender sobre este también cambiará con el tiempo. El conectivismo enfatiza que dos competencias importantes que contribuyen al aprendizaje son la capacidad de buscar información actual y la capacidad de filtrar

información secundaria y extraña. La capacidad de tomar decisiones sobre la base de la información que se ha adquirido se considera parte integral del aprendizaje, considerándolo como un proceso de creación de conocimiento y no solo de su consumo. (Siemens, 2005).

Este modelo propone que el proceso de aprendizaje es cíclico, ya que los alumnos se conectarán a una red para compartir y encontrar nueva información, modificarán sus creencias en función de un nuevo aprendizaje y luego se conectarán a una red para compartir estas realizaciones y encontrar nueva información una vez más La red de aprendizaje individual se forma sobre la base de cómo un alumno organiza la conexión con distintas comunidades de la red.

El conectivismo tiene también sus críticos, (Kerr, 2007) afirma que no constituye una nueva teoría de aprendizaje, puesto que ya existen otras que explican cómo tiene lugar el aprendizaje con tecnología y que no constituye una alternativa a las teorías actuales como ha declarado Siemens, por otro lado (Verhagen, 2006) no lo considera una teoría de aprendizaje sino una visión pedagógica, que se centra en el nivel curricular más que en el nivel instruccional. Por otro lado (Zapata Ros, 2013) sugiere que además de carecer de una estructura propia de una teoría, es un conjunto de enunciados que no están integrados sintáctica y semánticamente en un sistema cohesionado por reglas de la lógica, permitiendo evaluar, atribuir sentido, predecir y explicar fenómenos observables. Se argumenta también que carece de componentes imprescindibles en una teoría como son los valores y las condiciones de aplicación.

Si bien no se considera aún al conectivismo una teoría de aprendizaje en su totalidad, ha provocado un gran interés y una discusión en el mundo del aprendizaje digital, que debe tenerse en cuenta, sobre todo en la siguiente fase del e-learning, como lo hace la Universidad Nacional de

Colombia en su documento innovación académica (Torres Vargas, Reyes Montaño, Moreno Gómez, & López López , 2015).

1.5 Cursos masivos en línea y abiertos - MOOC

El uso de nuevas metodologías y tecnologías en el ámbito de la educación, particularmente el nacimiento y el uso de los cursos en línea, masivos y abiertos - *Massive Open Online Course* (MOOC) (García-LLuis Valencia, 2013) se considera como una revolución que tiene mucho potencial en el mundo académico y empresarial (Bouchard, 2011). Por lo tanto, el desarrollo de este tipo de materiales educativos es una alternativa ante el reto de llevar a cabo procesos educativos a audiencias numerosas y focalizadas, con las ventajas económicas y logísticas que traen consigo.

Los MOOC aparecen como una expresión de esta necesidad de globalizar y dar acceso abierto al conocimiento, pero trascienden una intención educativa con una iniciativa masiva, ubicua, gratuita y abierta (Raposo, Sarmiento, & Martínez, 2017). Este nuevo nivel educativo informal y masivo se cimienta en los pilares del modelo conectivista, descrito en el acápite anterior. La idea misma de llevar una apuesta de formación de miles de personas supone una necesidad de diseñar la experiencia centrada en la colaboración e instanciada en herramientas web 2.0 así mismo, se promueve la descentralización, la autonomía y la diversidad en los procesos de enseñanza-aprendizaje (Baggaley, 2014)

Las universidades norteamericanas fueron las pioneras en uso de los MOOC, aunque en la actualidad muchas universidades del mundo están utilizándolos con sus diferentes formatos

dentro de su oferta en todo tipo de cursos. Como antecedente histórico, el curso que es considerado como el paso disruptivo los MOOC es el curso *Introduction to Artificial Intelligence* en la universidad de Stanford de los profesores Sebastián Thrun y Peter Norvig, planteado como actividad complementaria a las clases presenciales. Dicho curso se desarrolló en 2011, acogiendo a más de 58.000 estudiantes de 175 países, mientras que 177 asistían en el campus físico (Markoff, 2011).

Las cuatro características de un MOOC son (Siemens, 2013):

- Masivo: el número de plazas es ilimitado, el ámbito es global y están dirigidas a alumnos con diferentes intereses y aspiraciones, lo que implica una gran diversidad.
- Abierto: sigue el movimiento Open, permite el acceso libre y gratuito sin exigencias académicas, administrativas, de tiempo o dedicación.
- En línea: todas las actividades se realizan exclusivamente a través de cualquier dispositivo que tenga acceso a internet.
- Curso: debe tener una estructura determinada, con objetivos y actividades claras enmarcadas en un área de conocimiento específica.

Desde su origen han existido varias tipologías de MOOC (Rosselle, Caron, & Heutte, 2014) como los cMOOC que siguen la filosofía de red del conectivismo y los xMOOC se basan más en la figura del experto con exposición de contenidos y los *blended* MOOC (bMOOC) que son una mezcla de los dos anteriores. Otra taxonomía es propuesta en la guía para formuladores

de políticas para países en desarrollo de la UNESCO en los siguientes grupos (Patru & Balaji, 2016) en orden alfabético:

- BOOC (*big open online course)*, curso grande en línea y abierto, limitado a 500 participantes
- COOC (*community open online course*), curso en línea y abierto centrado en la comunidad.
- DOCS (*digital open courses at scale)*, cursos digitales a escala y abiertos, que se cursarán sobre todo con *smartphones.*
- DOCC (*distributed open collaborative course),* cursos abiertos donde el aprendizaje es colaborativo y distribuido.
- HOOC (*hybrid open online course),* cursos que combinan la interacción en línea con la interacción *in situ.*
- LOOC (*little open online course)*, con pocos participantes y retroalimentación personalizada;

  o

  LOOC (*Local Open Online Course*), curso en línea abierto y local, ofrecidos en universidades locales o regionales.
- POOC *(personalized open online course),* curso en línea abierto y personalizado.
- SOOC *(selective open online course),* cursos en línea abiertos pero selectivos, con matrícula limitada.
- SPOC (*small private online course),* curso pequeño privado en línea, con interacción individualizada, que constituye una de las últimas tendencias;

  o

  SPOC (*self-paced online course),* donde los estudiantes completan los cursos a su propio ritmo.
- SMOC (*synchronous massive online course)*, curso en línea síncrono y masivo.

- ROOC (*regional open online course*) curso en línea regional y abierto.
- TORQUE (*tiny, open-with-restrictions course focused on quality and effectiveness*), curso muy pequeño con restricciones de apertura y centrado en la calidad y efectividad.
- VOOC (*vocational open online course),* centrado en ofrecer habilidades vocacionales.

Los MOOC por su diseño promueven que los aprendices accedan de forma individual a la información de forma que cada establece su propio ritmo, usando las herramientas y recursos disponibles. Por lo tanto, permiten responder a una gran variedad de usuarios con características cognitivas, sociales y educativas; en un marco de ubicuidad y movilidad digitales que dan soporte al *mlearning* (aprendizaje móvil). Así se puede hablar de una modalidad de EaD a distancia que lleva la característica de la flexibilidad al punto extremo, convirtiendo en ambulante o nómada el proceso de enseñanza-aprendizaje. Así lo que se puede afirmar es lo que caracteriza a un MOOC que se constituye como un punto de reunión de las partes interesadas en un tema común.

2 Marco metodológico

Para la identificación de competencias laborales se usa el método de incidentes críticos (Flanagan, 1954), el cual define un incidente crítico como un suceso de la práctica cotidiana extraído de la experiencia, que si bien no siempre representa gravedad o riesgo sí resulta fundamental para la consecución de un objetivo. Los incidentes críticos se pueden identificar en consulta individual a funcionarios que se consideren claves en un proceso en forma de entrevista, encuesta o en grupos focales en los que se discutan los problemas claves y las condiciones personales que permiten resolverlos.

Para darle sustento a lo anterior desde métodos de investigación, la metodología de este trabajo de grado corresponde a la complementariedad metodológica mixta que integra métodos cualitativos y cuantitativos con un enfoque mixto (Sampieri Hernández & Mendoza Torres, 2018), se basa en la recolección de información con diferentes modalidades sobre el mismo fenómeno, mezclando la lógica inductiva y deductiva para su análisis, y la contribución del método de triangulación para validar los resultados y potenciar las conclusiones derivadas (Aguilar & Barroso, 2015).

El componente cualitativo se aborda dos frentes: el primero es un análisis documental con el propósito de verificar la existencia de la normatividad interna de la CGR, las capacidades institucionales y los mecanismos de formación; el segundo usa grupos focales con los lineamientos de (Lewis, Bryman, & Liao, 2003), las preguntas abiertas en encuestas y el desarrollo de una entrevista guiada por preguntas orientadoras conducentes a obtener opinión subjetiva y abierta sobre las categorías de análisis. (Denzin & Lincoln, 2005).

Como en la mayoría de las ocasiones no es posible abordar al conjunto de los sujetos, eventos y sucesos que conforman el objeto de estudio, el componente cuantitativo establece las propiedades, características y perfiles de los funcionarios respecto a las variables de interés por medio de una encuesta de preguntas cerradas a una muestra probabilística para una población finita (Hernández, Fernández, & Baptista, 2003).

La triangulación hace referencia a la utilización de dos o más fuentes y métodos con el fin de comparar los resultados desde perspectivas distintas para lograr una mayor comprensión del fenómeno o situación que se está investigando y lograr a la construcción de un modelo más enriquecido (Cohen, Manion, & Morrison, 2017) .

El marco de metodológico para el diseño instruccional denominado ADDIE es una guía descriptiva para la construcción de herramientas de formación y apoyo al desempeño eficaz en cinco fases, el cual provee una metodología de intervención, el cual fue planteado por el comando naval de educación y entrenamiento del ejército americano; cuya implementación ha sido aplicada en diferentes ámbitos, incluyendo en el campo educativo y actualmente en la planificación de estrategias de creación de recursos de diversa índole, y en el caso particular, en la elaboración de recursos educativos digitales (Branson, y otros, 1975, pág. 6). Las cinco fases de ADDIE son:

1. Análisis: En esta fase se obtiene información sobre la naturaleza del problema, las estrategias y recursos de aprendizaje que brinda el experto. Se decide sobre la viabilidad de desarrollo de la propuesta, el tipo de material educativo y aspectos técnicos y pedagógicos que identifican los recursos que se quieren construir.

2. Diseño: Después de determinar las necesidades, se crea un listado de productos y el cronograma, definiendo las tareas que deben realizar el experto y el equipo de producción. Esta etapa tiene que ver con la planificación del proceso.
3. Desarrollo: Una vez que se cuenta con los recursos que el experto solicita, llevando a ejecución las estrategias de pedagogía, diseño y audiovisuales, se inicia este proceso
4. Implementación: Se pone a prueba el material elaborado, los avances o prototipos, de acuerdo con la revisión y ajustes que se hayan hecho en el material, en este proceso participa el experto para validar los cambios.
5. Evaluación: La evaluación del material se realiza a lo largo de todo el proceso, no obstante, se debe hacer una verificación de los objetivos de producción definidos desde la etapa de diseño.

Existe una propuesta de mejora para ADDIE hecha por Álvaro Galvis en su libro de ingeniería de software educativo (Galvis Panqueva, 1992), al crear un ciclo retroalimentado para una mejora continua y refinando elementos en las fases de análisis haciendo énfasis en que el apoyo informático debe ser tomado en cuenta siempre y cuando no exista un mecanismo mejor para resolver el problema: ver si el problema se soluciona al tomar decisiones de tipo administrativo; cambios en metodologías de clase; o mejoras a los medios y materiales de enseñanza contemplando el uso de medios informáticos y la fase de diseño se debe partir del qué subyace al recurso educativo: contenidos a tratar, derivados de las necesidades o problemas y la motivación de los alumnos.

3 Análisis de necesidades

En los capítulos previos, usando los marcos conceptual y metodológico, es preciso establecer las necesidades de aprendizaje. Para esto primero se examina el contexto institucional revisando sus antecedentes, estado actual y proyección y caracterizando su población. Posteriormente se busca identificar las necesidades para dicho contexto, estas se clasifican en necesidades normativas, sentidas y comparativas. Las necesidades normativas son las que provienen de marcos regulatorios, reglamentación interna o legislación que son aplicables; las necesidades sentidas se definen como necesidades que se pueden indagar en la población objetivo y las necesidades comparativas se definen como necesidades que nacen de la comparación con referentes o estándares a los que se quiere llegar (Galvis Panqueva & Mendoza, 1999).

3.1 Contexto institucional

La CGR es el máximo órgano de control fiscal del Estado. Como tal, tiene el objetivo de procurar el buen uso de los recursos y bienes públicos y contribuir a la modernización del Estado, mediante acciones de mejoramiento continuo en las distintas entidades públicas. Su misión es ejercer el control y la vigilancia fiscal a los recursos públicos de manera oportuna, independiente y efectiva, garantizando la participación de la ciudadanía y la articulación regional, con base en el conocimiento y la tecnología, que contribuya al desarrollo sostenible y al cumplimiento de los fines esenciales del Estado. Y su visión es busca ser reconocida a nivel nacional e internacional como un órgano de control y vigilancia fiscal líder, moderno y efectivo, con un enfoque preventivo y un control fiscal participativo y oportuno, que contribuya al buen manejo de los recursos públicos, y que genere una mejora en la gestión del Estado y calidad de vida de los colombianos.

Sus valores institucionales son la competencia, la honestidad, la lealtad, la imparcialidad, la transparencia, el respeto, la objetividad y el compromiso en lo declarado en su código de ética. Y en sus directrices se resalta la de mantener la confidencialidad y reserva de la información institucional.

En la familia de normas ISO 27000, se incluye una guía de buenas prácticas que permiten a las organizaciones mejorar la seguridad de su información. Con este fin, define una serie de objetivos de control y gestión para ser implementados de acuerdo con la prioridad establecida. Éstos se hallan distribuidos en diferentes dominios que abarcan de una forma integral todos los aspectos que han de ser tenidos en cuenta por las organizaciones para identificar, eliminar o minimizar las amenazas y peligros, haciéndolos conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática y estructurada. Con esta orientación se realiza un *assessment* como uno de los entregables del contrato 071 de 2016 supervisado y liderado por la USATI que incluye un inventario de buenas prácticas a fin de identificar el grado de madurez del grado de la implementación de controles (no implementado, implementado parcialmente, completamente implementado).

El instrumento principal fue una encuesta que fue contestada por los funcionarios de 76 dependencias del nivel central y de las gerencias departamentales; al ser la primera vez en la CGR que se realizaba un ejercicio de este tipo, por medio de un cuestionario de 293 preguntas, de las cuales se destacan las que tienen que ver con el ámbito del desarrollo de competencias laborales y se destacan a continuación por dominio (todas las preguntas se encuentran en el Anexo A). El tema de la seguridad de la información es esencialmente complejo y subjetivo, por lo tanto, es más fácil

abordarlo por medio de evaluaciones fáciles que aumenten la conciencia, que logren un consenso amplio y que motiven la mejora. Estas evaluaciones se pueden realizar ya sea contra las descripciones del modelo de madurez como un todo o con mayor rigor, en cada una de las afirmaciones individuales de las descripciones. La ventaja de un modelo de madurez (The Open Group, 2016) es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. La escala incluye al cero ya que es muy posible que no existan procesos en lo absoluto y va hasta cinco donde se cuenta con una capacidad optimizada.

A continuación, se listan los dominios y se destacan las preguntas relacionadas con el desarrollo de las competencias del personal.

A. Política de seguridad.

B. Organización de la seguridad.

C. Seguridad de recursos humanos.

> 39. ¿La política de RRHH establece un adecuado nivel de concientización, sensibilización y capacitación en procedimientos de seguridad?
>
> 43. ¿Existe un plan de capacitación regular orientado a la divulgación de actualizaciones de seguridad en la Entidad?

D. Gestión de activos.

E. Control de acceso.

> 85. ¿Las responsabilidades de seguridad de la información definidas en la Entidad han sido divulgadas, asimiladas y aplicadas por el personal?

.87. ¿En las evaluaciones del desempeño del funcionario se ha incluido la revisión de los aspectos de seguridad que son del resorte del empleado y en los cuales haya podido tener deficiencias en su cuidado?

.93. ¿Existen planes periódicos de capacitación sobre seguridad de TIC a los funcionarios de la Entidad?

F. Criptografía.

G. Seguridad física y del entorno.

.116. ¿El personal de las instalaciones ha sido entrenado por completo respecto a situaciones de emergencia, así como en prácticas de salud y seguridad?

H. Seguridad de operaciones.

I. Seguridad en comunicaciones.

J. Adquisición, desarrollo y mantenimiento.

210. ¿En la adquisición de software se asegura que el proveedor ha realizado capacitación a su personal sobre seguridad del mismo?

K. Relación con proveedores.

L. Gestión de incidentes.

M. Continuidad del negocio.

256. ¿Se han realizado sesiones de capacitación de forma regular respecto a los procesos, roles y responsabilidades en caso de incidente o desastre?

N. Cumplimiento.

O. Administración de los datos.

Como resultado general, se obtuvo una valoración promedio de 1,66 sobre 5 puntos, ubicándose en nivel de madurez de nivel 2, como se observa en la figura 3, dicho *assessment* declara:

> "Existen controles, pero no están documentados. Su operación depende del conocimiento y motivación de los individuos. La efectividad no se evalúa de forma adecuada. Existen muchas debilidades de control y no se resuelven de forma apropiada; el impacto puede ser severo. Las medidas de la Alta Dirección para resolver problemas de control no son consistentes ni tienen prioridades. Los empleados no están conscientes de sus responsabilidades". (CGR, 2016)

Figura 2. Nivel de Madurez y Capacidad TIC en la CGR

Fuente: Informe de Valoración de las Prácticas de Control en Seguridad de la Información *(CGR, 2016)*

Las preguntas específicas mencionadas anteriormente, relativas a temas de capacitación o formación, sólo tuvieron un máximo del 2,63% de respuestas positivas, con tres en cero constituyéndose en una necesidad expresada de forma general en el sentido que en los dominios donde pudieron manifestar interés en temas de mejorar el conocimiento y capacidades lo hicieron contundentemente.

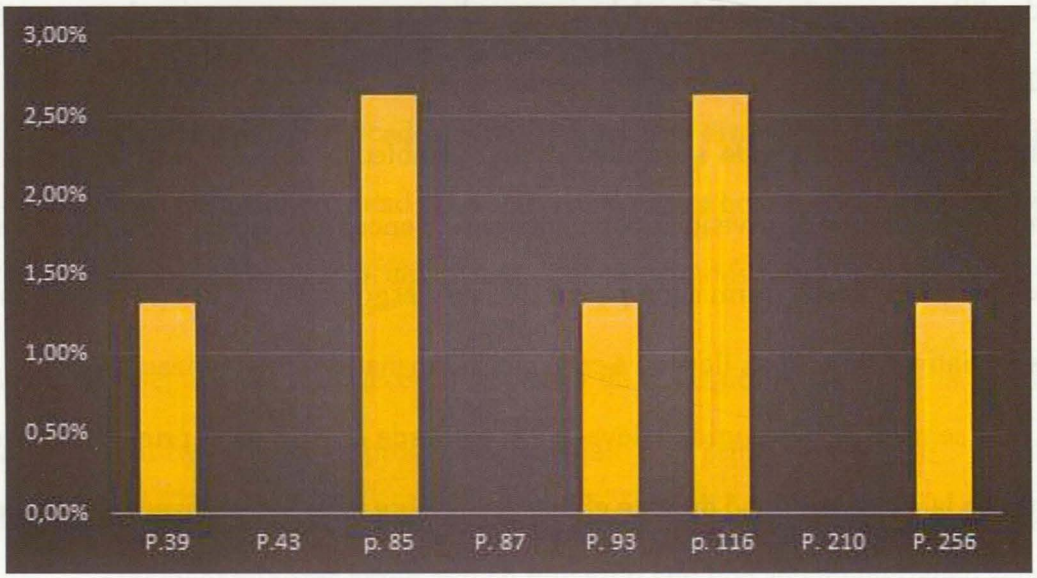

Figura 3. Porcentaje de niveles de formación

Fuente: Elaboración Propia a partir del Informe de Valoración de las Prácticas de Control en Seguridad de la Información *(CGR, 2016)*

Sin embargo, la oferta en los planes de capacitación para este han dado un buen cubrimiento al tema de gestión de riesgos de seguridad digital, en el pasado cuatrienio solamente hubo dos cupos para seguridad electrónica y 140 para elaboración de mapas de riesgos sectoriales (CGR, 2015); para el año 2018 respecto al tema de riesgos se ofreció de forma presencial el curso de Administración del Riesgo y Auditoría Forense con enfoque misional de control micro y procesos de responsabilidad fiscal (CGR, 2018) durante el 2019 la capacitación en tema de riesgos se hizo a través del contrato 232 suscrito entre la CGR y el ICONTEC con un curso de 16 horas titulado "Programa de gestión del riesgo, directrices para su implementación NTC ISO 31000:2018" para 24 funcionarios, teniendo así un vacío importante para apoyar más decididamente la política de seguridad digital establecida en el CONPES 3458 (DNP, 2016). Dentro de los trabajos de revisión documental, no se encontró evidencia de que se hayan ejecutado actividades diferentes de formación para temas de riesgo digital (CEF, 2017). En este aspecto, las únicas iniciativas que se han llevado a cabo son campañas de concientización de parte de la USATI como la la semana de la seguridad llevada a cabo desde el 2018 en el primer semestre de cada año y el mes de la ciberseguridad durante el mes de octubre y las sensibilizaciones presenciales en las gerencias departamentales con una duración de tres horas aproximadamente.

Por otro lado, la oferta actual sobre los temas de seguridad digital por parte de diferentes universidades locales, las cuales tienen programas de especialización y/o maestría, que tienen la desventaja de horarios (la mayoría nocturno), tiempos de duración (uno a dos años), costo (promedio $10'000.000 por semestre), cantidad (cohortes de 35 alumnos en promedio) y cubrimiento (solo en las cinco ciudades principales). En el servicio nacional de aprendizaje y en el portal Colombia Aprende (MEN, 2019) no hay cursos ni materiales relacionados con estos

temas, MinTIC con su portal de apps.co ofrece ocho cursos virtuales pero ninguno relacionado con ciberseguridad o riesgos digitales. Ante este panorama donde la coyuntura económica y presupuestal ha sido establecida por distintas directivas presidenciales, especialmente por lo determinado en el Plan de Austeridad 2016 (Directiva Presidencial 01, 2016) la cual restringe los gastos generales, en comunicaciones, nómina y la modificación de estructuras administrativas. La exigencia de cerrar la brecha de contar con funcionarios con competencias y capacidades en gestión del riesgo digital en un periodo de tiempo razonable para poder cumplir con las funciones institucionales es una necesidad sentida por la CGR en cabeza de la USATI.

A partir de los elementos identificados anteriormente, los directivos de la USATI (jefe y director), se vieron en la imperiosa necesidad de plantear una nueva hoja de ruta, que se cristalizó en el Plan Estratégico de Seguridad (PES), cuyos objetivos principales son:

1. Liderazgo de la Seguridad: Establecer el gobierno de la gestión integral de la seguridad; formular políticas y programas bajo principios de calidad, flexibilidad, interdisciplinariedad, internacionalización y sostenibilidad; y fortalecer los vínculos con socios estratégicos nacionales e internacionales.
2. Viabilidad, Efectividad e Innovación: Proponer elementos que tengan una buena relación costo-beneficio para las diferentes actividades, usando de manera creativa los recursos disponibles para definir nuevas formas de satisfacer los clientes internos y externos de una manera segura.
3. Continuidad de Negocio: Desarrollar un plan para mantener la entrega de los productos y servicios críticos en niveles aceptables, que sean parcial o totalmente afectados, después

de una interrupción o desastre, en un tiempo predeterminado; con una estructura de respuesta que articula los niveles estratégico, táctico y operativo con los mecanismos de medición, seguimiento y control acorde a los lineamientos establecidos por la gobernanza interna.

4. Gestión de Incidentes: Planificar, detectar, analizar, contener y documentar los eventos o serie de eventos relacionados con la seguridad que afecten las operaciones de la Entidad.
5. Cultura Organizacional: Aportar al conjunto de principios, valores, costumbres, actitudes y motivaciones que, para la adquisición de buenos hábitos y competencias laborales alrededor de la seguridad, la apertura a nuevas ideas, la mejora de la comunicación y el fomento de un aprendizaje continuo.

Estableciendo formalmente la necesidad de trabajar en pro de las personas, quienes son un componente esencial en el tema de la ciberseguridad y ciberdefensa. Este plan una vez socializado, fue un insumo para el nuevo plan estratégico de la CGR para la vigencia 2018-2022, denominado "Una Contraloría para todos" donde se destacan los siguientes objetivos:

> "Objetivo 5. Habilitar las capacidades y servicios tecnológicos para impulsar la transformación digital de la entidad por medio de la práctica de la arquitectura empresarial.
>
> (…)

Objetivo 6. Fortalecer el talento humano y la operación de la estructura organizacional, procesos y procedimientos para cumplir de manera efectiva la misión de la entidad" (CGR, 2018)

Conforme a los lineamientos y realidades de la CGR, la investigación usa estos elementos para tomar un curso de acción que los articule, el siguiente paso es establecer las características de los servidores públicos para diseñar la estrategia de formación en riesgo digital.

3.2 Caracterización de la población

A partir de los datos obtenidos del sistema de información de la GTH, se hace la caracterización de la población objetivo de este proyecto, a la fecha la entidad cuenta con una planta de personal de 4.122 servidores públicos. A continuación, se muestra la segmentación de dichas personas por las características tomadas como relevantes para este trabajo, los datos arrojan que no se dan diferencias significativas entre los grupos, en cuanto a género o al centro de trabajo, como se aprecia en la figura 5.

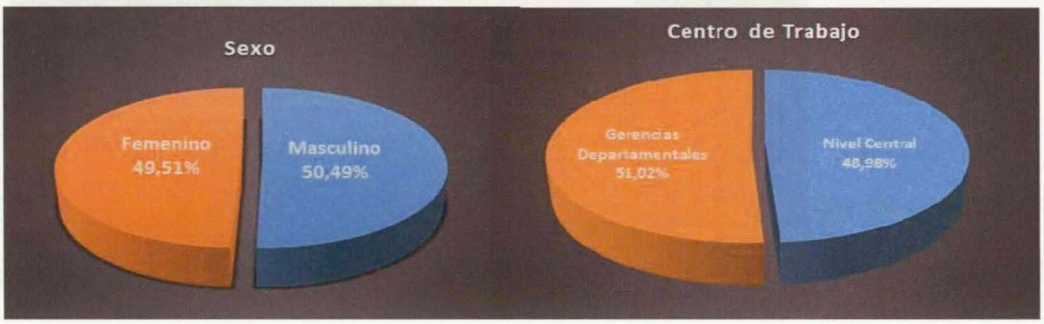

Figura 4. Distribución por sexo y centro de trabajo

Fuente: Elaboración propia

Al analizar la población de las gerencias departamentales en la figura 6, se identifican cuatro grandes grupos: las gerencias que tienen más del tres por ciento de la población las cuales suman un 14,10%, las que aglutinan entre el dos y tres por ciento con 12,98%, las que tienen entre el uno y dos por ciento que suman un 18,97% y las de menos de uno por ciento solo cuentan con un 4,97% del total. Se observa que las gerencias con menos personal son las que tienen más dificultades y restricciones de acceso, bien sea vía aérea o terrestre lo que incrementa los costos de desplazamiento hacia estos lugares, totalmente opuesto al primer grupo donde las condiciones de infraestructura y movilidad son muy superiores.

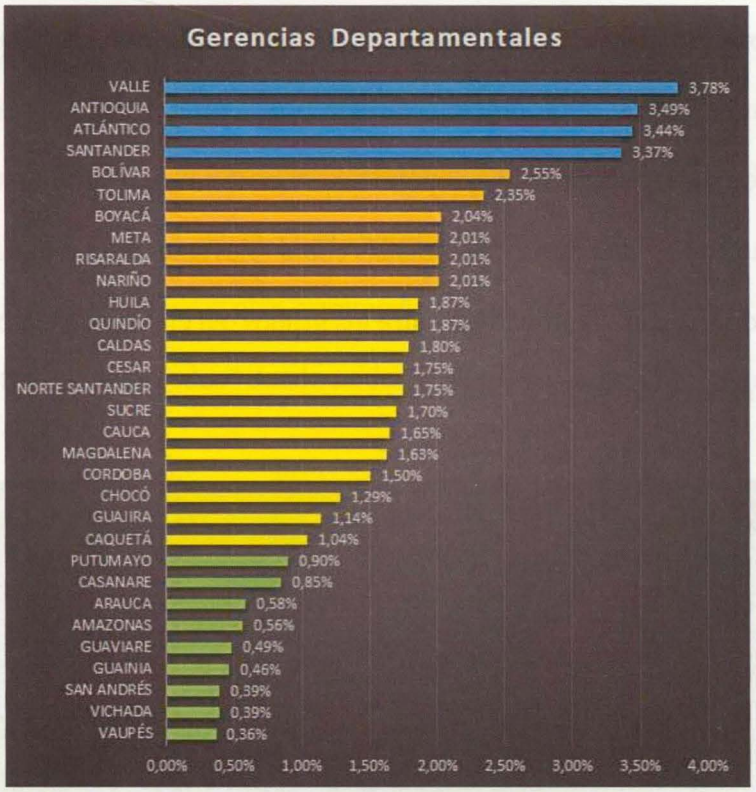

Figura 5: Distribución por las Gerencias Departamentales

Fuente: Elaboración propia

Otra característica importante de analizar es la edad, por rangos de décadas las personas se distribuyen así: menores de 30 años un 3, 57%, entre 30 y 39 años el 16,84%, entre 40 y 49 años el 24,72%, entre 50 y 59 años el 43,96% y mayores de 60 años el 10,92%. El análisis de Pareto (Kiremire, 2011) de esta variable arroja que el rango de edad entre 38 y 62 años cubre el 80,45%, lo cual a nivel general establece personas de edad adulta y madura. El histograma de estos datos, con rango 3 se ilustra en la figura 7.

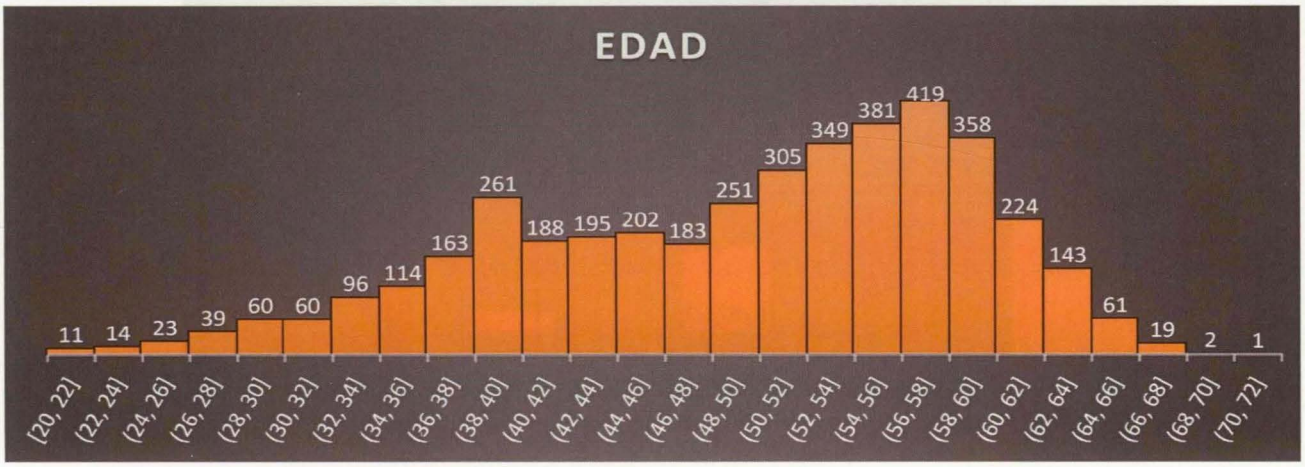

Figura 6: Distribución por edad

Fuente: Elaboración propia

El nivel jerárquico es una variable determinante para valorar el tipo de competencias a desarrollar acorde a la normatividad asociada a la Función Pública como se mencionó con anterioridad en el capítulo1, lo observado es el alto grado de nivel profesional lo que lleva a enfocar la atención en este segmento. El análisis a nivel de la jerarquía profesional arroja que el nivel de cargos tiene un 70,86% de personas en el nivel profesional, 14,92% en el nivel asistencial, 2,01%

ostentan el cargo de tecnólogo sumando un 87,80,18 a nivel operativo y el restante 12,20% se distribuye así: 5,82% nivel directivo, 2,57% asesores y un 3,81% de nivel ejecutivo, estos resultados se muestran en la figura 8.

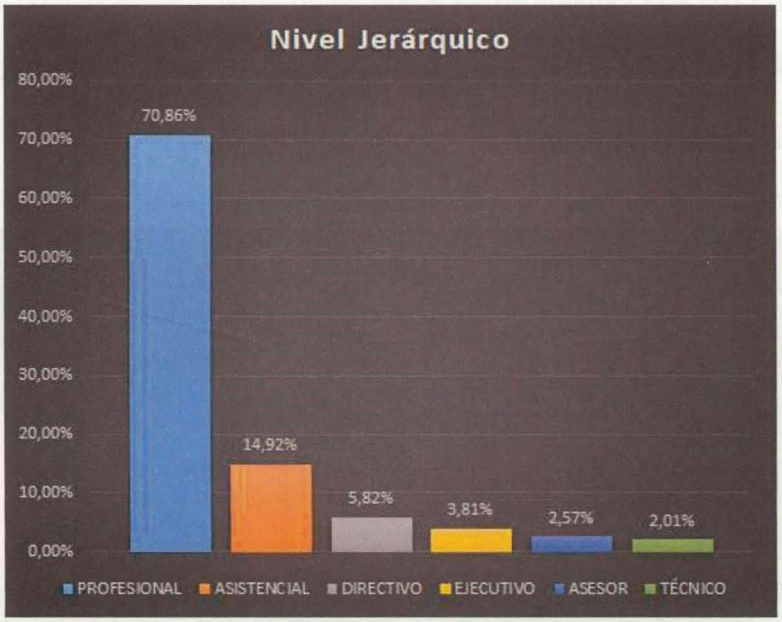

Figura 7: Distribución por grado de nivel jerárquico

Fuente: Elaboración propia.

A partir de lo anterior, enfocándose en las personas de nivel jerárquico profesional se usa el principio de Pareto para agrupar las personas con las profesiones con mayor número de frecuencia presentes en la muestra analizada, cuyos resultados porcentuales se ilustran en la figura 9, la cual muestra que el 80,79% concentra a las personas profesionales en derecho, contaduría pública, administración de empresas, economía e ingeniería de sistemas, importante para determinar el tipo de contenidos y la motivación de este segmento de personas.

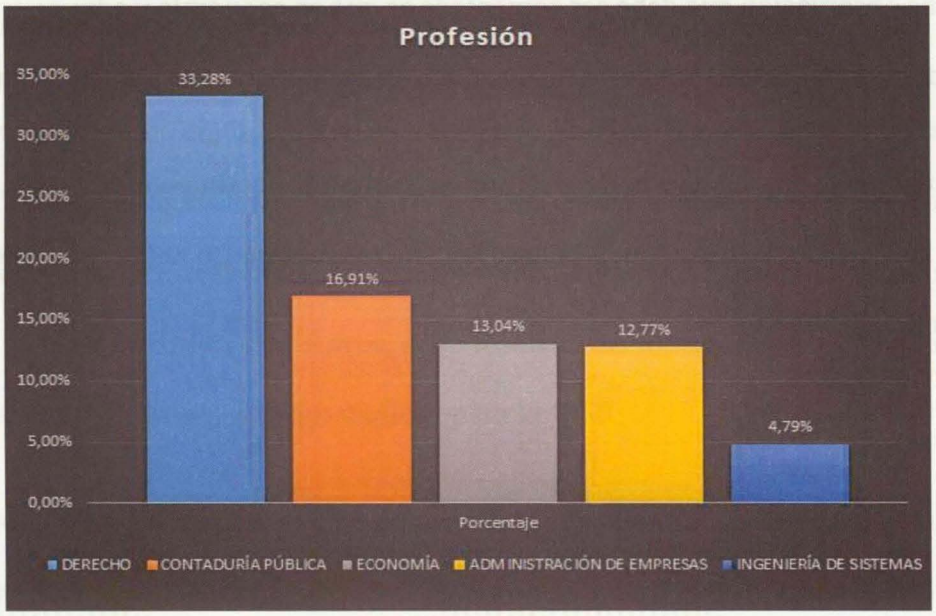

Figura 8: Distribución por profesión

Fuente: Elaboración propia

En este punto se completa el análisis descriptivo multivariado, observando los histogramas que combinan las variables de edad general, nivel jerárquico y de las profesiones que conforman el Pareto de la muestra, se observa que el comportamiento de la distribución es uniforme. Al hacer el comparativo con las profesiones de contaduría pública, administración de empresas y economía, se evidencia que el comportamiento se mantiene con una concentración entre los 40 y 60 años; los profesionales de derecho muestran una distribución similar, aunque presentan una atipicidad entre los 30 y 40 años la cual, después de validar los datos se acepta debido su peso relativo en el análisis.

Una observación que debe ser comentada es que en economía y administración de empresas el número de profesionales menores de 40 años son muy pocos, con un valor porcentual del 0,8%.

Finalmente, la ingeniería de sistemas se comporta totalmente diferente, su aporte, que es menor al 5%, no afecta considerablemente la caracterización. Lo anterior se puede observar en la figura número 10.

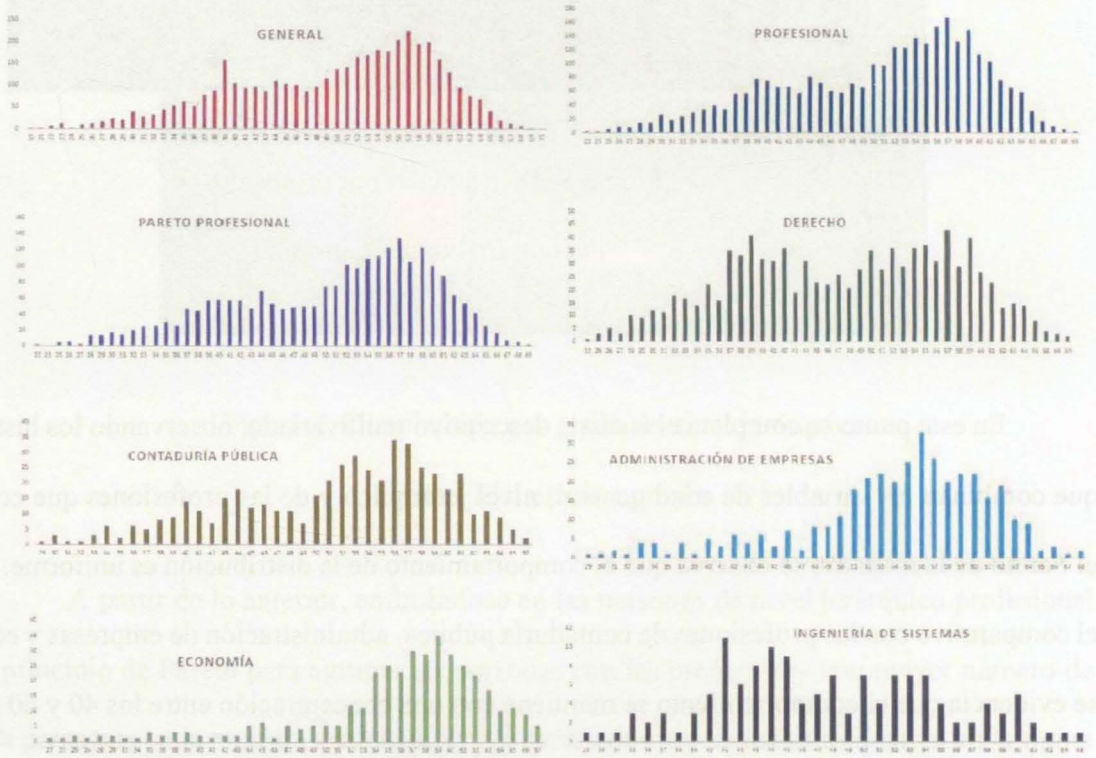

Figura 9: Histogramas por edades de los grupos de análisis

Nota: Elaboración propia

3.3 Necesidades normativas

Las necesidades desde el punto de vista normativo se identifican por medio de la revisión de la constitución, las leyes y decretos aplicables a la CGR, así como las resoluciones internas. En esta exploración documental se destacan los elementos relevantes a la seguridad de la información, gestión de riesgos y gobierno digital entre otros, cuyo resultado se muestra en la tabla número uno, así como los fundamentos legales sobre los cuales opera la CGR.

Cabe resaltar que la CGR como ente de control del Estado, está llamada a ser modelo de cumplimiento máxime cuando en sus labores misionales hace auditoría al Modelo Estándar de Control Interno, el cual se establece para las entidades del Estado y proporciona una estructura para el control a la estrategia, la gestión y la evaluación, cuyo propósito es orientarlas hacia el cumplimiento de sus objetivos institucionales y la contribución de estos a los fines esenciales del Estado; y está basado en los principios de autocontrol, autorregulación y autocontrol establecido por el decreto 1599 de 2005.

Tabla 1. Normatividad aplicable a la CGR

Descripción	Norma	Observaciones
Valores, principios, derechos y deberes constitucionales relacionados con el Estado Social de Derecho, los derechos y garantías individuales, derechos colectivos, organización del Estado y funciones de la Contraloría General de la República	Constitución Política de Colombia, artículos 1, 2, 15, 20, 23, 27, 53, 54, 74, 83, 86, 87, 88, 93, 113, 117,119, 267, 268, 269, 354	Se destacan los artículos 15, 20, 74 que tratan sobre datos personales e información pública. El artículo 267 le confiere autonomía administrativa y presupuestal a la CGR. El artículo 27 garantiza las libertades de enseñanza, aprendizaje, investigación y cátedra. Los artículos 53 y 54 sobre las garantías de capacitación y entrenamiento, así como la obligación de ofrecer formación y habilitación profesional y técnica El artículo 88 sobre la protección de intereses y derechos sobre el patrimonio, espacio y seguridad.

Por el cual se dictan normas sobre organización y funcionamiento de la Contraloría General de la República, se establece su estructura orgánica, se fijan las funciones de sus dependencias y se dictan otras disposiciones"	Decreto 267 de 2000, artículos 3, 5, 9, 30 a 35, 48, 50, 51 a 55, 62 a 64	Establece los objetivos, funciones generales, criterios para la organización, sectorización y planeación de la vigilancia de la gestión fiscal; funciones Oficina de Planeación, funciones Oficina de Sistemas, funciones Contralorías Delegadas para la vigilancia fiscal, funciones Contralorías Delegadas Generales.
Sobre la organización del sistema de control fiscal financiero y los organismos que lo ejercen	Ley 42 de 1993	Sujetos de control fiscal, principios, sistemas y procedimientos técnicos, contabilidad presupuestaria, registro de la deuda, certificaciones, auditaje e informes; de las contralorías territoriales; jurisdicción coactiva, y sanciones.
Por la cual se dictan normas orientadas a fortalecer los	Ley 1474 de 2011, artículos 124,126, 128, 129	Regulación del proceso auditor; sistemas de información; fortalecimiento institucional de la

mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública		Contraloría General de la República; planeación estratégica en las contralorías territoriales. Creación de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático
Por la cual se modifican parcialmente los Decretos-Ley 267 y 271 de 2000 y se crea la dependencia denominada "Centro de Estudios Fiscales (CEF)" de la Contraloría General de la República, se establecen sus funciones y se dictan otras disposiciones	Ley 1807 de 2016	Definir la orientación académica fundamentada en la pertinencia de los objetivos, los contenidos, la metodología y las competencias esperadas del proceso de investigación como fundamento de los procesos de formación.
Reglamente el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales	Ley 527 de 1999	Principio de equivalencia funcional de la autenticación electrónica
Concepto favorable a la nación para contratar un empréstito externo con la banca multilateral	Documento CONPES 3841 de 2015	Fortalecer la planeación, ejecución y seguimiento de las acciones de control fiscal.

hasta por usd 30 millones, o su equivalente en otras monedas, destinado a financiar el programa de fortalecimiento institucional de la Contraloría General de la República		Optimizar la gestión de la información de la CGR Optimizar los mecanismos a través de los cuales la CGR divulga información de interés público e interactúa con la ciudadanía,
Por la cual se dictan disposiciones sobre racionalización de trámites y Procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos	Ley 962 de 2005, artículos 6, 7, 8 y 14	Será permitido el intercambio de información entre entidades oficiales, en aplicación del principio de colaboración, mediante sistemas telemáticos compatibles que permitan integrar y compartir información de uso frecuente y el fortalecimiento tecnológico.
Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones	Ley 594 de 2000	Art 19. Las entidades del estado podrán incorporar tecnologías de avanzada en la administración y conservación de sus archivos, empleando cualquier medio

		técnico, electrónico, informático, óptico o telemático
Código Penal	Ley 599 de 2000	
Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal.	Ley 1032 de 2006	Violación a los mecanismos de protección de derecho de autor y derechos conexos, y otras defraudaciones
Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Ley 1437 de 2011, artículos 5, 7,8, 35, 53 a 64	Art 60. Sede electrónica. Toda autoridad deberá tener al menos una dirección electrónica. La autoridad respectiva garantizará condiciones de calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad de la información de acuerdo con los estándares que defina el Gobierno Nacional. Podrá establecerse una sede electrónica común o compartida por varias autoridades, siempre y cuando se identifique claramente

		quién es el responsable de garantizar las condiciones de calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad.
Importancia de la estrategia de Gobierno en Línea	Documento CONPES 3650 de 2010	Plataforma de interoperabilidad y de infraestructura tecnológica y de servicios
Lineamientos de Política para Ciberseguridad y Ciberdefensa	Documento CONPES 3701 de 2011	Implementa instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional
Concepto favorable a la nación para contratar un empréstito externo con la banca multilateral hasta por USD 30 millones, o su equivalente en otras monedas,	Documento CONPES 3841 de 2015	Fortalecer la planeación, ejecución y seguimiento de las acciones de control fiscal, Optimizar la gestión de la información de la CGR para el

destinado a financiar el programa de fortalecimiento institucional de la Contraloría General de la República		mejoramiento de la eficiencia Optimizar los mecanismos a través de los cuales la CGR divulga información de interés público e interactúa con la ciudadanía
Declaración de la importancia estratégica del proyecto de Fortalecimiento Institucional de la Contraloría General de República-Préstamo BID	Documento CONPES 3922 de 2018	Garantizar la integración de los sistemas y aplicaciones para soportar los procesos misionales. Fortalecer la sistematización de los procesos de gestión de sujetos de control, rendición de cuentas e informes. Desarrollar un sitio alterno para la implementación del plan de recuperación de desastres asegurando la disponibilidad y continuidad de los servicios de tecnologías de la información de la Implementar una estrategia de datos abiertos para promover la transparencia y la participación ciudadana

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales	Ley 1266 de 2008	Regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios
Por la cual se dictan disposiciones generales para la protección de datos personales	Ley 1581 de 2012	
Por el cual se reglamenta parcialmente la Ley 1581 de 2012	Decreto 1377 de 2013	Establece la forma como debe obtenerse la autorización para el tratamiento de datos personales, las políticas de tratamiento, los derechos de los titulares, la transferencia internacional de datos personales y la responsabilidad demostrada frente al tratamiento
Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos	Decreto 886 de 2014	Serán objeto de inscripción en el Registro Nacional de Bases de Datos, las bases de datos que contengan datos personales cuyo

		Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano
Por la cual se expide el Código Disciplinario Único	Ley 734 de 2002, artículo 34	Sobre los deberes del servidor público respecto a la gestión de información
Por medio de la cual se modifica el Código Penal	Ley 1273 de 2009	Se crea un nuevo bien jurídico tutelado - denominado *"de la protección de la información y de los datos"*, y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Guía para la administración del riesgo y el diseño de controles en entidades públicas	Versión 4.0	Administración de riesgos de gestión, corrupción y seguridad digital. Riesgo de seguridad digital: combinación de amenazas y

		vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Por el cual se organiza un sistema de aseguramiento de la calidad, almacenamiento y consulta de la información básica colombiana y se dictan otras disposiciones	Decreto 3851 de 2006	Define un sistema administrativo de información oficial básica, de uso público, consistente en una arquitectura de información estandarizada, apta para la transmisión, aseguramiento de calidad, procesamiento, difusión e intercambio electrónico de datos entre generadores y usuarios. En cumplimiento de trámites oficiales, las entidades públicas consultarán en la Infraestructura Colombiana de Datos (ICD) la información básica requerida respecto de las personas, y solo en caso de que no se halle allí disponible podrán demandarla a los particulares.

Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas	Decreto 235 de 2010	Para efectos del intercambio de Información, las entidades [estatales] a que hace referencia el artículo anterior deberán establecer mecanismos magnéticos, electrónicos o telemáticos para integrar, compartir y/o suministrar la información que por mandato legal se requiere, o permitir el acceso total …
Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional	Ley 1712 de 2014	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información
Por el cual se reglamenta parcialmente la Ley 1712 de 2014, en lo relacionado con la gestión de la información pública	Decreto 103 de 2015	

Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones	Decreto 1078 de 2015	Las entidades públicas deben realizar la implementación del Modelo de Seguridad y Privacidad de la Información
Política Nacional de Seguridad Digital	Documento CONPES 3854 de 2016	Estrategia E.25 promover en los diferentes niveles de formación comportamientos responsables en el entorno digital
Por el cual se crea el sistema nacional de capacitación y el sistema de estímulos para los empleados del Estado	Decreto 1567 de 1998	Art 11. Obligaciones de las Entidades. Es obligación de cada una de las entidades: a) Identificar las necesidades de capacitación, utilizando para ello instrumentos técnicos que detecten las deficiencias colectivas e individuales, en función del logro de los objetivos institucionales; …
Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública	Decreto 1083 de 2015, artículos 2.2.4.7 y 2.2.4.8	Los programas de capacitación deberán orientarse al desarrollo de las competencias laborales necesarias para el desempeño de

		los empleados públicos en niveles de excelencia. Define las competencias laborales comunes y por nivel jerárquico de los servidores públicos.
Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el Fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones	Decreto 415 de 2016, artículo 2.2.35.3.	Adelantar acciones que faciliten la coordinación y articulación entre entidades del sector y del Estado en materia de integración e interoperabilidad de información y servicios, creando sinergias y optimizando los recursos para coadyuvar en la prestación de mejores servicios al ciudadano. Desarrollar estrategias de gestión de información para garantizar la pertinencia, calidad, oportunidad, seguridad e intercambio con el fin de lograr un flujo eficiente de

		información disponible para el uso en la gestión y la toma de decisiones en la entidad y/o sector. Proponer e implementar acciones para impulsar la estrategia de gobierno abierto mediante la habilitación de mecanismos de interoperabilidad y apertura de datos que faciliten la participación, transparencia y colaboración en el Estado.
Por el cual 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 número 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la	Decreto 1413 de 2017	En el parágrafo del artículo 2.2.17.1.2 señala que la implementación de los servicios ciudadanos digitales en las Ramas Legislativa y Judicial, en los órganos de control, los órganos autónomos e independientes, y demás organismos del Estado no contemplados en este artículo, se

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.		realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en el artículo 209 de la Constitución Política.
Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones	Decreto 1008 de 2018	Establece el objeto, alcance, principios y elementos de la política de gobierno digital.
Por la cual se crea el Sistema de Gestión de Seguridad, se crea el Comité de Gestión de Seguridad de la Contraloría General de la República, se adopta la política general de seguridad, la política	Resolución Organizacional OGZ-0531-2016	Formalización del gobierno de la seguridad de personas, bienes e información.

de seguridad y privacidad de la información, la política de tratamiento de datos personales y se dictan otras disposiciones		
Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.	Ley 1928 de 2018	Su objetivo es unificar la política penal para hacerle frente a la ciberdelincuencia, incluyendo el deber de velar por los derechos del correcto uso y avance de las tecnologías de la información. Este proceso de adhesión ya cuenta con concepto favorable por parte de la Corte Constitucional

Política Nacional de Explotación de Datos (Big Data)	Documento CONPES 3920 de 2018	Masificar la disponibilidad de datos de las entidades públicas que sean digitales accesibles, usables y de calidad. Generar seguridad jurídica para la explotación de datos. Disponer de capital humano para generar valor con los datos. Generar cultura de datos en el país. El capital humano requerido para la explotación de datos no se limita a los profesionales en TI, haciéndose necesarios perfiles cualificados en todo el ecosistema.

Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad"	Ley 1955 de 2019, artículos 147, 148 y 332	Transformación Digital Pública con la aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital. La política de Gobierno Digital debe contemplar como acción prioritaria el aprovechamiento de tecnologías emergentes, el incremento en la seguridad digital y el fomento a la participación y la democracia por medios digitales. Reestructuración de la CGR, crear la Dirección de Información, Análisis y Reacción Inmediata (DIARI), modificar o establecer sus funciones y su planta de

		personal creando los empleos a que haya lugar
Por medio del cual se reforma el Régimen de Control Fiscal	Acto Legislativo 04 de 2019. Artículos 1 al 6	Reforma los artículos 267, 268, 271, 272 y 274 de la Constitución
Por el cual se desarrolla la estructura de la Contraloría General de la República, se crea la Dirección de Información, Análisis y Reacción Inmediata y otras dependencias requeridas para el funcionamiento de la Entidad.	DECRETO <LEY> 2037 DE 2019	Artículo 3: Dirección de información, análisis y reacción inmediata. Son funciones de la Dirección de Información, Análisis y Reacción Inmediata

Fuente: Elaboración propia

Después del análisis documental de la anterior normatividad, en el marco de este trabajo son de especial relevancia: el documento CONPES 3854 que define la Política de Seguridad Digital que establece como uno de sus principios fundamentales el asegurar una responsabilidad compartida entre las múltiples partes interesadas, promoviendo la máxima colaboración y cooperación para la gestión de riesgos digitales para lograr su objetivo general de "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" (DNP, 2016). La anterior política pública recibe un espaldarazo por parte del actual Plan Nacional de Desarrollo "Pacto por Colombia, Pacto por la Equidad" con la obligatoriedad de las entidades del orden nacional de incorporar la transformación digital usando el principio de una adecuada gestión de la seguridad digital para generar confianza y proteger los datos personales y la responsabilidad de Sector de la Función Pública de la formación del personal establecida en el decreto 1083 de 2015, así como la definición de las competencias laborales comunes a todos los servidores públicos: aprendizaje continuo, orientación a resultados, orientación al usuario y al ciudadano, compromiso con la organización, trabajo en equipo y adaptación al cambio; y las que corresponden al nivel jerárquico profesional: aporte técnico-profesional, comunicación efectiva, gestión de procedimientos e instrumentación de decisiones.

En este punto de la investigación, se cuenta con elementos que dan indicios significativos de la importancia del tema de la adecuada gestión de los riesgos de seguridad digital, para lo cual se continua con la identificación de las necesidades sentidas por la comunidad de la CGR, para lo cual se procedió a hacer trabajo de campo con el fin de tener más fuentes e instrumentos de captura de información y poder hacer el proceso de triangulación.

3.4 Necesidades comparativas

El producto 5.5.2 del plan estratégico institucional (CGR, 2018) es un sistema de gestión de seguridad alineado con la NTC-ISO-IEC 27000 para la seguridad de la información, teniendo

en cuenta que dicho documento hace referencia a una familia de normas que establecen estándares, se resumen en la tabla 3 las que son de interés para este trabajo.

Tabla 2 Normas relevantes de la familia ISO 27000

Norma	Descripción
NTC-ISO/IEC 27001	Requisitos para sistemas de gestión de la seguridad de la información
GTC-ISO/IEC 27002	Código de práctica para controles de seguridad de la información.
NTC-ISO/IEC 27005	Gestión del riesgo en la seguridad de la información. Incluye un catálogo de amenazas y vulnerabilidades
ISO/IEC 27014	Gobierno de la seguridad de la información para los procesos de evaluar, dirigir, monitorear y comunicar.
ISO IEC/27031	conceptos y principios de la disponibilidad de las TIC para la continuidad del negocio
ISO IEC/27032	Estandariza los lineamientos para aplicar y mejorar el estado de ciberseguridad e involucrar diferentes aspectos técnicos.

ISO IEC/27701	Protección de la privacidad, incluida la forma en que las organizaciones deben gestionar la información personal y demostrar el cumplimiento de la normativa en privacidad de la información

Fuente: Elaboración propia a partir de (ICONTEC, 2017)

Teniendo en cuenta que la ciberseguridad es un tema globalizado, la Unión Internacional de Telecomunicaciones para aumentar la conciencia de la ciberseguridad y medir el compromiso de los países con la ciberseguridad publica un informe anual del Índice Global de Ciberseguridad, a partir de cinco indicadores que son la parte legal, medidas técnicas, medidas organizacionales, construcción de capacidades y cooperación, Colombia ha pasado del puesto 46 en el año 2017 (ITU, 2018) al 73 en el 2018 (ITU, 2019) en el ranking global, a nivel continental bajo del puesto 6 al 7, el punto a resaltar es que el veinte por ciento del índice corresponde a la construcción de capacidades, la cual incluye campañas de concientización pública, la certificación y acreditación de profesionales, cursos de capacitación profesional y programas educativos en el ámbito de la ciberseguridad.

Los países europeos llevan la delantera en dicho índice, una de sus instituciones es la Agencia de Seguridad de las Redes y de la Información de la Unión Europea, la cual publicó a finales del año pasado una guía sobre aspectos comportamentales de la ciberseguridad (ENISA, 2018), documento que realza la importancia del factor humano y cultural, ya que las medidas administrativas y tecnológicas no operan en el vacío y deben armonizarse con las personas.

Propone que el punto de partida para cualquier organización es comprender su estado actual de ciberseguridad y las formas en que los factores humanos pueden apoyar o restar valor.

Por otro lado el Modelo de Madurez de Capacidad de Seguridad Cibernética para las Naciones desarrollado (Global Cyber Security Capacity Centre, 2017) que ha sido usado por varios organismos internacionales, como la OEA y el BID, establece cinco dimensiones entre las que se destacan la de cibercultura y sociedad, donde se hace énfasis en el novel de riesgos de la sociedad, el conocimiento sobre la protección de datos personales y los mecanismos de denuncia de los cibercrímenes, y por otro lado la dimensión de educación, capacitación y habilidades en ciberseguridad, la cual revisa programas de sensibilización en este tema, evaluando su disponibilidad, calidad y oferta en el sector privado y público.

Así las cosas, es una tendencia global considerar los siguientes elementos para la creación de una cultura de seguridad de la información: conciencia, responsabilidad, respuesta, ética, democracia, evaluación de riesgos, diseño y puesta en práctica de la seguridad, gestión de la seguridad y reevaluación. La teoría del aprendizaje social (Ellinger, 2004) plantea cómo percepción de las habilidades de las personas en sí mismas afectan su motivación y acciones. Propone que el comportamiento individual en el dominio de la seguridad de la información y el comportamiento responsable de los usuarios en el aseguramiento y mitigación del riesgo, que se complementa con la teoría del comportamiento planeado (Ajzen, 1991) la cual pretenden medir como se guían las acciones humanas y predice los comportamientos particulares intencionados, así estos permiten ejercer el control propio donde el eje clave es la intención de comportamiento.

Propone tres tipos de creencias: comportamiento, normativa y de control, y concluye que el logro del comportamiento depende de la motivación y la capacidad.

En ese sentido la teoría de la motivación a la protección explica cómo influyen las invocaciones de miedo en las actitudes y conductas de salud (Prentice-Dunn, 1986) (Campis, Lyman, & Prentice-Dunn, 1986) y como se evalúa una amenaza según se percibe su gravedad, susceptibilidad y ocurrencia. Se evalúa la respuesta recomendada y la autoeficacia para mitigar la amenaza. Las personas comprenden los términos de seguridad comunes y usan las precauciones recomendadas. Son capaces de evaluar las amenazas y los procesos de afrontamiento respecto al comportamiento de seguridad. (Anderson & Agarwal, 2010). Para mejorar el comportamiento se aplican elementos de la teoría de la autoeficacia. (Bandura, 1977) cuya propuesta de valor es que el comportamiento preventivo depende de tres factores: 1) La comprensión de que la persona está en riesgo. 2) Del cambio de comportamiento y 3) La adopción de un comportamiento preventivo o abstención de comportamientos riesgosos. Así las personas realizan un cálculo mental de las recompensas y los costos asociados con el comportamiento tanto seguro como inseguro. Llegando a tener la hipótesis de mejorar los comportamientos responsables al interior de la CGR con el modelo de la apropiación tecnológica (Quezada & Garbajosa, 2015), donde la tecnología pasa de ser desconocida a ser un elemento cotidiano en la vida de las personas. Las nuevas tecnologías se adaptan a las necesidades humanas y a las condiciones del entorno. Este proceso puede ser reversible e incluso desapropiable, la obsolescencia trae como consecuencia la adopción de nuevas alternativas.

3.5 Necesidades sentidas

Con el enfoque mixto planteado en el marco metodológico, continuando con el componente cuantitativo se realizó una encuesta para recabar información sobre tres elementos: el nivel de conciencia y apropiación (preguntas 1, 2 y 4), la gobernanza interna de la gestión del riesgo (preguntas 5 y 6) y la percepción sobre el desarrollo de competencias (pregunta 3), debido a que el instrumento anterior fue de carácter obligatorio, esta encuesta es aplicada a muestra aleatoria probabilística (Triola, 2009) definida de la siguiente manera:

$$n = \frac{N * Z^2 * p * (1 - p)}{e^2(N - 1) + (Z^2 * p * (1 - p))}$$

Donde **N** es el tamaño de la población 4122, e es el margen de error del 7%, **Z** valor de la distribución normal 1,56 que corresponde a un nivel de confianza del 88%, y **p** es la variación positiva 0,5, con un resultado final de la muestra probabilística **n** con un valor de 121.

Al aplicar el instrumento el 45,54% contestó la pregunta abierta (Si tiene propuestas para mejorar la gestión en riesgos digitales en la CGR, por favor cuéntenos) de los cuales el 67,39% propone mejorar los niveles de concientización, cultura y capacitación. Los datos muestran un buen nivel de conciencia y autocritica personal con un 97% y percepción de la gobernanza pues identifican institucionalmente los responsables con un 82,2%, aproximadamente el 61,4% considera que debe mejorar sus competencias sobre el tema y el 55,4% considera que la CGR no

tiene un buen proceso de gestión de riesgos digitales. La tabulación de los resultados se muestra en la tabla número tres.

Tabla 3 Tabulación de la encuesta

Pregunta	Opciones	Porcentaje
1. ¿Considera que la entidad puede estar expuesta a riesgos digitales?	SI	97,0%
	NO	3,0%
2. ¿Considera que los riesgos digitales pueden afectarle en lo laboral y/o personal?	En lo laboral	17,8%
	En lo personal	5,0%
	En lo personal y en lo laboral	75,2%
	No me afectan	2,0%
3. ¿Considera que tiene la capacitación y los conocimientos suficientes para gestionar los riesgos digitales en su entorno laboral?	SI	38,6%
	NO	61,4%
4. ¿Conoce usted algún caso en la CGR que haya involucrado algún riesgo digital a nivel institucional?	SI	41,6%
	NO	58,4%
5. ¿Sabe quién (o qué dependencia) es la encargada de la gestión de riesgos digitales en la entidad?	SI	82,2%
	NO	17,8%
6. ¿Considera que la CGR tiene una buena gestión de los riesgos digitales?	SI	44,6%
	NO	55,4%

Fuente: Elaboración propia

A partir de los resultados anteriores se realizan dos grupos focales con cinco personas cada para indagar las variables cualitativas (Flick, 2006), que representan a los funcionarios de distintas áreas. Para la selección de los participantes se estableció un perfil que permitiera cubrir

las edades y profesiones establecidas en el análisis descriptivo multivariado, con el fin de tener distintos puntos de vista. Cada grupo focal se desarrolla propiciando la discusión abierta para profundizar sobre los resultados de la encuesta, con un adecuado uso del tiempo, posibilitando la participación libre y espontánea de los participantes. Los resultados obtenidos se centran en los aspectos que mostraron mayor ocurrencia los cuales son: más información general acerca de los riesgos, sensibilización al interior de la entidad a través de varios medios destacándose las charlas y los cursos virtuales; formación especializada y focalizada y contar con información permanente y actualizada de los distintos tipos de riesgo y cómo actuar ante estos, además identifican las amenazas como*: hackers, malware, phishing*, problemas con la privacidad de datos personales y pérdida de información.

Respecto al primer grupo focal con los funcionarios realizado, se tienen las siguientes percepciones frente a las preguntas de la encuesta (Grupo Focal Número 1, 2017) . El primer aspecto tratado fue la percepción de afectación que pueden tener los riesgos digitales en la vida personal y laboral. los funcionarios reportan a nivel personal que existen riesgos que pueden afectar la pérdida de información o el acceso a la misma por personas que pueden usarla de mala manera.

Desde la experiencia de los participantes, uno de ellos reporta un evento donde el acceso a un sitio de descarga de música permitió la propagación de un virus en su computador. Otro de los participantes reporta que el no haber seguido buenas prácticas le resultó en una pérdida de información de trabajo:

"A mi si se me 'virusió' el computador porque yo no seguí a las seguridades que tocaban, que eran las debidas y me deje llevar del día a día y pues entonces no guarde la información y ahí fue grave por que perdimos el trabajo como de 10 horas que teníamos que entregar una información para tomar decisiones. " (Grupo Focal Número 1)

Desde el conocimiento de amenazas digitales en general, los participantes reconocen algunos eventos donde la información de usuarios fue comprometida de alguna forma por redes sociales:

"Por ejemplo en Facebook, la vez que se filtró la información de la mayoría de los usuarios… o por ejemplo una vez vi una noticia de un canal de citas que reveló todo y pues generó problemas de todo tipo: de parejas, de dinero, de trabajo" (Grupo Focal Número 1)

Uno de los participantes también afirma que conoció a una persona que hacía parte de un grupo de *hackers* que publicaba una lista de sitios atacados. El participante reconoce que los ataques de *hackers* son muy cercanos a el mismo y que inclusive se le invitó a participar.

Otro de los participantes relaciona como riesgo digital el acceso que tienen los menores de edad a las redes sociales, especialmente señala que los niños pueden suministrar información que podría ser usada para extorsionarlos. Señala también que el acceso no autorizado a las cámaras de dispositivos, a información de tarjetas de crédito, suplantación de sitios web por medio de *phishing*.

Otro elemento considerado riesgoso por uno de los participantes es el hecho de que los sistemas registren información biométrica y del comportamiento de las personas:

> "Y yo siento también que desde los mismos creadores se pueden generar esos riesgos, no sé si son esperados o no, eso de uno vaya metiendo la huella, eso del reconocimiento facial, la voz ese aparatico que tiene Google que uno habla y te dice todo, pues que tenga todas tus conversaciones, que tenga todo de ti; eso es un riesgo tenaz porque saben todo de ti … todo…" (Grupo Focal Número 1)

También los participantes señalan los peligros de la publicación de información personal en las redes sociales, pero al mismo tiempo consideran que no son conscientes a la hora de usar dichos servicios:

> "Uno no mide el riesgo de seguridad para uno mismo, por ejemplo, en Facebook que uno se deja llevar por la emoción de publicar lo que no debe de uno mismo, de la familia, las fotos, los lugares, que después van en contra de uno mismo, pero uno no lo mide porque uno se deja llevar de la emoción …" (Grupo Focal Número 1)

Sobre la capacitación y el conocimiento para gestionar los riesgos digitales, el grupo focal de funcionarios reporta que no tiene los conocimientos para enfrentarlos. Uno de los participantes dice que le enseñaron a reportar a la USATI cuando hay una posible amenaza. Otro participante señala las herramientas de antivirus como una manera de gestionarlo, pero resalta que él no "ser tan ingenuo" es algo que se ha tratado de enseñar y que puede ayudar.

Otro participante reporta que en su caso ni siquiera utiliza una herramienta de antivirus:

"Y ni siquiera antivirus, porque digamos con un computador marca Mac uno se siente seguro … yo no le he hecho nada, yo nunca le he puesto antivirus y yo bajo todo lo que tenga que bajar y ni idea" (Grupo Focal Número 1)

También se afirma que usualmente se descargan aplicaciones sin saber muy bien que pueden contener:

"Uno siempre ha escuchado que a Mac no le entran virus por nada del mundo, pero cuando uno quiere descargar aplicaciones, uno tiene que descargar esa de Mac Keeper como requisito, entonces uno no tiene ni idea que descarga o cuando le da solamente aceptar, aceptar, aceptar con tal de descargar lo que necesita. Como que uno no mide ese tipo de riesgos, sino que uno descarga, le da aceptar y punto." (Grupo Focal Número 1)

De estos testimonios se puede ver que los participantes expresan no ser conscientes de ese tipo de riesgos o no sabrían que hacer para enfrentarlos. Incluso en ocasiones deciden ignorar estos peligros. Sin embargo, los participantes manifiestan que sería importante tener capacitación sobre temas asociados al riesgo digital:

"Me parece que si [Quisiera recibir capacitación], pero de una manera práctica, porque yo siento que ese tema es muy lejano a mí, como que yo digo: Fijo van a sacar un manual o un texto por allá que eso es inentendible, entonces yo propondría algo que fuera así como muy didáctico y como ya, soluciones concretas a posibles problemas. Obviamente siempre van a salir como algo que excede los límites que uno se imagina porque siempre

hay cosas inimaginables, pero si como un recetario: con esto haga esto, y esto … muy didáctico, o sea como que sea de fácil acceso y sin enredos." (Grupo Focal Número 1)

Del anterior testimonio también se puede interpretar que los participantes valorarían guías prácticas que les permitan entender el riesgo digital y cómo afrontarlo. También se señala que estas guías deberían ser segmentadas para los diferentes tipos de persona y la información que usan. Los siguientes testimonios apoyan la necesidad de enseñanza y difusión.

"Hay que concientizar a todo el mundo que la usa [la tecnología], de los riesgos de que hay que saberse proteger" (Grupo Focal Número 1)

"Hacer más difusión para que la gente no esté tan desprevenida y tan confiada pues porque nos apasiona el mundo digital y entre más vamos adentrándonos no medimos el riesgo sino se vuelve casi una adrenalina. Entonces que haya como muchas campañas que alerten a la gente que también está asumiendo un riesgo " (Grupo Focal Número 1)

Respecto al segundo grupo focal con el personal de la USATI como grupo de control (Grupo Focal Número 2, 2017), se tienen las siguientes percepciones frente a las preguntas de la encuesta. Sobre la percepción de la exposición a riesgos digitales, el grupo focal de funcionarios reporta que uno de los factores de riesgo es el hecho de que muchas de las personas de la entidad no tienen el conocimiento o experiencia en riesgos digitales.

"En la entidad hay personas con diferentes especialidades y profesionales en diferentes ramas, pero muchos de ellos no tienen experiencia ni el conocimiento en este tipo de riesgos informáticos" (Grupo Focal Número 2)

"La gran mayoría de abogados, ellos poco de sistemas entonces ignoran esos riesgos a nivel informático y así en muchísimos campos porque tenemos profesionales de todo tipo" (Grupo Focal Número 2)

Sobre la capacitación y el conocimiento para gestionar los riesgos digitales, el grupo focal reporta la necesidad de formación técnica específica para los roles que tienen responsabilidades en el área de TIC, pero también sensibilización al resto del personal.

"Un poco más de capacitaciones especializadas, ISO 27001, análisis de riesgos informáticos" (Grupo Focal Número 2)

"Sería importante aprender desde lo básico hasta lo específico, para tener esos conocimientos y aplicarlos a las necesidades" (Grupo Focal Número 2)

"Para la generalidad de los funcionarios de la entidad se debe continuar con la sensibilización de la amenaza real y como deben afrontarlas" (Grupo Focal Número 2)

Dentro de estas necesidades de formación, se expresa que una intención de capacitación virtual podría ser una solución útil. Una de las características que se señalan es que un posible esquema de capacitación virtual sea constantemente actualizado y que motive a la comunidad a revisarlo.

"Sería tener una herramienta que nos brinde la posibilidad de estar en constante aprendizaje, herramientas virtuales por ejemplo para hacer inducción a los nuevos funcionarios" (Grupo Focal Número 2)

"ya teniéndolas herramientas necesarias para la autocapacitación o capacitación pues es necesario mantenerla actualizada y motivar a toda la comunidad" (Grupo Focal Número 2)

"por ejemplo con cursos virtuales de carácter obligatorio para todos los funcionarios en el tema de seguridad sería una buena forma de hacerlo" (Grupo Focal Número 2)

De los anteriores testimonios, se puede interpretar la necesidad de diseñar un espacio de capacitación y sensibilización acerca de temas de riesgo digital.

Sobre la percepción de la exposición a riesgos digitales, el grupo focal reporta que ha atendido varios incidentes asociados con riesgos digitales. Además de ello, reportan que es común que sucedan intentos de ataque y son reportados a diario en la entidad. Algunos de los intentos reportados son *phishing*, *ransomware* y *spam*.

"personalmente he tenido que atender varios incidentes de ciberseguridad, recientemente por ejemplo tuve que atender un incidente de *ransomware* en una de las gerencias departamentales, que afecto a por lo menos la mitad de los equipos de esa gerencia" (Grupo Focal Número 2)

"He tenido conocimiento que prácticamente a diario ocurre uno o dos incidentes, pero son intentos, es decir algunos de nuestros funcionarios accede por ejemplo a una página que se sabe es maliciosa" (Grupo Focal Número 2)

> "eventos suceden todos los días, pero incidentes graves realmente han sido pocos en los últimos años" (Grupo Focal Número 2)

> "he tenido conocimiento que, de diferentes sitios del mundo, en especial de Japón y China envían pues diferentes intentos de acceder a nuestra plataforma" (Grupo Focal Número 2)

> "tenemos un sinnúmero de correos tipo spam, que están afectando a gerencias y a nivel central" (Grupo Focal Número 2)

Acorde a la metodología de un enfoque mixto, se recurre a la entrevista con un experto en la materia para poder así dar una mayor precisión sobre los diversos elementos permiten determinar las necesidades comparativas para proceder a triangular los resultados obtenidos hasta el momento. El experto es el exjefe de la USATI el Ingeniero William Fernando Halaby Rodríguez quien ha laborado más de 20 años en el sector público en temas de seguridad de la información principalmente en el Banco de la República, según sus palabras su experiencia:

> "ha sido forjadora y ejemplo para muchos profesionales y la mayoría de estos años he sido docente en varias de las universidades del país" (Entrevista con William Fernando Halaby Rodríguez, 2017)

Ante la pregunta sobre las amenazas a las que se ve enfrentado en su trabajo en entidades públicas y a nivel personal manifiesta que:

> "es claro que el mundo cibernético tiene relevancia, ya no hay nadie que no tenga su información en un dispositivo informático" (Entrevista con William Fernando Halaby Rodríguez, 2017)

> "cuando no se protege bien puede ser el fracaso, la quiebra o la desaparición de un ente estatal" (Entrevista con William Fernando Halaby Rodríguez, 2017)

> "la principal amenaza es no tener el personal capacitado ni las herramientas necesarias para protegerse"

> "el punto más débil siempre serán las personas … la principal vulnerabilidad está relacionada con el tema de falta de conocimiento y prevención que tienen los usuarios" (Entrevista con William Fernando Halaby Rodríguez, 2017)

Establecida la problemática comparativa por él, se indaga sobre las formas de enfrentar la situación, dónde propone el balance de trabajar en un triángulo de personas, procesos y herramientas, enfatizando el trabajo sobre el nivel de competencias de las personas, tratando de dar alto cubrimiento a costos razonables, usando herramientas de las TIC:

> "indudablemente el tema de las personas es vital, las herramientas se adquieren, los procesos están establecidos, pero no se ejecutan solos, siempre detrás de eso están las personas" (Entrevista con William Fernando Halaby Rodríguez, 2017)

"es imposible para entidades muy grandes estar realizando permanentemente charlas para todos los empleados y tenerlos sentados todo el tiempo se vuelve inefectivo" (Entrevista con William Fernando Halaby Rodríguez, 2017)

"es importante crear estrategias novedosas, usar las herramientas tecnológicas para crear cursos interactivos en la red" (Entrevista con William Fernando Halaby Rodríguez, 2017)

"es clave un buen diseño de un material que sea ameno, no ladrilludo en el cual la gente entre y aprenda de verdad" (Entrevista con William Fernando Halaby Rodríguez, 2017)

Finalmente expresa que también esto debe llegar a la ciudadanía, quien es una parte muy importante a tener en cuenta por todas las entidades del sector público, pues su objetivo primordial es darle servicio al ciudadano colombiano, expresa que:

"todas las entidades tenemos un tema de responsabilidad social, sería altamente valioso la difusión de temas de seguridad, si ya las hemos diseñado para usuarios internos, podemos ponerlas al servicio de la ciudadanía" (Entrevista con William Fernando Halaby Rodríguez, 2017)

3.6 Competencias para la CGR

En el primer capítulo se mencionó que la gestión de competencias, se tiene en cuenta una serie de acciones que llevan al desarrollo del talento humano en cada una de sus dimensiones, considerando sus capacidades y la motivación de incrementar su desempeño, es claro que sin una formación adecuada, los funcionarios pueden convertirse rápidamente en fuentes de riesgo dentro

de la institución, propiciando la ocurrencia de incidentes o creando vulnerabilidades que los adversarios puedan utilizar para violar las distintas medidas de seguridad.

Para contar con la trilogía de que las personas deben estar en capacidad de ser, hacer y saber, utilizando el enfoque integral de (Cequea, Rodríguez Monroy, & Núñez Bottini, 2011) apuntando a la productividad en los ámbitos de la gestión del riesgo digital, la productividad organizacional está esencialmente determinada por su dimensión humana y los aspectos que hacen parte del contexto laboral, como lo son el clima organizacional, el liderazgo y la cultura corporativa. Dentro de los aspectos individuales se incluyen: la motivación y la satisfacción laboral, los cuales tienen relación con la identificación que tiene el trabajador con su cargo. La identificación del funcionario con su cargo depende en del conocimiento y las habilidades que tiene para desarrollarlo con buenos resultados y esfuerzo moderado.

Unido al concepto de productividad están los conceptos de mérito y valor público. El mérito es el principio orientador del ingreso y la permanencia en la carrera administrativa pues determina la imparcialidad en la calificación del servicio, con bases en principio de igualdad y dando un marco de moralidad, transparencia y eficiencia al desempeño de las labores estatales, mucho más relevante si lo entendemos desde el contexto de la CGR. Por su parte, el valor público se evidencia en la gestión institucional cuando logra dar respuestas efectivas y útiles a los ciudadanos; es decir, cuando hay compromiso con el impacto de resultados en las diferentes partes interesadas.

Durante el desarrollo del presente trabajo de grado, la CGR en la implementación del Programa de Fortalecimiento Institucional establecido por el CONPES 3841 (DNP, 2015) , por

medio de la ejecución del contrato CGR_BID 17 de 2018 cuyo objeto fue el de adelantar un diagnóstico para determinar el modelo de competencias requeridas para los recursos humanos asociados, principalmente, a los cuatro (4) procesos misionales de la Contraloría General de la República – CGR, estableció el siguiente conjunto de competencias laborales. Esta situación se capitalizó para armonizar tanto la ejecución contractual y los objetivos de esta investigación, estableciendo las siguientes competencias para la gestión de riesgo digital las cuales están alineadas con el Decreto 1083 de 2015 pero conservando la independencia administrativa y presupuestal de la CGR.

Las competencias organizacionales que son transversales a todos los servidores, que fueron determinadas son las siguientes:

Competencias Organizacionales Transversales:

1. Orientación al logro: Capacidad para realizar las labores y alcanzar los resultados propuestos, aun cuando se presenten dificultades, con eficacia, calidad y oportunidad.

   Conductas asociadas:

   - Supera las barreras que aparecen en la ejecución de los procesos en los que interviene.
   - Identifica riesgos que podrían interferir en el logro de los resultados y se prepara para asumirlos.
   - Asume retos que favorezcan el logro de sus objetivos en mejores condiciones.
   - Asume la responsabilidad por sus resultados.
   - Trabaja con base en objetivos claramente establecidos y realistas.

2. Integridad Institucional: Capacidad para obrar en armonía con los valores organizacionales, haciendo uso responsable y transparente de los recursos públicos, eliminando cualquier discrecionalidad indebida en su utilización.

   Conductas asociadas:

   - Preserva la razonabilidad, integridad, formalidad, validez, conservación, confidencialidad, privacidad, inteligibilidad y transparencia de los actos administrativos en los que participa.
   - Resguarda los activos y utiliza los recursos en las condiciones de funcionamiento y prestación, en que le fueron entregados.
   - Maneja con responsabilidad la información personal e institucionales de que dispone y facilita el acceso a la información relacionada con sus responsabilidades y el servicio de la entidad en la que se desempeña.
   - Organiza y custodia de forma adecuada la información a su cuidado, teniendo en cuenta las normas legales y de la organización.

3. Autoaprendizaje: Identificar, incorporar y aplicar nuevos conocimientos sobre regulaciones vigentes, tecnologías disponibles, métodos y programas de trabajo, para mantener actualizada la efectividad de sus prácticas laborales y su visión del contexto para incrementar su capacidad de realización y generación de ideas a partir de iniciativas personales.

   Conductas asociadas:

- Utiliza sus propias experiencias como lecciones aprendidas que utiliza para mejorar su gestión y que comparte abiertamente con otros.
- Busca información técnica o profesional que incorpora mediante ajustes a su gestión.
- Se mantiene en constante actualización, incorporando a su gestión nuevos conceptos, aplicaciones y formas innovadoras que contribuyen a la mejora continua.
- Mantiene sus competencias actualizadas en función de los cambios que exige la Administración pública en la prestación de un óptimo servicio.
- Comparte sus saberes y habilidades con sus compañeros de trabajo, y aprende de sus colegas habilidades diferenciales, que le permiten nivelar sus conocimientos en flujos informales de interaprendizaje.

Competencias para el nivel jerárquico profesional, independientes del macroproceso al que pertenezcan:

4. Pensamiento Crítico: Capacidad de valorar la información y las variables del proceso para distinguir entre información verdadera y falsa, contenidos apropiados y prejudiciales, y contactos confiables y cuestionables.

   Conductas asociadas:

   - Estructura en forma lógica y racional los planteamientos a situaciones difíciles o complejas.
   - Es capaz de establecer relaciones válidas entre los componentes de un problema y su contexto para reconocer la consistencia de la información.

- Realiza un análisis crítico constructivo de las decisiones o acciones orientadas para identificar riesgos o inconsistencias y notifica a quien corresponda cuando reconoce amenazas o vulnerabilidades.
- Realiza preguntas y búsquedas de información que permitan clarificar las dudas e inconsistencias que emergen de un problema.
- Realiza acciones recurrentes encaminadas a obtener la máxima y mejor información posible de todas las fuentes disponibles, necesaria en su gestión y en la de su equipo.

5. Comunicación Técnica: Capacidad para comunicar las ideas y argumentos que sustentan sus decisiones y su gestión recurriendo a un lenguaje propio de su tema de experticia, de acuerdo con las características y necesidades de sus interlocutores.

   Conductas asociadas:

   - Sustenta sus decisiones y actuaciones con argumentos claros y pertinentes.
   - Apoya en la comprensión de conceptos técnicos a personas que no tienen su nivel de experticia, utilizando ejemplos acordes a las posibilidades de comprensión de su interlocutor.
   - Propone acciones conjuntas con sus proveedores, clientes internos y externos encaminadas a armonizar los procesos, sistemas e interacciones que les afecten mutuamente.
   - Reconoce los grupos de interés de su gestión y procura mantener una interlocución clara y precisa sobre las condiciones de calidad esperadas.

- Realiza acciones recurrentes encaminadas a obtener la máxima y mejor información posible de todas las fuentes disponibles, necesaria en su gestión y en la de su equipo.

3.7 Resultados

Como producto del proceso de triangulación (Aguilar & Barroso, 2015) de fuentes usando distintos recursos humanos y escritos; del uso de varios métodos cuantitativos y cualitativos y de tiempo y espacio recolectando datos en varios momentos y lugares, se busca una mejor comprensión de la problemática, evitando el riesgo de la subjetividad del investigador o el sesgo de algún método o fuente. De acuerdo con el análisis realizado, se puede concluir que la CGR requiere de intervención frente a las siguientes necesidades:

1. Cubrimiento a nivel nacional: La CGR debe adelantar procesos de formación para todos sus servidores públicos, el análisis cuantitativo arroja que la mitad de las personas laboran en las gerencias departamentales, adicionalmente los procesos de formación y capacitación deben ajustarse a las realidades presupuestales y administrativas. Por lo cual se deben considerar estrategias y modelos que satisfagan esta situación que consideren las particularidades de las características identificadas en la población objetivo, especialmente las que tienen que ver con la edad, la profesión y la ubicación del centro de trabajo.
2. Cumplimiento normativo: La CGR debe velar por que la gestión de los procesos, la información y las tecnologías en general que apoyen la misión de la entidad, cumplan con el marco jurídico institucional y adopten todas las leyes, políticas, regulaciones existentes en el Estado Colombiano y los acuerdos internacionales relacionados con su gestión, en

especial con las nuevas responsabilidades del control preventivo y concomitante a través del uso intensivo de las TICs.

3. Generar conciencia sobre el riesgo digital: A pesar de la existencia de los riesgos digitales en la Entidad y la inminencia de que este tipo de riesgos se materialicen, expresada por los funcionarios, se puede interpretar una percepción de riesgo lejana y desatendida. Es imperativo que la orientación al logro y la integridad institucional contengan elementos que a nivel global son estándares, especialmente en el marco de la cuarta revolución industrial. Potenciado por el nuevo manual de funciones adoptado por medio de la resolución organizacional 745 del siete de febrero de 2020 que explicita la responsabilidad para la identificación, valoración y administración de los riesgos en la seguridad interna y externa, de los servidores, los bienes y la información de la Entidad, a fin de garantizar su adecuada protección y custodia de los funcionarios, especialmente los de la recientemente creada DIARI.
4. Promover la apropiación de elementos prácticos que permitan la gestión del riesgo digital: Una percepción común entre los funcionarios encuestados y los participantes de los grupos focales es la falta de herramientas para enfrentar los distintos riesgos de seguridad digital. Particularmente se expresa desconocimiento de los riesgos en sí, lo cual desencadena acciones de los servidores públicos que pueden poner en peligro tanto los activos de información de la CGR como los propios apalancando un ambiente que permita desarrollar pensamiento crítico.
5. Fortalecer el autoaprendizaje y la comunicación técnica: Estas son competencias que la CGR debe desarrollar en sus funcionarios, a través de un proceso de autoaprendizaje

guiado con una participación más proactiva que la mera asistencia a clases y generando espacios para una comunicación más asertiva tanto de forma oral como escrita. En línea con las orientaciones y directrices del CEF que, en el ámbito educativo de su competencia, tiene como objetivo realizar y fomentar la investigación que soporte el conocimiento en ciencia y tecnología y a través de ella la formación de alta calidad, propendiendo por la consolidación de una cultura respetuosa de la ética y los principios del Estado Social de Derecho, así como por la preparación de personal altamente calificado, en todos los niveles. Para ello podrá desarrollar y ejecutar proyectos de investigación, programas de estudio, formación, preparación y actualización permanente, apoyado en el desarrollo de tecnologías de la información y la comunicación.

4 Diseño de la mediación pedagógica

En el capítulo anterior, se establecieron las necesidades educativas, según ADDIE (Branson, y otros, 1975) para dar el siguiente paso, el cual es el diseño de una mediación pedagógica apoyada en recursos educativos digitales, se requiere resolver cuestiones acerca del qué se aprende, el ambiente en que esto sucederá, las actividades de aprendizaje que se llevarán a cabo y como evaluarlas. De acuerdo con ello, este capítulo contempla varios de estos elementos, guiados por principios de diseño que van desde lo pedagógico hasta lo logístico.

Como objetivos de formación se consideran los siguientes:

1. Adquirir conciencia sobre la existencia de riesgos digitales en el ámbito personal y laboral.
2. Identificar y gestionar riesgos digitales en sus actividades laborales.
3. Reconocer el marco legal colombiano que reglamenta las temáticas asociadas a la gestión de riesgos digitales y tratamiento de la información
4. Construir buenas prácticas de gestión de los riesgos digitales en la Entidad atendiendo los estándares internacionales.

Partiendo del marco de diseño conectivista (Siemens, 2013), se postulan algunos principios pedagógicos que guían el diseño de un MOOC, que aproveche las características de apertura, masividad y ubiquidad que lo definen.

- Búsqueda de la diversidad de opiniones: Los elementos más importantes de aprendizaje no nacen de la exploración de contenido, sino de la confrontación de posiciones y argumentos. El diseño debe incluir actividades que promuevan esta confrontación, sin olvidar que una gran parte de los aprendices son profesionales del área de derecho.
- Conexión de nodos expertos: Cada participante del proceso de formación representa una experticia en un área particular. El diseño debe ayudar a encontrar las conexiones que existen entre esas experticias y la forma de expresarlas para fortalecer la comunicación técnica.
- Potenciación del autoaprendizaje: Los contenidos son recopilaciones de conocimiento, pero el ejercicio de aprendizaje debe incitar a la acción para aprender más y construir conocimiento tácito y contextualizado.
- Reconocimiento de patrones: El reconocer patrones implica la posibilidad de abstraer conocimientos específicos y transferirlo a contextos diferentes mediante el reconocimiento de comportamientos comunes. El diseño del curso debe promover que los participantes puedan desarrollar esta habilidad para inferir y aplicar lo aprendido en sus propios contextos potenciando el pensamiento crítico.

4.1 Diseño general

Para responder a los objetivos definidos, la propuesta general del curso se plasma en el formato desarrollado por la ESDEGUE para la estructuración de cursos virtuales, el cual se desarrolla en la tabla número cuatro, sin los apartados de control y aprobación del documento.

Tabla 4. Formato de estructuración de un curso virtual

DISEÑO CURRICULAR	
NOMBRE DEL CURSO	**GESTIÓN DE RIESGOS DIGITALES EN LA CGR**
DURACIÓN	40 horas
JUSTIFICACIÓN	La cuarta revolución industrial en la que estamos inmersos ofrece novedosos desafíos e interesantes oportunidades, pero plantea incertidumbres y amenazas significativas, dando lugar al surgimiento de riesgos en el campo de la seguridad digital. Esta tipología de riesgos requiere un nuevo paradigma de gestión, que demanda una óptica holística e interdisciplinaria. Los ataques e incidentes en el ciberespacio son transversales a todos los sectores; la fuga de información sensible, la suspensión de la prestación del servicio, la indisponibilidad de la infraestructura crítica, la violación de la privacidad y los datos personales, la afectación de los bienes físicos, las operaciones de sabotaje o espionaje y, peor aún, el daño a la integridad de las personas, son una realidad que afectan el desarrollo económico, político y social.

	Por esta razón, surge la necesidad de aportar al conjunto de principios, valores, costumbres, actitudes y motivaciones que, con el fin de propiciar la adquisición de buenos hábitos y competencias laborales alrededor de la seguridad, la apertura a nuevas ideas, la mejora de la comunicación y el fomento de un aprendizaje continuo, con la mayor cobertura posible tanto a nivel jerárquico profesional como en su cubrimiento a todos los centros de trabajo. Lo anterior haciendo uso de las TIC y de nuevas formas de llevar procesos de enseñanza aprendizaje.
REQUISITOS DE INGRESO	Ser servidor público activo de la Contraloría General de la República.
ESTRATEGIA METODOLÓGICA	La estrategia metodológica utilizada para el desarrollo del curso está basada en el conectivismo como modelo pedagógico, usando la modalidad de curso en línea, masivo y abierto (MOOC) con un enfoque de aprendizaje activo basado en casos. Las actividades de formación, aprendizaje y evaluación deben estar orientadas al desarrollo de las competencias laborales de los servidores de la CGR, la evaluación debe contar con evidencias de desempeño, producto y conocimiento.

COMPETENCIA GENERAL
Motivar el desarrollo de aptitudes y actitudes en los servidores públicos de la CGR, de manera que les permita aplicar sus conocimientos y habilidades en la gestión de riesgos de seguridad digital, para fortalecer las capacidades institucionales con el fin de desarrollar su misión con criterios de seguridad y efectividad.
MÓDULOS
NOMBRE MÓDULO 1: INTRODUCCIÓN **2 horas**
TEMAS • Uso de la plataforma tecnológica de educación virtual, cómo navegar, uso de recursos y evaluaciones. • Descripción del curso, objetivos de formación, metodología, estructura y reglas generales de uso y participación.
NOMBRE MÓDULO 2: EL RIESGO DIGITAL EN NUESTRA VIDA DIARIA **8 horas**

TEMAS

- El riesgo digital es cosa de todos. A usted también le ha pasado, casos de la vida real.
- Conceptos básicos: Activo, amenaza, vulnerabilidad, impacto y probabilidad.
- ¿Qué es la gestión de riesgos? (Análisis y tratamiento)
- Caracterización de los riesgos de seguridad digital y los principios para su gestión.

NOMBRE MÓDULO 3:

GESTIONANDO EL RIESGO DIGITAL EN NUESTRO TRABAJO **10 horas**

TEMAS

- Caso de una situación del ámbito laboral.
- Contraste de hipótesis e identificación de responsables.
- Riesgos inherentes de la seguridad digital.
- Acciones concretas para el tratamiento.

NOMBRE MÓDULO 4:

LA NORMATIVIDAD SOBRE EL RIESGO DIGITAL ... ... **10 horas**

TEMAS
• Normatividad internacional. • Constitución política, leyes y decretos. • Caso de estudio: La cadena de custodia de la evidencia digital.
NOMBRE MÓDULO 5: CONSTRUCCIÓN DE BUENAS PRÁCTICAS **10 horas**
TEMAS
• Catálogo de buenas prácticas en el espacio de trabajo. • Estándares internacionales y marcos de trabajo vigentes. • Revisión del código de políticas de seguridad de la CGR. • Propuestas de caminos de mejoramiento
POBLACIÓN A LA QUE VA DIRIGIDO
Funcionarios de carrera, provisionales, de libre nombramiento y remoción, además de los contratistas que cumplan con las condiciones de ser servidor público de la CGR

Fuente: Elaboración propia

4.2 Diseño detallado

De acuerdo con Galvis (Galvis, 1992) se debe contar con un conjunto de actividades de aprendizaje que reconozcan un estado inicial , es decir las conductas de entrada y lleven a un objetivo terminal. Así mismo, se requiere de la definición de actividades que permitan evaluar los aprendizajes logrados, con el fin de dar retroalimentación a los participantes. Cada módulo se especifica con base el formato de la ESDEGUE para el diseño programático de módulos virtuales, adaptándolo a una sola tabla y sin los apartes de control y aprobación.

Tabla 5 Módulo 1 - Introducción

NOMBRE MÓDULO 1: INTRODUCCIÓN
COMPETENCIA GENERAL DEL MÓDULO
Promover el autoaprendizaje para identificar, incorporar y aplicar nuevos conocimientos sobre regulaciones vigentes, tecnologías disponibles y métodos, para mantener actualizada la efectividad y seguridad de sus prácticas laborales, a través de un MOOC.
1 ¿CÓMO SABER QUE ESTE MÓDULO ES PARA USTED?
Reconocer la importancia de desarrollar una conciencia de gestionar los riesgos de ciberseguridad por medio de valores, actitudes y prácticas que incluyen buenas prácticas y conocimientos específicos.
2 ¿QUÉ VA A LOGRAR? – UNIDADES DE COMPETENCIA
Mantener sus competencias actualizadas en función de los cambios que exige la administración pública incorporando a su gestión nuevos conceptos, aplicaciones y formas innovadoras que contribuyen a la mejora continua.

3 ¿QUÉ VA A APRENDER?
• Uso de la plataforma tecnológica de educación virtual, cómo navegar, uso de recursos y evaluaciones. • Descripción del curso, objetivos de formación, metodología, estructura y reglas generales de uso y participación
4 MATERIAL COMPLEMENTARIO PARA ESTUDIANTES
• Principales riesgos que enfrenta el planeta en 2019 según el Foro Económico Mundial. https://www.larepublica.co/globoeconomia/principales-riesgos-que-enfrenta-el-planeta-en-2019-segun-el-foro-economico-mundial-2816333 • ¿La ciberseguridad es algo más que protección? Encuesta Global de Seguridad de la Información 2018-19 https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf • Costos del Cibercrimen en Colombia. https://caivirtual.policia.gov.co/sites/default/files/costos_del_cibercrimen_v4.pdf
5 ACTIVIDADES EVALUATIVAS

Tipo de actividad:	**Propósito de actividad:**
Nube de palabras sobre las expectativas del aprendiz	Obtener información de los participantes para establecer mejor las conductas de entrada y refinar los elementos de motivación,

Tipo de actividad:	**Propósito de actividad:**
Foro de discusión	Presentarse ante la comunidad educativa para consolidar relaciones más cercanas con los compañeros.

6 GLOSARIO DE TÉRMINOS	
TÉRMINO	**DEFINICIÓN**
Ciberseguridad	La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. (ITU)
Competencia laboral	Capacidad de una persona para desempeñar, en diferentes contextos y con base en los requerimientos de calidad y resultados esperados en la Contraloría General de la República, las funciones inherentes a un empleo; capacidad que

	está determinada por los conocimientos, destrezas, habilidades, actitudes y aptitudes que debe poseer y demostrar el empleado público. (CGR)
MOOC	*Massive Open Online Course.* Curso en línea, masivo y abierto.

7 BIBLIOGRAFÍA

- (CCIT, 2014) Avances y retos de la defensa digital en Colombia. Bogotá D.C.: Fedesarrollo
- (CGR, 2018) Plan Estratégico 2018 - 2022 "Una Contraloría para Todos". https://www.contraloria.gov.co/web/guest/contraloria/planeacion-gestion-y-control/gestion-estrategica/plan-estrategico
- (CGR, 2008) Resolución Reglamentaria 0067 del 28 de Mayo de 2008. https://normativa.colpensiones.gov.co/colpens/docs/resolucion_contraloria_0067_2008.htm
- (OECD, 2013) Competency Framework. https://www.oecd.org/careers/competency_framework_en.pdf

Fuente: Elaboración propia

Tabla 6 Módulo 2 - El riesgo digital en nuestra vida diaria

NOMBRE MÓDULO 2: EL RIESGO DIGITAL EN NUESTRA VIDA DIARIA
COMPETENCIA GENERAL DEL MÓDULO
Capacidad para obrar en armonía con los valores organizacionales, haciendo uso responsable y transparente de los recursos públicos, eliminando cualquier discrecionalidad indebida en su utilización
1 ¿CÓMO SABER QUE ESTE MÓDULO ES PARA USTED?
Nuestra vida digital es también nuestra vida real, la cuarta revolución industrial basada en las TIC ha abierto un mundo de posibilidades sin precedentes para todos los actores de la sociedad: informarse, expresarse, compartir, aprender, emprender, trabajar, recrearse, entre otras. El autocuidado es un valor intrínseco en la convivencia en el ciberespacio, por lo que se debe conocer y afrontar los riesgos asociados a este aspecto de nuestras vidas a nivel personal e individual.
2 ¿QUÉ VA A LOGRAR? – UNIDADES DE COMPETENCIA
Identificar de forma básica los ciberriesgos que pueden afectar e interferir en el logro de los objetivos personales y familiares, con el fin de asumir los retos del entorno digital de una manera informada y consciente para tomar mejores decisiones en la vida diaria con un enfoque de gestión de este tipo de riesgos y situaciones.
3 ¿QUÉ VA A APRENDER?
• Conceptos básicos: activo, amenaza, vulnerabilidad, impacto y probabilidad. • ¿Qué es la gestión de riesgos? Aspectos de análisis y tratamiento. • Caracterizar riesgos de seguridad digital e identificar los principios para su debida gestión.

4 MATERIAL COMPLEMENTARIO PARA ESTUDIANTES	
• DEIA. (2019) ¿Cuánto valen tus datos personales en el mercado? https://www.deia.eus/2019/03/24/ocio-y-cultura/internet/cuanto-valen-tus-datos-personales-en-el-mercado • Semana (2014) 7 enfermedades producidas por el exceso de tecnología. https://www.semana.com/tecnologia/tips/articulo/enfermedades-producidas-exceso-tecnologia/373968-3 • (DQ Institute, 2017) *Digital Citizenship Skills*. https://www.dqinstitute.org/dq_everychild/	
5 ACTIVIDADES EVALUATIVAS	
Tipo de actividad:	**Propósito de actividad:**
Comentar un video sobre la vida digital de la familia	Sensibilizar al aprendiz sobre la ubiquidad en tiempo y espacio de los riesgos que corren los miembros de la familia en su vida diaria.
Tipo de actividad:	**Propósito de actividad:**
A usted también la ha pasado, compartir cuales riesgos digitales se han materializado a nivel personal.	Hacer un proceso de introspección para identificar las problemáticas afrontadas en el ámbito de las TIC, socializarlas con los compañeros y retroalimentarse de las experiencias de los demás, para compartir su experiencia personal y nutrirse de la de los demás

Tipo de actividad:	**Propósito de actividad:**
Cuestionario de preguntas de selección múltiple sobre los activos, amenazas, vulnerabilidades, y las matrices de impacto y probabilidad.	Establecer el grado de apropiación de conceptos fundamentales introducidos en el módulo.

6 GLOSARIO DE TÉRMINOS	
TÉRMINO	**DEFINICIÓN**
Activo	Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854).
Amenaza cibernética	Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854)

Gestión del riesgo	Proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de los desastres, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse. (UNGRD)
Impacto	Efecto de largo plazo, positivo y negativo, primario y secundario, producido directa o indirectamente, por una intervención para el desarrollo, intencionalmente o no. (DAFP)
Probabilidad	Medida de la posibilidad de que un evento ocurra. Puede ser definida, medida o determinada y se representa de forma cualitativa o cuantitativa en términos de la probabilidad o frecuencia. (UNGRD)

7 BIBLIOGRAFÍA

- DAFP. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas. https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499

- DNP. (2016). Política de Seguridad Digital. (Documento CONPES 3854). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
- (Europe Commission, 2017) *The Digital Competence Framework 2.0.* https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework
- (IRM, 2018) Professional Standards in Risk Management. https://www.theirm.org/media/1406416/IRM-PSRM-Brochure_Web.pdf
- UNGRD. (2017) Terminología sobre Gestión del Riesgo de Desastres y Fenómenos Amenazantes. https://repositorio.gestiondelriesgo.gov.co/bitstream/handle/20.500.11762/20761/Terminologia-GRD-2017.pdf;jsessionid=4C84120373CA42C7B88551C1509C2416?sequence=2

Fuente: Elaboración propia

Tabla 7 Módulo 3. Gestionando el riesgo digital en nuestro trabajo

NOMBRE MÓDULO 3: GESTIONADO EL RIESGO DIGITAL EN NUESTRO TRABAJO
COMPETENCIA GENERAL DEL MÓDULO
Conocer las herramientas de la gestión de riesgos para desarrollar las funciones asignadas según su nivel jerárquico en armonía con los valores institucionales, haciendo uso responsable, seguro y transparente de los recursos a su cargo, eliminando cualquier discrecionalidad indebida en su utilización.

1 ¿CÓMO SABER QUE ESTE MÓDULO ES PARA USTED?
Las amenazas e incidentes en el ciberespacio se han incrementado en los últimos años dando lugar a importantes consecuencias económicas y sociales tanto para individuos como para organizaciones públicas y privadas. Un número cada vez mayor de las partes interesadas son conscientes de la necesidad de gestionar mejor los riesgos de seguridad digital para aprovechar los beneficios de la economía digital, este manejo requiere primero entender que existen dichos riesgos y adquirir las competencias adecuadas para tomar decisiones responsables en este aspecto.
2 ¿QUÉ VA A LOGRAR? – UNIDADES DE COMPETENCIA
• Contar con el marco conceptual y metodológico de la gestión de riesgos digitales. • Preservar razonablemente la integridad, formalidad, validez, conservación, confidencialidad, privacidad, inteligibilidad y transparencia de los activos de información de los cuales es responsable.
3 ¿QUÉ VA A APRENDER?
• Caso de una situación del ámbito laboral. • Contraste de hipótesis e identificación de responsables. • ¿Cuáles son los riesgos inherentes de la seguridad digital? • Acciones concretas para la gestión de riesgos: identificación, valoración y tratamiento.
4 MATERIAL COMPLEMENTARIO PARA ESTUDIANTES
• CGR (2018). Libro de Políticas de Seguridad. https://clic-online.contraloria.gov.co/USATI/Documents/libro_SGS_USATI_FINAL_web.pdf

- ISACA (2017). La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial. https://www.isaca.org/Journal/archives/2017/Volume-5/Pages/the-arem-window-spanish.aspx
- MinTIC, (2018) Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b
- PWC (2019) Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018 https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html

5 ACTIVIDADES EVALUATIVAS

Tipo de actividad:	**Propósito de actividad:**
Análisis de un caso en el contexto laboral.	Los aprendices analizarán una situación hipotética de la materialización riesgo digital en su ámbito laboral, trabajando el caso en grupos previamente seleccionados y resolviendo los siguientes interrogantes: ¿Quiénes estuvieron involucrados con la situación?

	¿Quiénes son responsables de que haya sucedido? ¿Quiénes colaboraron directa o indirectamente para que sucediera?
Tipo de actividad:	**Propósito de actividad:**
Revisión entre pares con un ejercicio de argumentación.	Los estudiantes deben revisar las respuestas a la actividad anterior que hayan producido otros grupos. Debe señalar los puntos de acuerdo o desacuerdo argumentando cada uno con los elementos conceptuales apropiados previamente.
Tipo de actividad:	**Propósito de actividad:**
Creación colaborativa de un listado de riesgos digitales aplicables a las labores al interior de la CGR.	Identificar riesgos de seguridad digital en el contexto laboral y retroalimentarse de los planteados por sus pares, para tener una visión mas amplia de la gestión de riesgos.
Tipo de actividad:	**Propósito de actividad:**
Cuestionario de preguntas de selección múltiple sobre las fases y las principales actividades de la gestión de riesgos de seguridad digital.	Establecer el grado de apropiación de los principales cursos de acción para llevar a cabo el proceso de gestión de riesgos.
6 GLOSARIO DE TÉRMINOS	

TÉRMINO	DEFINICIÓN
Análisis del riesgo	Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).
Cibercrimen	Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio. (CONPES 3854)
Compartir el riesgo	Compartir con otra de las partes el peso de la pérdida o el beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).
Control	Medio para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. (NTC ISO 31000:2011).
Evaluación del riesgo	Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (NTC ISO 31000:2011).

Gestión de riesgos de seguridad digital	Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854).
Responsabilidad	Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de

	seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales. (CONPES 3854).
Seguridad digital	Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854).

7 BIBLIOGRAFÍA

- DAFP. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas. https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499
- DNP. (2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa. (Documento CONPES 3701) https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

- DNP. (2016). Política de Seguridad Digital. (Documento CONPES 3854). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
- ICONTEC (2009) NTC ISO/IEC 27005:2009 Gestión del riesgo en la seguridad de la información. https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27005.pdf
- ICONTEC (2018) NTC ISO/IEC 31000:2018 Gestión del riesgo. Directrices. https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO31000.pdf
- OECD (2015) *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document.* http://www.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en
- (Deloitte, 2017) *What key competencies are needed in the digital age?* https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-automation-competencies.pdf

Fuente: Elaboración propia

Tabla 8 Módulo 4. La normatividad sobre el riesgo digital

NOMBRE MÓDULO 4: LA NORMATIVIDAD SOBRE EL RIESGO DIGITAL
COMPETENCIA GENERAL DEL MÓDULO

Identificar la normativa colombiana sobre aspectos relacionados con la ciberseguridad, la ciberdefensa y el manejo de la información con un enfoque de gestión de riesgos, como lo plantea el actual Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad" y la política de seguridad digital CONPES 3854, para realizar análisis crítico constructivo de las decisiones o acciones orientadas en el quehacer misional de la CGR con criterios de autocontrol, autorregulación y autogestión .
1 ¿CÓMO SABER QUE ESTE MÓDULO ES PARA USTED?
• El uso de las tecnologías de la información y comunicaciones genera retos jurídicos en campos como: protección de datos personales, propiedad intelectual, propiedad industrial, contratos de colaboración internacional, derechos de autor, derecho de la competencia, protección al consumidor, seguridad informática, comercio electrónico, policía judicial y cadena de custodia. En un equipo interdisciplinario el componente legal es fundamental, máxime cuando la CGR es el máximo ente del control fiscal del país y sus actuaciones deben ser ejemplo del cumplimiento normativo.
2 ¿QUÉ VA A LOGRAR? – UNIDADES DE COMPETENCIA
• Contar con un normograma inicial para plantear soluciones innovadoras que se adapten al ordenamiento jurídico colombiano. • Establecer relaciones válidas entre los componentes de un problema y su contexto para reconocer la normativa asociada.

• Comprender las implicaciones que los conceptos de privacidad y seguridad de la información clasificada y reservada tienen en la actualidad para los servidores públicos y las funciones de policía judicial asignadas a la CGR.
3 ¿QUÉ VA A APRENDER?
• Normatividad internacional. • Constitución política, leyes y decretos. • Caso de estudio: La cadena de custodia de la evidencia digital.
4 MATERIAL COMPLEMENTARIO PARA ESTUDIANTES
• ASOSEC (2018) ¿Qué es el Convenio de Budapest, clave en seguridad digital para Colombia? https://asosec.co/2018/06/que-es-el-convenio-de-budapest-clave-en-seguridad-digital-para-colombia/ • Fiscalía General de la Nación (2018) Manual del sistema de cadena de custodia. https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf • OEA (2018) Gestión del riesgo cibernético nacional. https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf • OEA (2019) Programa de Ciberseguridad. http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp • Sánchez, Héctor (2019) La Ciberseguridad en el contexto de las regulaciones y las políticas nacionales. https://www.linkedin.com/pulse/la-ciberseguridad-en-el-contexto-de-las-regulaciones-h%C3%A9ctor

• https://www.iusatic.com http://dataytic.com/ https://www.adalid.com/	
5 ACTIVIDADES EVALUATIVAS	
Tipo de actividad:	**Propósito de actividad:**
Cuestionario de preguntas de selección múltiple sobre los elementos jurídicos y legales relevantes al contexto de la CGR	Establecer el grado de apropiación de los principales cursos de acción para llevar a cabo el proceso de gestión de riesgos.
Tipo de actividad:	**Propósito de actividad:**
Análisis de un caso real.	Los aprendices analizarán un incidente real, trabajando en grupos afines a las dependencias donde laboran y resolviendo las siguientes preguntas: ¿Qué normatividad es aplicable al caso? ¿Qué tipo de consecuencias legales (administrativas, penales, disciplinarias o fiscales) deben enfrentar los involucrados? ¿Qué falló en la gestión de riesgos de seguridad digital?
6 GLOSARIO DE TÉRMINOS	
TÉRMINO	**DEFINICIÓN**

Autocontrol	capacidad que deben desarrollar todos y cada uno de los servidores públicos de la organización, independientemente de su nivel jerárquico, para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos de manera oportuna para el adecuado cumplimiento de los resultados que se esperan en el ejercicio de su función, de tal manera que la ejecución de los procesos, actividades y/o tareas bajo su responsabilidad, se desarrollen con fundamento en los principios establecidos en la Constitución Política. (Decreto 1599 de 2005)
Autorregulación	Capacidad de cada una de las organizaciones para desarrollar y aplicar en su interior métodos, normas y procedimientos que permitan el desarrollo, implementación y fortalecimiento incremental del Sistema de Control Interno, en concordancia con la normatividad vigente. (Decreto 1599 de 2005)
Autogestión	Capacidad de toda organización pública para interpretar, coordinar, aplicar y evaluar de manera efectiva, eficiente y eficaz la función

	administrativa que le ha sido asignada por la Constitución, la ley y sus reglamentos. (Decreto 1599 de 2005)
Cadena de custodia	Capacidad demostrativa, que permite a las partes intervinientes en el proceso penal, contar con una adecuada conceptualización de los Elementos Materiales Probatorios y Evidencia Física y su adecuado uso dentro del sistema (Fiscalía General de la Nación)
Índice de Información Reservada y Clasificada	Inventario de la información pública que puede causar daño a determinados derechos o intereses públicos, por lo que no es publicable. Este índice es útil para que la ciudadanía conozca de antemano cuáles documentos o qué tipo de información tienen acceso restringido y es útil al momento de la elaboración de las respuestas a las solicitudes de información de la entidad, con el fin que no se publique información que no debe serlo ni se niegue el acceso a información que sí debe ser publicada y facilitada a la ciudadanía. (Ley 1712 de 2014)
7 BIBLIOGRAFÍA	

- Council of Europe (2001) Convenio sobre la ciberdelincuencia. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- DAFP. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas. https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499
- DNP. (2016). Política de Seguridad Digital. (Documento CONPES 3854). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
- World Economic Forum (2018) Centre for Cybersecurity https://www.weforum.org/centre-for-cybersecurity/

Fuente: Elaboración propia

Tabla 9 Módulo 5 Construcción de buenas prácticas

NOMBRE MÓDULO 5: CONSTRUCCIÓN DE BUENAS PRÁCTICAS
COMPETENCIA GENERAL DEL MÓDULO
Utilizar el pensamiento crítico y las competencias potenciadas o adquiridas en los módulos anteriores para proponer buenas prácticas en la gestión de los riesgos de seguridad digital con un uso responsable de las fuentes disponibles.
1 ¿CÓMO SABER QUE ESTE MÓDULO ES PARA USTED?

• Tener a disposición un conjunto de conceptos, elementos y criterios, que permiten utilizar una situación particular como ejemplo para enfrentar y resolver situaciones similares. • Reconocer los grupos de interés y mantener una interlocución clara y precisa sobre las condiciones de seguridad esperadas. • Sustentar sus aportes y propuestas con argumentos claros y pertinentes.
2 ¿QUÉ VA A LOGRAR? – UNIDADES DE COMPETENCIA
• Realizar preguntas y búsquedas de información que permitan clarificar las dudas e inconsistencias que emergen de un problema. • Apoyar en la comprensión de conceptos técnicos a personas que no tienen su nivel de experticia, utilizando ejemplos acordes a las posibilidades de comprensión de su interlocutor. • Proponer acciones conjuntas con sus proveedores, clientes internos y externos encaminadas a armonizar los procesos, sistemas e interacciones que les afecten mutuamente. • Realizar acciones recurrentes encaminadas a obtener la máxima y mejor información posible de todas las fuentes disponibles, necesaria en su gestión y en la de su equipo.
3 ¿QUÉ VA A APRENDER?
• Buenas prácticas en el espacio de trabajo. • Estándares internacionales y marcos de trabajo vigentes. • El código de políticas de seguridad de la CGR.
4 MATERIAL COMPLEMENTARIO PARA ESTUDIANTES

- Ley 1955, Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad". http://www.secretariasenado.gov.co/senado/basedoc/ley_1955_2019.html
- INCIBE (2018). La ciberseguridad es cosa de todos, establece buenas prácticas https://www.incibe.es/protege-tu-empresa/blog/ciberseguridad-cosa-todos-establece-buenas-practicas
- (CSIS Center for Strategic & International Studies) https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index
- (Galindo Arranz, Blanco Ruiz, & Ruiz San Miguel, 2017) Competencias digitales ante la irrupción de la Cuarta Revolución Industrial. http://ojs.labcom-ifp.ubi.pt/index.php/ec/article/view/277/144

5 ACTIVIDADES EVALUATIVAS

Tipo de actividad:	**Propósito de actividad:**
Los participantes deben proponer un conjunto de diez prácticas que permitan gestionar el riesgo digital.	Al elaborar el decálogo de buenas prácticas, se sintetizan los elementos previamente apropiados para ser usados en un proceso de argumentación.
Tipo de actividad:	**Propósito de actividad:**
Contrastar el decálogo propuesto contra las políticas del Sistema de Gestión de Seguridad (SGS) de la CGR.	Proponer un ciclo de mejora al libro de políticas, al identificar cuales prácticas se deben incluir y cuales retirar. Los resultados de los argumentos

	los usará la USATI en su ciclo Planear Hacer Verificar Actuar del SGS.
6 GLOSARIO DE TÉRMINOS	
TÉRMINO	**DEFINICIÓN**
Ciberseguridad	La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. (ITU)
Marco de trabajo	Conjunto de conceptos, elementos y criterios, que permiten utilizar una situación particular como ejemplo para enfrentar y resolver situaciones similares. (www.rae.es)
Plan de desarrollo nacional	Documento que sirve de base y provee los lineamientos estratégicos de las políticas públicas formuladas por el Presidente de la República a través de su equipo de Gobierno. Su elaboración, socialización, evaluación y seguimiento es responsabilidad directa del DNP. El PND es el instrumento formal y legal por

	medio del cual se trazan los objetivos del Gobierno permitiendo la subsecuente evaluación de su gestión. (DNP)

7 BIBLIOGRAFÍA

- CGR (2018). Libro de Políticas de Seguridad. https://clic-online.contraloria.gov.co/USATI/Documents/libro_SGS_USATI_FINAL_web.pdf
- ICONTEC (2009) NTC ISO/IEC 27005:2009 Gestión del riesgo en la seguridad de la información. https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27005.pdf
- ICONTEC (2018) NTC ISO/IEC 31000:2018 Gestión del riesgo. Directrices. https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO31000.pdf
- ISACA (2017). La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial. https://www.isaca.org/Journal/archives/2017/Volume-5/Pages/the-arem-window-spanish.aspx
- ISO (2012) ISO/IEC 27032:2012 *Information technology. Security techniques. Guidelines for cybersecurity* https://www.iso.org/standard/44375.html
- NIST (2019) National Institute for Standards and Technology. Cybersecurity. https://www.nist.gov/topics/cybersecurity

Fuente: Elaboración propia

4.3 Recursos TIC

Existen múltiples plataformas posicionadas en el mundo para la distribución y ejecución de MOOC, sin embargo, varias de las más populares son de licencia cerrada y comercial (específicamente Coursera, que se podría catalogar como la plataforma de MOOC más utilizada en el mundo). Sin embargo, hay diversas alternativas que pueden ser utilizadas para la creación de MOOCS y que permiten utilización libre e incluso plataformas de software libre que pueden ser instaladas y modificadas a la medida de las necesidades de una organización.

Algunas de las herramientas más populares y que pueden ser utilizadas de manera gratuita o similar son:

- edX es una plataforma para MOOC creada por la Universidad de Harvard y el MIT en colaboración con Google. Permite cursos de hasta 300 mil estudiantes, tiene versiones en la nube o hospedadas, puede ser personalizada para la organización, tiene un sistema configurable de analíticas, puede monetizar sus cursos y tiene versión móvil mediante una aplicación para Android y iOS.
- Moodle es una plataforma de administración de aprendizaje de software libre muy difundida y utilizada por instituciones educativas desde su lanzamiento en 2002 basado en la idea de crear una herramienta de cursos acorde con principios constructivistas de colaboración y construcción social. Permite cursos hasta de 300 mil estudiantes, permite ser hospedada en infraestructura propia, tiene a su favor una enorme comunidad de desarrollo de temas y extensiones, tiene analíticas personalizadas, permite monetización y además tiene versiones móviles de sus temas y una aplicación móvil.

- Coursesites (Blackboard learn) es un servicio en la nube basado en el LMS Blackboard. Blackboard es uno de los LMS comerciales más utilizados por instituciones de educación superior en el mundo, sin embargo, Coursesites permite que los instructores creen sus cursos para una cantidad ilimitada de estudiantes, no permite personalizar la organización, tiene analíticas personalizadas, no permite monetizar los cursos y tiene una aplicación móvil.
- Udemy es una plataforma para la publicación de MOOC que está orientada en la generación de habilidades para el trabajo y en potenciar los cursos monetizados de creación abierta (Cualquiera que quiera publicar un curso puede hacerlo y cobrarlo). Udemy permite la apertura de cursos para un número ilimitado de estudiantes, no permite la personalización de la organización, no tiene analíticas personalizadas, permite monetizar los cursos y tiene aplicación móvil.

De acuerdo a las necesidades de formación, facilidad de uso, alcance del curso y necesidad de personalización de la organización, se propone la implementación de la presente propuesta sobre edX. En esta sección se revisarán las funcionalidades que edX provee y que son relevante para la realización de esta propuesta, otros aspectos no serán cubiertos dada la gran cantidad de funcionalidades que ofrece.

1. Administración de cursos: edX provee las siguientes configuraciones para el modo de curso: Asincrónico a rimo del estudiante, asincrónico dirigido por el instructor, sincrónico y mixto. Para la necesidad de este curso se requiere un curso que sea a ritmo del estudiante

en sus actividades, pero con fechas de inicio y fin del curso definidas, para lo cual una configuración asincrónica sería adecuada.

2. Administración de usuarios: edX permite administración de usuarios, configuración de campos de perfil personalizados y obligatorios, realización de acciones masivas sobre usuarios y manejo de diferentes roles. De acuerdo a la propuesta realizada, se requiere de la inscripción de los usuarios con elementos de perfil como son la unidad en la que trabajan.
3. Inscripción a cursos: edX soporta diferentes maneras de inscribir a los usuarios en los cursos, entre ellas están la inscripción como invitado, inscripción manual, auto-inscripción (El usuario se inscribe en lo que desee), inscripción mediante encuesta, inscripción automática basada en los datos de usuario. De acuerdo con la actual propuesta del curso, se podrían manejar auto- inscripciones o inscripciones manuales.
4. Creación de cursos: edX ofrece herramientas para la creación de cursos, manejo de archivos, sistema de pruebas, encuestas, entregas, copias de seguridad de cursos, calendario y administración de eventos en vivo (Webinars, talleres o similares) y administración de currículos. Esta propuesta utilizará las herramientas de creación de cursos, pruebas y entregas.
5. Calificación de actividades: edX también ofrece herramientas para administrar calificaciones de actividades como son un libro de calificaciones, comentarios a notas, escalas de evaluación, marcación manual. En esta propuesta se utilizará el libro de calificaciones para llevar control y calcular la aprobación de actividades y del curso.

6. Certificados: Las funcionalidades de certificados permiten llevar la información de qué estudiantes han participado en cursos o programas dentro de la plataforma. Inicialmente se espera emitir un certificado de participación en el curso a modo de motivación, pero puede ser utilizado posteriormente como requisito de otros cursos o de iniciativas diferentes de formación dentro de la organización.
7. Seguridad: edX provee las siguientes funcionalidades de seguridad: Bloqueador de direcciones IP, herramientas para el rastreo y bloqueo de SPAM, herramientas para detección de virus, sistema de validación y sugerencia de contraseñas seguras, manejador de restricciones de dominio, etc. Se revisará que configuraciones de este tipo aplican para la infraestructura y políticas de la organización.

5 Conclusiones

Es fundamental tener en cuenta que, sin adoptar las precauciones adecuadas, internet, las redes y los dispositivos de información y en general el ciberespacio no son seguros. Los modernos sistemas de información empresariales son el objetivo de una serie de agentes maliciosos. Un concepto útil para establecer las expectativas de quienes se dedican a la gestión de riesgos digitales es esta simple afirmación: "Si algo de valor está en línea, está en riesgo, y es probable que ya esté comprometido" (Cámara de Comercio Internacional, 2015, pág. 5). Si bien existen técnicas y procesos que pueden ayudar a reducir los riesgos de compromiso, determinados agentes maliciosos se benefician del eslabón más débil en los sistemas interconectados el cual generalmente es el componente humano.

Las organizaciones deben desarrollar y fomentar capacidades clave para tener éxito en la gestión de riesgos de ciberseguridad, tales como:

- Realizar un análisis de riesgos para su organización y priorizar los activos que requieran una mayor protección.

- Contar con el liderazgo para tomar las medidas adecuadas y garantizar que la organización adopta las mejores prácticas de seguridad de la información.

- Prepararse para detectar y responder interna y externamente a eventos a través de procesos organizativos formalizados.

Para lograr lo anterior se debe contar con personal que tenga las competencias laborales necesarias para hacer una buena gestión de riesgos de seguridad digital, como se mencionó anteriormente, de allí surge el concepto de segunda brecha digital que se refiere ya no a las diferencias de acceso sino a las diferencias en la capacidad de usar las TIC y beneficiarse de ellas con un uso seguro y responsable.

El desarrollo de competencias requiere llevar a cabo procesos de enseñanza aprendizaje, estableciendo a la educación como un proceso continuo y en cambio permanente que se debe apoyar en las tecnologías, las cuales se constituyen en vehículos de contenidos educativos a la vez que como entornos de aprendizaje. Se necesita estimular la gestión del conocimiento del modo más autónomo y solidario posible en todos los sujetos y organizaciones, de cara a las necesidades de una sociedad impactada por las TIC y el aprendizaje electrónico. El entorno en el que se mueven las personas debe de generar a futuro, de modo sostenible, nuevos procesos, productos y servicios a través de la combinación de competencias de individuos calificados, procesos inteligentes y herramientas tendientes al desarrollo de capital intelectual o talento humano que hace que las instituciones sean cada vez más productivas, innovadoras y competitivas.

Sin embargo, se presentan nuevos retos a la hora de hacer más efectiva la formación ya que el cambio tecnológico que implica un mayor acceso a la información, la interrelación entre los actores y la globalización de la formación, hacen que los modelos educativos anteriores o clásicos ya no sean vigentes ni efectivos a la hora de alcanzar los objetivos necesarios en el proceso de adquisición de conocimientos y desarrollo de competencias. Aquí los MOOC aparecen como una

alternativa interesante para llevar a cabo procesos de enseñanza y aprendizaje con alto cubrimiento y bajo costo.

La educación deja de tener un papel de generador de expectativas profesionales, para ser un instrumento de integración laboral. Los cuatros pilares de la Educación del siglo 21, se centran en el: Aprender a Aprender; Aprender a Hacer; Aprender a Ser; y Aprender a Convivir. En el de Aprender a Hacer, se definen por primera vez el concepto de competencias, que hoy se denomina "*learning outcomes*", y supone uno de los cambios más potentes en el proceso de transformación de la educación industrial del siglo XX, al nuevo modelo del siglo en el que vivimos actualmente. Pero no solo afecta a la educación, sino al propio funcionamiento del mercado de trabajo

El proceso de análisis educativo se considera una prioridad ante la creación de un proceso de formación, debido a la naturaleza diversa y cambiante del contexto en que una propuesta educativa será ejecutada. La población, historia, disposiciones organizacionales y necesidades del público potencial no solo representan un norte para cualquier proceso de diseño, si no un marco de funcionamiento y un conjunto de restricciones que, al ser tenidas en cuenta, sino que aumenta la probabilidad de alcanzar los objetivos formativos esperados.

El diseño de un ambiente de aprendizaje requiere de una comprensión de las posibilidades y limitaciones que conlleva un cierto marco sociocultural que enmarca el ambiente de aprendizaje que se diseña. La elección acerca de la modalidad (presencial, virtual, mixta, etc.), los recursos de apoyo, la apuesta pedagógica, el currículo y demás no son elementos que deban ser tomados a la ligera.

Pedagógicamente se puede tener un cierto sesgo a pensar que cierta teoría de aprendizaje puede abordar gran parte de los elementos que necesitamos para que una propuesta de aprendizaje, es decir un diseño, sea relativamente exitosa. Sin embargo, la realidad es otra y la afiliación teórica que se tiene dependerá mucho de lo que se necesita del contenido y del público objetivo. En este caso se encontró una teoría de aprendizaje que une fuertemente las posiciones educativas y tecnológicas, dado que el mismo conectivismo define su posición con base en premisas propias de la era tecnológica en la que estamos.

Las actividades basadas en el conectivismo tienen una fuerte componente de discusión, en la cual más que potenciar aprendizajes conceptuales o memorísticos, se ayuda a que se formen lazos de conocimiento que la gente forja sin darse cuenta. Esto va muy de acuerdo con un adagio popular que afirma que "es mejor saber quién sabe, que saber mucho". En plena era de la información, posiblemente los conocimientos adquiridos previamente se devalúen con rapidez, pero nunca se perderán esas habilidades de aprender a aprender y cuanto más se desarrollen en un contexto específico, más aptas y competentes serán las personas en el mismo.

Las elecciones tecnológicas no solamente se basan en funcionalidades que concuerden con las necesidades establecidas. En esta propuesta se puede ver que, desde el punto de vista tecnológico, las elecciones también tienen que ver con elementos de practicidad, de sencillez y otros que tienen un fuerte impacto en la usabilidad de quienes serán usuarios de un sistema y de un diseño de una estrategia educativa.

Tal vez cuando se analiza la experiencia de los usuarios, no se debería generar la divergencia entre lo tecnológico y lo educativo, ya que a la par que se diseña una propuesta, es la

conjugación de estos elementos lo que permite configurar una mejor experiencia del participante y posiblemente no se puede analizar desde una perspectiva diferente a la sistémica.

También se puede concluir que las plataformas de aprendizaje han ido tendiendo a la simplicidad. En la década pasada se popularizaron herramientas robustas y repletas de funcionalidad en el dominio de los *Learning Management Systems* (LMS), sin embargo, ahora las plataformas más utilizadas se han ido a conceptos más simples y han dejado de lado múltiples sistemas que se sentían necesarios hace tan solo unos años. En conjugación con lo anterior se ha visto un fuerte cambio en la filosofía de uso de estas y en la forma misma que se percibe la educación desde las mismas, ponderando fuertemente la tendencia social sobre la versión positivista de sistema que apoya la adquisición de conocimientos.

Finalmente, se pudo diseñar una mediación pedagógica a través de medios digitales una herramienta que incluye recursos educativos en una plataforma abierta y de uso masivo, bajo el análisis de los distintos tipos necesidades de la CGR y para mejorar las competencias establecidas para un buen desempeño tanto personal como laboral. El proceso que se llevó a cabo es incluyente y consensuado con las partes interesadas, asesorado por expertos de varios dominios, meticuloso con las fases de un desarrollo de este tipo de proyectos por lo que se considera que si es una herramienta útil para la generación de competencias sobre la gestión de riesgo digital al interior de la CGR pues fue aprobado por el Centro de Estudios Fiscales después de ser presentado por el autor a la convocatoria de banco de docentes a finales del año pasado (CEF, 2019), y como se menciona a lo largo de este escrito debe seguir en desarrollo y actualización constantes (Deming, 1993).

6 Bibliografía

Aguilar, S., & Barroso, J. (2015). La triangulación de datos como estrategia en investigación educativa. *Revista de Medios y Educación*(47), 73-88. doi: http://dx.doi.org/10.12795/pixelbit.2015.i47.05

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Alles, M. A. (2013). *La incertidumbre y la gestión de recursos humanos por competencias.* Obtenido de http://www.marthaalles.com: http://enriquecetupsicologia.com/e-learning/wp-content/uploads/2009/11/Incertidumbre-y-gestion-por-competencias-Martha-Alles.pdf

Anderson, C., & Agarwal, R. (2010). Practicing Safe Computing: a multimedia empirical examination of home computer security behavoiral intentions. *MIS Q., 34*(3), 613-643.

APA. (2010). *Publication Manual of the American Psychologycal Association* (Vol. 6 Ed). Washington, DC.: American Psychological Association.

Ardila Castro, C. A., & Cubides Cárdenas, J. A. (2017). Política Pública de Seguridad en Colombia frente a la convergencia y las nuevas amenazas. En *Políticas Públicas de Seguridad y Defensa* (págs. 23-55). Ediciones Escuela Superior de Guerra.

Baggaley, J. (2014). MOOC postscript. *Distance Education, 35*(1), 126-132.

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. *Pysichological Review, 84*(2), 191-215.

Bouchard, P. (2011). Network Promises and Their Implications. *Universities and Knowledge Society Journal, 8*(1), 288-302. Obtenido de Revista de Universidad y Sociedad del Conocimiento: http://rusc.uoc.edu/index.php/rusc/article/viewFile/v8n1-bouchard/v8n1-bouchard-eng

Branson, R. K., Rayner, G. T., Cox, J. L., Furman, J. P., King, F. J., & Hannum, W.H, W. H. (1975). *Interservice procedures for instructional systems development: Executive summary and model.* Tallahassee: Naval Education and Training Command. Obtenido de http://www.dtic.mil/dtic/tr/fulltext/u2/a019486.pdf

Bruner, J. (1997). *La educación, puerta de la cultura.* Madrid: Visor.

Butcher, N. (2015). Open Educational Resources (OER). (A. Kanwar, & S. Uvalic Trumbic, Edits.) Paris, Francia. Obtenido de A Basic Guide to Open Educational Resources (OER).

Campis, L., Lyman, R., & Prentice-Dunn, S. (1986). The Parental Locus of Control Scale: Development and Validation. *Journal of Clinical Child Psycology, 15*(3), 260-267.

CCIT. (2014). *Avances y retos de la defensa digital en Colombia.* Bogotá D.C.: Fedesarrollo.

CEF. (2017). *Centro de Estudios Fiscales*. Obtenido de Plan de Choque: https://portalcef.contraloria.gov.co/Oferta-academica/Plan_Choque/Antecedentes-y-Objetivos

CEF. (2019). *Centro de Estudios Fiscales.* Obtenido de Convocatoria Banco de Docentes: https://portalcef.contraloria.gov.co/CEF/Convocatoria-Banco-de-Docentes

Centro Cibernético de la Policía Nacional. (2017). *Costos del Cibercrimen en Colombia.* Recuperado el 05 de 08 de 2019, de https://caivirtual.policia.gov.co/sites/default/files/costos_del_cibercrimen_v4.pdf

Cequea, M. M., Rodríguez Monroy, C., & Núñez Bottini, M. A. (2011). La productividad desde una perspectiva humana: Dimensiones y factores. *Intangible Capital, 7*(2), 549-584. doi:http://dx.doi.org/10.3926/ic.2011.v7n2.p549-584

Cervera, M. G., & Johnson, L. (2015). Education and technology: New learning environments from a transformative perspective. *RUSC, 12*(2), 1-13. Obtenido de http://search.proquest.com/docview/1692488715?accountid=143348

CGR. (28 de Mayo de 2008). *Resolución Reglamentaria 0067 del 28 de Mayo de 2008.* Obtenido de Contraloría General de la República: https://normativa.colpensiones.gov.co/colpens/docs/resolucion_contraloria_0067_2008.htm

CGR. (05 de Marzo de 2015). *Plan General de Capacitación.* Obtenido de Contraloría General de la República: http://campusvirtual.contraloria.gov.co/campus/docs15/PLAN_GENERAL_CAPACITACION_2015-2018.pdf

CGR. (2016). *Informe de Valoración de las Prácticas de Control en Seguridad de la Información.* Bogotá D.C.: Contraloría General de la República.

CGR. (2018). *Plan Estratégico 2018 - 2022 "Una Contraloría para Todos".* Recuperado el 04 de 08 de 2019, de https://www.contraloria.gov.co/web/guest/contraloria/planeacion-gestion-y-control/gestion-estrategica/plan-estrategico

CGR. (2018). *Programa Anual de Capacitación.* Obtenido de Centro de Estudios Fiscales: https://portalcef.contraloria.gov.co/assets/docs/55-319b4860-f46e-43bc-b864-bce0b5c44d79/ProgramaAnualCapacitacion2018CEF.pdf

CGR, C. d. (12 de Junio de 2017). Entrevista con William Fernando Halaby Rodríguez. (G. Aristizábal Restrepo, Entrevistador)

Cohen, L., Manion, L., & Morrison, K. (2017). *Research Methods in Education.* Londres: Taylor & Francis.

Colombia, Congreso de la República. (25 de mayo de 2019). *Ley 1955, por la cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad".* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1955_2019.html

Colombia, Presidencia de la República. (10 de febrero de 2016). *Directiva Presidencial 01.* Obtenido de http://es.presidencia.gov.co/normativa/normativa/DIRECTIVA%2001%20DEL%2010%20DE%20FEBRERO%20DE%202016.pdf

Corominas, J. (1987). *Breve diccionario etimológico de la lengua castellana.* Madrid: Gredos.

Cortes Mendez, M. (02 de abril de 2019). Obtenido de In India, MOOCs Are Now Part of the Education System: https://www.classcentral.com/report/swayam-for-credit/

CSIS Center for Strategic & International Studies. (s.f.). Obtenido de Global Cyber Strategies Index: https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index

DAFP. (octubre de 2018). *Guía para la administración del riesgo y el diseño de controles en entidades públicas.* Obtenido de Departamento Administrativo de la Función Pública: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499

DANE. (09 de abril de 2019). *Boletín Técnico: Indicadores básicos de tenencia y uso de Tecnologías de la Información.* Obtenido de https://www.dane.gov.co/files/investigaciones/boletines/tic/bol_tic_hogares_2018.pdf

de Gregory, W. (2002). *Construcción familiar-escolar de los tres cerebros.* Bogotá: Editorial Kimpres Ltda.

Deloitte. (2017). *What key competencies are needed in the digital age? The impact of automation on employees, companies and education.* Obtenido de https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-automation-competencies.pdf

Deming, E. M. (1993). *The New Economics for Industry, Government, and Education.* Boston: MIT Press.

Denzin, N. K., & Lincoln, Y. S. (2005). *The SAGE handbook of qualitative research.* Los Angeles: Thousand Oaks : Sage Publications.

DNP. (23 de julio de 2011). *Lineamientos de Política para Ciberseguridad y Ciberdefensa. (Documento CONPES 3701).* Obtenido de Consejo Nacional de Política Económica y Social: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

DNP. (14 de 08 de 2015). *Concepto favorable a la nación para contratar un empréstito externo con la banca multilateral hasta por usd 30 millones destinado a financiar el programa de fortalecimiento institucional de la Contraloría General de la República. (Documento CONPES 3841).* Recuperado el 04 de 08 de 2019, de Consejo Nacional de Política Económica y Social: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3841.pdf

DNP. (11 de abril de 2016). *Política de Seguridad Digital. (Documento CONPES 3854).* Obtenido de Consejo Nacional de Política Económica y Social: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Doring, H., Demmin, P. E., & Gabel, D. (1990). *Chemistry. The study of matter* (3 ed.). Englewood Cliffs: Prentice Hall, Inc.

Downes, S. (2008). Places to Go: Connectivism & Connective Knowledge. *Innovate: Journal of Online Education, 5*(1). Obtenido de https://nsuworks.nova.edu/innovate/vol5/iss1/6/

DQ Institute. (2017). *8 Digital Citizenship Skills.* Obtenido de Digital Quotient Institute: https://www.dqinstitute.org/what-is-dq

Ducci, M. A. (1996). El enfoque de competencia laboral en la perspectiva internacional. En Cinterfor (Ed.), *Seminario Internacional sobre Formación Basada en Competencia Laboral: Situación Actual y Perspectivas.* Guanajuato.

Ellinger, A. D. (2004). The Concept of Self-Directed Learning and its Implications for Human Resource Development. *Advances in Developing Human Resources, 6*, 158-178.

ENISA. (Diciembre de 2018). *European Union Agency For Network and Information Security.* doi:10.2824/324042

Escuela Superior de Guerra. (2015). Obtenido de Guía de formato y citación de fuentes : http://www.esdegue.edu.co

Europe Commission. (2017). *The Digital Competence Framework 2.0.* Obtenido de DigComp: https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework

EY. (2018). *¿La ciberseguridad es algo más que protección? Encuesta Global de Seguridad de la Información 2018-19.* Recuperado el 05 de 08 de 2019, de https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf

Flanagan, J. (1954). The critical incident technique. *Psychological Bulletin, 51*(4), Psychological Bulletin. doi:http://dx.doi.org/10.1037/h0061470

Flick, U. (2006). *An Introduction to Qualitative Reseaerch.* London: Sge Publications.

Gagné, R. M. (1962). Military Training and Principles of Learning. *American Psychologist, 17*(12), 83-91. doi:http://dx.doi.org/10.1037/h0048613

Galindo Arranz, F., Blanco Ruiz, S., & Ruiz San Miguel, F. (2017). Competencias digitales ante la irrupción de la Cuarta Revolución Industrial. *Estudos em Comunicação*. doi:10.20287/ec.n25.v1.a01

Galvis Panqueva, A. H. (1992). *Ingeniería de Software Educativo.* Santafé de Bogootá: Ediciones Uniandes.

Galvis Panqueva, A. H., & Mendoza, P. (1999). Ambientes Virtuales de Aprendizaje: Una Metodología para su Creación. *Informática Educativa*, 295-317. Obtenido de http://colombiaaprende.edu.co/html/mediateca/1607/articles-106223_archivo.pdf

García Aretio , L. (1998). Indicadores para la evaluación de la enseñanza en una Universidad a distancia. *RIED Revista Iberoamericana de Educación a Distancia, 1*(1), 63-85. doi:https://doi.org/10.5944/ried.1.1.2123

García-LLuis Valencia, A. (28 de julio de 2013). *MOOCs: El efecto transformador de las tecnologías sobre la educación.* Obtenido de INED21: http://ined21.com/moocs-el-efecto-transformador-de-las-tecnologias-sobre-la-educacion/

Gartner. (s.f.). *Gartner Hype Cycle.* Obtenido de https://www.gartner.com/en/research/methodologies/gartner-hype-cycle

Global Cyber Security Capacity Centre. (2017). *Cybersecurity Capacity Maturity Model for Nations (CMM).* Obtenido de Cibersecurity Capacity Portal: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

Hernández, R., Fernández, C., & Baptista, M. d. (2003). *Metodología de la Investigación* (5 ed.). México D.F.: McGraw-Hill.

ICC. (2015). *ICC Cyber Security Guide for Business.* Obtenido de International Chamber of Commerce: https://iccwbo.org/publication/icc-cyber-security-guide-for-business/

ICONTEC. (2011). *NTC-ISO 31000 – GESTIÓN DEL RIESGO.* Obtenido de https://tienda.icontec.org/producto/impreso-ntc-iso-31000-gestion-del-riesgo-principios-y-directrices/?v=42983b05e2f2

ICONTEC. (2017). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información (SGSI).* Obtenido de NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27000: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27000.pdf

IRM. (2018). *Professional Standards in Risk Management.* Obtenido de Institute of Risk Management: https://www.theirm.org/media/1406416/IRM-PSRM-Brochure_Web.pdf

ITU. (2018). *International Telecommunication Union.* Obtenido de Global Cybersecurity Index (GCI) 2017: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU. (2019). *International Telecommunications Union.* Obtenido de Global Cybersecurity Index: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ITU. (2019). *International Telecommunication Union.* Obtenido de Global Cybersecurity Index (GCI) 2018: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Johnstone, S. M., & Poulin, R. (2002). What Is Open Course Ware And Why Does It Matter? *Change: The Magazine of Higher Learning , 34*(4), 48-50.

Jones Chaljub, S. (10 de febreo de 2017). ¿Es Whatsapp una vulnerabilidad para el Estado Colombiano? *Observatorio S&D, 2*(1), 19-21. Obtenido de https://issuu.com/observatoriosd/docs/bolet__n_1_-_2017

Kerr, B. (2007).

Kiremire, A. R. (19 de octubre de 2011). *The application of the pareto principle in software engineering.* Obtenido de http://www2.latech.edu/~box/ase/papers2011/Ankunda_termpaper.PDF

Kop, R. (2011). The Challenges of Connectivist Learning on Open Online Networks: Learning Experiences During a Massive Open Online Course. *International Review of Research in Open and Distance Learning, 12*. doi:10.19173/irrodl.v12i3.882

Levy-Leboyer, C. (2003). *Gestión de las competencias: cómo analizarlas, cómo evaluarlas, cómo desarrollarlas.* Barcelona: Ediciones Gestión.

Lewis, M. S., Bryman, A., & Liao, T. F. (2003). *The SAGE Encyclopedia of Social Science Research Methods.* New Delhi: SAGE Publication.

Markoff, J. (15 de agosto de 2011). Virtual and Artificial, but 58,000 Want Course. *The New York Times.* Obtenido de https://www.nytimes.com/2011/08/16/science/16stanford.html

McClelland, D. C. (1973). Testing for competence rather than for intelligence. *American Psychologist, 28*(1), 1-14.

MEN. (2019). *Portal Colombia Aprende.* Obtenido de Ministerio de Educación Nacional:

Mertens, L. (1996). *Competencia laboral: sistemas, surgimiento y modelos.* Obtenido de https://www.oitcinterfor.org/sites/default/files/file_publicacion/mertens.pdf

Nagowah, L., & Nagowah, S. (2009). A Reflection on the dominant learning theories: Behaviourism, cognitivism and constructivism. *The International Journal of Learning, 9*, 279-286.

Necuzzi , C. (2013). *Estado del arte sobre el desarrollo cognitivo involucrado en los procesos de aprendizaje y enseñanza con integración de las TIC.* Obtenido de https://www.unicef.org/argentina/spanish/Estado_arte_desarrollo_cognitivo.pdf

NIIS. (2019). *Nordic Institute for Interoperability Solutions*. Recuperado el 05 de 08 de 2019, de X-Road – the data exchange layer: https://www.niis.org/data-exchange-layer-x-road

OECD. (08 de octubre de 2013). *Competency Framework.* Obtenido de Sitio Web de la OECD: https://www.oecd.org/careers/competency_framework_en.pdf

OECD. (01 de octubre de 2015). *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document.* Paris: OECD Publishing. doi:http://www.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en

Patru, M., & Balaji, V. (2016). *Making Sense of MOOCs. A Guide for Policy-Makers in Developing Countries.* Paris: UNESCO.

Pérez Cárdenas, S., Rosas Mercado, A., & Martínez Valdés, F. D. (2017). (Humanidades, Tecnología y Ciencia del Instituto Politécnico Nacional) Recuperado el 04 de 08 de 2019, de La navaja de Ockham y los cálculos termodinámicos: http://revistaelectronica-ipn.org/Contenido/18/CIENCIA_18_000515.pdf

Piaget, J. (1952). *The origins of intelligence in children.* New York: International University Press. Obtenido de http://www.pitt.edu/~strauss/origins_r.pdf

Popper, K. R. (2002). *Búsqueda sin término: una autobiografía intelectual.* Alianza Editorial.

PwC. (2018). *Strengthening digital society against cyber shocks. Key findings from The Global State of Information Security Survey 2018.* Recuperado el 05 de 08 de 2019, de

PricewaterhouseCoopers International Limited: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

Quezada, P., & Garbajosa, J. (2015). Uso de Body of Knowledge y Clopud Computing Tools para la Gestión de Proyectos de Software Basados en Principios de Innovación Educativa. *Tendencias y Desafios de la Innovación Educativa: Un Debate Abiertro*, 1937-1949.

Rabanal, N. (2017). Cursos MOOC: un enfoque desde la economía. *RIED: Revista Iberoamericana de Educación a Distancia, 20*(1), 145-160. doi:10.5944/ried.20.1.16664

RAE. (2005). *Sigla*. Obtenido de Diccionario panhispánico de dudas (1 ed): http://lema.rae.es/dpd/srv/search?id=nNmc4LzNaD6zHPhgWc

RAE. (2014). Obtenido de Diccionario de la lengua española (23ª ed.).: http://dle.rae.es/?id=WT8tAMI

Ramírez Montoya, M. S., & García Peñalvo, F. J. (2015). Movimiento educativo abierto. *Virtualos: Revista de cultura digital, 6*(12). Obtenido de http://www.revistavirtualis.mx/index.php/virtualis/article/view/125

Raposo, M., Sarmiento, J., & Martínez, M. (2017). El perfil pedagógico de los MOOC a partir de un estudio exploratorio. *Estudios Pedagógicos, XLIII*(2), 277-292.

Ravia, P., Najma, Z., Bhasina, S., Khairallahb, M., Gupta , S. S., & Chattopadhyay, A. (07 de 2019). *Security is an architectural design constraint.* Recuperado el 05 de 08 de 2019, de https://www.sciencedirect.com/science/article/abs/pii/S0141933118302229

Revelo-Sánchez, O., Collazos-Ordoñez, C., & Jimenez Toledo, J. A. (30 de diciembre de 2018). la gamificación como estrategia didáctica para la enseñanza/aprendizaje de la programación: un mapeo sistemático de literatura. *Lámpsakos*. doi:https://doi.org/10.21501/21454086.2347/doi.org/10.21501/21454086.2347

Rosselle, M., Caron, P. A., & Heutte, J. (2014). A typology and dimensions of a description framework. *European MOOCs Stakeholders Summit 2014, eMOOCs 2014*, 130-139. Obtenido de https://hal.archives-ouvertes.fr/hal-00957025/document

Sampieri Hernández, R., & Mendoza Torres, C. P. (2018). *Metodología de la Investigación: Las rutas cuantitativa, cualitativa y me}ixta.* México D.F.: Mc Graw Hill.

Schunk, D. H. (1991). *Learning theories: An educational perspective* (6 ed.). Boston: Pearson.

Siemens, G. (2004). Connectivism: A Learning Theory for the Digital Age. *International Journal of Instructional Technology and Distance Learning (ITDL)*. Obtenido de https://www.semanticscholar.org/paper/elearnspace.-Connectivism%3A-A-Learning-Theory-for-Siemens/a25f84bc55488d01bd5f5acac4eed0c7d8f4597c

Siemens, G. (10 de agosto de 2005). *Connectivism: Learning As Network-Creation.* Obtenido de http://masters.donntu.org/2010/fknt/lozovoi/library/article4.htm

Siemens, G. (2013). Massive Open Online Courses: Innovation in education? En R. McGreal, W. Kinuthia, & S. Marshall (Edits.), *Open Educational Resources: Innovation, Research and Practice* (Vol. 2, págs. 5-16). Vancouver: Commonwealth of Learning. Obtenido de https://oerknowledgecloud.org/sites/oerknowledgecloud.org/files/pub_PS_OER-IRP_web.pdf

Skinner, B. F. (1974). *Sobre el Conductismo.* Barcelona: Planeta-De Agostini,S.A.

Snowden, B. L., & Daniel, J. S. (1980). The economics and management of small post-secondary distance education systems. *Distance Education, 1*(1), 68-91. doi:10.1080/0158791800010105

Spencer, L. M. (1992). *Competency Assessment Methods: History and State of the Art.* Boston: Hay/McBer Research Press.

Spencer, L. M., & Spencer, S. M. (1993). *Competence at work: Models for Superior Performance.* (J. W. Sons, Ed.) New York, United States of America. doi:https://doi.org/10.1002/hrdq.3920050411

Taleb, N. N. (2012). *The black swan : the impact of the highly improbable.* New York: Random House.

The Open Group. (2016). *Open Information Security Management Maturity Model.* Obtenido de https://publications.opengroup.org/downloadable/download/link/id/MC40NTkxMzAwMCAxNTcwMDMxMDQ4NDYyOTU0NDc2ODAyODI3/

The Open Group. (s.f.). *TOGAF*. Recuperado el 04 de 08 de 2019, de The Open Group Architecture Framework - TOGAF: https://www.opengroup.org/togaf

Torres Vargas, G., Reyes Montaño, E., Moreno Gómez, Á. D., & López López , D. (2015). *Reflexión y debate sobre innovación académica.* Bogotá D.C.: Universidad Nacional de Colombia. Obtenido de http://www.dnia.unal.edu.co/sites/default/files/ebook/pagina-doble-innovacion-academica.pdf

Triola, M. F. (2009). *Estadística.* México: Pearson. Obtenido de https://www.uv.mx/rmipe/files/2015/09/Estadistica.pdf

UNESCO. (2013). *United Nations Educational, Scientific and Cultural Organization.* Obtenido de Policy guidelines for mobile learning: https://unesdoc.unesco.org/ark:/48223/pf0000219641

UNESCO. (2017). *United Nations Educational, Scientific and Cultural Organization.* Obtenido de Ljubljana OER Action Plan 2017 : https://en.unesco.org/sites/default/files/ljubljana_oer_action_plan_2017.pdf

Uniandes. (junio de 2019). La Tríada: educación de Latinoamérica para el mundo. *Nota Uniandina*(53).

USATI. (08 de Mayo de 2017). Grupo Focal Número 2. (G. A. Restrepo, Entrevistador)

Vaill, P. B. (1996). *Learning as a Way of Being: Strategies for Survival in a World of Permanent White Water.* San Francisco: Jossey-Bass.

Varios. (07 de Abril de 2017). Grupo Focal Número 1. (G. A. Restrepo, Entrevistador)

Verhagen, P. (2006). *2006.* Obtenido de Surf e-learning themasite: http://elearning.surf.nl/e-learning/english/3793

Wagner, L. (1977). The economics of the open university revisited. *Higher Education, 6*, 359-381. doi:https://doi.org/10.1007/BF00141373

World Economic Forum. (2019). *The Global Risks Report 2019 14th Edition*. (ISBN: 978-1-944835-15-6) Recuperado el 05 de 08 de 2019, de http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Zapata Ros, M. (2013). MOOCs, una visión crítica y una alternativa complementaria. *Revista Campus Virtuales, 2*(1), 20-38. Obtenido de http://uajournals.com/ojs/index.php/campusvirtuales/article/view/26

Anexo A

Los dominios, objetivos de control y las preguntas relacionadas son:

- Dominio: Políticas de seguridad
- Objetivo de control 1: Orientación de la Dirección para la Gestión de la Seguridad de la Información
- Preguntas:

.1. ¿La organización reconoce la necesidad de la seguridad para TIC?

.2. ¿Existe conciencia sobre la seguridad y ésta es promovida por la alta dirección?

.3. ¿La seguridad en TIC es una responsabilidad de todas las partes interesadas de la institución?

.4. ¿Se cuenta con una estrategia de seguridad de TIC, definida, implementada y operacionalizada en la Entidad?

.5. ¿Existe una función definida y dedicada a un Ejecutivo de Seguridad que monitorea todo el contexto de las actividades relacionadas con la seguridad de TIC?

.6. ¿Se cuenta con una planeación para la revisión, adecuación y mejora de las Políticas de Seguridad de la Información?

.7. ¿La Entidad cuenta con un proceso integrado que permita evaluar la aplicación y los resultados de las políticas de seguridad que incluya los aspectos organizacionales, operacionales y tecnológicos con la mejora continua?

.8. ¿La Entidad dispone de un Modelo de Seguridad con alcance a los recursos, capacidades, talento humano y gestión de los riesgos aplicando los lineamientos establecidos en el Estado Colombiano?

.9. ¿Los lineamientos definidos por la Alta Dirección incluyen la gestión de la seguridad de la información como un proceso permanente documentado, monitoreado y mejorado continuamente?

.10. ¿El Modelo de Seguridad existente permite emitir Informes periódicos para el Comité de Seguridad de la Información sobre el estado actual de la seguridad de TIC en la Entidad?

.11. ¿Cuenta la Entidad con procedimientos para realizar revisiones periódicas de la seguridad de TIC?

.12. ¿Se ha implementado un Modelo de Seguridad de la Información constituido por Políticas, Normas, Procedimientos y Estándares de Seguridad?

.13. ¿El Modelo de Seguridad está alineado con las mejores prácticas y estándares de seguridad?

.14. ¿La Organización conoce y acata las prescripciones de seguridad contenidas en el Modelo de Seguridad?

.15. ¿Se han definido Acuerdos de Servicio (ANS) e Indicadores que supervisen y evalúen la función de seguridad y estos son divulgados a toda la Organización?

.16. ¿Existe un comité de seguridad que participa activamente en la evaluación y el fortalecimiento del Modelo de Seguridad de la Entidad?

.17. ¿Existen métricas definidas para establecer el grado de despliegue y adopción de las políticas de seguridad de TIC?

.18. ¿La seguridad está vinculada con el código de ética de la Organización y sus excepciones son consideradas como una falta grave en la misma?

- Dominio: Organización de la seguridad
- Objetivo de control 1: Organización interna
- Objetivo de control 2: Dispositivos móviles y teletrabajo
- Preguntas:

.19. ¿Se ha definido y publicado una Política de Seguridad de la Información en la Entidad?

.20. ¿La Política ha definido claramente los roles y responsabilidades (Matriz RACI) relacionados con la Seguridad de la Información?

.21. ¿Se ha definido un Plan para la implementación del Modelo de Seguridad de la Información?

.22. ¿La Política de Seguridad establecida en la Organización ha previsto la clara separación de deberes en la misma de tal forma que las responsabilidades asociadas a cada rol (función) sean las que correspondan?

.23. ¿Se ha contemplado y aplica el principio del menor privilegio?

.24. ¿La Entidad cuenta con mecanismos que le permitan fortalecer permanentemente su Modelo de Seguridad con las actualizaciones e innovaciones de la Industria de Seguridad de la Información?

.25. ¿En los programas o proyectos realizados en la Entidad la Unidad encargada participa o emite los lineamientos correspondientes a fin de garantizar la implementación de los lineamientos establecidos en la Política de Seguridad?

.26. ¿En las áreas de la Entidad se dispone de métricas que establezcan el grado de exposición de los activos de información en especial los más críticos?

.27. ¿Se cuenta con métricas que establezcan el número de los funcionarios que han recibido y aceptado roles y responsabilidades de seguridad de la información?

.28. ¿En la Entidad se utilizan entornos de desarrollo y operación con dispositivos móviles que incluyan las medidas de seguridad requeridas para proteger la información que se procesa y almacena en ellos?

.29. ¿La seguridad prevista en la infraestructura tecnológica (entornos de red LAN, WAN, etc.) incluye los adecuados niveles de protección para los dispositivos móviles (portátiles, PDA, etc.) en aspectos tales como antivirus, parches, firewalls, proxys, entre otros?

.30. ¿La Política de Seguridad tiene alcance al uso de los dispositivos móviles de forma que la información que se procesa y almacena en ellos sea objeto de seguimiento y control?

.31. ¿La transmisión de información y el uso de la red WiFi son protegidos?

.32. ¿La información y los recursos utilizados y accedidos en ambientes de teletrabajo en la Entidad son controlados y han sido incluidos en la Política de Seguridad?

.33. ¿El ambiente de teletrabajo y de acceso remoto es autorizado y contiene medidas básicas de protección?

.34. ¿El ambiente de teletrabajo ha sido debidamente reglamentado con alcance a los dispositivos cliente, servidores de acceso remoto, identificación de recursos, autenticación, etc., los cuales deben estar protegidos contra amenazas?

- Dominio: Seguridad de los recursos humanos
- Objetivo de control 1: Antes de asumir el empleo
- Objetivo de control 2: Durante la ejecución del empleo
- Objetivo de control 3: Terminación y cambio del empleo
- Preguntas:

.35. ¿Existe dentro de las políticas un proceso de verificación de antecedentes con base en las funciones a desempeñar por parte del funcionario o contratista?

.36. ¿El procedimiento contempla la clasificación de la información que va a ser accedida o administrada por el funcionario o contratista?

.37. ¿Se incluye dentro de la contratación un acuerdo sobre las funciones y responsabilidades con relación a la seguridad de la información?

.38. ¿El departamento de RRHH genera e informa las estadísticas relacionadas con excepciones de seguridad y violaciones del código de ética por parte del personal?

.39. ¿La política de RRHH establece un adecuado nivel de concientización, sensibilización y capacitación en procedimientos de seguridad?

.40. ¿El proceso de control interno y de evaluación de personal contempla aspectos específicos de administración de la seguridad en puestos de trabajo, instalaciones y equipos?

.41. ¿El régimen de contratación ha previsto una cláusula de responsabilidad en seguridad de la información?

.42. ¿El departamento de RRHH revisa y refresca de manera periódica y en conjunto con los funcionarios aspectos especiales de la seguridad de la información?

.43. ¿Existe un plan de capacitación regular orientado a la divulgación de actualizaciones de seguridad en la Entidad?

.44. ¿Los procedimientos y políticas permiten que el personal devuelva las credenciales, permisos de acceso, bienes, datos e información que le fueron entregados?

.45. ¿Los procedimientos y prevén la actualización inmediata de los roles y responsabilidades relativos a la seguridad cuando hay cambio de trabajo?

.46. ¿Las novedades de personal están vinculadas a procedimientos para permitir revocatoria de permisos y privilegios al momento de presentarse un cambio empezando por los recursos o sistemas críticos?

.47. ¿Se bloquean las cuentas de correo electrónico al momento de presentarse el retiro de la Entidad a fin de prevenir fuga de información? recursos, autenticación, etc., los cuales deben estar protegidos contra amenazas?

- Dominio: Gestión de activos
- Objetivo de control 1: Responsabilidad por los activos
- Objetivo de control 2: Clasificación de la información
- Objetivo de control 3: Manejo de medios de almacenamiento
- Preguntas:

.48. ¿Todos los activos (Bases de Datos, datos, archivos, equipos informáticos, medios magnéticos, software, aplicaciones, infraestructura de comunicaciones, etc.) sin excepción están identificados (ubicación, número de serie, versión, estado), se conoce en todo momento el poseedor o "propietario" de los mismos y se realizan conciliaciones del inventario para establecer diferencias?

.49. ¿Se cuenta con un inventario de activos clasificados de acuerdo a su importancia para la Organización?

.50. ¿Los procedimientos de seguridad han establecido regulaciones para el uso adecuado de la información y se conoce e informa cualquier eventualidad al respecto?

.51. ¿Los activos son devueltos convenientemente una vez finalizada la relación contractual?

.52. ¿La Política y procedimientos de Seguridad establecen regulaciones para el uso de los activos de información, las excepciones son analizadas y se toman las medidas que corresponden con base en el código de ética y en el código disciplinario de la Entidad?

.53. ¿La entidad cuenta con una librería o biblioteca de infraestructura de TIC (CMDB) para la gestión del inventario y se utilizan herramientas alineadas a buenas prácticas para su control?

.54. ¿En la Entidad se ha clasificado y calificado la información de acuerdo con los preceptos legales aplicables en el país y estos se cumplen estrictamente?

.55. ¿La clasificación de la información de la Entidad ha tenido en cuenta su importancia, nivel de protección requerido, medidas especiales para su tratamiento con base en la confidencialidad, seguridad, disponibilidad e integridad?

.56. ¿Se han definido los roles y responsabilidades (Matriz RACI) en relación con los usos de la información en la Entidad: consulta, producción, tratamiento, disposición final de la información y demás aspectos relacionados con el ciclo de vida de esta?

.57. Cuando se publica y utiliza la información en la Entidad ¿Se califica la misma a efectos de establecer los controles físicos, administrativos y de protección a tener en cuenta en su administración?

.58. ¿Se ha reglamentado el tipo y uso de los medios de almacenamiento y transmisión de información tanto fijos como removibles y es de conocimiento general en la Entidad?

.59. ¿Los medios de almacenamiento y soporte utilizados en la Entidad han sido plenamente identificados y se cuenta con un inventario de ellos?

.60. ¿Todos los medios de almacenamiento fijos, extraíbles y en tránsito utilizados en la Entidad están adecuadamente protegidos contra acceso no autorizado, mal uso o corrupción?

.61. ¿La Política y los procedimientos de seguridad contemplan el borrado o destrucción de la información que ya no tiene utilidad para la organización con base en la legislación vigente?

.62. ¿Se utilizan en la Entidad procedimientos de cifrado de información, particiones con cifrado y protección y similares a fin de evitar su uso por parte de interesados no autorizados?

.63. ¿Se generan estadísticas de los soportes de respaldo de información en la Entidad y se verifica su contenido frecuentemente?

- Dominio: Control de acceso

- Objetivo de control 1: Requisitos del negocio
- Objetivo de control 2: Gestión de acceso al usuario
- Objetivo de control 3: Responsabilidades del usuario
- Objetivo de control 4: Control de acceso a sistemas y aplicaciones
- Preguntas:

.64. ¿Existe una Política de Control de Acceso clara y gestionada a través de los procedimientos de seguridad establecidos con base en las necesidades de seguridad de la Entidad?

.65. ¿Los requerimientos de seguridad de TIC tienen alcance al uso de las redes de comunicaciones de la Entidad y a todos sus servicios en general?

.66. ¿En los acuerdos de servicio se identificaron e incluyeron características de seguridad?

.67. ¿Los responsables de la red implementan controles que aseguren la información y la protección de los servicios?

.68. ¿La función de control de acceso se ha construido a partir de los Roles y Responsabilidades definidos en la Entidad?

.69. ¿Existen informes periódicos para el Comité de Seguridad de la Información sobre los intentos de acceso no autorizados a los recursos de la entidad y sobre éste se toman medidas efectivas?

.70. ¿El Sistema Operativo, las Bases de Datos y Aplicativos en general se han diseñado y/o configurado a fin de permitir la trazabilidad de los eventos de seguridad?

.71. ¿Los logs y eventos de seguridad se revisan diariamente y las excepciones y desviaciones presentadas se comunican al comité de seguridad de la Organización?

.72. ¿La Gestión de la Seguridad se realiza en el marco de la mejora continua en la Entidad?

.73. ¿El Modelo de Seguridad incluye políticas y/o procedimientos formales (aprobados, actualizados y debidamente divulgados) para la administración del acceso lógico a los sistemas operativos, Bases de Datos, Aplicaciones e información crítica para la Entidad?

.74. ¿Los sistemas de información de la Entidad disponen de un módulo de administración de seguridad que permita configurar privilegios dentro de los sistemas?

.75. ¿Existen controles, políticas y procedimientos para el acceso remoto a los recursos de computación de la Entidad?

.76. ¿Se realizan pruebas de intrusión o de vulnerabilidades periódicamente y sus resultados son divulgados a fin de adoptar las medidas de precaución correspondientes?

.77. ¿La configuración de los parámetros de seguridad de los diferentes sistemas de información se encuentran configurados conforme a las políticas de seguridad de la Información de la Entidad?

.78. ¿Existe y es monitoreado un procedimiento de asignación y control de altas, bajas y actualización del registro de los usuarios, así como para la revocatoria de privilegios y permisos a los distintos recursos y servicios de la Entidad por parte de los usuarios?

.79. ¿Los perfiles de autorización que se otorgan a los usuarios de los sistemas de información se configuran de acuerdo con sus funciones dentro de la Organización?

.80. ¿Existe una matriz de segregación de funciones documentada que permita la asignación de privilegios de acceso en los diferentes sistemas de información que permitan evitar situaciones de fraude?

.81. ¿Existen procesos para revisar periódicamente los privilegios del sistema y controles de acceso a las diferentes aplicaciones y bases de datos en la infraestructura de TIC para determinar si son apropiados?

.82. ¿Al finalizar la relación contractual se retiran automáticamente los privilegios y derechos asignados a los usuarios?

.83. ¿Se generan estadísticas sobre las peticiones de cambio de acceso y el uso de los recursos, así como el tiempo requerido para llevarlos a cabo?

.84. ¿Las modificaciones a los perfiles de acceso a los recursos y servicios de la Entidad se realizan a través de un proceso de gestión de cambios?

.85. ¿Las responsabilidades de seguridad de la información definidas en la Entidad han sido divulgadas, asimiladas y aplicadas por el personal?

.86. ¿Hay reportes de seguridad de TIC o un proceso de respuesta para resolver brechas de seguridad de TIC?

.87. ¿En las evaluaciones del desempeño del funcionario se ha incluido la revisión de los aspectos de seguridad que son del resorte del empleado y en los cuales haya podido tener deficiencias en su cuidado?

.88. ¿Se tiene diseñado un procedimiento de control de acceso que considere control de tiempo por sesión, número de intentos de acceso y *Single Sign On*?

.89. ¿Se han definido, aplican y divulgan indicadores relativos al control de seguridad en TIC?

.90. ¿Los incidentes de seguridad se incluyen en la gestión de incidentes de la Entidad?

.91. ¿Los incidentes de seguridad en TIC se clasifican, categorizan y escalan de acuerdo a su criticidad e impacto para el negocio?

.92. ¿Las políticas, procedimientos y reglas de seguridad se extienden a la protección de los activos críticos?

.93. ¿Existen planes periódicos de capacitación sobre seguridad de TIC a los funcionarios de la Entidad?

.94. ¿La seguridad está vinculada con el código de ética de la Organización y sus excepciones son consideradas como una falta grave en la misma?

- Dominio: Criptografía
- Objetivo de control: Controles criptográficos
- Preguntas:

.95. ¿Se aplican herramientas de criptografía para asegurar la información?

.96. ¿Se usan controles criptográficos claves de acceso a los sistemas, datos, servicios, transmisiones de información reservada o crítica?

.97. ¿Se usan algoritmos de cifrado simétricos o asimétricos para proteger las claves de usuario?

.98. ¿Se emplean firmas digitales para asegurar los documentos electrónicos?

.99. ¿Se ha definido una política de controles criptográficos?

.100. ¿Se mantiene copia de las llaves de cifrado de forma segura y es factible recuperar la información en caso de ausencia temporal o permanente de su custodio?

.101. ¿Hay responsables de la documentación, divulgación y actualización de los procedimientos de cifrado?

- Dominio: Seguridad física y del entorno
- Objetivo de control 1: Áreas seguras
- Objetivo de control 2: Seguridad de equipos
- Preguntas:

.102. ¿Existe o se ha planeado el fortalecimiento de las condiciones de seguridad física de las instalaciones (por ejemplo, control biométrico de acceso, tarjetas magnéticas, panel de identificación, vigilancia por cámaras de circuito cerrado de televisión, entre otros)?

.103. ¿Existen políticas y/o procedimientos formales (aprobados, actualizados y debidamente divulgados) para el control de acceso al centro de cómputo (por ejemplo, reglamentos, bitácoras de acceso de personal autorizado y/o visitantes, etc.)?

.104. ¿Se han realizado pruebas y verificaciones del Centro de Procesamiento de Datos alineadas con las mejores prácticas a efectos de certificar su cumplimiento?

.105. ¿Los medios de procesamiento de información crítica o confidencial se ubican en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados?

.106. ¿Está debidamente documentado a nivel de procedimientos el sistema de control de acceso al *Data Center*?

.107. ¿Se tienen establecidos y comunicados los roles y responsabilidades en temas de seguridad física?

.108. ¿La Organización reconoce que en el sitio en donde funciona el Centro de Procesamiento de Datos sean consideradas medidas de seguridad especiales para preservar los activos que resguarda?

.109. ¿Están claramente definidas las áreas del *Data Center* (Unidades de almacenamiento, racks de servidores, firewall, centros de cableado, centro de operación, impresión, cintoteca, papelería, etc.)?

.110. ¿Están claramente identificadas las rutas de evacuación?

.111. ¿El sistema de potencia se encuentra estabilizado de suerte que se mantenga su estado de operación equilibrado bajo condiciones normales?

.112. ¿Se cuenta con un programa de señalización de las áreas restringidas?

.113. ¿Se cuenta con instalación con tierra física para todos los equipos?

.114. ¿La instalación eléctrica se realizó específicamente para el centro de cómputo?

.115. ¿Se cuenta con Planta de emergencia?

.116. ¿El personal de las instalaciones ha sido entrenado por completo respecto a situaciones de emergencia, así como en prácticas de salud y seguridad?

.117. ¿Se cuenta con herramientas de la mesa de servicio en la Entidad?

.118. ¿Los controles ambientales se implementan y monitorean por parte del personal de operaciones?

.119. ¿Se ha prohibido almacenar en el área elementos como papelería, utensilios de trabajo y material fungible?

.120. ¿Existen prohibiciones para fumar, consumir alimentos y bebidas?

.121. ¿Se generan informes de inspecciones periódicas de seguridad física de las instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes?

.122. ¿Existen políticas y/o procedimientos de mantenimiento preventivo debidamente documentados y divulgados aplicados a toda la infraestructura informática?

.123. ¿Los equipos son revisados antes de ser retirados de las instalaciones?

.124. ¿Existe un plan de mantenimiento preventivo de los equipos del *data center*?

.125. ¿Las instalaciones del *data center* disponen de protección contra incendios?

.126. ¿Se chequean todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído?

.127. ¿Las instalaciones del *data center* disponen de un sistema eléctrico de respaldo apropiado (por ejemplo, UPS, banco de baterías alterna, etc.)?

.128. ¿El Centro de Cómputo dispone de protección contra inundación (por ejemplo, pisos falsos, conexiones eléctricas protegidas contra inundaciones, detectores de humedad, etc.)?

.129. ¿Se generan informes periódicos sobre aspectos tales como movimientos no autorizados de equipos, inspecciones a los equipos, etc.?

.130. ¿Existen condiciones apropiadas para aire acondicionado en el Centro de Cómputo y se toman constantes mediciones de la temperatura del Data Center?

.131. ¿Los estándares están definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad de personal, sistemas eléctricos y mecánicos, y protección contra factores ambientales?

- Dominio: Seguridad en las operaciones
- Objetivo de control 1: Responsabilidades y procedimientos
- Objetivo de control 2: Protección contra código malicioso
- Objetivo de control 3: Copias de seguridad
- Objetivo de control 4: Registro y seguimiento
- Objetivo de control 5: Control de software operacional
- Objetivo de control 6: Gestión de vulnerabilidades
- Objetivo de control 7: Consideraciones de las auditorías
- Preguntas:

.132. ¿Se entiende y acepta dentro de la organización, la necesidad de administrar de manera óptima las operaciones de cómputo?

.133. ¿La organización dedica tiempo y recursos al establecimiento de soporte básico de TIC y a actividades operativas?

.134. ¿Las operaciones de soporte de TIC son efectivas y eficientes para cumplir con los niveles de servicio con una pérdida de productividad mínima?

.135. ¿La Entidad tiene definidos, implementados y mantiene procedimientos estándar para operaciones de TIC (manuales, planes de cambio, procedimiento de escalamiento, etc.)?

.136. ¿La Entidad garantiza que el personal de operaciones esté familiarizado con todas las tareas de operación relativas a ellos?

.137. ¿Las operaciones de cómputo y las responsabilidades de soporte están definidas de forma clara y han sido entendidas por el personal?

.138. ¿Los procedimientos de operación de TIC cubren procesos de entrega de turno (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalamiento, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones?

.139. ¿Los procesos de administración de operaciones de TIC están estandarizados y documentados en una base de conocimiento, y están sujetos a una mejora continua?

.140. ¿La Entidad tiene establecido un proceso de administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica con costos justificables?

.141. ¿El proceso de administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica de la Entidad se encuentra formalmente documentado y divulgado?

.142. ¿Las responsabilidades para la administración, el monitoreo del desempeño, capacidad y disponibilidad de la infraestructura tecnológica de la Entidad, se encuentran claramente definidas?

.143. ¿La Entidad revisa la capacidad y el desempeño actual de los recursos de TIC en intervalos regulares para determinar si son eficientes para prestar los servicios con base en los niveles de servicio acordados?

.144. ¿Se tienen definidos indicadores de desempeño para medir la administración actual del ambiente de cómputo?

.145. ¿La Entidad lleva a cabo un pronóstico de desempeño y capacidad de los recursos de TIC en intervalos regulares, para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño?

.146. ¿La Entidad identifica el exceso de capacidad para una posible redistribución?

.147. ¿Se identifica las tendencias de las cargas de trabajo y determina los pronósticos que serán parte de los planes de capacidad y de desempeño?

.148. ¿Se controlan los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información?

.149. ¿Existe y se aplica un proceso de Gestión de Cambios en la Entidad para la gestión de TIC?

.150. ¿En la Entidad se han implementado controles para la detección, prevención y recuperación por afectaciones de virus, malware, spyware, spam y existen programas de sensibilización, concientización y entrenamiento a los usuarios?

.151. ¿Los procedimientos de seguridad establecidos en la Entidad incluyen medidas de protección contra código malicioso, scripts dañino y programas tipo adware, phishing, inyección de SQL y otros?

.152. ¿Se generan reportes periódicos sobre las excepciones de seguridad presentadas y software malicioso oculto detectado y contrarrestado?

.153. ¿Se han considerado medidas de protección que prevengan situaciones de riesgo en las *appstores*, datos procesados y almacenados en móviles, SMS, *emails*, entre otros?

.154. ¿Existen sistemas para monitorear y responder a interrupciones potenciales del negocio debido a incidentes de intrusión maliciosa y actualizar los protocolos de seguridad para prevenirlos?

.155. ¿Existen políticas y/o procedimientos formales (aprobados, actualizados y debidamente divulgados) para el manejo de antivirus (actualizaciones/Monitoreo/Informes/*Hotfix*) al interior de la Entidad?

.156. ¿Existe una Política de Respaldo de información establecida en la Entidad aprobada y divulgada que responda a los requerimientos de seguridad y del negocio?

.157. ¿La Estrategia de respaldo responde a una valoración de los activos críticos de la Organización que considere la aplicación de *backup*, frecuencia de copia, prueba de soportes y medios de almacenamiento?

.158. ¿Se realizan pruebas frecuentes de la información que ha sido respaldada (información, imágenes, correos) y ésta es adecuadamente inspeccionada a partir de su importancia para la Entidad?

.159. ¿Se generan estadísticas de las operaciones de BK realizadas, de las pruebas efectuadas, porcentaje de recuperaciones de prueba exitosas, porcentaje de información cifrada teniendo en cuenta su importancia para la Entidad?

.160. ¿Se producen, mantienen y revisan periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información?

.161. ¿Los *logs* de actividades, registros de la operación, bitácoras de acceso, copias de respaldo se protegen contra accesos, usos y alteraciones no autorizados?

.162. ¿Se registran las actividades del administrador y del operador del sistema, DBA y los registros asociados se protegen y revisan de manera regular?

.163. ¿Se sincronizan los relojes de todos los sistemas de procesamiento de información, servidores e infraestructura crítica en relación a una fuente de sincronización única (estándar) de referencia tipo NTP?

.164. ¿Se generan estadísticas de revisión de logs realizadas en un periodo determinado y las excepciones son revisadas y divulgadas en el Comité de Seguridad de la Información?

.165. ¿Se producen reportes de acceso a recursos: archivos, directorios y programas y las excepciones se informan a todas las partes interesadas?

.166. Para prevenir los riesgos de alteración de los sistemas de Información mediante controles de implementación de cambios ¿Dispone la Entidad de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones?

.167. ¿Los cambios son gestionados por personal autorizado y en atención a los términos y condiciones formalizados en la Entidad?

.168. Existe un proceso de gestión de cambios alineado a las buenas prácticas existentes que incluya: a) Registro y aceptación de la solicitud de cambio b) Clasificación del cambio c) Aprobación y planeación del cambio d) Implementación del cambio e) Monitoreo del cambio f) Evaluación, mejora continua y cierre.

.169. ¿Existe un Comité de Gestión de Cambios en la Entidad?

.170. ¿El proceso de gestión de cambios incluye la entrega de la documentación y el control de las versiones del código desarrollado?

.171. ¿El proceso de gestión de cambios está vinculado con la gestión de la capacidad, la gestión de incidentes, gestión de la continuidad, gestión de la disponibilidad y de Niveles de servicio?

.172. ¿La instalación de software en producción supone primero la revisión exhaustiva del código en ambiente de test?

.173. ¿Se realizan test de vulnerabilidades en la Organización para establecer el grado de exposición de los activos?, los resultados son conocidos y adoptadas las medidas preventivas y correctivas?

.174. ¿Toda instalación de software está procedimentada y sus resultados son conocidos y evaluados?

.175. ¿Se siguen estándares de la industria para realizar las pruebas de vulnerabilidades como OWASP, NIST, OSSTMM?

.176. ¿Se ha instituido en la Entidad la función de Auditoría de Sistemas que abarque todo el ciclo de vida como a) Origen y preparación de los datos b) Entrada de

Información c) Proceso y actualización de información d) Respaldo y recuperación de información e) Exposición de Información f) Salida de información?

.177. ¿Se evalúan las aplicaciones periódicamente con base en un Plan de Auditoria y este abarca tanto el desarrollo como la producción de sistemas de información?

.178. ¿Los sistemas de información sin excepción son auditables y se han implementado en estos los controles que contrarresten las debilidades del sistema de control interno?

.179. ¿Se generan informes de auditoría periódicos y estadísticas de implementación de controles, así como el tiempo de resolución /cierre de recomendaciones de control por parte de las áreas auditadas?

- Dominio: Seguridad en las telecomunicaciones
- Objetivo de control 1: Gestión de seguridad en redes
- Objetivo de control 2: Transferencia de información
- Preguntas:

.180. ¿Se cuenta con un inventario actualizado de recursos y servicios de red?

.181. ¿La red cuenta con mecanismos de protección adecuados, acordes con la política de la Entidad?

.182. ¿La red es permanentemente monitoreada?

.183. ¿La matriz RACI contempla segregación de funciones (usuarios, administradores, etc.)?

.184. ¿Se generan estadísticas de los firewalls?

.185. ¿Se generan estadísticas de los incidentes en las redes?

.186. ¿Se maneja el cifrado para contrarrestar la exposición de la información?

.187. ¿Para los servicios de acceso remoto se usan conexiones seguras?

.188. ¿Se han implementado herramientas especializadas para la detección de intrusos?

.189. ¿Se han definido y se aplican políticas y procedimientos de intercambio de información que incluyan controles formales?

.190. ¿Se tienen suscritos acuerdos de confidencialidad y no divulgación tipo NDA (*Non Disclosure Agreement)*?

.191. ¿Los acuerdos de intercambio de información se renuevan periódicamente o cuando existe una actualización de la política?

.192. ¿Existen ANS (Acuerdos de Nivel de Servicio) suscritos con terceros para la regulación de los intercambios de información?

.193. ¿Las restricciones o regulaciones de intercambio de información se extienden a los metadatos a fin de evitar fugas ocultas en estos?

- Dominio: Adquisición, desarrollo y mantenimiento de sistemas de información
- Objetivo de control 1: Requisitos de seguridad de los sistemas de información
- Objetivo de control 2: Seguridad en los procesos de desarrollo y soporte
- Objetivo de control 3: Datos de prueba
- Preguntas:

.194. ¿El proceso de desarrollo de sistemas de información incluye la especificación de controles de seguridad durante todo el ciclo de vida?

.195. ¿Los requisitos de control son adecuadamente identificados y se mantienen en una librería y forman parte de la documentación del sistema?

.196. ¿En la definición de requisitos de seguridad participan áreas de negocio, control y seguridad de la información?

.197. ¿Los requisitos de seguridad se aplican por igual a desarrollos, mejoras y adquisiciones?

.198. ¿La información de los servicios de las aplicaciones que se transmiten por medio de redes públicas se protegen contra posibles actividades fraudulentas?

.199. ¿La información de las aplicaciones está protegida en su transmisión y enrutamiento incorrectos para evitar alteración, divulgación o reproducción no autorizadas?

.200. ¿En la especificación y aprobación de los requerimientos se define la matriz RACI?

.201. ¿Se efectúan pruebas periódicas de la fortaleza de los controles definidos para los sistemas de información?

.202. ¿En la fase de *testing*, se realizan pruebas de los requerimientos de seguridad y control?

.203. ¿Se ha incorporado y se aplica formalmente un proceso de gestión de cambios?

.204. ¿Todas las aplicaciones sin excepción han cumplido un plan riguroso de pruebas para certificar su seguridad?

.205. ¿Los cambios o modificaciones al software son sometidos a un procedimiento de aprobación por parte de un comité (CAB) conformado para esa tarea?

.206. ¿El entorno de desarrollo dispone de la seguridad para el desempeño de esa tarea y las excepciones son informadas y corregidas?

.207. ¿Los controles de seguridad se incorporan en las especificaciones contractuales con las fábricas de software?

.208. ¿Los controles de seguridad se extienden al soporte y mantenimiento del software en desarrollo?

.209. ¿Los sistemas de información cuentan con mecanismos de autenticación, integridad, control de acceso, respaldo y log de auditoría?

.210. ¿En la adquisición de software se asegura que el proveedor ha realizado capacitación a su personal sobre el mismo?

.211. ¿Para la realización de las pruebas se dispone de vistas o conjuntos de datos de prueba que eviten acceder a datos operativos?

.212. ¿Los datos de prueba son seleccionados cuidadosamente de tal forma que cumplan con los escenarios previamente definidos de acuerdo a las mejores prácticas?

.213. ¿Se emiten informes periódicos de las aplicaciones que han sido formalmente para la inclusión de los estándares de pruebas definidos previamente?

.214. ¿Se aplica algún modelo de madurez para el proceso de pruebas de las aplicaciones?

- Dominio: Relación con proveedores
- Objetivo de control 1: Requisitos de seguridad de los sistemas de información
- Objetivo de control 2: Seguridad en los procesos de desarrollo y soporte
- Objetivo de control 3: Datos de prueba
- Preguntas:

.215. ¿La Entidad dispone de una Política de contratación de servicios de TIC que integre la seguridad de la información?

.216. ¿La Entidad tiene identificados todos los servicios de TIC provistos por terceros?

.217. ¿Los servicios de los proveedores de TIC se encuentran catalogados de acuerdo con el tipo de proveedor, la importancia y la criticidad de los servicios provistos?

.218. ¿Los requisitos de seguridad de TIC se han acordado y documentado con el objetivo de mitigar los riesgos asociados al acceso a los activos de información por parte de proveedores y terceras personas?

.219. ¿Los contratos firmados con los terceros son revisados de forma periódica para establecer si está cubierto apropiadamente el acceso, proceso, almacenamiento y modificación de la información?

.220. ¿Se mantienen actualizados los ANS suscritos con terceros en todo lo referente a sus responsabilidades con los servicios que prestan?

.221. ¿El proceso de contratación con terceros siempre tiene en cuenta la definición de ANS y estos son permanentemente revisados durante el periodo de duración del contrato?

.222. ¿Se tiene documentado un procedimiento para la administración de Acuerdos de Niveles de Servicio (ANS) con los diferentes proveedores de TIC?

.223. ¿Se tiene en cuenta el proceso de Gestión de Cambios en la provisión de servicios de TIC que realizan los proveedores manteniendo y mejorando las políticas de seguridad de la información, los procedimientos y controles específicos?

.224. ¿La provisión de servicios de TIC con terceros aplica las mejores prácticas existentes como el Modelo e SCM (*e-source capability management)* y otros estándares de la industria?

.225. ¿Se evalúa la calidad de los servicios de TIC permanentemente y las deficiencias encontradas se tienen en cuenta en el proceso de contratación de nuevos servicios?

.226. ¿La administración del riesgo con proveedores contempla la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad?

.227. ¿La Entidad se asegura que los contratos con proveedores de TIC estén de acuerdo con los estándares universales del negocio y de conformidad con los requerimientos legales y regulatorios?

.228. ¿Se generan reportes de monitoreo y desempeño de los proveedores de TIC?

.229. ¿La Entidad ajusta el proceso de adquisición y monitoreo de servicios de terceros con base en los resultados de los KPIs y KGIs?

- Dominio: Gestión de incidentes
- Objetivo de control 1: Gestión de incidentes de seguridad de la información y mejoras
- Preguntas:

.230. ¿Se aplica un proceso de mejora continua en respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información?

.231. ¿En la Entidad se ha formalizado y aplica un proceso de gestión de Incidentes con base en las buenas prácticas existentes en la industria?

.232. ¿Dentro del proceso de mejora continua se tiene en cuenta las debilidades del Sistema de Control Interno detectadas a través de los incidentes de TIC presentados en especial aquellos que ha representado fraudes, pérdida y alteración de la información y han comprometido la confidencialidad, disponibilidad e integridad de la información?

.233. ¿Todos los empleados, contratistas y terceros son conscientes de los procedimientos y políticas de seguridad de la Entidad a fin de evitar el compromiso de la seguridad de los activos organizacionales?

.234. ¿La Entidad maneja una matriz de escalamiento y resolución de incidentes de acuerdo con las buenas prácticas existentes para garantizar una respuesta rápida a los incidentes de seguridad presentados?

.235. ¿Los eventos de seguridad presentados se informan y resuelven oportunamente para evitar que se conviertan en un problema en la Organización?

.236. ¿Se dispone de una herramienta que apoye la gestión de incidentes que permita administrar todo el ciclo del proceso?

.237. ¿La Gestión de Incidentes está articulada con la Gestión de Problemas, la Gestión de Cambios, la Gestión de la Disponibilidad, la Gestión de la Capacidad y la Gestión de Niveles de Servicio?

.238. ¿Los incidentes de seguridad de TIC se comunican, así como las soluciones implementadas a fin de evitar su persistencia?

.239. ¿Existe y se administra una Base de Conocimiento que registre los incidentes y las soluciones presentadas a fin de propiciar el aprendizaje y la mejora continua?

.240. ¿Se generan estadísticas de gestión de incidentes detectados y resueltos por orden de criticidad e impacto para la Organización?

- Dominio: Gestión de continuidad de negocio
- Objetivo de control 1: Continuidad de la seguridad de la información
- Preguntas:

.241. ¿Se dispone de un plan de continuidad de negocios que incorpore el plan de recuperación de desastres y las necesidades de los departamentos usuarios para recuperar oportunamente las funciones críticas, los sistemas, procesos e información del negocio?

.242. ¿Existe un plan puntual de recuperación de desastres para componentes importantes de la infraestructura de TIC?

.243. ¿El plan de continuidad del negocio tiene en cuenta los requerimientos de seguridad y se ha alineado con estándares de la industria?

.244. ¿Existe documentación de los procedimientos detallados para restaurar equipos, aplicativos, sistemas operativos, bases de datos, archivos de información, entre otros, actualmente definidos por la Entidad?

.245. ¿Hay revisiones regulares del plan de continuidad y sus resultados se han documentado?

.246. ¿Los responsables del negocio entienden los tiempos de recuperación de TIC y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio?

.247. ¿Los cambios en el plan de continuidad se realizan a través de un proceso de gestión de cambios?

.248. ¿La Entidad ha establecido, documentado, implementado y mantiene los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones de contingencia?

.249. ¿Se evalúa el Impacto en la organización ante eventos de desastres que afecten la continuidad del negocio?

.250. ¿Desde el punto de vista de la Seguridad de la Información se han determinado los puntos más críticos en el plan de continuidad de TIC, para evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, a un nivel aceptable de costo y cumpliendo con los requerimientos regulatorios y contractuales?

.251. ¿Se ha identificado y evaluado la disponibilidad de plataformas computacionales, comunicaciones e información, necesarias para soportar las operaciones definidas como de misión crítica de negocio en los tiempos esperados y acordados?

.252. ¿Se dispone de evidencia de la evaluación con los proveedores, sobre la disponibilidad de equipos y tiempos necesarios para su instalación, en préstamo, arriendo o sustitución?

.253. ¿Existen procedimientos de actualización de los planes de continuidad de negocios, de acuerdo a cambios en las condiciones de la Entidad?

.254. ¿Existe un procedimiento de actualización periódica del plan de recuperación ante desastres de acuerdo con los cambios en plataformas tecnológicas (hardware, software y comunicaciones), para reflejar permanentemente la realidad operativa y tecnológica?

.255. ¿Existen procedimientos formales para la ejecución de pruebas periódicas a los planes de continuidad de negocios y recuperación de desastres?

.256. ¿Se han realizado sesiones de capacitación de forma regular respecto a los procesos, roles y responsabilidades en caso de incidente o desastre?

.257. ¿Existe documentación de los procedimientos manuales a seguir por las distintas áreas usuarias durante el periodo de la contingencia y entrenamiento a los usuarios en estos procedimientos?

.258. ¿Está definido el personal involucrado y sus responsabilidades antes, durante y después de una posible emergencia?

.259. ¿Existe un plan puntual de recuperación y reanudación de los componentes importantes de la infraestructura de TI?

.260. ¿Los responsables del negocio entienden los tiempos de recuperación de TIC y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio?

.261. ¿Se aplican actualmente políticas y procedimientos de copias de periódicas sobre los programas de aplicación y archivos de la Entidad?

.262. ¿Existen procedimientos formales de respaldo diario de la información y almacenamiento fuera de las instalaciones físicas de la Entidad?

.263. ¿Existe un esquema de redundancia aprobado, documentado y divulgado a través de procedimientos para garantizar la continuidad de la operación teniendo en cuenta el Análisis de Impacto y la importancia de los activos de información de la Entidad?

.264. ¿Se generan estadísticas sobre la recuperación de las operaciones teniendo en cuenta a) Tiempo medio entre fallas b) Tiempo medio de Recuperación de la Falla c) Tiempo medio para que la operación falle?

.265. ¿Se generan estadísticas de gestión de incidentes detectados y resueltos por orden de criticidad e impacto para la Organización?

- Dominio: Cumplimiento
- Objetivo de control 1: Cumplimiento de los requisitos legales y contractuales
- Objetivo de control 2: Revisiones de la seguridad de la información
- Preguntas:

.266. ¿La Entidad tiene definido e implementado un procedimiento para garantizar la identificación oportuna de los requerimientos legales, contractuales, de política y regulatorios relacionados con la seguridad de la información emitidos por las autoridades competentes?

.267. ¿El procedimiento definido tiene en cuenta las leyes y regulaciones de comercio electrónico, flujo de datos, privacidad, controles internos, propiedad intelectual y derechos de autor?

.268. ¿Los requisitos de seguridad de la información han sido definidos expresamente en los contratos de servicios de TIC y estos han sido aceptados por los usuarios, contratistas y proveedores de la Entidad?

.269. ¿Los registros de propiedad intelectual y de derechos de autor se protegen contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con la legislación vigente?

.270. ¿Existe una política de seguridad para garantizar la privacidad y la protección de la información personal con base en la legislación vigente?

.271. ¿Se generan estadísticas sobre los aspectos de seguridad cubiertos y sin cubrir de acuerdo con las prescripciones legales teniendo en cuenta el impacto para el negocio?

.272. ¿Se conocen en la Organización las regulaciones existentes sobre protección de datos, usos de la información y demás que apliquen al contexto organizacional?

.273. ¿La función de auditoria de la Entidad incluye la revisión periódica de los sistemas de información y en estos se evalúa y divulga el sistema de control interno?

.274. ¿La revisión de los sistemas de información responde a una programación definida y divulgada en la Entidad a fin de propiciar el compromiso de las partes interesadas?

.275. ¿La evaluación de los Sistemas de Información tiene en cuenta las Políticas de Seguridad definidas en la Organización?

.276. ¿La evaluación del sistema de control interno de los procesos y sistemas de información tiene en cuenta las buenas prácticas existentes con alcance a aspectos de gobierno corporativo, cumplimiento legal, lineamientos de seguridad, entre otros?

.277. ¿Las desviaciones y excepciones del sistema de control interno de los procesos y aplicaciones son catalogadas, documentadas y sobre ellas se realiza seguimiento permanente con el fin de evitar su recurrencia?

.278. ¿Se generan estadísticas de cumplimiento e incumplimiento de la implementación de controles surgidos en las Auditorías y en la especificación de requerimientos y estos son divulgados a las instancias correspondientes?

.279. ¿Se generan reportes de hallazgos de auditoría relacionados con seguridad de la información que hayan sido resueltos y cerrados en relación con las desviaciones del sistema de control interno evaluado?

- Dominio: Administración de los datos
- Objetivo de control 1: Establecer controles de entrada, procesamiento y salida para garantizar la autenticidad e integridad de los datos.
- Objetivo de control 2: Verificar la exactitud, suficiencia y validez de los datos de transacciones que sean capturados para su procesamiento
- Objetivo de control 3: V Establecer procedimientos para que la validación, autenticación y edición de los datos sean llevadas a cabo tan cerca del punto de origen como sea posible.
- Preguntas:

.280. ¿Los datos son reconocidos como parte de los recursos y activos de la empresa y, se entiende y acepta la necesidad de realizar todas las actividades requeridas para la administración y seguridad de los mismos?

.281. ¿La Entidad tiene plenamente identificadas y clasificados los activos de información y ha establecido los controles para garantizar la integridad, confidencialidad y disponibilidad de la información considerada como crítica?

.282. ¿Para cumplir con los requerimientos legales, regulatorios y de negocio, se tienen establecidos mecanismos de almacenamiento y conservación de documentos, datos, archivos, programas, reportes y mensajes (entrantes y salientes), así como la información (claves, certificados) utilizada para cifrado y autenticación?

.283. ¿La Organización tiene establecidos los mecanismos necesarios para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información?

.284. ¿Se lleva a cabo un procedimiento para verificar la exactitud, suficiencia y validez de los datos generados por los sistemas de información?

.285. ¿Se tienen establecidos mecanismos al interior de la Organización para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información recibida, que se preparen y entreguen todos los reportes de salida emitidos y se destruyan los que no se requieran?

.286. ¿Se tienen definidas matrices de segregación de funciones que faciliten la definición y construcción de roles y perfiles de acceso para los diferentes sistemas de información críticos de la Entidad?

.287. ¿La Organización tiene definidos e implementados procedimientos para garantizar la validación, autenticación y edición de los datos?

.288. ¿La Organización tiene definidos e implementados procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad?

.289. ¿Se lleva a cabo algún tipo de monitoreo dentro de TI sobre actividades clave de la administración de datos (respaldos, recuperación y desecho)?

.290. ¿La Entidad tiene plenamente identificadas y clasificadas las transacciones electrónicas sensibles y críticas?

.291. ¿Se tienen definidos procedimientos para garantizar la integridad y autenticidad de las transacciones electrónicas consideradas como sensitivas y críticas?

.292. ¿La Entidad tiene establecidos controles para garantizar la integración y consistencia de los datos entre las plataformas y en ambientes de interoperabilidad e integración?

.293. ¿Existe documentación sobre la administración de las interfaces de las plataformas?