CAPÍTULO IV

MODELO DE AUDITORÍA DE SEGURIDAD CIBERNÉTICA APLICADO A LA SECRETARÍA GENERAL DE LA ALCALDÍA DE BOGOTÁ*

María del Pilar Niño Campos

* Ponencia resultado del proyecto de investigación titulado *Gestión de riesgos en seguridad digital para la infraestructura crítica*, de la Maestría en Ciberseguridad y Ciberdefensa, de la línea de investigación *Seguridad Digital*, del grupo de investigación *Masa crítica*, reconocido y categorizado en (B) por Minciencias, registrado con el código COL0123247, adscrito y financiado por la Escuela Superior de Guerra de la República de Colombia. Ponencia resultado de la investigación presentada como opción de grado para optar por el título de Magíster en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Resumen

Este capítulo presenta un modelo de auditoría cibernética que permita 1) identificar, enumerar y describir las diversas vulnerabilidades que pueden identificarse en una revisión exhaustiva de procesos y tecnología, y 2) determinar el nivel de ciberseguridad de una entidad, de forma que esta se convierta en una herramienta estratégica para el área de seguridad de la información y riesgos. Así, puede ser útil para el equipo auditor interno de una entidad o como herramienta de control para las auditorías externas de validación.

Este modelo se basa en un lenguaje común para gestionar riesgos de ciberseguridad, pues maneja un enfoque priorizado, flexible, repetible y neutral, basado en las necesidades de la entidad distrital. Permite a los responsables identificar, catalogar y gestionar los riesgos de ciberseguridad, estableciendo criterios y métricas para el control y la correspondiente emisión de una opinión objetiva e independiente del estado de ciberseguridad auditado.

El modelo propuesto gira en torno a seis ejes temáticos principales, que se unen e interrelacionan entre sí como las fuerzas de un átomo. El núcleo de este átomo es la información que reposa en la entidad y que forma parte esencial del negocio. Los ejes temáticos serán calificados con base en quince indicadores por cada uno, para un total de noventa preguntas. Aquellos tendrán una calificación de inicial, maduro y avanzado, con lo cual los hallazgos identificados tendrán una parte cuantitativa (numérica) y otra cualitativa (descriptiva) en la calificación. Para completar el set de cien preguntas, existen diez extra que interrelacionan los ejes temáticos.

Palabras clave: Auditoría de ciberseguridad; modelo de auditoría cibernética; riesgos cibernéticos; aseguramiento de ciberseguridad; controles de ciberseguridad; auditoria interna y externa cibernética.

Abstract

This chapter presents a model of cyber security audit that allows 1) describe and list vulnerabilities that can be identified in a comprehensive review of processes and technology. And 2) Determinate the level of cybersecurity of an entity. Thus, it becomes a strategic tool for the information, security, and risk areas, this model can also be useful for internal audit teams or as a control tool for external validation audits.

This model uses common language to manage cybersecurity risks, as it handles a prioritized, flexible, repeatable, and neutral approach, based on the needs of the district entity. It allows the person who is using this model identify, catalog, and manage cybersecurity risks, establishing criteria and metrics for control, and creating an objective, professional, and independent opinion of the audited cybersecurity status.

The proposed model goes around six main thematic points, which are related to each other like the forces of an atom. The nucleus of this atom is the information sitting in the entity, which is essential part of the business. The thematic points will be qualified based on 15 indicators for each one, for a total of ninety questions. These indicators will have a qualification of initial, mature, and advanced. Therefore, the found results will have a quantitative (numerical) and a qualitative (descriptive) segment. To complete the set of hundred, there are ten extras question that are connected to the thematic points.

Keywords: Cybersecurity audit; cyber audit model; cyber risks; cybersecurity assurance; cybersecurity controls; internal and external cyber audit.

1. Introducción

El hiperconectividad al ciberespacio es tal vez uno de los productos más visibles de la cuarta revolución industrial. Está beneficiando el nacimiento de nuevos ecosistemas complejos que proporcionan información en tiempo real y posibilitan las interacciones autónomas entre máquinas, sistemas, objetos y cosas.

Estos ecosistemas digitales permiten sacar el máximo partido y rendimiento a la internet de las cosas (IoT), a la nube, al *big data* y a la analítica de datos; tendencias de consumo del tipo *Bring Your Own Device* (BYOD), las aplicaciones de última generación, redes inalámbricas de sensores WSN (Wireless Sensor Networks), impresión 3D, robótica avanzada, realidad aumentada y ciberseguridad, entre otros.

En mundo cada vez más interconectado, la trasmisión de mensajes de datos, de acuerdo con la Ley 527 de 1999, se ha convertido en una necesidad para la gran mayoría de los colombianos, que encuentran en la internet la mejor herramienta para realizar sus actividades laborales y de esparcimiento personal: tareas, búsquedas de información, envío de correos electrónicos, compra y venta de artículos y acceso a redes sociales.

En una sociedad caracterizada por la explosión de las redes sociales y el uso de la internet de las cosas, la interconexión digital a escala global es un hecho, como también lo es la vulnerabilidad de los ciudadanos virtuales. Si bien hay aspectos positivos, como la socialización y el intercambio de información, hay riesgos que pueden trascender del mundo virtual al mundo real, y este es el principal estímulo de los ciberdelincuentes.

En los últimos años, los ciberataques contra los sistemas de información del sector público, de las empresas e instituciones de interés estratégico o de aquellas poseedoras de importantes activos de propiedad intelectual e industrial —y, en general, contra todo tipo de entidades y ciudadanos— se han venido incrementando en número, tipología y gravedad. Esto, según los informes presentados por la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria). Según esta, los ciberataques en Colombia crecieron el 28 % en 2018.

Ante este panorama de riesgos cibernéticos que provienen de la amenaza continua a los activos digitales, las operaciones y la información corporativa, se requirieron directrices que permitieran afrontar dicha situación. Una de estas fue el CONPES 3701 de 2011, por medio del cual se dictan los lineamientos de política para la ciberseguridad y la ciberdefensa. Tales lineamientos buscan fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la seguridad y la defensa en el ámbito cibernético, creando un ambiente propicio para la protección en el ciberespacio.

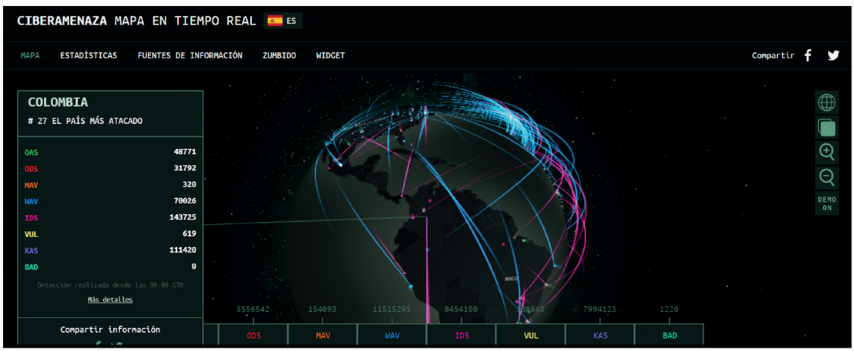
2. Antecedentes para comprender el riesgo cibernético

De acuerdo con los mapas de ciberamenzas en tiempo real, dispuestos por firmas como Kaspersky Lab (figura 4.1), y que pueden ser consultados en internet, se puede evidenciar que en promedio cien países son víctimas de ataques cibernéticos, en periodos menores a un minuto.

Los objetivos de los ciberdelincuentes varían según sus propios intereses o de terceros, y dentro de las múltiples razones esgrimidas se encuentran: la rentabilidad que ofrece su explotación, la producción de un deterioro económico directo a una compañía, el sabotaje a infraestructuras críticas, activismo político, la facilidad y el bajo costo de las herramientas utilizadas para la consecución de ataques, delitos informáticos, la sustracción de información corporativa estratégica —como la relativa a la propiedad industrial o intelectual—, robo de datos personales de

clientes y empleados, y ataques específicos a plataformas de e-commerce y redes financieras —como las relacionadas con criptomonedas. Esto se suma a una variable que genera descompensa respecto a las actividades lícitas y las contrarias a la ley en el ciberespacio, como lo es la facilidad que tiene el atacante de ocultarse. Su trazabilidad y seguimiento resulta sumamente complejo.

Figura 4.1. Mapa de amenazas en tiempo real



Fuente: Kaspersky (2019).

Por la naturaleza misma del ciberespacio, donde la conexión entre diferentes sistemas es intrínseca, cualquier sistema que dependa de una u otra manera de dicho entorno se encuentra conectado y, con esto, vulnerable a un ataque (Refsdal et al., 2015).

Si bien el término *ciberespacio* suele confundirse con el término *internet*, hay una diferencia: la expresión ciberespacio se refiere a los objetos y los recursos que coexisten en una red informática; es decir, los fenómenos que ocurren en la internet ocurren en el ciberespacio, y no en el espacio geográfico donde los cibernautas se encuentran físicamente. Así, entenderemos el ciberespacio como "un mundo no físico, el cual no tiene límites y donde cualquier persona puede estar interconectada con una conexión a la red de tal manera que pueda interactuar con el mundo entero sin barreras" (Facultad de Informática de la Universidad Complutense de Madrid, 2017a).

En el ciberespacio, el eslabón más débil de la cadena de seguridad de la información son las personas que interactúan allí, hecho que se refleja en las cifras proporcionadas por el CAI Virtual de la Policía Nacional, con corte a septiembre de 2019. Según estas, hubo un total de 7879 denuncias por hurto a través de medios informáticos.

Con corte al mes de septiembre del año 2019, se habían presentado en promedio 7800 denuncias específicamente por el Delito de Hurto por medios informáticos y semejantes, tal como lo exponen las cifras de la policía nacional.

Asimismo, hay un aumento de estos delitos a escala corporativa debido al uso extendido de la internet, que genera un mayor nivel de exposición y superficie de ataque para los cibercriminales. Además, en la mayoría de los casos no existen medidas de protección adecuadas y efectivas.

Entre otras, estas razones explican por qué el ciberespacio representa el quinto dominio de las Fuerzas de Ley. De igual manera, cualquier suceso que ocurra en el ciberespacio podría tener efectos en los mundos físico y virtual, pues da lugar a nuevas ciberamenazas que atentan contra la seguridad nacional, el Estado de derecho, la prosperidad económica, el bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas. De ahí que el ciberespacio tenga un carácter de escenario estratégico, operacional y táctico (XIX Conferencia de Directores de Colegios de Defensa Iberoamericanos, 2018).

Khuel (2009), por ejemplo, se refiere al ciberespacio como un "espacio operacional donde los humanos y sus organizaciones hacen uso de las tecnologías necesarias para actuar o crear efectos, los cuales pueden ser en el mismo ciberespacio o sobre otros dominios, operaciones o elementos del poder" (p. 29). El planteamiento de este autor nos permite comprender cómo el ciberespacio es similar a los otros cuatro dominios que existen (tierra, mar, aire y espacio), en la medida en que nace como otro dominio operacional por ser un elemento del poder dentro del cual opera la seguridad nacional. Esta característica le permite influir en los acontecimientos que surgen en todos los ambientes operativos.

Por último, vale la pena mencionar el *Informe de Riesgos Globales 2017*, publicado por el Foro Económico Mundial en su duodécima edición, donde se menciona que el riesgo cibernético emerge como uno de los diez principales riesgos por ser considerados en el entorno global, debido al aumento de su frecuencia y de su severidad por la internet de las cosas. El sinnúmero de conexiones entre personas y máquinas que esta ha provocado ha generado una ciberdependencia que aumenta las probabilidades de un ciberataque, con alto potencial de efecto dominó a través del ciberespacio (World Economic Forum, 2017).

Esta reflexión, aportada por el Foro Mundial de Economía, es muy valiosa y nos lleva a pensar que los temas que se refieren a la administración y a la contención de los riesgos asociados a las Tecnologías de información y Comunicaciones (TIC) y las tecnologías de Operación (TO) cobran en adelante un nivel de complejidad mayor, toda vez que la amenaza cibernética tiene múltiples aspectos y, sin lugar a dudas, es potencialmente peligrosa.

Sobre esto, Gastón Sack y Ierache (2015) llaman la atención sobre las características asimétricas que tiene el ciberespacio y que lo convierten en algo más complejo de definir y de defender:

> 1. la inteligencia y el engaño son aspectos críticos en el ciberespacio;
> 2. el ciberespacio es extenso, y es fácil esconderse en el mismo;
> 3. los efectos que producen los ataques son desproporcionados de cara a las herramientas que se utilizan para producirlos (pp. 3-5).

3. Riesgos de la seguridad digital

De acuerdo con lo publicado en el documento *Ciberseguridad: una guía de supervisión*, del Instituto de Auditores Internos de España (2016, pp. 9-10), los principales riesgos cibernéticos a los que se exponen todos los usuarios del ciberespacio pueden clasificarse como lo expone la tabla 4.1.

Tabla 4.1. Riesgos de la seguridad digital

Riesgo cibernético	Descripción
Fraude financiero	Es uno de los principales objetivos de los ciberdelincuentes.
Robo de información	La información de carácter personal o los documentos clasificados son algunos de los principales activos de información que deben ser especialmente protegidos. La filtración pública o la pérdida de la información confidencial tienen un riesgo elevado, cuyos impactos o pérdidas pueden resultar significativos.
Indisponibilidad de servicios	Es la interrupción puntual o prolongada de los servicios ofrecidos en línea, como correos, pagos financieros, cobro de impuestos, registros públicos, entre otros.
Sabotaje de infraestructuras	Son los ataques contra los servicios o las infraestructuras críticas de un país o Estado. Provocan desabastecimientos, interrupciones de las comunicaciones, etc., con el objetivo de provocar una paralización puntual o prolongada de aquellos.
Pérdida de reputación	Es una de las principales consecuencias de las agresiones cibernéticas y el objetivo de gran parte de los ciberataques, cuyos efectos pueden resultar altamente significativos.

Fuente: Adaptación propia con base en datos del Instituto de Auditores Internos de España (2016).

Desde sus inicios, estos riesgos han sufrido una evolución tecnológica y operacional, ya que los ciberdelincuentes se han adaptado a los cambios y están al acecho de las debilidades de nuestros sistemas de información.

Específicamente en los ámbitos laborales, dichas debilidades se convierten en vulnerabilidades por la ausencia o la ineficiencia de algún tipo de control de seguridad, ya sea de tipo procedimental, tecnológico, etc. En otras palabras, la ausencia de control aumenta de forma significativa la probabilidad de que se produzca un incidente de seguridad y que el impacto sea mayor.

Por lo anterior, y con base en los autores citados, entenderemos *ciberriesgo* como aquella posibilidad de que una amenaza proveniente del ciberespacio ataque la información administrada, almacenada, procesada, comunicada y transmitida de la entidad.

3.1. Agentes generadores de ciberriesgos internos

Un *agente generador de riesgo* puede definirse como una persona o una cosa que produce una falla. En el caso de las personas que laboran para las entidades, por ejemplo, la falta de formación y de concientización, el descontento laboral, la impericia, la ausencia de políticas y de procedimientos o la ausencia de mecanismos de disuasión son causas habituales y suficientes para facilitar un incidente de fuga de información.

Para el caso particular de los agentes generadores de ciberriesgo a escala interna, está la falta de clasificación de la información con base en su nivel de confidencialidad y en función de diversos parámetros, como el valor que tiene para la organización, el impacto público que puede generar su difusión, su nivel de sensibilidad o si se trata de información de carácter personal o no.

3.2. Agentes generadores de riesgos externos

Son aquellos originados por terceros ajenos a la propia red o sistema y que consiguen acceder a información no autorizada, modificar o interferir el propio funcionamiento del sistema, mediante la explotación de sus vulnerabilidades.

Medios nacionales como el periódico *El Tiempo* han hablado de una "profesionalización del cibercrimen", basados en criterios como el conocimiento experto de los atacantes (Medina, 2016). De igual manera, se manifiesta en informes periciales dispuestos en revistas de la Policía Nacional que los ciberdelincuentes cuentan con recursos humanos, técnicos y financieros a su libre disposición, cuando de realizar ataques gubernamentales se trata (*Semana*, 2017).

En el mercado hay múltiples amenazas capaces de infiltrarse en los sistemas y obtener información. A continuación, se exponen algunas de ellas, con base en el informe presentado por Symantec (2019).

Ataque de denegación de servicio (DOS): es un intento de hacer que un recurso deje de estar disponible para sus usuarios. Un ataque de denegación de servicio distribuido (DDoS) se produce cuando varios atacantes lanzan ataques simultáneos DoS contra un solo objetivo.

Ataques de inyección de código: son técnicas de ataque contra aplicaciones web, como la inyección SQL, *cross-site scripting* (XSS), la solicitud a través del sitio de la falsificación (CSRF), etc. Utilizando este tipo de técnicas, se persigue extraer los datos, robar credenciales o tomar el control del servidor web.

Botnet: son un conjunto de ordenadores comprometidos que están bajo el control de un atacante. Se les llama *zombies*, y estos se comunican con el sistema maestro que los puede dirigir.

Drive-by Exploits: se basa en la inyección de código malicioso en el código HTML de sitios web que explotan vulnerabilidades en los navegadores web de usuario.

Exploit kits: son paquetes de *software* creados para "automatizar" delitos informáticos. Descargan código malicioso en sitios web comprometidos.

Falsos antivirus: son cualquier tipo de *software* falso que los ciberdelincuentes distribuyen con el fin de infectar los equipos a través de falsas alertas de seguridad.

Gusanos: son programas maliciosos con capacidad de replicarse y redistribuirse mediante la explotación de las vulnerabilidades de los sistemas de destino.

Troyanos: son programas maliciosos que se inyectan sigilosamente en los sistemas de los usuarios. Pueden tener capacidades de puerta trasera, es decir, permiten que un usuario remoto pueda acceder al equipo infectado (como los troyanos de acceso remoto [RAT]) y robar datos de usuario y credenciales.

Spam: uso abusivo de correos electrónicos para saturar los buzones del usuario con mensajes no solicitados.

La evolución de estas amenazas y sus combinaciones marcó el panorama de los ataques en 2018 y 2019. La aparición de los *cryptoworms*, un tipo especializado de *ransomware* que elimina la necesidad del elemento humano, se basa en el lanzamiento de campañas de *ransomware* a través de la red, de forma autopropagada. Se considera el más peligroso, pues tiene el potencial de acabar con la internet, según los investigadores de amenazas de Cisco.

Por esto, es clave entender la evolución de estas capacidades desarrolladas por los ciberdelincuentes. Para estos personajes, la motivación para lanzar este tipo de ataques no es solo el dinero —como fuese el pago de un rescate—, sino también la eliminación de sistemas y de datos, como lo demostró Nyetya —*malware* de borrado disfrazado de *ransomware*.

Los ciberataques permiten destruir las comunicaciones y la coordinación de las ciberinfraestructuras; asimismo, crean confusión, desinformación, desorganización, caos, casos de espionaje, robo de información, entre otros problemas.

Respecto a la clasificación de los ciberdelincuentes, la empresa Arkavia Networks listó los tipos de *hackers* con sus principales características (*24 horas*, 2017).

Black hat: son los *hackers* con malas intenciones. Usan sofisticadas técnicas para acceder a sistemas, apoderarse de ellos, destruir y vender los datos.

White hat: son *hackers* éticos, que trabajan asegurando y protegiendo sistemas de tecnologías de la información (TI). Usualmente se desempeñan en empresas de seguridad informática y dan cuenta de las vulnerabilidades de las empresas para poder tomar medidas correctivas.

Grey hat: es un híbrido, ya que a veces actúa de manera ilegal, aunque con buenas intenciones. Puede penetrar sistemas y divulgar información de utilidad al público general y, con ello, acusar con pruebas a grandes compañías por la recopilación no autorizada de datos de los usuarios.

Dentro de la clasificación específica de los *black hat* existe una descripción presentada por la empresa Malware Bytes, entre la cual se mencionan los siguientes perfiles:

Carder: experto en fraudes con tarjetas de crédito. Genera números falsos y códigos de acceso que violan exitosamente los sistemas de control para robar y clonar tarjetas.

Cracker: persona que *rompe* y penetra un sistema informático con el fin de robar o destruir información valiosa, realizar transacciones ilícitas o impedir el buen funcionamiento de redes informáticas o computadoras. Puede estar motivado por una multitud de razones, desde fines de lucro y protesta hasta un simple desafío.

Defacer: busca *bugs* de páginas web en internet para poder infiltrarse en ellas y, así, modificarlas.

Lammers: son aquellos que aprovechan el conocimiento adquirido y publicado por los expertos. Si el sitio web que intentan vulnerar los detiene, su capacidad no les permite continuar más allá. Generalmente, son despreciados por los verdaderos *hackers*, que los desestiman por su falta de conocimientos y herramientas propias. Muchos de los jóvenes que hoy en día se entretienen en este asunto forman parte de esta categoría.

Pharmer: se dedica a realizar ataques de *phishing*, a través de los cuales el usuario cree que está entrando a un sitio real e introduce sus datos en uno creado por el *hacker*. Posteriormente, usa las credenciales obtenidas para robar fondos de las cuentas de sus víctimas.

Phreaker: es una persona con amplios conocimientos en telefonía. Puede construir equipos electrónicos artesanales para interceptar y ejecutar llamadas desde aparatos telefónicos celulares, sin que el titular se percate de ello.

Piratas informáticos: este apelativo se atribuye a las personas que usan *software* creado por terceros, a través de copias obtenidas ilegalmente, es decir, sin permiso o licencia del autor. Al *software* no original se le denomina "copia pirata", pero en términos reales y crudos debe llamarse "*software* robado".

Script-kiddie: es un tipo de ciberdelincuente que se limita a recopilar información, herramientas de *hacking* gratuitas y otros programas para probar sus efectos en posibles víctimas. Más de alguna vez terminan comprometiendo sus propios equipos.

Spammer y diseminador de *spywares*: hay empresas que le pagan por

la creación de *spams* de sus principales productos. También se lucra con publicidad ilegal.

Trasher: recientemente relacionado con los delitos informáticos, este ciberdelincuente obtiene información secreta o privada a través de la revisión no autorizada de la basura descartada por una persona, una empresa u otra entidad, con el fin de utilizarla en actividades delictivas.

War driver: es un *hacker* que sabe aprovechar las vulnerabilidades de todo tipo de redes de conexión móvil (*24 horas*, 2017).

Estas definiciones han surgido en diferentes espacios de discusión, como ponencias, páginas web y foros relacionados con el crimen cibernético, pero para la investigación se tomaron las mencionadas en el *Boletín Criminológico n.º 11* (Instituto de Criminoloxía, Universidad Santiago de Compostella, 2009, pp.10-19).

Todos estos personajes son cada vez más expertos en evasión y en usar como armas los servicios de la nube y otras el *sandboxing*, un mecanismo para ejecutar programas con seguridad y de manera separada (en el caso particular, para ejecutar código nuevo o *software* de dudosa confiabilidad proveniente de terceros). Los sistemas de SandBoxing, se consideran un entorno controlado, donde el área TI, puede, entre otras, ejecutar tareas de revisión de *software*, programas, códigos, todo asegurando que este no va a generar daños en los ambientes productivos.

En esta amalgama de ciberdelincuentes, es característico el uso y la adopción del cifrado para evitar la detección, así como el ocultamiento de su dirección original de navegación, con el fin de cubrir actividades de comando y control. Esto les brinda más tiempo para operar e infligir daños.

3.3. Clasificación de las ciberamenazas

Las ciberamenazas se pueden clasificar en dos: contra la información y contra la infraestructura TIC, como se muestra en la tabla 4.2 (Instituto de Auditores Internos de España, 2016, pp. 10 y 11).

Tabla 4.2. Descripción de las ciberamenazas

Ciberamenaza	Descripción	Ejemplos
Contra la información	Las materializaciones de estas ciberamenazas provocan pérdida, manipulación, publicación o uso inadecuado de la información.	• Espionaje (de Estado o industrial). • Robo y publicación de información clasificada o sensible (datos personales, datos bancarios). • Robo de identidad digital. • Fraude.
Contra la infraestructura de tecnologías de la información y las comunicaciones	Son aquellas cuya materialización puede provocar la interrupción temporal, parcial o total de determinados servicios o sistemas.	• Ataques contra infraestructuras críticas. • Ataques contra redes y sistemas. • Ataques contra servicios de internet. • Ataques contra sistemas de control y redes industriales. • Infecciones con *malware*. • Ataques contra redes, sistemas o servicios a través de terceros.

Fuente: Elaboración propia con base en información del Instituto de Auditores Internos de España (2016).

4. Estado de los delitos cibernéticos nacionales e internacionales

Se consideran delitos en el ciberespacio aquellos que están tipificados en la Ley 1273 de 2009 y que se han convertido en un negocio (*cybercrime as a service*). En la actualidad, es posible contratar, a través de la *deep-web*, la realización de un ataque de DoS, *spam*, *phishing*, el alquiler de una *botnet* o los servicios de un *hacker*.

De acuerdo con el Índice de Tendencias Ciber de la empresa consultora Deloitte, en su informe Ciber Riesgos y Seguridad de la Información en América Latina & Caribe, Tendencias 2019 Reporte Colombia (Deloitte, 2019):

- 4 de cada 10 organizaciones sufrieron un incidente de ciberseguridad en los últimos 24 meses.
- El 70 % de las organizaciones afirma no tener certeza de la efectividad de su proceso de respuesta ante incidentes de ciberseguridad.
- Solo el 3 % realiza simulaciones para probar sus capacidades efectivas de respuesta ante una amenaza *ciber*.

Otro dato relevante frente al impacto de la materialización de un ciberataque se relaciona directamente con las pérdidas económicas que se ocasionan en la entidad, dato que no suele ser fácil de estimar. Calcular el perjuicio económico debido a un incidente de ciberseguridad es una tarea compleja, dada la multiplicidad de tipos de ataques, actores y factores. (Se debe destacar que frente a la materialización de un incidente de ciberseguridad pueden ser muchos los servicios afectados, y esto complica el cálculo de las pérdidas totales).

Dentro de los costos involucrados a la hora de determinar el impacto en la entidad, debemos contemplar como mínimo si existe la necesidad de pagar por el rescate de la información, por la pérdida de los datos y por las demandas judiciales. Asimismo, hay que considerar los costos que pueden afectar la reputación de la entidad, el deterioro de la confianza de los usuarios en un servicio, la pérdida de la propiedad intelectual o la disminución de la ventaja tecnológica frente a los competidores, entre otros.

La llamada "seguridad digital" nos exige fortalecer no solo las capacidades técnicas, tecnológicas y operativas, sino también los esfuerzos civiles orientados a lograr un ciberespacio más seguro y confiable para todas las entidades públicas y privadas, y para la sociedad en general.

El esfuerzo interinstitucional está encabezado por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT). Este coordina aspectos sobre ciberseguridad, como la protección de infraestructuras críticas, y sobre cooperación, como la gestión y el intercambio de información a escalas nacional e internacional.

Por su parte, el Comando Conjunto Cibernético (CCOCI) está conformado por las unidades cibernéticas de las Fuerzas Militares de Colombia, que son la Armada Nacional, la Fuerza Aérea y el Ejército

Nacional. Aquellos proporcionan la defensa del país mediante la creación y puesta en marcha de las estrategias que permiten prevenir y contrarrestar toda clase de ataque de naturaleza cibernética que ponga en riesgo los valores y los intereses nacionales.

Finalmente, el Centro Cibernético de la Policía (CCP) tiene entre sus funciones apoyar en ciberseguridad el territorio colombiano, ofreciendo investigación y judicialización ante los delitos cibernéticos. Para ello, incorporó dentro de su infraestructura el llamado CAI Virtual, donde los ciudadanos podemos denunciar todo tipo de delitos informáticos.

Países como Chile y España han determinado que es hora de intervenir en el mercado, y están utilizando regulaciones o leyes para exigir que ciertos sectores identifiquen, evalúen y corrijan las deficiencias en sus sistemas de seguridad. Los sectores regulados incluyen: servicios eléctricos, servicios financieros, atención en salud, transporte y telecomunicaciones.

Entre tanto, la Unión Europea (UE) impuso un enfoque especial en las infraestructuras críticas y operadores de servicios esenciales, mediante la adopción de un reglamento titulado *Directiva de Seguridad de las Redes y de la Información* (NIS, por sus siglas en inglés) (Parlamento Europeo, Consejo de la Unión Europea, 2016). Este documento comprende los aspectos del mercado interior, justicia y política exterior relacionados con el ciberespacio.

La estrategia de ciberseguridad y la propuesta de la directiva sirven de apoyo a la Agenda Digital para Europa, cuyo objetivo es ayudar a los ciudadanos y a las empresas europeas a aprovechar al máximo las tecnologías digitales. Guía a las empresas para que estas adopten las medidas oportunas para gestionar los riesgos que enfrentan en seguridad y notificar a las autoridades nacionales competentes los incidentes que tendrían un efecto perturbador significativo. Además, propone la creación de una red de cooperación entre todos los Estados miembro.

Esta directiva es un referente internacional y ha sido un derrotero para un sinnúmero de implementaciones de medidas de ciberseguridad. Cuenta con una serie de requisitos comunes en materia de:

- despliegue de capacidades;
- planificación;

- intercambio de información;
- cooperación;
- requisitos comunes de seguridad.

De la directiva NIS, resaltamos el establecimiento de reglas de seguridad cibernética que deben ser implementadas por las empresas que suministran servicios y que están clasificadas como esenciales. Los servicios cubiertos por la regulación incluyen energía; transporte; banca; finanzas; servicios públicos como el agua, la electricidad y la salud; servicios digitales como los mercados en línea (eBay, Amazon, Best Buy, Etsy, entre otros); motores de búsqueda (Google, Bing, YouTube, entre otros), y proveedores de servicios en la nube (Amazon, Google, Microsoft, entre otros).

La directiva requiere la notificación de la autoridad nacional pertinente sobre cualquier incidente cibernético grave del cual sea víctima. Este enfoque obliga a la rendición de cuentas e implica la reducción del riesgo cibernético porque la industria debe tomar medidas para reducir las vulnerabilidades y aumentar la resiliencia cibernética de las infraestructuras que administra.

Estados Unidos se ha abstenido de adoptar un enfoque regulatorio en esta materia, y, por el contrario, ha recomendado a la industria que invierta de forma voluntaria en estrategias que reduzcan el riesgo cibernético que enfrentan las infraestructuras y los servicios críticos del país. Esto, posiblemente porque el Gobierno estadounidense planea la creación de un centro encargado de proteger bancos, compañías de electricidad y otra infraestructura clave de ataques cibernéticos, una amenaza que ahora excede el peligro de un ataque físico por un grupo hostil extranjero, de acuerdo con lo dicho por la secretaria de Seguridad Nacional Kirstjen Nielsen (2018).

Si bien estamos frente a una institucionalidad definida, las cifras demuestran que los ataques son cada vez más complejos, por lo que las entidades de gobierno deben generar estrategias para contrarrestarlos. La ciberseguridad en un reto complejo que comprende diversos aspectos de gobernanza, operativos, técnicos y jurídicos.

El presente modelo de auditoría de seguridad cibernética aborda, organiza y prioriza dichos aspectos, recurriendo a modelos, marcos,

buenas prácticas y otras referencias existentes, que proveen un enfoque homogéneo para reducir el riesgo cibernético vinculado a las amenazas en el ciberespacio. Por medio de indicadores, permite el seguimiento continuo de este tipo de riesgo, a fin de robustecer los mecanismos existentes en las entidades y a mitigar el impacto de aquel.

5. Marco general de auditoría y de gestión de riesgos

En este acápite se repasan las metodologías de auditoría disponibles en el mercado de la ciberseguridad. Aunque algunos marcos se adaptan a ciertos tipos de organizaciones, no existe una única alternativa utilizada por todas las empresas. Si bien son un buen comienzo, la clave para agregar valor es ajustar las buenas prácticas a la necesidad de la entidad, con un enfoque basado en la gestión del riesgo en ciberseguridad, alineado a la estrategia de seguridad de la empresa y enmarcado siempre en función de los clientes, de la actividad principal de la entidad y del sector del mercado que representa.

Según la Unión Internacional de Telecomunicaciones (UIT, 2010), 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.

De acuerdo con las metodologías existentes, para medir el nivel de riesgo se deben implementar ciertos pasos de manera organizada, con el fin de detectar qué tan seguro es el sistema de información y los riesgos y frecuencias que se pueden presentar. Estos procedimientos permiten determinar, con datos reales, las acciones por tomar para mitigar la materialización de dichos riesgos.

Los modelos conocidos de ciberseguridad y de auditoría están basados comúnmente en la gestión de riesgos conocidos. Por tanto, se hace un énfasis especial en este acápite para determinar la

articulación existente entre la gestión del riesgo y la auditoría de seguridad cibernética.

El proceso de gestión de riesgos es crítico para proteger de forma adecuada los activos de información de la entidad. Para ello, se requiere identificar la criticidad de dichos activos, las potenciales amenazas y las vulnerabilidades a las que están expuestos, además de los riesgos que con mayor probabilidad e impacto pueden afectan los procesos estratégicos, misionales y de apoyo de la entidad.

La gestión de riesgos permite tener un panorama actualizado de las posibles pérdidas en confidencialidad, integridad y disponibilidad de los activos de información. Este proceso es fundamental en la estructura del gobierno corporativo, puesto que implica la aplicación sistemática de políticas, procedimientos y prácticas que permitan:

1. identificar y analizar el riesgo, con el fin de establecer el contexto para las decisiones basadas en aquel;
2. evaluar el riesgo;
3. Tratar al riesgo una vez determinado;
4. Monitorear el riesgo de forma continua, utilizando comunicaciones organizacionales efectivas y un circuito de retroalimentación para la mejora continua de las actividades relacionadas con los riesgos de las organizaciones.

La gestión del riesgo es una actividad multidisciplinaria que requiere la participación de toda la organización, desde la alta gerencia —que proporcione la visión estratégica, las metas y los objetivos institucionales— hasta los líderes de nivel medio —que planifiquen, ejecuten y administren proyectos—, pasando por el recurso humano que apoya y opera los sistemas de información de la organización (National Institute of Standards and Technology, 2011, pp. 6-9).

Las tablas 4.3-4.5 exponen las metodologías de gestión del riesgo más conocidas y rescatan los criterios en los cuales se apoyará este modelo de auditoría.

Tabla 4.3. Metodología CRAMM

Nombre de la norma	Method CRAMM (CCTA Risk Analysis and Management Method)
Versión actual	5.0
Año de expedición	1985
Empresa	Central Computer and Telecommunications Agency del Reino Unido, gestionada por Insight Consulting Limited (Grupo Siemens).
Alcance	CRAMM utiliza métodos cualitativos y cuantitativos para identificar riesgos y amenazas. Para ello, usa una matriz cuyas filas representan los diferentes activos de información, y las columnas, los riesgos que amenazan la integridad, la confidencialidad y la disponibilidad de estos activos. Integridad es la precisión de información, así como su validez, de acuerdo con ciertas expectativas, confidencialidad, protección de la información contra la divulgación no autorizada y la disponibilidad de esta cuando sea requerida. Es distribuida de forma gratuita en idioma inglés.
Beneficios que aporta	Como resultado final de la aplicación de la metodología de CRAMM, se obtiene una matriz de análisis de riesgos y un reporte que establece como objetivo principal la gestión y el análisis del riesgo.
Enlace de interés	https://managementmania.com/en/cramm-ccta-risk-analysis-and-management-method

Fuente: Elaboración propia con base en la metodología CRAMM (Central Computer and Telecommunication Agency Risk Analysis and Management Method).

Tabla 4.4 Metodología MAGERIT

Nombre de la norma	Metodología MAGERIT
Versión actual	3
Año de expedición	1996
Empresa	Consejo Superior de Administración Electrónica
Alcance	MAGERIT implementa el proceso de gestión de riesgos dentro de un marco de trabajo útil para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de las tecnologías de la información. Esta metodología usa medios electrónicos, informáticos y telemáticos, por los beneficios que estos brindan para los empleados y los ciudadanos, pero también hace un llamado sobre sus posibles riesgos, que se tienen que minimizar.
Beneficios que aporta	El ciclo de MAGERIT inicia con la identificación de los activos de información, luego de las amenazas lógicas y del entorno. Estima las frecuencias y el impacto, para inmediatamente pasar a las salvaguardas y gestionar el riesgo residual. MAGERIT considera como activos de información el *hardware*, el *software*, la información electrónica, las personas, las instalaciones, los medios de soporte y los elementos de comunicación de datos.
Enlace de interés	https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Fuente: Elaboración propia con base en la metodología MAGERIT – versión 3.0 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método).

Tabla 4.5. Estándar ISO 31000

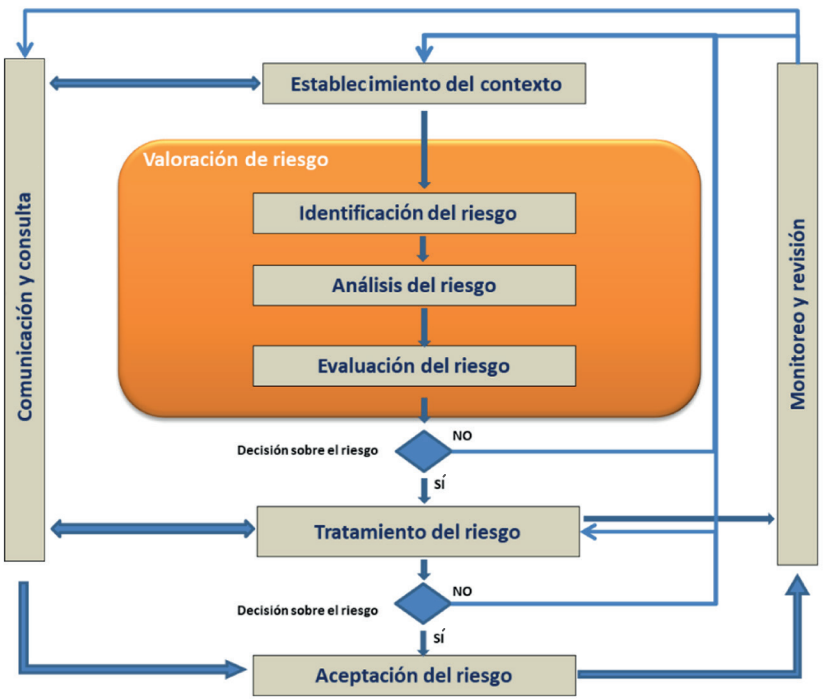
Nombre de la norma	Norma ISO 31000
Versión actual	ISO 31000:2009 - Gestión de riesgos - principios y directrices
Año de expedición	2009
Empresa	International Organization for Standardization
Alcance	La norma ISO 31000 incluye los principios del riesgo como factor clave del éxito en el diseño, implementación, operación, mantenimiento y mejora de un sistema de decisión de riesgos. Es importante aclarar que esta norma no tiene un propósito de certificación, ya que más bien aporta ciertas directrices para la implementación de una cultura organizacional. Puede utilizarse por cualquier empresa pública, privada o social, asociación, grupo o individuo. Por lo tanto, no es específica de una industria o sector concreto.
Beneficios que aporta	Incluye la valoración del riesgo, que contempla las fases de identificación, análisis, evaluación y tratamiento del riesgo. Todo ello, enmarcado en la comunicación y la consulta, así como en el monitoreo y la revisión, de lo cual se obtiene el reporte y el registro, necesarios para el Sistema de Gestión. Se aplica a metodologías que permitan hacer seguimiento sistemático de las políticas, los procedimientos y las diferentes prácticas que se han diseñado y dimensionado en el marco de referencia.
Enlace de interés	https://www.isotools.org/2018/10/15/resumen-nueva-norma-iso-31000-gestion-riesgos/

Fuente: Elaboración propia con base en la norma ISO 31000:2009 - Gestión de riesgos - principios y directrices.

El manejo que se le da a la gestión del riesgo en las entidades del distrito forma parte de un proceso estructurado y alineado con la gestión de riesgos sugerida por el Departamento Administrativo de la Función Pública (DAFP); la propuesta del *Modelo Nacional de Gestión de Riesgos de Seguridad Digital* del MinTIC; metodologías como ISO 27005, ISO 31000 y MAGERIT, y el *Documento metodológico guía 4: gestión de riesgos de la información*, publicado por la Alta Consejería Distrital de TIC.

La figura 4.2 describe las etapas de la gestión de riesgos que deben ser aplicadas en la entidad para buscar una mejora continua de la seguridad digital, en concordancia con lo establecido por el MinTIC, la función pública y las mejores prácticas internacionales, como la ISO/IEC 27001 y la ISO 31000.

Figura 4.2. Modelo de gestión de riesgo



Fuente: ISO 31000 (2018).

Los modelos vigentes de auditoría y los que estén relacionados —de manera transversal— con la ciberseguridad se basarán en una gestión de riesgos con un enfoque principalmente reactivo.

1. Inventario de sistemas de información.
2. Revisiones de configuración de seguridad de los sistemas (parches y actualizaciones).
3. Revisión de *logs* y registros de eventos.
4. Cumplimiento de los estándares de calidad.

Estos modelos de auditoría, en su mayoría, se realizan por exigencias de cumplimiento; se les dedica escasos recursos económicos y de personal, y no aportan en el proceso de concientización sobre el riesgo cibernético al que está expuesta la entidad.

6. Marco conceptual

La propuesta del Modelo de Auditoría de Seguridad Cibernética busca contemplar los dominios de ciberseguridad desde una visión holística y transversal de la gestión de riesgos que asegure que los procesos de auditoría de seguridad cibernética permitan reducir los riesgos de pérdida, alteración, manipulación y fuga de información corporativa. Busca, además, que lo que hasta hoy se conoce como "auditorías de seguridad de la información" —que mantienen un enfoque reactivo— maduren, dado el contexto actual, y que se implementen auditorías en seguridad cibernética que permitan identificar, de manera anticipada, los riesgos y una gestión continua de las amenazas. Ahí es fundamental la colaboración de la alta dirección.

En otras palabras, dicho modelo permite evolucionar de la actual cultura reactiva a una de prevención ciberresiliente, que se ajusta rápidamente a las demandas del entorno y permite detectar, de forma anticipada, las vulnerabilidades y las amenazas en el ciberespacio, con una respuesta proactiva.

Con la implementación de este modelo, se pueden medir las propiedades de seguridad de los activos de la organización y de los usuarios

contra los riesgos de seguridad en el ciberespacio. Las propiedades de seguridad analizadas dentro del modelo incluyen:

- disponibilidad;
- integridad —que incluye la autenticidad y el no repudio;
- confidencialidad.

Este modelo también incluye un apartado relacionado con la resolución de incidentes de ciberseguridad, como lo menciona Bartnes (2017). Este autor explica por qué es tan importante la colaboración interdepartamental entre varias categorías de personal y dice que para lograrlo con éxito se requiere la capacitación de todos en el tema en cuestión.

Es importante resaltar que las condiciones para la realización de las auditorías basadas en este modelo deben estar alineadas a los requerimientos específicos plasmados en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y demás planes mencionados en el Decreto 612 de 2018, expedido por el DAFP, o a lo requerido internamente, de acuerdo con el Modelo Estándar de Control Interno (MECI), por el que se regula el modelo estándar de control interno en el ámbito de la administración pública.

Esta propuesta de modelo de auditoría de seguridad cibernética es una herramienta de apoyo a la gestión del oficial de seguridad de la información y permite a las áreas de planeación y riesgos cumplir la política de seguridad digital requerida por el DAFP y el Decreto 2106 de 2019, expedido por la función pública. De este, específicamente el capítulo 2, artículo 16. "Gestión documental electrónica y preservación de la información", parágrafo 1, en el cual se requiere que las entidades dispongan de una estrategia de seguridad digital, al convertirse en una herramienta para el seguimiento de la misma.

El modelo se basa en procesos sistemáticos, independientes y documentados para obtener evidencias y evaluarlas de manera imparcial, con el fin de determinar el grado de madurez de los controles cibernéticos aplicados en la entidad. Así, permite a esta adoptar los controles oportunos para subsanar las deficiencias de su sistema de seguridad y atender las observaciones del equipo auditor.

El equipo auditor propuesto en este modelo tiene la potestad para definir el alcance de la auditoría (autoevaluación o formal), pues se adapta a sistemas con diferentes requisitos de seguridad.

7. Premisas contempladas en el modelo de auditoría de seguridad cibernética

Con el fin de lograr el éxito en la implementación del modelo de auditoría de seguridad cibernética en una entidad vinculada a la Alcaldía de Bogotá, se debe garantizar la implementación de los siguientes prerrequisitos:

1. Compromiso de la alta dirección

   Se establece como actividad previa, pues garantiza que la gestión del riesgo sea oportuna, verificada y progresiva en el tiempo y, con ello, mejorada continuamente.

   Este compromiso se materializa a través del establecimiento de políticas, guías y procesos que aporten los recursos financieros, de personal y demás necesarios para que el proceso sea exitoso y adecuado para la entidad.
2. Identificación de roles y responsabilidades para gestionar los riesgos de seguridad digital.

   Este proceso deberá ser dirigido y comunicado por la alta dirección, en razón de la importancia, para la entidad, de determinar quién debe realizar cada actividad. Para ello, se propone crear un equipo auditor.

   Frente al alcance de la auditoría, se debe aclarar que son las unidades o las oficinas de control interno (auditoría interna o quien haga sus veces) las encargadas de medir y evaluar la eficiencia, eficacia y economía de los controles por ejecutar en la entidad. Para ello, asesoran a la dirección en la continuidad del proceso administrativo, la reevaluación de los planes establecidos y la introducción de los correctivos necesarios para el cumplimiento de

los objetivos previstos. Por ello, deben estar al tanto del alcance propuesto por la alta dirección y ser actores primordiales en la implementación del modelo de auditoría.

Este modelo propone que el equipo auditor disponga de la siguiente serie de cualidades a la hora de aplicar los conocimientos y las habilidades en la entidad:

- Objetividad
- Imparcialidad
- Orientación al objetivo
- Discreción y confidencialidad
- Capacidad para informar con veracidad y exactitud
- Capacidad de aplicación de la debida diligencia
- Juicio experto al auditar de forma ética
- Mente abierta para considerar ideas y puntos de vista alternativos
- Diplomacia y tacto en el trato con las diferentes personas
- Alta capacidad de observación

Para implementar este modelo, el equipo auditor debe estar conformado por un conjunto de profesionales interdisciplinarios. La tabla 4.6 presenta la propuesta de roles y responsabilidades.

Tabla 4.6. Roles y responsabilidades específicas para auditoría

Rol	Responsabilidades
Auditor de seguridad de la información	Verificar la implementación y el cumplimiento de las políticas, normas y procedimientos que fortalezcan la seguridad de la información.
	Implementar el modelo de auditoría de seguridad cibernética.
	Presentar los informes de auditoría de seguridad cibernética, incluyendo las principales novedades.
	Estar al tanto del desempeño del sistema de gestión de seguridad de la información y de cualquier necesidad de mejora.
	Estar al tanto de los inventarios de los nuevos activos digitales de información y de los riesgos cibernéticos asociados.
	Estar en contacto con grupos especializados en seguridad digital, con el fin de estar documentado acerca de los nuevos métodos y herramientas de auditoría.
Auditor de protección de datos personales	Auditar la política de datos personales.
	Garantizar el cumplimiento del procedimiento de custodia de la aceptación de uso y almacenamiento de datos personales que realicen los ciudadanos.
Líder del proceso de auditoría	Vigilar el seguimiento a las no conformidades, el estado de las acciones correctivas y las quejas, los reclamos y las sugerencias sobre la auditoría de seguridad cibernética.
	Verificar los informes de auditorías realizadas a la seguridad cibernética y velar porque se apliquen las acciones correctivas identificadas y las recomendaciones entregadas por los auditores.
	Realizar el análisis de riesgos detectados en la auditoría de seguridad cibernética y coordinar el plan de tratamiento con el líder o responsable de ciberseguridad.
	Organizar las reuniones del equipo de auditoría de seguridad cibernética y convocar, cuando las circunstancias lo requieran, a uno de sus miembros.
	Validar las evidencias pertinentes para verificar los criterios de auditoría, cuya evaluación constituirá los hallazgos en que se basarán las conclusiones recogidas en el informe de auditoría.

Fuente: Elaboración propia con base en experiencias del autor.

Con el fin de crear dichos roles, la alta gerencia debe considerar las siguientes actividades de manera previa:

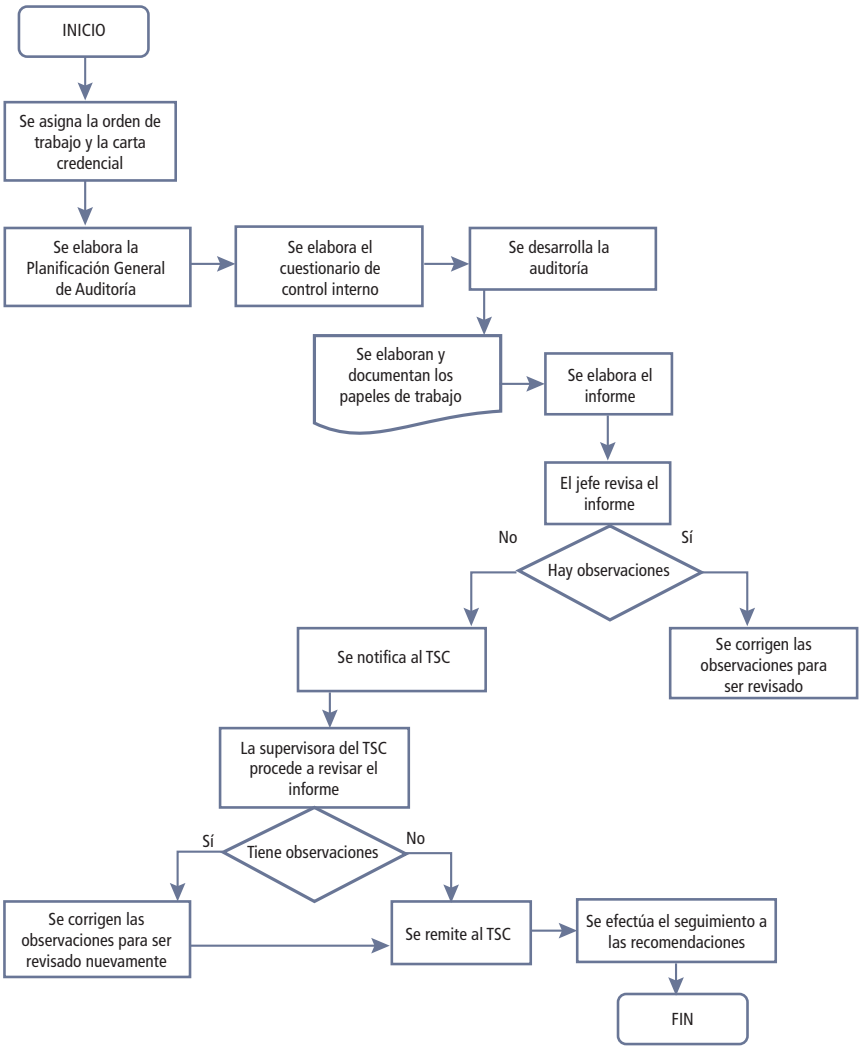
1. Identificar si existe información previa donde se describan los roles y las responsabilidades de auditoría de la entidad para procesos tecnológicos.
   La información se puede identificar en:
   - manuales de seguridad de la información o seguridad digital;
   - documentación de perfiles y funciones de los cargos de los servidores públicos;
   - políticas definidas en la entidad sobre la gestión de riesgos;
   - metodologías de gestión de riesgos que tenga actualmente la entidad.
2. Definir en el comité institucional de gestión y desempeño, de acuerdo con el Decreto 1499 de 2017 —o quien haga sus veces— los roles y las responsabilidades para la auditoría de seguridad cibernética. De ser posible, validar, mediante acto administrativo, si existe una norma jurídica que mencione el cargo.
3. Tener en cuenta la propuesta de roles y responsabilidades del equipo auditor desarrollada.

La figura 4.3 expone la estructura del proceso de auditoría que se adelanta en la entidad vinculada a la Alcaldía Mayor de Bogotá.

Si bien esta metodología está aprobada, no tiene en cuenta la gestión del riesgo cibernético ni involucra trabajo conjunto entre áreas de la entidad.

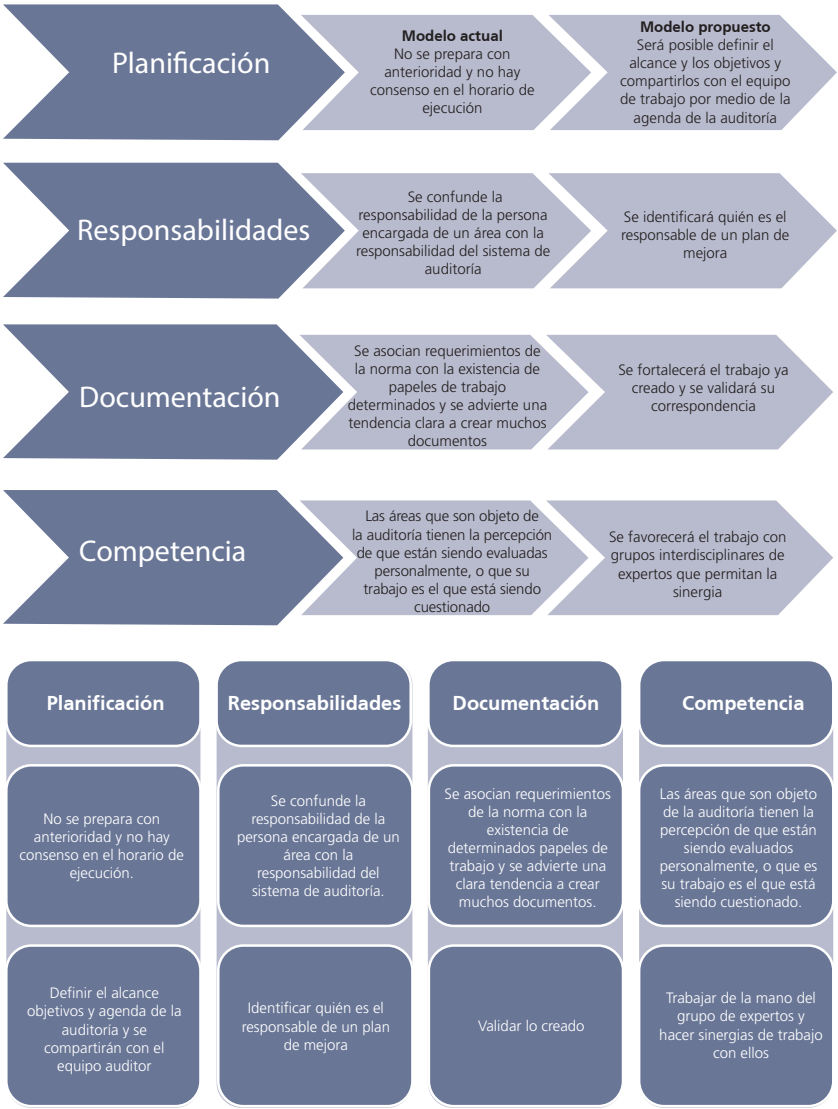
En la actualidad, el modelo implementado tiene dificultades con la comunicación entre auditado y auditor, ya que el hecho de que un auditor comience a profundizar en temas específicos, y que para ello requiera una mayor cantidad de evidencias físicas del tema, normalmente genera una reacción negativa, y en la mayoría de los casos se evidencia la falta de compromiso del auditado. La figura 4.4 ejemplifica los beneficios del modelo propuesto.

Figura 4.3. Modelo de auditoría interna



Fuente: Proceso de auditoría de entidad vinculada a la Alcaldía Mayor de Bogotá.

Figura 4.4. Puntos críticos en el modelo de auditoría actual



Fuente: Elaboración propia con base en la experiencia del autor.

Todo esto nos lleva a concluir que la metodología propuesta con el modelo de auditoría es mucho más amigable, pues convierte a los auditados en expertos, cerrando con esto la barrera cultural frente a la auditoría.

8. Metodología

Para adelantar el proceso de auditoría con base en la propuesta de un modelo de seguridad cibernética, se utilizará la metodología Delphi. Esta se basa en la suposición de que los juicios en grupo son más válidos que los juicios individuales (Reguant y Torrado, 2016).

Esta es una técnica netamente cualitativa, que permite tratar con algún grado de precisión problemas técnicamente complejos. Mediante un ciclo de entrevistas, permite recoger las ideas y las opiniones más cualificadas en el ámbito de la auditoría de seguridad cibernética. Dentro de los puntos que serán juzgados por los expertos, se tratarán temas como:

- Valoración de activos
- Gestión de riesgos
- Manejo de incidentes
- Identificación de amenazas e impactos

Lo primero que se solicita para iniciar con el modelo de auditoría de seguridad cibernética son los resultados de la auditoría anterior, para desarrollar este ejercicio a partir de un escenario inicial. La idea es que permita una adecuada recapitulación e identificación de los problemas que existen actualmente.

El uso de la metodología Delphi asegura que, en la implementación del modelo de auditoría de seguridad cibernética, el riesgo de que los auditores no detecten debilidades en el diseño o en la implementación de los controles de seguridad de las TIC se reduzca con base en las interacciones adelantadas con el grupo de expertos.

Esta metodología se propone porque si llegan a existir debilidades en los controles de ciberseguridad dispuestos por la entidad, y estos se

convierten en una vulnerabilidad, existe la posibilidad de tener un efecto adverso en las operaciones, activos o personas de la entidad y provocar la pérdida de confidencialidad, integridad o disponibilidad de la información.

El procedimiento se adelanta de la siguiente manera:

1. Definir el Tema, para este caso será lo relacionado con el modelo de auditoría
2. Hacer el cuestionario: Se prepara un cuestionario con los temas cuya valoración se desea conocer. Este punto es crítico para el éxito de los siguientes pasos. Por esta razón, el modelo de auditoría de seguridad cibernética propuesta gira en torno a seis ejes temáticos principales, que se unen e interrelacionan entre sí como las fuerzas de un átomo. Estos se ven con mayor detalle en el capítulo siguiente.
3. Definir los expertos: Se distribuye entre los sujetos que tienen una opinión relevante sobre el tema por investigar. Se recomienda que este personal forme parte del equipo de tecnología de la entidad, como el jefe de área, los administradores de sistemas de información y bases de datos, web master, coordinadores de plataformas web, personal de infraestructura y redes, oficiales de seguridad de la información, directores de protección de datos y personal de las áreas funcionales clave en la ejecución de procesos que tengan apalancamiento tecnológico.
4. Informar a los expertos su papel: Explicando que deberán de acuerdo a su experticia aplicar los cuestionarios a la vida practica enmarcado en los procesos de la entidad.
5. Distribuir los cuestionarios: El cuestionario deberá rellenarse de forma anónima para que no se puedan ver afectados los resultados, además antes de hacerlo se recomienda informar a los expertos de los objetivos que se persiguen con dicho cuestionario.
6. Tabular respuestas y analizar resultados: Con las respuestas recibidas, se prepara un histograma por cada eje temático,

indicando cuántos entrevistados se descartarán por cada nivel de valoración. Esto, con el fin de obtener unos resultados más acertados y rendir un informe de auditoría alineado y ajustado a la realidad técnica de la entidad. Si hay una clara concentración de respuestas en torno a un único valor, el proceso ha acabado: hay un claro consenso en el valor buscado. Esto demostraría que el valor obtenido de forma cuantificable se ajusta a la realidad técnica de la entidad, aunque parta de una calificación cualitativa. Si hay diferencias importantes de opinión, se remite de nuevo el mismo cuestionario en cada uno de los ejes temáticos que sean foco de desacuerdo, pero esta vez acompañado del histograma. Si se han apreciado ambigüedades en el primer cuestionario, deben aclararse en esta segunda ronda. A los entrevistados expertos de las áreas técnicas se les debe preguntar si consideran que deben mantener su primera opinión o si prefieren modificarla, con el fin de buscar consenso en las respuestas.

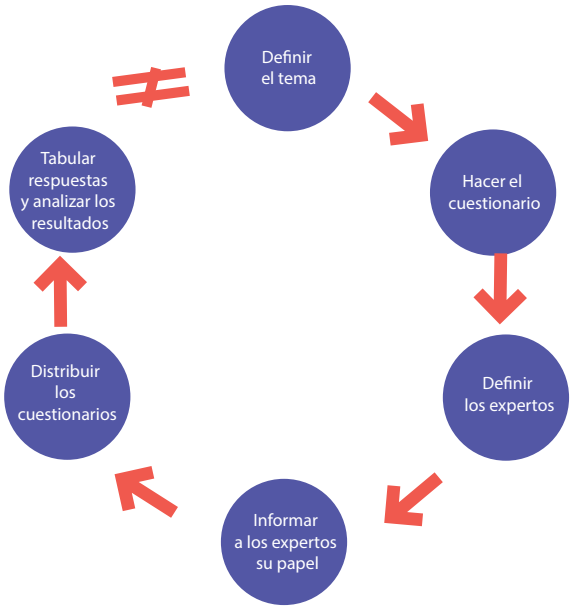
Si el histograma de esta segunda ronda sigue sin mostrar una respuesta clara, se recomienda convocar a los entrevistados a una reunión conjunta para llegar a un consenso entre el grupo de expertos de la entidad y el equipo auditor.

Es importante tener en cuenta que en el caso de que exista un histograma disperso, siempre hay que rectificar si se ha hecho la pregunta correcta a las personas correctas, si la pregunta estaba claramente expresada o si, por el contrario, se debe volver a empezar con nuevas preguntas o nuevos entrevistados. En el caso de que se requiera, se deben ajustar las preguntas, pues este modelo es evolutivo.

Después de existir un consenso entre las áreas en cada uno de los seis ámbitos, se procede, por parte del equipo auditor, a realizar el informe de auditoría, que se sustentará en los cuestionarios, los histogramas y las calificaciones cuantitativas y cualitativas del estado de la entidad frente a las medidas de seguridad cibernética implementadas.

Finalmente, se presenta el informe de auditoría (figura 4.5).

Figura 4.5. Paso a paso de la metodología Delphi aplicada al modelo



Fuente: Elaboración propia.

Buscando la evolución del modelo, se sugiere que, al terminar el proceso, si existe dispersión y hay diferencias entre el grupo de expertos, se inicie nuevamente el ciclo, ajustando las preguntas del cuestionario.

9. El informe de auditoría

El informe de auditoría deberá contener información suficiente para justificar, como mínimo:

- la fecha y el lugar en el que se ha realizado la auditoría;
- los ejes temáticos cubiertos por la auditoría de seguridad cibernética;
- las personas que han formado parte del equipo auditor —deben aparecer el nombre, los apellidos y la figura que ocupa dentro del equipo;

- el grupo de expertos evaluadores del modelo;
- el análisis de los resultados de las auditorías de seguridad cibernéticas previas;
- comentarios sobre el cumplimiento e integración del sistema de gestión de seguridad de la información y sobre si existe una referencia a la versión de la declaración de aplicabilidad;
- los hallazgos que se han identificado con el modelo de auditoría de seguridad cibernética —se recomienda que queden evidenciados y claramente numerados, para así realizar un seguimiento de estos;
- conclusiones sobre el sistema de gestión de seguridad y privacidad de la información;
- observaciones y recomendaciones.

El informe de auditoría resultante de la implementación del modelo debe contar con las características descritas en la tabla 4.7.

Tabla 4.7. Características del informe de auditoría

	Característica	Descripción
1	Claridad	Expresar las ideas de forma sencilla, legible y entendible para quien las lea.
2	Confiabilidad	Esperar confianza y fiabilidad de la información que reporta el auditor.
3	Brevedad	Expresar las ideas y los conceptos con el menor número de palabras.
4	Sencillez	Expresar con naturalidad las ideas y los conceptos.
5	Temporalidad	Presentar el informe en los tiempos requeridos.
6	Conexión	Llegar a las conclusiones con respecto a lo que reporta el informe, a través de un nexo lógico de pruebas y procedimientos.

	Característica	Descripción
7	Precisión	Redactar el informe utilizando solo conceptos completos, sin agregar datos innecesarios.
8	Exactitud	Narrar los hechos tal y como se presentaron.
9	Coherencia	Cuidar que lo que se esté reportando corresponda con lo que en realidad esté sucediendo.
10	Imparcialidad	Actuar de forma equitativa en el cumplimiento del trabajo, tratando de ser justo, honesto y razonable.
11	Objetividad	Describir las ideas y los conceptos con base en la realidad que ve el auditor.
12	Utilidad	Procurar que la lectura del informe sea útil y ágil, de tal forma que se entienda de inmediato lo que el auditor quiere decir.

Fuente: Elaboración propia con base en la Red Global de Auditores Auditool (2016).

10. Ejecución del modelo de auditoría de seguridad cibernética

Las actividades de auditoría normalmente son llevadas a cabo en una secuencia definida. Esta secuencia puede sufrir modificaciones para ajustarse a las circunstancias de auditorías específicas. Las siguientes son premisas que el equipo auditor debe contemplar al inicio de la auditoría, pues con esto se aseguran resultados positivos con la implementación del modelo.

- A fin de realizar de forma correcta la auditoría de seguridad cibernética, es necesario que la entidad en la que se lleve a cabo facilite la mayor cantidad de información pertinente para realizar los trabajos respectivos.

- Siempre que se pretenda determinar un hallazgo, este deberá estar respaldado por evidencias.
- Se deberán adoptar, por parte de las áreas responsables, las medidas oportunas para subsanar los hallazgos y atender las observaciones del equipo auditor, todo con miras a una mejora continua.
- Las recomendaciones de mejora que se desprendan de la implementación del modelo de auditoría de seguridad cibernética deberán tener en cuenta las eventuales limitaciones derivadas del ordenamiento jurídico.

10.1. Desarrollo argumental del planteamiento

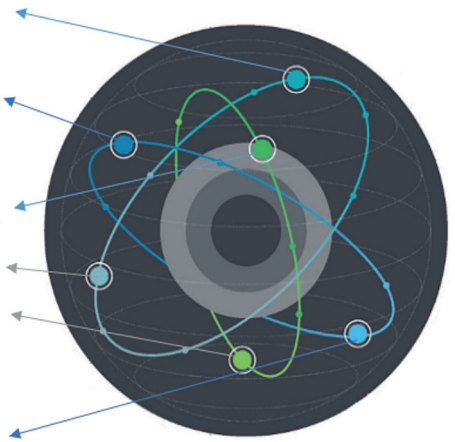
Este modelo propone incluir áreas funcionales de la entidad y al grupo de expertos del área de Tecnología, y presentar un modelo unificado y adaptable para la planificación y la realización de auditorías de seguridad cibernética, alineando metodologías existentes y requisitos regulatorios que permitan aportar un criterio técnico, administrativo y jurídico sobre la problemática planteada con un alto nivel de objetividad como herramienta de gestión de la seguridad digital de la entidad.

La idea del modelo de auditoría es mostrar el estado real de la entidad. Por lo tanto, no debe ser tomado como base para cuestionamientos, sino para tomar medidas proactivas, en caso de tener una calificación que se aleje de lo esperado en cado uno de los seis ejes temáticos.

El modelo propuesto gira en torno a seis ejes temáticos principales, que se unen e interrelacionan entre sí como las fuerzas de un átomo. El núcleo de este átomo es la información que reposa en la entidad y que forma parte de la actividad principal de la entidad (figura 4.6).

Figura 4.6. Propuesta de temas valorados por eje temático de tipo átomo

EJE	TEMAS VALORADOS EN EL EJE TEMÁTICO
1	Seguridad, protección y resiliencia de los sistemas de información, redes y telecomunicaciones que soportan las infraestructuras tecnológicas.
2	Capacidades de prevención, detección, gestión, respuesta, investigación y coordinación frente a los incidentes cibernéticos; y fomento del intercambio de información sobre ciberamenazas.
3	Conocimientos, habilidades experiencia y capacidades tecnológicas necesarias para alcanzar los objetivos de ciberseguridad establecidos en la estrategia de seguridad digital.
4	Activos de información, riesgos cibernéticos y planes de mitigación.
5	Gobernanza estratégica, arquitectura TI y marcos regulatorios y jurídicos.
6	Formación y concienciación en materia de ciberseguridad, con el fin de contribuir a la creación de una cultura de ciberseguridad.



Fuente: Elaboración propia.

Los ejes temáticos se definieron en seis grupos según los temas relacionados (tablas 4.8-4.13).

10.2. Ejes temáticos

Tabla 4.8. Eje temático número 1

Número de eje temático	Temas desarrollados
1	Seguridad, protección y resiliencia de los sistemas de información, redes y telecomunicaciones que respaldan las infraestructuras tecnológicas. **Pertinencia entre temas.** La seguridad, la protección y la resiliencia forman parte de este grupo porque permiten conocer el estado actual de seguridad cibernética al que están expuestos los activos de información de la entidad. Ante todo, se busca reconocer claramente las vulnerabilidades y las posibles brechas en la cadena de valor de la entidad, incluyendo infraestructuras, *cloud*, dispositivos móviles y, en general, los activos de información que forman parte del centro del negocio. También se evalúa la capacidad de la empresa para garantizar la continuidad de su negocio; es decir, si tiene los recursos humanos y tecnológicos necesarios para afrontar, con flexibilidad y fortaleza, las situaciones de ciberriesgo y para sobreponerse a ellas, minimizando y absorbiendo sus consecuencias negativas.

Tabla 4.9. Eje temático número 2

Número de eje temático	Temas desarrollados
2	Capacidades de prevención, detección, gestión, respuesta, investigación y coordinación frente a los incidentes cibernéticos; y fomento del intercambio de información sobre ciberamenazas. **Pertinencia entre temas.** Estos temas tratan del manejo de los incidentes que se puedan presentar por la afectación de los activos de información debido a una ciberamenaza. Este eje temático fue pensado para ayudar a los directores de tecnología de la información (TI) y oficiales de seguridad de la información de las entidades, quienes deben desarrollar un informe de incidentes de seguridad cibernética que no requiera un análisis de causa raíz, pero que amerite una investigación profunda, ágil y eficiente.

Tabla 4.10. Eje temático número 3

Número de eje temático	Temas desarrollados
3	Conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para alcanzar los objetivos de ciberseguridad establecidos en la estrategia de seguridad digital. **Pertinencia entre temas.** Se vincularon los temas referidos a los procesos de capacitación en este eje temático, con el fin de identificar la brecha de cumplimiento frente a los objetivos institucionales y de cara a la estrategia de seguridad digital que busca implementar el MinTIC. En este eje temático, se busca determinar la necesidad de desarrollar nuevas estrategias de capacitación para los funcionarios del área tecnológica sobre ciberseguridad, de acuerdo con las directrices de la Alta Consejería Distrital de las TIC, y que tales estrategias permitan potenciar la creación, difusión y aplicación de las mejores prácticas en materia de ciberseguridad en la Alcaldía Mayor de Bogotá.

Tabla 4.11. Eje temático número 4

Número de eje temático	Temas desarrollados
4	Activos de información, riesgos cibernéticos y planes de mitigación. **Pertinencia entre temas.** Se busca validar el estado de las estructuras de seguridad con las que cuentan los activos de información; en particular, los que manejan información clasificada o del centro del negocio que se encuentra almacenada, manejada o transmitida en las infraestructuras tecnológicas de la entidad. Esto, con el fin de validar el ámbito —físico y digital— de los riegos cibernéticos. Para ello, se evaluará la inclusión de las medidas de ciberseguridad oportunas en los distintos planes que se establezcan en la entidad.

Tabla 4.12. Eje temático número 5

Número de eje temático	Temas desarrollados
5	Gobernanza estratégica, arquitectura TI y marcos regulatorios y jurídicos. **Pertinencia entre temas.** Estos temas se vincularon de forma que se pueda evaluar la existencia y la pertinencia de un marco de gestión de ciberseguridad en los ámbitos técnico, operativo y jurídico. Se han integrado con el marco legal colombiano sobre delitos informáticos y con lo referido en el convenio de Budapest, con el fin de integrar soluciones a los problemas relacionados con la ciberseguridad. Esto, para determinar los tipos penales y el trabajo mancomunado de los departamentos competentes, tanto en la entidad como con terceros involucrados, y asegurar la coordinación de estas capacidades con las entidades policiales.

Tabla 4.13. Eje temático número 6

Número de eje temático	Temas desarrollados
6	Formación y concienciación en materia de ciberseguridad, con el fin de contribuir a la creación de una cultura de ciberseguridad. **Pertinencia entre temas.** Aquí se les evaluarán a los funcionarios de la entidad las actividades de sensibilización y desarrollo de programas de concienciación en ciberseguridad concernientes a vulnerabilidades, ciberamenazas e información sobre cómo proteger mejor su entorno tecnológico, no solo internamente, sino también en colaboración con agentes de los sectores público y privado.

Los ejes temáticos serán calificados con base en quince indicadores por cada uno, para un total de noventa preguntas, según "inicial", "maduro" y "avanzado". Con esto, los hallazgos identificados tendrán una parte cuantitativa (numérica) y otra cualitativa (descriptiva) en la calificación. Para completar el set de cien preguntas, existen diez extra, que tienen una interrelación entre los ejes temáticos (tablas 4.14-4.16).

Tabla 4.14. Calificación asignada al indicador

Indicador	Valor cualitativo	Valor cuantitativo	Definición
Pregunta número 1 a 15	Rojo	0	*En el nivel rojo de madurez:* no cumple con los requisitos mínimos de seguridad cibernética. Tiene conocimiento del requisito. La actividad no existe o no se está haciendo. Puede que el proceso exista, pero no se gestiona. El éxito o fracaso de la actividad depende de la competencia, no de la buena voluntad de las personas, y es difícil prever la reacción ante una situación de emergencia. Es impredecible el resultado, si se dan circunstancias nuevas. Existe un riesgo significativo de materialización de un ciberriesgo.
	Amarillo	1	*En el nivel amarillo de madurez*: cumple parcialmente. Dicha actividad se está haciendo de manera parcial, se está haciendo diferente, no está documentada en todas las ocasiones o se definió y aprobó, pero no se gestiona. Se ejerce un mantenimiento regular y el funcionamiento de los procesos está bajo control (con técnicas manuales o esporádicas).
	Verde	2	*En el nivel verde de madurez:* cumple satisfactoriamente. Existen actividades gestionadas y se cumple con la tarea solicitada. El indicador está documentado, es conocido y aplicado por todos los involucrados en la entidad. Dichas actividades se centran en la evolución continua de los procesos, con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora, se revisan continuamente para reflejar los cambios en los objetivos del negocio y se utilizan como indicadores en la gestión del perfeccionamiento de los procesos. En este nivel, la entidad es capaz de mejorar el desempeño de los sistemas a partir del progreso continuo de los procesos (con base en los resultados de las medidas e indicadores).
	Azul	N/A	El control no es aplicable para la entidad. En el campo, se observa la necesidad de indicar la justificación respectiva de su no aplicabilidad.

La sumatoria de la puntuación dada a cada uno de los indicadores en los seis ejes temáticos permitirá determinar el estado del avance en cada área. La calificación de cada indicador dependerá del nivel de madurez alcanzado por la entidad. Por consiguiente, la entidad tendrá una de las tres calificaciones que se muestran en la tabla 4.15, en cada uno de los ejes temáticos.

Tabla 4.15. Calificación asignada al eje temático

Calificación	Valoración numérica	Descripción
Inicial	Desde 0 hasta 14	La entidad no tiene ningún plan para administrar su ciberseguridad. Los controles para las áreas críticas de ciberseguridad son inexistentes o muy débiles. La organización no ha implementado un programa integral de seguridad cibernética. La preparación de ciberseguridad es inexistente en esta área. **Reproducible, pero intuitivo.**
Equilibrado	Desde 15 hasta 24	La organización está comenzando a centrarse en la ciberseguridad. Si existen tecnologías, debe enfocarse en las áreas clave para proteger los activos cibernéticos, al igual que en el personal, los procesos, los controles y las regulaciones. La preparación de la ciberseguridad se está desarrollando en esta etapa. Se requieren mejoras en las áreas clave en las que se han identificado debilidades. **Proceso definido.**
Evolucionado	Desde 25 hasta 30	La organización se ha destacado en la implementación de las mejores prácticas de ciberseguridad. Siempre hay un margen de mejora. Se debe mantener la documentación actualizada y revisar continuamente los procesos de ciberseguridad a través de auditorías. La preparación en ciberseguridad está en un nivel avanzado, pero la organización debe actualizar continuamente su estrategia de ciberseguridad. **Gestionado y medible.**

Fuente: Elaboración propia.

Como resultado de la auditoría, se puede identificar una serie de hallazgos por cada uno de los ejes temáticos. La suma total de los valores obtenidos en dichos ejes más el cálculo de las diez preguntas extra, que tienen interrelación entre los ejes temáticos y que se valoran de acuerdo con la explicación anterior, darán un valor máximo de doscientos puntos. Con esto, el resultado final de la implementación del modelo de auditoría arrojará una las calificaciones que se muestran en la tabla 4.16.

Tabla 4.16. Nivel de madurez en seguridad cibernética

Calificación	Valoración numérica (en puntos)	Descripción
Desfavorable	Menor de 69	Con respecto de la entidad, existen incumplimientos de las regulaciones establecidas que le han generado afectaciones económicas. Se observan riesgos que propician la falta de control en los activos de información a su disposición y afectan el cumplimiento de sus objetivos estratégicos y operacionales. Existen controles, pero no son reiterativos o documentados y se realizan de forma reactiva. El plan de prevención no tiene identificados algunos puntos vulnerables con relación a las deficiencias detectadas. Esto genera resultados negativos en determinados procesos de la entidad y perjudica la efectividad de las medidas adoptadas para minimizar los riesgos. En este caso, se requerirá la realización de una auditoría extraordinaria que verifique la adopción de las medidas correctivas adecuadas. Ante esto, se puede requerir la verificación de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad.
Con oportunidad de mejora	Desde 70 hasta 150	Se requieren mejoras en las áreas clave en las que se han identificado debilidades. Si bien los hallazgos no afectan de manera significativa la ciberseguridad de la entidad, se debe validar cómo realizar el cumplimiento de los indicadores. Pueden existir vulnerabilidades que afecten las operaciones, siempre que no distorsionen la información en términos de confidencialidad, integridad y disponibilidad de manera significativa en la entidad.

		Los procesos relacionados con los controles de los activos de información dan cuenta de que los incumplimientos de la legislación aplicable y las debilidades comprobadas no influyen en los requerimientos de información ni en el patrimonio de la entidad. El plan de controles dispuestos para el set de indicadores de la entidad cumple con su objetivo en cuanto a su estructura y contenido. Están identificados los puntos vulnerables y las medidas adoptadas son efectivas y minimizan los riesgos de ciberseguridad.
Favorable	Mayor de 150	Se debe mantener la documentación correspondiente actualizada y revisar continuamente los procesos de ciberseguridad, a través de auditorías y con base en el marco general de riesgos. Se puede determinar que la entidad cuenta con un nivel de ciberseguridad eficiente y eficaz que asegura el funcionamiento correcto en las operaciones, pues se puede establecer un nivel alto de confiabilidad en la información. Cumple con las leyes, reglamentos y políticas establecidas. Garantiza un control razonable de los activos de información a disposición de la entidad. Se cumplen los indicadores establecidos para medir la efectividad de los seis ejes temáticos del presente modelo de auditoría cibernética.

Fuente: Elaboración propia.

10.3. Resultados y análisis

Se está en el proceso de desarrollo y prueba de los indicadores, a fin de identificar los más concluyentes y que permitan tener una visión holística del panorama de seguridad cibernética en la entidad.

Se considera que el modelo es bastante robusto, pues cuenta con un set específico de indicadores por eje temático. Con base en el método Delphi, permite tener una menor dispersión en la respuesta respecto al cumplimiento y control del mismo.

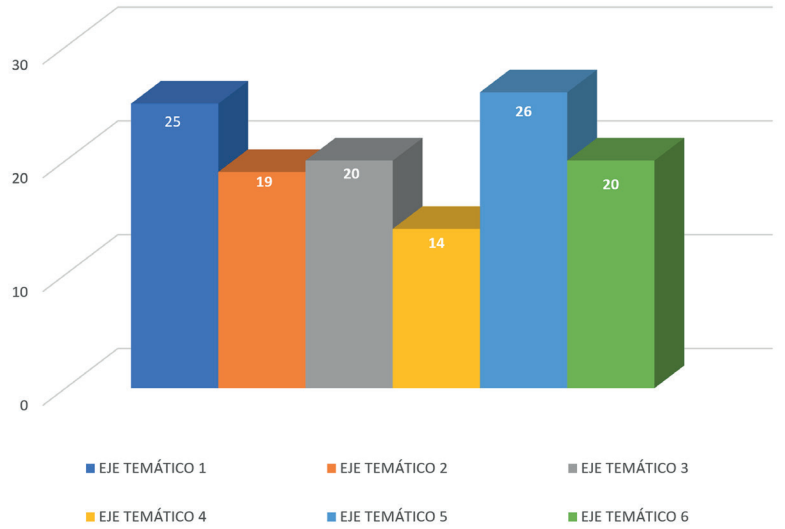
Con base en los resultados de la prueba del modelo *in situ*, los avances han demostrado que la propuesta de realizar las auditorías

cibernéticas por ejes temáticos puede ser muy efectiva para evaluar los controles. De ser requerido, no se realiza la auditoría completa, sino solo en el eje temático afectado. La tabla 4.17 expone la calificación de los ejes temáticos.

Tabla 4.17. Calificación de ejes temáticos en la entidad

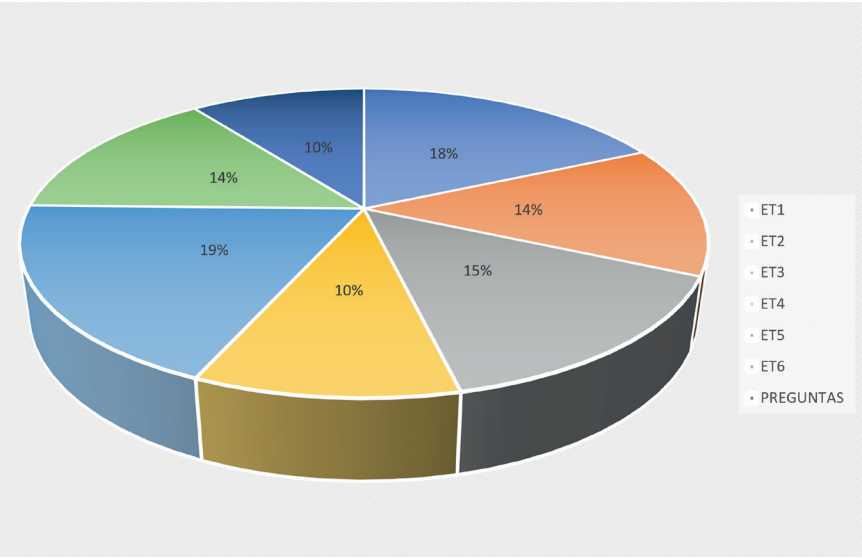
Eje temático	Temas valorados en el eje temático	Calificación
1	Seguridad, protección y resiliencia de los sistemas de información; y redes y telecomunicaciones que respaldan las infraestructuras tecnológicas.	25
2	Capacidades de prevención, detección, gestión, respuesta, investigación y coordinación frente a los incidentes cibernéticos; y fomento del intercambio de información sobre ciberamenazas.	19
3	Conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para alcanzar los objetivos de ciberseguridad establecidos en la estrategia de seguridad digital.	20
4	Activos de información, riesgos cibernéticos y planes de mitigación.	14
5	Gobernanza estratégica, arquitectura TI y marcos regulatorios y jurídicos.	26
6	Formación y concienciación en materia cíber, con el fin de contribuir a la creación de una cultura de ciberseguridad.	20

Figura 4.7. Calificación de los ejes temáticos



Fuente: Elaboración propia.

Figura 4.8. Porcentajes de los ejes temáticos



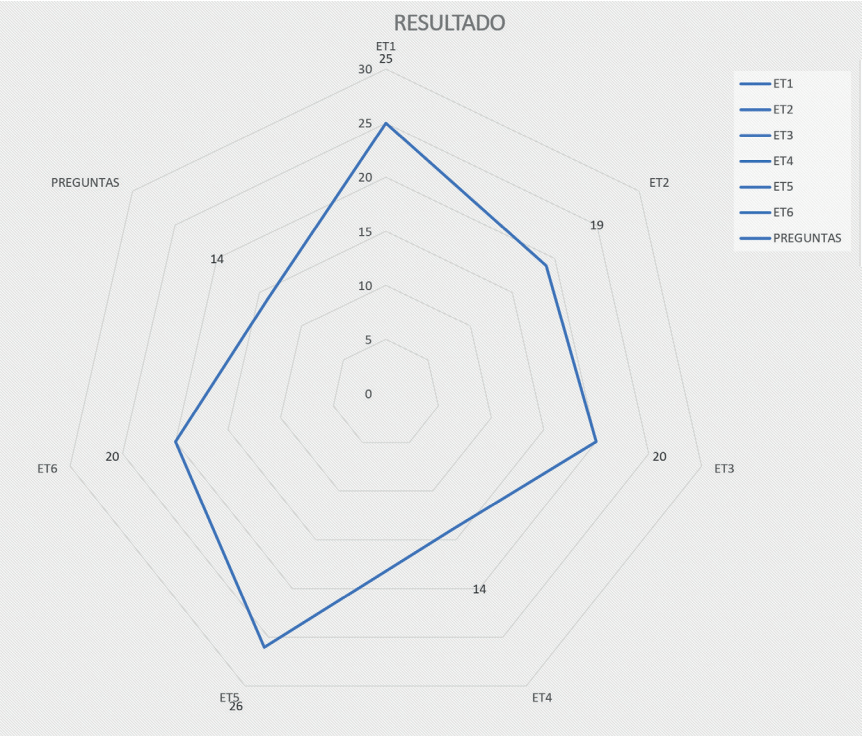
Fuente: Elaboración propia.

Según el análisis de las calificaciones obtenidas (figura 4.7) y su análisis (figura 4.8), se puede sostener que la entidad vinculada a la Alcaldía Mayor de Bogotá está en proceso de hacer cambios y obtener oportunidades de mejora en cuestiones de ciberseguridad. De igual manera, se observó que por parte de la alta gerencia se han establecido procedimientos documentados que están siendo objeto de actualización y que se requiere que se ajusten a la menor brevedad posible.

Por su parte, los controles tecnológicos se han implementado en la entidad, pero existen vacíos respecto al manejo de tablas de retención documental. Por lo tanto, es importante que las áreas involucradas se enfoquen en proteger los activos de información.

Frente a los procesos de capacitación, hay que trabajar con el área de Recursos Humanos e integrar el plan estratégico de tecnologías de la información con el plan de capacitación anual, a fin de trabajar en la ciberseguridad. La calificación final de madurez de ciberseguridad se posiciona en el nivel de "Oportunidad de mejora", con una calificación de 138 puntos, que se encuentra desagregado por ejes tal como lo muestra la figura 4.9.

Figura 4.9. Calificación general del modelo



Fuente: Elaboración propia.

11. Conclusiones

- Se cumplió con el objetivo general de esta investigación: diseñar y validar un modelo de auditoría cibernética que permita conocer el estado real del cumplimiento de los controles, mediante un proceso de auditorías integrales.
- Las organizaciones nacionales e internacionales e instituciones académicas están desarrollando metodologías para apoyar a la comunidad en general a diagnosticar y reducir el riesgo cibernético. De forma conexa, se puede entender cómo estos marcos son necesarios para aumentar la productividad y la eficiencia y reducir los costos.

- Si bien existe en Colombia una gran cantidad de referencias normativas, técnicas y jurídicas referentes a la ciberseguridad, no existe —a escalas nacional e internacional— un único marco unificado que permita hacer una auditoría y revisar el manejo de riesgos de manera conjunta.
- Se requiere el compromiso de la alta gerencia de atender y definir el alcance de la auditoría, pues de este depende el interés y los recursos asignados en el desarrollo del trabajo.
- Se observó la necesidad de identificar roles y responsabilidades para realizar el proceso de auditoría —interna o externa—, y se presentó una propuesta de los mismos.
- Ser partícipe de la toma de decisiones es un factor que contribuye a vencer las resistencias frente a los cambios; formar parte de los órganos decisorios al participar en estos procesos participativos convierte al Delphi en un instrumento generador de confianza.
- Con base en los resultados del modelo, los avances han demostrado que la propuesta de realizar las auditorías cibernéticas mediante la técnica de ejes temáticos puede ser muy efectiva para evaluar los controles. De requerirse, no se realiza la auditoría completa, sino solo en el eje temático afectado.
- Independientemente de haber sido probado en la entidad vinculada a la Alcaldía Mayor de Bogotá, el modelo propuesto no es exclusivo para esta entidad. Por el contrario, se puede utilizar para planificar, realizar y verificar auditorías cibernéticas en cualquier entidad del Gobierno o del sector privado.
- Valdría la pena validar la pertinencia de sistematizar el set de indicadores de cada eje temático, a fin de que la auditoría sea más dinámica.