Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de proyecto de investigación aplicada

Tema:

Guía de optimización de infraestructura tecnológica para la prevención y recuperación de incidentes de ciberseguridad

Elaborado por:

Mike Sandoval Ulloa

Fecha: Enero de 2024

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Sandoval Ulloa Mike.**

LUIS ALONSO RAMIREZ JIMENEZ (FIRMA)
PERSONA FISICA, CPF-02-0562-0491.
Fecha declarada: 01/04/2024 07:20:50 PM
Esta es una representación gráfica únicamente, verifique la validez de la firma.

M.Sc. Luis Alonso Ramírez Jiménez
Tutor

Patricia Herrera Herrera
Digitally signed by Patricia Herrera Herrera
Date: 2024.03.18 18:14:45 -06'00'

MSeg. Hannia Patricia Herrera Herrera
Lector 1

ROY VALENCIANO GONZALEZ (FIRMA)
Firmado digitalmente por ROY VALENCIANO GONZALEZ (FIRMA)
Fecha: 2024.03.18 11:46:42 -06'00'

M.Sc. Roy Valenciano González
Lector 2

San José, Costa Rica, 9 de marzo de 2024

Declaratoria de derechos de autor

Yo, Mike Sandoval, autor del presente documento, presentado con el fin de adquirir el grado de Maestría en Ciberseguridad en la universidad Cenfotec, declaro que soy el autor único del documento, más no el creador de las regulaciones, ni de las buenas prácticas que se utilizaron en la elaboración del documento y la propuesta de solución.

Se autoriza la consulta del documento con fines académicos y se prohíbe cualquier uso no autorizado del documento investigativo, herramientas o metodologías contenidas dentro del mismo para su comercialización.

Al ser este un documento que incluye información de negocios de la compañía Kyndryl y de un subsegmento de la cartera de clientes cuenta con diferentes acuerdos de confidencialidad y de protección a sus clientes. Por tanto, no se tendrá acceso ilimitado a los datos, se utiliza el esquema de información confidencial o también conocido en el ámbito como "*Need-to-Know*", en donde solo se revela la información crítica y absolutamente necesaria para completar el objetivo de la investigación.

El resultado de la investigación en ninguno de sus formatos (digital, escrito) será utilizado como punto focal de información, como apoyo, ni como evidencia definitiva en la resolución de los incidentes o disputas legales.

Carta de aprobación del filólogo

Cartago, 02 de febrero de 2024

Los suscritos, Elena Redondo Camacho, mayor, casada, filóloga, incorporada a la Asociación Costarricense de Filólogos con el número de carné 0247, portadora de la cédula de identidad número 3-0447-0799 y, Daniel González Monge, mayor, casado, filólogo, incorporado a la Asociación Costarricense de Filólogos con el número de carné 0245, portador de la cédula de identidad número 1-1345-0416, ambos vecinos de Quebradilla de Cartago, revisamos el trabajo final de graduación que se titula: *Guía de optimización de infraestructura tecnológica para la prevención y recuperación de incidentes de ciberseguridad*, sustentado por Mike Sandoval Ulloa.

Hacemos constar que se corrigieron aspectos de ortografía, redacción, estilo y otros vicios del lenguaje que se pudieron trasladar al texto. A pesar de esto, la originalidad y la validez del contenido son responsabilidad directa de la persona autora.

Esperamos que la participación de Filólogos Bórea Costa Rica satisfaga los requerimientos de la Universidad Cenfotec.

X

Elena Redondo Camacho
Filóloga - Carné ACFIL n.º 0247

X

Daniel González Monge
Filólogo - Carné ACFIL n.º 0245

Dedicatoria

Quiero empezar por dedicarle este esfuerzo en todas sus definiciones a mi madre. A pesar de que la vida nos puso pruebas complejas, nunca se rindió. Me enseñó a jamás rendirme y a luchar por las cosas con todo mi corazón. Soy lo suficientemente afortunado de que hoy aún me apoya. ¡Gracias, mita!

Segundamente, me gustaría dedicarle esto a mi hermano mayor. No tengo palabras para explicarle lo que significó para mí tener su apoyo a lo largo de tantos años. El profesional, el estudiante y la persona que soy hoy es gracias a él y su ejemplo.

A mi amorcito, gracias por tenerme paciencia y ser siempre la mejor compañía. Tus palabras y tu apoyo fueron la plataforma que me ayudó a estar aquí hoy.

Agradezco a todos, amigos, conocidos y demás personas, por las lecciones que me brindaron a lo largo de todo el proceso.

Tabla de contenidos

Tabla de ilustraciones

Resumen

El objetivo principal del estudio es generar una guía de optimización de infraestructura tecnológica para prevenir y recuperar incidentes de ciberseguridad. Por lo tanto, se realiza una revisión de literatura sistemática utilizando como herramienta el estándar *Casi-oro* con criterios objetivos y subjetivos. El enfoque del proyecto investigativo es la seguridad de la infraestructura informática, con énfasis en negocios y gestión de procesos.

Se buscó definir una base de conocimientos conceptual referente a los temas de ciberseguridad y sus subdominios. Además, se trabajó en la recopilación, procesamiento y análisis de información proveniente de los diferentes estándares de mercado y repositorios de *buenas prácticas* con el afán de presentar un concepto más holístico y que abarque la mayor cantidad de aristas posibles. Este mismo concepto comprende elementos como la definición de los criterios de búsqueda, selección de conocimiento base, herramientas técnicas, definición de perfiles, implicaciones financieras, población y muestreo, entre otros.

La propuesta final se presenta con un enfoque de negocios, con énfasis en procesos de mejora continua y prevención de incidentes. Asimismo, tiene el potencial de ser un proceso reproducible en diferentes tipos de ecosistemas o ambientes.

Palabras clave:

Ciberseguridad, infraestructura, arquitectura de seguridad, *social hardening*.

Capítulo 1: Introducción

1.1 Generalidades

Parte de los detalles importantes por resaltar del proyecto son los siguientes: Kyndryl maneja un esquema de negocios enfocado en los servicios tercerizados y capital humano experto. Por lo tanto, se mantiene inicialmente el anonimato de los clientes debido a la índole de los datos por recopilar, el posible impacto negativo que puede tener la relación de negocios entre ambas organizaciones y las demás condiciones de privacidad establecidas entre Kyndryl, Cenfotec y el investigador.

Este proyecto investigativo tiene como punto de partida la congregación de tres factores diferentes:

- El investigador
- Kyndryl Inc.
- Clientes/mercado

En este fragmento, el investigador utiliza a Kyndryl como campo o área de investigación y recolección de datos. Además, se usa a los clientes como referencia teórica, con el fin de generar casos de uso. Asimismo, se recolectaron potenciales historias y casos de estudio que acompañan la fundamentación de la propuesta.

1.2 Antecedentes del problema

Inicialmente, cuando un cliente hace el primer contacto con Kyndryl o con cualquiera de sus empleados, el modelo de servicios, personal, herramientas, mantenimiento y soporte asociados a las áreas de infraestructura y seguridad informática

suelen ser costeados, planificados y administrados internamente de manera operativa, táctica y estratégica.

Estos modelos pueden tener una infinidad de sabores y vertientes distintas de implementación y operación. Factores críticos como el capital, la gobernanza o regulación de la industria, el ADN corporativo, el nivel de conocimiento técnico y de experiencia del personal, el apetito por el riesgo, el mercado actual y sus tendencias y las relaciones corporativas y personales desempeñan un rol crítico en su desarrollo, adopción y transformación a través del tiempo.

El objetivo principal del cliente (en la mayoría de los casos) es reducir su operación, evadir la planificación de los recursos, disminuir la inversión de capital, relegar responsabilidad arquitectural y financiera sobre los servicios de infraestructura y seguridad. Esto desemboca en un proceso de licitación formal o informal. Kyndryl utiliza su experiencia y personal experto para absorber las operaciones o los servicios y rediseñarlos, de manera que sean rentables para ambas partes a través del tiempo de contrato acordado.

1.3 Definición y descripción del problema

El fundamento de este proyecto se basa en el hecho de que la organización ha recibido al menos cinco licitaciones o proyectos de ciberseguridad y resiliencia durante el periodo 2022/2023, donde se denota una tendencia hacia el aumento y no la disminución. Debido a este fenómeno, Kyndryl cambió su modo de operar, el tipo de producto/servicio final que vende y, por consiguiente, su nicho de mercado está mutando gradualmente hacia un nuevo esquema donde los clientes ya no buscan soluciones enfocadas en silos o áreas específicas.

La tendencia de mercado demuestra cómo los clientes necesitan ahora, más que nunca, soluciones que cubran diferentes capas y productos al unísono, mientras se busca disminuir la complejidad en estas. Por complejidad se hace referencia a todas las aristas: compra, instalación, implementación, soporte y mantenimiento.

En la Ilustración 1 se retrata de manera comparativa un ejemplo de una infraestructura orientada a silos y un ejemplo de una infraestructura más simplificada, centralizada y potencialmente hiperconvergente (ambas son muy básicas).

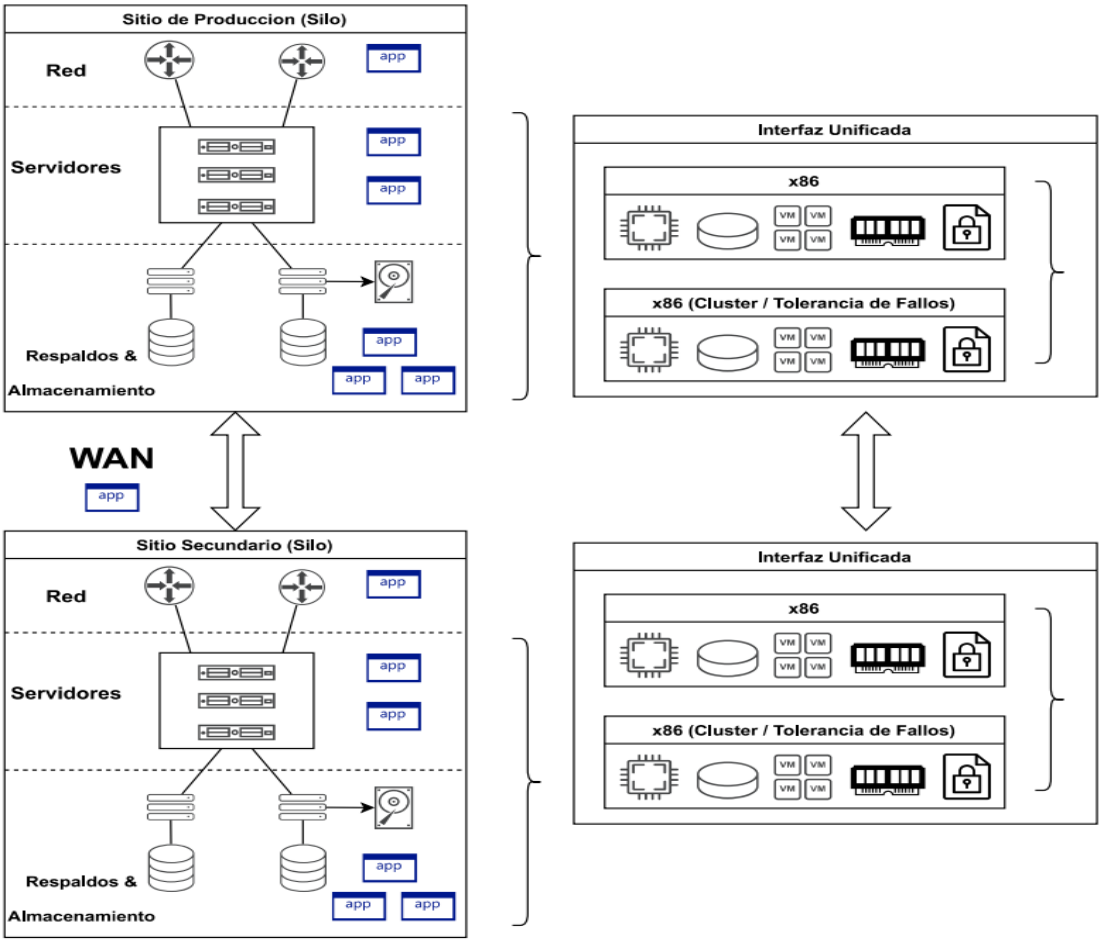


Ilustración 1: Infraestructura en silos vs. hiperconvergente

En todas las incidencias recibidas los clientes experimentaron al menos una incidencia de seguridad, lo cual generó un impacto amplio, tanto en la relación del cliente

con sus diferentes accionistas o usuarios finales como en el impacto financiero de la materialización.

Se tuvieron pérdidas difíciles de cuantificar debido a la falta de información, inventario y capacidad para medir el área de impacto. Aún se trabaja en determinar el impacto económico de la pérdida de datos y las interrupciones de las operaciones y servicios en los diferentes países de algunas de las incidencias.

En cuanto a los procesos, se realizan diferentes tipos de estudios de negocios, financieros y de viabilidad para determinar la capacidad que puedan tener ambas organizaciones de establecer una relación de servicio tercerizado.

1.4 Justificación

En los tiempos modernos, los factores de seguridad ya no se limitan a una sola organización y al grado técnico de su personal de seguridad informática. Tampoco se limitan a su capacidad económica para adquirir una solución técnica altamente efectiva contra ciberataques ni a su capacidad de planificar una estrategia que les permita operar de manera ininterrumpida. Mucho menos se limitan a su capacidad de prevenir y anticipar cada factor de impacto que puede afectar su negocio.

El comportamiento corporativo revela un complejo patrón de anidación entre los diferentes actores. En la actualidad, existen sistemas de almacenamiento y respaldo en la nube, proveedores de servicios internos, externos y de *streaming*. Además, hay una variedad de aplicativos que contienen datos bancarios, información personal y confidencial e incluso empresarial.

Asimismo, se maneja un amplio rango de usuarios finales con perfiles que van desde expertos hasta personas completamente incultas. El uso de los recursos

tecnológicos ya no es una opción, sino un cambio de paradigma en la forma en la que se vive y en la que opera la sociedad.

Este fenómeno distribuye el peso de la responsabilidad de seguridad en muchas direcciones. Como corporación, no se tiene mejor control sobre estas direcciones, por lo que la resolución más acertada, que tomó mucha validez con el paso de los años, es desarrollar campañas de educación y concientización empresarial.

La industria ha asimilado la idea de que la estrategia de seguridad es tan fuerte como su eslabón más débil. Por ende, deben invertir en cerrar la brecha entre los empleados y sus diversos niveles de conocimiento hasta alcanzar un nivel donde puedan recargar el peso de las responsabilidades en los diferentes sistemas, tanto informáticos como de negocios.

La respuesta corporativa a este comportamiento social cambió su modo de operación a uno más colaborativo. Esto se hace en vías de crear un frente unido en contrapropuesta a la creciente industria de crímenes cibernéticos.

En junio de 2019, el Departamento de Ciencia Informática y Tecnología de la Universidad de Ciencia y Tecnología de Pekín realizó una publicación junto con el Departamento de Ciencia Informática y de Tecnologías de Información de la Universidad de Mulungushi de Zambia. En dicha publicación se resaltan algunos datos importantes, los cuales se detallan en los siguientes párrafos.

El valor neto de la industria cibercriminal ha superado los mil millones de dólares, excluyendo los réditos que se generan a través de procesos de generación de criptomonedas y la minería de recursos.

La adopción de las criptomonedas como un elemento económico alternativo al esquema mundial y su anonimidad ha dado paso a la cibercriminalidad como una disciplina rentable. Si se toma en cuenta solo Monero y *Bitcoin*, se estima que un individuo u organización puede generar aproximadamente $100,000,000 USD por año.

Los laboratorios de Kaspersky reportaron un aumento del 50 % en *crypto-jacking* a lo largo del año 2017, lo cual da un valor total aproximado de 2 700 000 de ataques. Symantec reportó en el último cuarto del 2017 un incremento del 8500 % en ataques resultantes en *cripto-mineo*. Para 2018, en Reino Unido se reportó un aumento total del 1200 % en ataques referentes a criptomonedas.

Es relevante resaltar la importancia de los aspectos de seguridad en los tiempos modernos. El impacto de los ciberataques se ha extendido y no solo afecta a un usuario o tiene un impacto único. Se ha acuñado el concepto de ataque mediante cadena de suministros, donde el objetivo no es solo generar un impacto negativo, sino también propagarse a través de los diferentes sistemas, lo que genera posibles materializaciones de futuros ataques.

En la charla realizada por Rob Gates, uno de los principales exponentes de seguridad para IBM en la actualidad, se presenta la idea sobre cómo hoy en día nadie se encuentra seguro y de que los sistemas ya no son totalmente invulnerables. Se debe pensar en cuánto tiempo deben invertir los atacantes en resolver los sistemas de seguridad, en comparación con el beneficio que recibirán como resultado de esto. Los tres primordiales factores que lo denominaron así son la popularidad que tomó esta disciplina, la exposición mediática que tiene, lo cual la hace aún más atractiva para estas organizaciones y la rentabilidad que hay detrás de cada potencial ataque.

Se considera que realizar la presente investigación presenta no solo un valor inmediato y tangible financiero, sino también la posibilidad de utilizarla como referencia para generar un cambio en la cultura organizacional de las diferentes instituciones. En el largo plazo, este estudio puede convertirse en un método o buena práctica para la comunidad informática y sus ramas subyacentes.

Asimismo, se tomó más consciencia del factor de *proveedor de servicios* al trabajar en una corporación donde se diseñan arquitecturas de seguridad. Se sensibiliza al personal al hecho de que muchas empresas, de diferentes tamaños y con distintos fines de negocios, no tienen la misma fluidez en el tema. Por lo tanto, su personal de trabajo no necesariamente cuenta con la experiencia, conocimiento o profundidad en temas de seguridad y sus distintas vertientes.

1.5 Viabilidad técnica, operativa y económica

Una vez detallados los argumentos principales de la investigación es claro que el impacto trasciende. El recurso deja de ser únicamente una propuesta teórica y se convierte en una herramienta de negocios para la toma de decisiones. Por ende, se busca prevenir materializaciones de incidentes mientras se reducen los tiempos de recuperación, los riesgos y su respectivo impacto.

Kyndryl, como proveedor de servicios, se beneficiará de la propuesta teórica, ya que esta puede convertirse en una metodología o buena práctica dentro de la corporación. Esto aumentará positivamente los factores de calidad, seguridad e imagen corporativa.

1.5.1 Punto de vista técnico

El investigador cuenta con un grado de bachillerato en Tecnología de la Información para la Gestión de los Negocios y está finalizando el proceso de tesis en ambos posgrados: Manejo de Ti y Ciberseguridad. Además, es un recurso de la empresa Kyndryl, ya que ha trabajado como empleado regular y permanente durante 10 años. Durante al menos 8 años, ha desempeñado un rol de arquitectura en el área de preventas, especializándose en *respaldo como servicio*, *coordinación y planificación de recuperación de desastres*, gestión *del espacio dentro de los centros de datos* y *ciberseguridad y resiliencia*.

Como parte de los recursos adicionales disponibles, Kyndryl cuenta con un SOC o *Centro de operaciones de seguridad*, el cual brinda servicios en el ámbito global con un esquema de 24 horas, 7 días a la semana. Además, se brindan servicios de consultoría de seguridad y resiliencia que cubren una amplia gama de componentes de servicio.

Los clientes en estudio cuentan con diferentes contratos de soporte y seguridad con Kyndryl y, por consiguiente, tienen acceso a todos los beneficios que el centro puede ofrecer. Algunos ejemplos de servicio son: manejo y respuesta a incidentes, análisis e investigación de amenazas, protección de ataques de día cero, análisis y mejora del grado de madurez organizacional, servicios de consultoría y auditoría, validación e implementación de regulaciones, recomendación y puesta en funcionamiento de mejores prácticas y gobernanza, entre otros.

Como último recurso alternativo, Kyndryl cuenta con una plataforma de aprendizaje, la cual se alimenta y es gestionada por los diferentes sistemas de inteligencia artificial que tiene la organización. La plataforma tiene acceso a distintos

repositorios de información, capacitaciones, certificaciones y demás elementos asociados al área de interés del documento.

Al realizar una búsqueda inicial y superficial de los contenidos relevantes o que se relacionan con la investigación, se pudieron denotar al menos unas 100 horas de capacitación. Los contenidos varían entre documentos, páginas web, videos, libros y demás materiales, de manera gratuita.

1.5.2 Punto de vista operativo

El modelo organizacional de Kyndryl asigna flexibilidad en las tareas diarias a los empleados según su rol, antigüedad y confianza de la Gerencia, entre otros criterios. Esto se denomina *empleado de confianza* en la documentación contractual, lo cual permite al investigador escoger y ajustar los tiempos y proyectos que considere de mayor valor en el ámbito empresarial en su operación diaria.

Además del costo por hora del recurso, la empresa no necesita invertir dinero adicional en la investigación, ya que internamente cuenta con todas las herramientas necesarias para realizarla en profundidad.

El investigador presentó el potencial proyecto a la Gerencia del centro de servicios de Kyndryl Costa Rica para determinar el interés y la posición de esta en iniciar o desarrollar la investigación internamente. Todas las partes estuvieron de acuerdo en que hay un valor agregado muy alto, por lo tanto, este proyecto recibió aprobación unánime y se acordó asignar los recursos necesarios.

Durante el proceso investigativo, se puede recurrir al uso racional de recursos humanos adicionales, lo cual quedará a criterio de la persona investigadora para alcanzar el resultado óptimo.

1.5.3 Punto de vista económico

A pesar de que las organizaciones tienen el mismo objetivo, ambas se enfocan en diferentes aspectos. Por ejemplo, Kyndryl como organización proveedora del servicio busca mejorar la imagen corporativa y la relación de negocios, por lo que evita incurrir en penalidades por incumplimiento de servicios o contratos. En el caso del cliente final, este busca pagar la menor cantidad de dinero posible por un servicio que cumpla con todos los requerimientos de negocios, al mismo tiempo que diseña e implementa controles que le permitan prevenir golpes económicos adicionales. Estos golpes pueden analizarse en distintos ámbitos, como la pérdida o secuestro de datos, la pérdida de equipo o componentes de infraestructura y el impacto en la imagen y credibilidad corporativa.

Debido a un tema de confidencialidad, no se pueden revelar las tarifas más recientes dentro del documento. Sin embargo, se tiene la posibilidad de utilizar referencias para generar una cifra lo suficientemente acertada y así dar un estimado o cotización por las labores investigativas.

Se utilizan los factores financieros del año 2022, en los cuales se detallan los siguientes rubros: el valor por hora del recurso de investigación es de $75.6 USD por hora y está disponible por 40 horas efectivas por semana. Para fines de cálculo salarial mensual, se emplea como referencia un rango de productividad que varía entre 155 y 180 horas mensuales por recurso.

Parte del motivo por el cual se genera este estudio es la reducción del personal de servicio. Anteriormente, se contaba con diversos recursos que ejercían labores de mantenimiento de negocio, auditoría y consultoría. El perfil de estos recursos mantiene

una similitud en los factores financieros a los de la persona investigadora, pero presenta una variación en la tarifa por hora de un 15 % de sobrecargo, lo cual da un valor de $86.94 USD por hora.

Debido a la complejidad técnica que puede presentar la investigación y los diferentes actores internos y externos, se consideró la inclusión de un gerente de proyectos técnico. Este inicia sus labores en el mismo momento en que el proyecto investigativo comienza su curso. En términos de perfil, tanto el gerente de proyectos técnico como el investigador mantienen un nivel de responsabilidades muy similar, además, su costo es igual. El valor por hora de este en tiempo completo es de $68.3 USD, manteniendo los mismos parámetros de eficiencia.

El recurso de gerencia de proyectos se puede catalogar como deseable o ideal, sin embargo, lo puede optimizar o absorber el investigador, ya que el perfil de negocios le permite fungir en ambos segmentos (negocios y técnico) de manera efectiva. El costo de este recurso no está previsto dentro del esquema actual de operación del cliente, por lo tanto, se debe tomar una decisión de negocios donde se determine si los costos de este recurso serían trasladados al cliente o, por el contrario, si la Gerencia de Kyndryl estaría dispuesta a invertir en esta actividad en miras de mejorar la relación con el cliente y evitar futuras materializaciones.

Potencialmente, se evalúa el costo de incluir un consultor de servicios de seguridad con enfoque en infraestructura y ciberseguridad. El valor oscila alrededor de los $300 USD por hora y debe usarse con mucha discreción para prevenir un impacto financiero contundente. Por lo tanto, se incluye en el presupuesto un estimado porcentual de horas que se utiliza como parte de la holgura y contingencia.

Es importante aclarar que estos rangos y parámetros varían según las diferentes geografías, niveles técnicos de los recursos y la complejidad del rol o las tareas por realizar por ellos. La estimación del total de los costos de mano de obra que se relacionan con el proceso investigativo se estimó utilizando una métrica cuatrimestral. Además, se tomó en cuenta que los recursos no estarían dedicados al 100 % del tiempo a la investigación.

En cuanto a la distribución de los costos, la empresa absorbe el 100 % de los costos que se relacionan con el investigador, ya que se maneja en la categoría de *proyecto especial* o trabajo de categoría *misceláneo local*. Los costos relacionados con el auditor son actualmente cubiertos por diferentes clientes siguiendo el modelo de *shared resources* o *shared pool*, donde el recurso invierte solo una fracción del tiempo en un mismo cliente o cuenta.

Idealmente, una vez concluido el proceso, los resultados deben ser reproducibles y reutilizables por más clientes dentro del modelo de servicios de Kyndryl, tomando en cuenta que al inicio se deben completar los procesos de saneamiento de datos y contenido.

1.5.4 El impacto de no tomar acciones

Durante el análisis de la viabilidad del proyecto se determinó que contar con un punto de datos sobre el impacto que las organizaciones pueden percibir al no implementar las diferentes soluciones, incumplir estándares, no acatar las regulaciones y mejores prácticas, es de mucha relevancia para poner en perspectiva la realidad que presenta el panorama, tanto informático como de seguridad.

Por lo tanto, se utilizaron dos recursos no conceptualizados previamente en el segmento de viabilidad, pero su figura funcional existe en la comunidad organizacional. Estos recursos participaron de manera esporádica mediante entrevistas informales y realizando recomendaciones de posibles maneras de afrontar los retos que presentó la investigación. Al seguir los lineamientos de confidencialidad antes establecidos, no se presentan más detalles de estos.

Sin utilizar ninguna escala de relevancia, ya que ambos roles tienen funciones similares en el proceso de preventas y ventas, pero con diferentes enfoques, se tiene a los Client Technical Solutioners o *CTS*. Estos son recursos altamente técnicos y responden a la función de arquitectura, además, son encargados de los diseños, implementaciones teóricas y de manejo detallado de los distintos servicios y productos, donde su entregable final es una solución que cumpla con todos los requerimientos técnicos funcionales y no funcionales del cliente.

Los Client Technical Advisors o CTA trabajan directamente con los clientes y forman parte del cuerpo de ventas de la organización, además, son responsables de evaluar de manera generalizada los requerimientos del cliente, tanto técnicos como de negocios. Estos requisitos después se asocian con los diferentes productos y servicios del catálogo, lo que generan los conceptos que sirven como guía y punto de referencia para el resto de los solucionadores.

Ambos se consultaron con el mismo enfoque y se determinó lo siguiente:

- El costo de no tomar acciones está alineado con los costos y a las pérdidas asociadas a la materialización de una amenaza y sus ramificaciones.

- En el ámbito organizacional se crean puntos de referencia internos y externos para que los equipos de ventas utilicen referencias similares y así mantener un argumento unificado a través del mercado en el que participa Kyndryl.
- Cada proveedor de servicios y de productos toma la información disponible en el mercado y la presenta de manera que favorezca la venta. Por lo tanto, cuando hay uniones entre diversos proveedores o específicamente en el caso de Kyndryl que funge como integrador, se toman los puntos de datos de los suplidores y se utilizan como referencia para informar o en algunos casos educar al cliente.
- A pesar de que las grandes corporaciones tienen documentación preaprobada, tanto interna como externa; cada recurso tiene libertad de utilizar cualquier información disponible y presentarla, de manera que beneficie el concepto o solución que se desarrolla. Esto sin infringir las regulaciones de confidencialidad, privacidad de datos y patrimonio intelectual de todas las partes interesadas.

Por último, se indicó que existen diversas organizaciones que llevan a cabo estudios de mercado y recopilan información de distintas fuentes en el ámbito global. Por lo tanto, su modelo de negocios se fundamenta en la popularidad, exposición y confiabilidad, lo que genera puntos de datos para la toma de decisiones de los diferentes mandos dentro de las corporaciones. Muchos de estos mandos, a la vez, solicitan investigaciones específicas según su conveniencia y necesidad de negocios.

Como ejemplo práctico, se tomaron las organizaciones Cyber Risk Alliance y Sumologic. De ellas se pudieron extraer algunas referencias de relevancia para la investigación que encuadra este documento.

Se establece como primera máxima en el contexto actual que, con la cantidad de recursos y tiempo necesarios, no hay una sola entidad que sea totalmente invulnerable. Los recientes ataques y amenazas solo fortifican esta noción.

Los negocios de tamaño pequeño hasta medio, que se definen en adelante como SMB (*small to medium businesses*), reconocen cada vez más la necesidad de estructurar y proteger sus datos, sistemas y activos. Sin embargo, cuando se enfrentan a soluciones de alta inversión, les surge la gran incógnita de si el costo contra el beneficio justifica la decisión.

Según estadísticas, a las organizaciones de menor escala les cuesta entre un 2 % y un 4 % más de su presupuesto general implementar soluciones complejas. Estas mismas entidades admiten no estar totalmente preparadas para afrontar una amenaza o una afectación en su defecto.

Las SMB aún mantienen una mentalidad desafortunada de que los *hackers* se enfocan exclusivamente en atacar organizaciones de gran escala o de renombre en el mercado global. La realidad es muy distinta, según un estudio realizado por Hiscox en Reino Unido, los ciberataques a SMB aumentaron en un 15 % año tras año, incrementando la cifra total a un 55 % del mercado total impactado.

Estas cifras pueden incluso no reflejar la realidad actual, ya que desde la implementación de las regulaciones de GDPR (esta regulación se profundiza más adelante en el documento), muchos incidentes pueden haber sido reportados o no a

conveniencia. No obstante, sin lugar a duda, demarca el hecho de que los actores han encontrado un oasis, pues presumen que las SMB no manejan conocimiento holístico de ciberseguridad defensiva.

Con respecto al impacto, una materialización puede llevar a una entidad a la banca rota. Según el mismo estudio de Hiscox, el costo de las vulneraciones aumentó en un 61 % desde el año 2018, donde el costo rondaba los $229,000 USD, hasta el año 2019, donde incrementó a $369,000 USD.

Ahora se debe tener en cuenta que estos indicadores varían considerablemente entre un caso y otro debido a que las industrias sobre las que trabajan las organizaciones tienen diferentes penalidades. Un ejemplo de un caso de estudio en la industria de salud evidenció pérdidas estimadas de $408 por registro o transacción comprometido, en referencia a los $148 que reportan otras industrias afectadas.

Al hablar de organizaciones de gran escala o corporaciones globales, existen algunas referencias y puntos de vista disponibles en los repositorios aprobados para el uso externo de Kyndryl:

- *46 % de las organizaciones tuvieron interrupciones de servicio a lo largo del año.*
- *69 % de las organizaciones han experimentado afectaciones en la escala, variando desde mediano hasta amplio; lo que ha generado un impacto negativo en los réditos, la imagen, la confiabilidad y en la experiencia del cliente.*

Fuente: The Role Of Automation In Managing Resilience In Hybrid Multicloud, a Forrester Consulting Study commissioned by Kyndryl, 2020.

- *El promedio actual del costo por materialización es de $4.25 millones de dólares.*
- *En promedio el número de días para identificar y contener una afectación es de 287.*

Fuente: Cost of a Data Breach Report 2021, Kyndryl 2021.

- *16 % de las interrupciones en los data centers en el año del 2020 culminaron en pérdidas financieras por encima de 1 millón de dólares.*

Fuente: Uptime Institute: Annual Outage Analysis 2021.

- *Actualmente, 200TWh de electricidad se consume por los data centers.*
- *Un 8 % total de la demanda global de electricidad provendrá de los data center para 2030.*

Fuente: International Energy Agency Report 2020.

- *En promedio una megaafectación puede alcanzar aproximadamente el rango de los $401 millones de dólares y abarcar o comprometer entre 50 y 60 000 000 de transacciones.*

Fuente: Cost of Data Breach Report 2021, Ponemon Institute.

- *54 % de las organizaciones ha experimentado un aumento en el volumen de los ciberataques en el último año.*

Fuente: IDC Security Survey, 2022; FBI Internet Crime Complaint Center Report.

- *Se ha reportado un aumento del 62 % de crecimiento en las incidencias de ransomware año a año.*
- *El promedio de la interrupción del servicio por ataques de ransomware trasciende a los 22 días.*

Fuente: How ransomware Complacency Could Cost Your Company, 2022.

Por último, el impacto de no tomar acciones no radica solo en los aspectos financieros y técnicos o, en su defecto, en la remediación de las incidencias. Además, se deben tener en cuenta los siguientes factores:

- Acciones legales o demandas de parte de los clientes, proveedores de servicios, socios de negocios y demás partes que se relacionan.
- Multas por infracciones de cumplimiento.
- Reembolso e incentivos para clientes.
- Ventas y oportunidades de negocios perdidas.
- Primas o coberturas de seguros.
- Interrupciones en los servicios y procesos de captación de ingresos.

1.6 Objetivo general y específicos

Con el propósito de estructurar los objetivos de manera efectiva, consistente y ordenada, se utilizó una taxonomía cognitiva. Específicamente, se usó la taxonomía original de Bloom de 1956.

Una de las razones primordiales por las cuales se selecciona esta taxonomía es que permite estructurar los objetivos de manera jerárquica. Los seis niveles que se utilizan son los siguientes:

- Conocimiento
- Comprensión
- Aplicación
- Análisis
- Síntesis
- Evaluación

El segundo criterio por el que se utilizó la taxonomía de Bloom para elaborar esta investigación es que está ampliamente aceptada por la comunidad y, a la vez, se utiliza *de facto* por los diferentes entes académicos estatales y privados, lo que incluye Cenfotec. Esto aumenta su viabilidad y probabilidad de éxito.

Por último, al ser una taxonomía ampliamente aceptada, su popularidad aumentó con el paso del tiempo. Esto permite obtener mucha información y diversos casos de estudio que pueden utilizarse como referencias o fuentes de conocimiento.

1.6.1 Objetivo general

Generar una guía de optimización de infraestructura tecnológica para la prevención y recuperación de incidentes de ciberseguridad.

1.6.2 Objetivos específicos

- Conocer los requerimientos y parámetros actuales de mercado que definen una arquitectura como *segura* o *protegida*.
- Identificar las diferentes regulaciones y repositorios de *buenas prácticas* disponibles de la comunidad de seguridad informática que hagan referencia a temas de infraestructura.
- Seleccionar los diferentes procedimientos, metodologías o controles que tengan relevancia para la investigación que se realiza de la infraestructura.
- Evaluar la información y resultados recolectados durante la fase de recopilación de datos, de manera que se filtre para un mayor aprovechamiento.

- Elaborar una guía de referencia de seguridad que se enfoca en infraestructura informática.

1.7 Alcances y limitaciones

A continuación, se detallan los alcances y limitaciones del proceso investigativo por realizar como resultado de este documento. Estos se enfocan en su totalidad en las necesidades de negocios, historias e información que recopiló el investigador, que pueda tener el cliente, Kyndryl y cualquier otro referente en el mercado (historias de éxito y casos de uso).

1.7.1 Alcances

- Inicialmente, se realiza un documento formal donde se detallan los distintos componentes, elementos, factores, ambientes o sistemas analizados o en vías de optimización, según los casos de uso. El mismo debe especificar los distintos pasos, controles, procesos y demás métodos para seguir como parte de la investigación.
- El documento final es una guía detallada de optimización a los sistemas e infraestructura informáticos, mediante el cual se busca la prevención y recuperación de incidentes de ciberseguridad.
- Por último, a través de esta investigación se busca generar puntos de datos que potencialmente sirvan de base de referencia en la toma de decisiones de y para arquitecturas de seguridad. Por lo tanto, este documento también incluye el detalle del resultado del proceso investigativo, el cual, a la vez, funge como fundamentación de la propuesta.

1.7.2 Limitaciones

- Al ser Kyndryl un proveedor de servicios tercerizados cuenta con diferentes acuerdos de confidencialidad y de protección a sus clientes, debido a los cuales no se tiene acceso ilimitado a los datos ni a los distintos sistemas implicados o en estudio y, por consiguiente, debe apegarse a las regulaciones que encasillan la investigación por realizar.
- La implementación de la propuesta a nivel práctico no se lleva a cabo como parte de los objetivos de la investigación, la misma quedará a criterio, tanto de los lectores como de los usuarios finales su validez, aplicabilidad y periodicidad.
- El resultado de la investigación en ninguno de sus formatos (digital y escrito) se utiliza como punto focal de información, como apoyo ni como evidencia definitiva en la resolución de los incidentes o disputas legales.

1.8 Marco de referencia. Organizacional y socioeconómico

Cabe resaltar que dentro del marco de referencia se incluyen dos principales proveedores de servicios: Kyndryl e IBM. Esto resulta del *spin-off* que tuvo IBM de su división de administración de servicios, la cual se independizó como corporación en el mercado. En la Ilustración 2 se puede apreciar la totalidad de las industrias sobre las que opera Kyndryl actualmente.

Ilustración 2: Kyndryl Inc., principales industrias

Fuente: Kyndryl Inc. (s. f.f).

Durante el proceso investigativo, tanto el cliente como el fenómeno y los recursos se encontraban dentro de la cartera y la nómina, respectivamente, de IBM. Sin embargo, en el procedimiento de separación de ambas corporaciones, todo el personal de infraestructura y regulaciones quedó bajo la sombrilla de Kyndryl, mientras que todo el área de cumplimiento y servicios de seguridad se mantuvo en el alcance de IBM. Por ende, se toma un poco de cada una para poder retratar la realidad de la situación en su totalidad.

1.8.1 Historia de Kyndryl

The Heart of Progress™ o El corazón del progreso, como su versión en español indica, es el *slogan* patentado de la organización. La compañía busca modernizar y

administrar los sistemas de misión-crítica del mundo. Uno de sus principales objetivos consiste en diseñar, construir y elaborar sistemas informáticos en los cuales el globo pueda depender.

Kyndryl es actualmente el proveedor más grande de servicios de infraestructura para tecnologías de información. Tiene una cartera de varios miles de clientes en el ámbito corporativo, los cuales están distribuidos a lo largo de 60 países. Su estrategia se enfoca en construir las nuevas bases de su excelencia, al integrar a los proveedores y aliados adecuados, invertir en el negocio y trabajar lado a lado con los clientes para ayudarles a alcanzar su mayor potencial.

1.8.2 Ficha técnica

A continuación, se presentan dos de las tres fichas técnicas asociadas a Kyndryl Inc. Estas fichas detallan algunos datos relevantes sobre la creación y razón social de la empresa.

Kyndryl Holdings, Inc.	
Country	United States
Founded	2020
Industry	Information Technology Services
Sector	Technology
Employees	90,000
CEO	Martin J. Schroeter
Headquarters	New York, New York 10017

Ilustración 3: Ficha técnica #1

Fuente: Kyndryl Inc. (s. f.f).

Stock Details	
Ticker Symbol	KD
Exchange	NYSE
Fiscal Year	April - March
Reporting Currency	USD
CIK Code	1867072
CUSIP Number	50155Q100
ISIN Number	US50155Q1004
Employer ID	86-1185492
SIC Code	7373

Ilustración 4: Ficha técnica #2

Fuente: Kyndryl Inc. (s. f.f).

1.8.3 Tipo de negocio y mercado meta

Kyndryl experimenta una transformación significativa, ya que se concibió como una empresa con márgenes de ganancia bajos al trabajar en el área de servicios de posventa. En la actualidad, aunque mantiene la mayoría de las áreas de servicios con las que operaba para IBM, su enfoque principal es trabajar en consultoría, integración y seguridad.

Cómo Kyndryl Consult aporta valor a sus clientes

- Entrega éxito en misión crítica con experiencias comprobadas.
- Integra de forma segura tecnologías emergentes en entornos híbridos, beneficiándose de sus décadas de experiencia y patrones de éxito.
- Transforma pragmáticamente con un enfoque en la innovación. Divide los problemas complejos en proyectos alcanzables, utilizando su método exclusivo de creación conjunta y conocimientos prácticos.

- Acelera los resultados comerciales con pericia; ejecuta más rápido aprovechando las amplias habilidades y recursos internos, mientras que apalanca su amplio ecosistema de socios.

En el Apéndice 1 se puede observar un compilado de todas las áreas tecnológicas y servicios sobre los cuales opera y ofrece consultoría Kyndryl. Esto genera una ventaja competitiva, ya que la empresa cuenta con el conocimiento operativo, los expertos y las alianzas necesarios para ayudar a redefinir la relación comercial de cualquier cliente, compañía o corporación con necesidades de TI.

A continuación, se pueden denotar algunas de las áreas que Kyndryl considera pilares en su estrategia. Estas áreas sirven de norte en el momento de trabajar con sus clientes y hasta ahora los mantienen con esa ventaja de mercado.

Experiencia en misión crítica: es el mayor proveedor global de consultoría, implementación y servicios gestionados de infraestructura, con más de 30 años de experiencia en la creación y ejecución de algunos de los entornos tecnológicos más complejos del mundo.

Enfoque de asociación abierta: combina la vasta experiencia y habilidades en todos los ecosistemas, lo que incluye a los proveedores existentes, *hyperscalers* y nuevos socios tecnológicos emergentes**,** para adaptar las soluciones adecuadas a las necesidades de los clientes.

Kyndryl Bridge y Kyndryl Vital: aceleran la transformación empresarial con los conocimientos con base en los datos de la exclusiva plataforma *Kyndryl Bridge* y la resolución colaborativa de problemas de *Kyndryl Vital***.**

Kyndryl se enfoca en generar los mejores resultados comerciales. Estos son algunos ejemplos de áreas en las cuales maneja alianzas estratégicas y casos de éxito:

- Aceleración de la nube híbrida
- Operaciones modernas de TI
- Modernización de aplicaciones y *mainframe*
- Resiliencia cibernética
- Experiencias digitales mejoradas

El trabajo investigativo tiene como enfoque los servicios tecnológicos. Se finaliza con un resumen breve de la estrategia de operaciones e inserción de mercado que Kyndryl presenta a sus clientes y al mercado de tecnologías de la información. El objetivo principal la su estrategia es modernizar y administrar los sistemas y servicios de misión crítica en los que se basa el mundo.

La meta de Kyndryl es brindar experiencia y tecnologías innovadoras que permitan la transformación digital. Las empresas y organizaciones de todo el mundo han comprendido la importancia de poder mover y administrar las cargas de trabajo de TI de manera flexible, dónde y cuándo se necesiten. Para lograrlo, Kyndryl ofrece una cartera integral que aprovecha las soluciones de nube híbrida, la resiliencia empresarial y los servicios de red.

Con el fin de optimizar las transformaciones y cargas de trabajo de TI de sus clientes Kyndryl se encarga de:

- Proteger el patrimonio de TI con seguridad y resiliencia de nivel empresarial.
- Simplificar la gestión de datos empresariales para entornos locales y en la nube.

- Maximizar la eficiencia operativa de TI con una gestión multinube.
- Aumentar la agilidad de TI mediante la modernización de la infraestructura privada.

Adicionalmente abarca los siguientes aspectos:

Modernización de la infraestructura de TI: crear una infraestructura de nube híbrida y privada con capacidad bajo demanda (CoD) que incluya autoservicio, automatización, seguridad y confiabilidad.

Excelencia en la prestación de servicios: maximizar la eficiencia operativa de TI con una gestión multinube híbrida coherente, rentable y escalable.

Gestión de datos simplificada: gestionar datos *end-to-end* agnósticamente de la plataforma, con componentes modulares fáciles de consumir, tanto para datos comerciales como para sistemas.

Ciberseguridad: la seguridad cibernética es primordial para la misión central de Kyndryl de satisfacer las necesidades críticas y estratégicas de sus clientes. Kyndryl impulsa el éxito y garantiza la continuidad, disponibilidad, integridad, crecimiento y confidencialidad de todos los datos y sistemas.

La Oficina Principal de Seguridad de la Información (CISO) persigue esta misión con un enfoque holístico que utiliza el talento altamente experimentado y los activos innovadores. A medida que las amenazas se vuelven cada vez más sofisticadas, también lo hace el método progresivo de diseño e implementación de seguridad que anticipa, detecta, mitiga, recupera y restaura operaciones con un impacto comercial limitado, por parte de Kyndryl.

1.8.4 Misión, visión y valores

A continuación, se transcriben la misión, visión, valores y la cultura orientada al cliente tomados del portal de Kyndryl:

Misión: “Damos poder a los Kyndryls para integrar la inclusión, la diversidad y la equidad en todos los aspectos de nuestro negocio para una fuerza laboral diversa e inclusiva; una cultura equitativa que brinde un servicio excepcional a nuestros clientes y promueva los sistemas vitales que impulsan el progreso humano” (Kyndryl Inc., s. f.g, s. p.).

Visión: “Somos ciudadanos globales empáticos y devotos que se esfuerzan por hacer que el mundo sea mejor y más inclusivo para nuestros empleados, clientes y nuestras comunidades” (Kyndryl Inc., s. f.g, s. p.).

Valores: “Buscar el trabajo en conjunto para construir una cultura de responsabilidad y excelencia” (Kyndryl Inc., s. f.g, s. p.).

Una cultura orientada en el cliente: “Esta busca topar al cliente en el punto del viaje donde se encuentran actualmente y ofrecer soluciones transformativas enfocadas en resolver desafíos específicos de negocios y comerciales” (Kyndryl Inc., s. f.g, s. p.).

1.8.5 Políticas institucionales

La estrategia de responsabilidad social corporativa (RSC) yUnderstо ambiental, social y de gobierno corporativo (ESG) de Kyndryl está en el centro de su misión de convertirse en una empresa impulsada por un propósito. Kyndryl impulsa el progreso humano a través de sólidas prácticas ESG que brindan valor de manera confiable y consistente a los empleados, clientes, partes interesadas y comunidades.

La manera de Kyndryl consiste en una iniciativa corporativa (parte de la cultura empresarial), la cual busca construir valores de marca que auténticamente abarquen las experiencias compartidas con los clientes. Su primordial deseo consiste en ofrecer a los clientes, inversionistas, socios y empleados una experiencia de mutuo beneficio y éxito.

The Kyndryl Way fue desarrollado a través de un intercambio cultural entre los líderes y los empleados alrededor del mundo. Este proceso requiere una inmensa cantidad de confianza entre las diferentes partes, una profunda empatía con los diversos puntos de vista, y una absoluta transparencia.

The Kyndryl Way sustenta todas las acciones, desde la forma en la que se relaciona con los clientes hasta la manera en la que se organiza. Se realiza un esfuerzo diario por construir esta cultura, siendo:

- Incansables: anticipando, aprendiendo e innovando continuamente.
- Empáticos: para servir con confianza y transparencia.
- Dedicados: a compartir el éxito.
- Consistentes: empoderando equipos responsables e inclusivos.
- Rápidos: cultivando simplicidad en todas partes.
- Enfocados: en ofrecer los mejores servicios de su clase.

Prioridades estratégicas

- Cultura conectada e inclusiva: impulsar una cultura en la que los empleados tengan un sentido de inclusión y pertenencia.
- Equipos diversos y representativos: atraer, desarrollar y retener talento diverso en todos los niveles y geografías.

- ID&E en el negocio y operaciones: integrar las prioridades en cada parte del negocio.
- Participación y dedicación a la comunidad: cultivar oportunidades y promover la equidad en comunidades desatendidas.
- La confianza es esencial: el propósito, la promesa y la misión de Kyndryl se basan en un principio fundamental: todo comienza con la confianza.

1.8.5 Spin Off

En Armonk, Nueva York, el 3 de noviembre de 2021 IBM anunció formalmente la separación de su segmento de servicios de administración de infraestructura. Este inició con sus operaciones de manera independiente con el nombre de Kyndryl.

Según las negociaciones realizadas entre las diferentes entidades, utilizando como fecha de corte el 25 de octubre de 2021, los acreedores de las acciones de IBM recibieron una acción de Kyndryl por cada cinco acciones de IBM que tenían en su posesión. El proceso fue fiscalizado por la entidad reguladora de impuestos de los Estados Unidos, la cual externó que la distribución se realizó mediante un procedimiento abreviado:

> La separación de Kyndryl es una de las muchas acciones que se están tomando en vías de afinar el enfoque en el área de Nube Hibrida e Inteligencia artificial; Apalancando una cartera enfocada en tecnología y consultaría, potenciara el crecimiento y cumplimento de los objetivos organizacionales (Krishna, 2020, s. p.).

IBM retuvo aproximadamente el 19.9 % de las acciones de Kyndryl, con la intención de intercambiarlas en un periodo de 12 meses por el valor adeudado con la

empresa. Esta acción se consideró como sujeta a revisión o *cuestionable* en ese momento.

El área de servicios de administración de infraestructura representó aproximadamente una privación en la captación de $19,000,000,000 USD en ganancia para IBM en el mercado de tecnologías de información. Por lo tanto, la entidad se mostró consistente en el mensaje de que era lo mejor para su futuro y crecimiento.

Hoy en día, se reporta que la separación de Kyndryl le ha costado un aproximado del 5 % del mercado a IBM. Al no estar estratégicamente obligados a vender sus productos, Kyndryl ha podido diversificar la cartera de servicios y clientes, al establecer nuevas relaciones y dinámicas con diferentes corporaciones del mercado de tecnologías de información, lo cual ha afectado de forma negativa a IBM. Esta última aún se encuentra en terreno escabroso, adeudando aproximadamente $500,000,000 USD en costos como resultado de la transacción.

Además, IBM buscó separar todas sus operaciones Legacy como un negocio independiente. Kyndryl, por otra parte, busca definir su propio camino en dirección a la automatización y la infraestructura híbrida después de un inicio truncado.

Sin embargo, Kyndryl inició el desarrollo de nuevos servicios y alianzas en busca de aumentar sus ganancias. Las nuevas oportunidades de mercado rondan los $415,000,000,000 USD y se estima que están al alza en un 7 %. Algunas de las áreas en las que buscan competir son:

- Seguridad.
- Automatización Inteligente.
- Servicios de administración de nube.

1.8.6 Historia de IBM

IBM es una de las corporaciones de tecnología más reconocidas en el ámbito mundial. En sus inicios, respondía al nombre de *C-T-R*. Fue fundada por Herman Hollerith a finales del siglo XIX, pero su origen se dio a través de la fusión de tres organizaciones existentes:

- The Computing Scale company.
- The Tabulating Machine company.
- The Time Recording company.

Su fundador, Charles Ranlett Flint, tomó esta firma nacida en Nueva York en el año 1911 con aproximadamente 1300 empleados y dio los primeros pasos en dirección a lo que se conoce hoy como el Gigante Azul. La compañía creció rápidamente utilizando los contratos gubernamentales como plataforma de salida. En la primera mitad de la década de 1920, Thomas Watson asumió la responsabilidad de la empresa y la renombró como *International Business Machines*.

El nicho de mercado de Watson radicaba principalmente en sistemas computacionales, tanto de negocios como científicos. El principal foco de Watson era desarrollar productos especializados y personalizados a las necesidades de sus clientes. Además, hicieron grandes inversiones en el área de ventas y desarrollaron estrategias de negocios y de mercadeo sumamente efectivas.

En 1950, la compañía entró formalmente a la industria de la computación e invirtieron su capital en investigación y desarrollo. Para el año de 1964, presentaron al

mercado la primera familia de lo que se conoce hoy como *computadoras*. Este evento fue de particular relevancia, tanto para la empresa como para la industria informática.

En la década de los 60, IBM produjo el 70 % de las computadoras en el ámbito global. Los sistemas modelo 360 llevaron a muchos competidores a la quiebra, lo cual dejó a IBM en una posición de mercado privilegiada y dominante.

Durante aproximadamente 20 años, IBM abarcó la mayor parte del mercado utilizando como producto estrella sus *mainframes*. En 1981, presentaron al mercado la primera computadora personal llamada *The IBM PC*. Esta utiliza un sistema operativo base llamado MS-DOS de una corporación relativamente nueva en ese momento llamada Microsoft.

Este acontecimiento los mantuvo en la parte superior del mercado hasta 1990, en donde la explosión de la industria informática los llevó a atrincherarse y a reestructurar su estrategia de mercado. Esto ocasionó la adquisición de una compañía de manufactura de *software* con el nombre de Lotus Development Corp.

En esta misma época dorada, IBM desarrolló la arquitectura inicial de las redes locales de telecomunicaciones (LAN) y se convirtió en pionero en el desarrollo de redes de trabajo para las empresas. Desde ahí, tomó rumbo hacia lo que se conoce hoy como Internet.

Adicionalmente, crearon las bases de la inteligencia artificial moderna con su sistema de pensamiento llamado *Deep Blue*. El hito más importante de este sistema fue la serie de partidas de ajedrez contra el campeón mundial y *grandmaster* Garry Kasparov en el momento, las cuales culminaron con la derrota de Kasparov en el 97.

A finales de los años 90 y principios de los años 2000, el tamaño, rendimiento y accesibilidad de los sistemas informáticos impactaron financieramente a IBM, obligándolos a reinventar de nuevo su estrategia de mercado. IBM se alejó de una industria informática con un mercado sumamente saturado y empezó a desarrollar un modelo de negocios orientado a servicios corporativos, instalando redes de telecomunicaciones y servidores.

En 2005, IBM vendió su división de computadoras personales a Lenovo, lo cual los alejó aún más del mercado tecnológico y su *hardware*. Sin embargo, al mismo tiempo, los acercó todavía más al modelo de servicios corporativos.

En 2011, IBM lanzó su primera iteración de una plataforma de computación en la nube, lo cual reveló una nueva pieza en su estrategia siempre cambiante. Esto los acercó nuevamente al ámbito tecnológico, pero desde un ángulo de servicios diversificado.

En el año 2013 se anunció al público la adquisición de la compañía Softlayer. No se revelaron los términos negociados entre las partes, pero estimaciones no oficiales colocaron esta compra de IBM como la más grande en la historia de IaaS en el sector privado en el ámbito mundial.

Softlayer, proveedor de servicios de nube pública, sirvió de base para la división de servicios de nube de IBM. De esta surgió su primer ofrecimiento de IaaS para el 2014, su beta salió al mercado con el nombre de Bluemix. Este se desarrolló utilizando código libre y operaba sobre infraestructura Softlayer, lo cual puso a IBM en el mercado de PaaS para mediados del mismo año.

Desde 2017 hasta la actualidad, la corporación ha continuado enfocando sus recursos financieros y su estrategia en los servicios de nube. Esto les ha permitido

extender y diversificar su catálogo de productos y servicios en diversas áreas de negocios, lo que eventualmente les dará el alcance y la infraestructura necesaria para competir en el mercado con corporaciones del calibre de Amazon, Google y Microsoft.

A pesar de que IBM ya no mantiene la misma cultura y reputación de ser una organización innovadora, aún invierte una cantidad significativa de su capital en investigación y desarrollo. El segmento de la compañía que trabaja con supercomputadoras sigue a la vanguardia y produce poderosos sistemas, mientras sigue licenciando y patentando diseños de negocios gubernamentales y militares.

1.8.7 Ficha técnica

A continuación, se presenta la ficha técnica asociada a IBM. Estas fichas detallan algunos datos de relevancia asociados a la creación y razón social de la empresa.

NAME	International Business Machines (IBM)
FOUNDED	1911
HEADQUARTERS	Armonk, NY, USA
SIC CODE	3571
STATUS	Public Independent Company of NYSE
INDUSTRY SECTOR	Computer Integrated Systems
EMPLOYEES	350,600
TRADING SYMBOL	NASDAQ: IBM

Ilustración 5: Ficha técnica de IBM

Fuente: International Business Machines (IBM) (s. f.b).

1.8.8 Tipo de negocio y mercado meta

A continuación, se pueden denotar algunos de los servicios que IBM presenta a sus clientes en los diferentes segmentos de la gama de negocios.

IBM Watson: con base en las últimas innovaciones en *machine learning*, Watson le permite aprender más con menos datos. No importa cómo utilice Watson, sus datos y conocimientos le pertenecen a usted y solo a usted.

Nube: permite construir con datos avanzados y herramientas de inteligencia artificial en IBM Cloud, una plataforma de nube que abarca entornos públicos, privados e híbridos.

Investigación: *IBM Research* lidera las tecnologías más prometedoras y disruptivas de la inteligencia artificial, *blockchain* y la computación cuántica.

Infraestructura de TI: la infraestructura de IBM es la piedra angular de la arquitectura de su empresa, combina el *hardware* y el *software* que impulsa la transformación digital.

Servicios: *IBM Services* tiene la habilidad comprobada de cambiar industrias enteras, lo que ayuda a liderar un camino pragmático hacia la nube y la inteligencia artificial. Esto permite que las empresas puedan crecer a través de la reinvención digital.

Seguridad: *IBM Security* se enfrenta a los problemas de seguridad cibernética más desafiantes del mundo para proteger a sus clientes**,** las personas que están detrás de los datos.

Como parte de los recursos adicionales disponibles, IBM cuenta con un SOC o *Security Operations Center*. El mismo recibió una fuerte inversión de capital en el periodo 2020, de aproximadamente $21,000,000 USD, para poder triplicar su capacidad de operación y brindar servicios a todo el globo en un esquema de 24 horas, 7 días a la semana.

1.8.9 Misión, visión y valores

Misión: Liderar en la creación, desarrollo y fabricación de las tecnologías de información más avanzadas de la industria, incluidos los sistemas informáticos, software, sistemas de redes, dispositivos de almacenamiento y microelectrónica. Y nuestra red mundial de profesionales de servicios y soluciones de IBM traduce estas tecnologías avanzadas en valor comercial para nuestros clientes. Traducimos estas tecnologías avanzadas en valor para nuestros clientes a través de nuestras soluciones profesionales, servicios y negocios de consultoría en todo el mundo (IBM, s. f.b, s. p.).

Visión: Ser la empresa de tecnología de la información más exitosa e importante del mundo. Éxito en ayudar a los clientes a aplicar tecnología para resolver sus problemas. Exitoso en la introducción de esta extraordinaria tecnología a nuevos clientes. Importante, porque seguiremos siendo el recurso básico de gran parte de lo que se invierte en esta industria (IBM, s. f.b, s. p.).

Valores: Los valores fundamentales de IBM comprenden: “Diversidad e inclusión, innovación, ser uno mismo y centrarse en el cambio” (IBM, s. f.b, s. p.). Aunque la empresa no ha definido claramente sus valores fundamentales, se pueden extraer de la cultura creada en IBM.

1.8.10 Políticas institucionales

IBM (International Business Machines) llama a su fuerza de trabajo IBMers y considera que absorber a expertos con diversos antecedentes es la fuente de su rica cultura. Obtener conocimiento de todo el mundo es la fuente de innovación de IBM, especialmente cuando estas personas aportan todo su ser al propósito de la empresa.

La integración de estos valores promueve la capacidad de asumir riesgos y prosperar en ellos, tal como IBM es más conocido.

El lema con el que se rige IBM en estos tiempos modernos es: “Vivir según nuestros valores: Dedicación al éxito de todos nuestros clientes; Innovación que importa, para nuestra empresa y para el mundo; Confianza y responsabilidad personal en todas las relaciones” (IBM, s. f.b, s. p.).

1.9 Revisión sistemática de la literatura y estado de la cuestión

La revisión sistemática de literatura se ha convertido en uno de los métodos de investigación más importantes en el área de ingeniería de *software* desde los inicios del siglo XXI. En este método, el desarrollo y ejecución de una óptima estrategia de búsqueda determina la viabilidad de la investigación por realizar. Sin embargo, completar este objetivo efectivamente consume mucho tiempo y está sujeto a potenciales errores.

Por lo tanto, existía una potencial necesidad de desarrollar, ejecutar y evaluar una estrategia de búsqueda óptima que permitiera procesar y recolectar literatura de librerías digitales de manera sistemática.

En el caso específico de esta investigación, se consideró e incorporó el concepto del *Estándar casi-oro* (al que se hace referencia, en adelante, como ECO). Este concepto consiste en agregar a la búsqueda colecciones de estudios relevantes con sus respectivas *casi-sensibilidades*, lo que permite evaluar el rendimiento de las búsquedas.

Las revisiones sistemáticas (RSL) pretenden identificar, valorar y combinar evidencias de diferentes estudios investigativos primarios usando un método explícito y rigoroso. Estas inspecciones, a la vez, dieron cabida a problemas potenciales o consideraciones que se detallan a continuación:

- ¿Cómo se pueden diseñar estrategias de búsqueda rigorosas que maximicen la recopilación de estudios relevantes?
- ¿Cuáles criterios son accesibles y confiables para balancear efectivamente la sensibilidad (calidad) y la precisión (esfuerzo) de los criterios de búsqueda?
- ¿Es posible evaluar estrategias y cadenas de búsqueda predefinidas?

La aplicación efectiva de este método mejora el rigor y la sensibilidad de las diferentes estrategias de búsqueda y sus respectivas cadenas. Estas estrategias dan como resultado estudios relevantes que tienen un potencial más alto de convertirse en insumos primarios de la investigación.

Inicialmente, se busca definir la base de búsqueda más apropiada para cumplir con los requisitos investigativos. Esta base está conformada por aspectos como:

- Conocimientos de los diferentes expertos en el área por investigar.
- Diferentes repositorios de datos recomendados por la comunidad, expertos o por el mismo investigador(es).
- Repositorios y periódicos de organizaciones reconocidas o definidas previamente como confiables o viables.
- Técnicas de búsqueda *Thesauri*.
- Previas iteraciones o búsquedas referentes al tema que se identificaron dentro del campo de estudio. Estas incluyen diferentes términos, combinaciones, cadenas o estrategias.

1.9.1 Definición de la estrategia de búsqueda

Un proceso de búsqueda optimizado busca contestar efectivamente algunas interrogantes, por ejemplo:

1. ¿Cuál enfoque se utiliza en el proceso de búsqueda (manual, automatizado o mixto)?
2. ¿Dónde (fuente o lugar) se realiza la búsqueda y cuál sección o campo de los artículos es investigado?
3. ¿Qué (tema, tipo de evidencias) es investigado y que parámetros se utilizan (cadenas de búsqueda) dentro de los diferentes buscadores?
4. ¿Cuándo la investigación se realiza y qué periodo debe ser considerado como parámetro(s)?

En referencia al enfoque por utilizar, existen diferentes guías y repositorios que cuentan con recomendaciones sobre cómo elaborar búsquedas efectivas a través de diversos recursos disponibles. Sin embargo, en la práctica, las personas investigadoras suelen realizar distintos tipos de búsquedas.

Durante los procesos de búsqueda manuales, las personas investigadoras analizan los diferentes recursos, revisando publicación por publicación y artículo por artículo, para asegurar la captura de estudios relevantes al caso. Sin embargo, este proceso también implica revisar documentos que pueden ser irrelevantes para la investigación, lo cual consume cantidades considerables de tiempo.

En la contra propuesta, las búsquedas automatizadas permiten cubrir una mayor cantidad de temas, material, repositorios y demás, lo cual las hace más efectivas que las búsquedas manuales. Sin embargo, su rendimiento está directamente relacionado con

la calidad de las cadenas de búsqueda, las capacidades de la plataforma de búsqueda y la diversidad del tema por investigar.

Es relevante destacar el concepto de *fuente de búsqueda*, ya que durante el proceso de definición de la estrategia de búsqueda también se puede emplear el concepto de *plataforma de búsqueda*. Las búsquedas automatizadas generarán exclusivamente los resultados de las plataformas sobre las cuales se utilizan. No obstante, si se extiende el concepto a las búsquedas manuales, estas pueden proporcionar resultados de diversas fuentes o recursos (los cuales se definen en las citas).

Las cadenas de búsqueda que se apegan a diferentes operadores lógicos predefinidos generan los mejores resultados. Estos permiten remover los estudios de baja calidad y potenciales resultados irrelevantes al caso. Algunos ejemplos de estos evocan el uso de la disciplina, campo de estudio u otros factores.

La definición de las fechas o periodos relevantes siempre es determinada por el interés o el objetivo del RSL y las premisas sobre las que se basa. La revisión de la literatura usualmente toma una cantidad considerable de tiempo. De hecho, se puede hablar incluso de meses o años. Esto permite descubrir potenciales tendencias y también periodos importantes en donde se materializó un fenómeno. Dicho fenómeno puede aún estar vigente o, en su defecto, permitir encausar su comportamiento o periodicidad.

Estos fenómenos aún pueden estar en etapas de recopilación de datos por parte de los diferentes actores. Por ende, interesa a la investigación observar, tanto la progresión que ha tenido el fenómeno como la evolución que puede tener a lo largo del proceso. Independientemente del resultado que pueda tener, se puede definir de manera

subjetiva si debe usarse como insumo de la estrategia de investigación o incluso como estudio primario.

1.9.2 Evaluación de la estrategia de búsqueda

El rendimiento de la estrategia de búsqueda puede determinarse al examinar las respuestas a las preguntas diseñadas por el investigador y los resultados como producto de su aplicación. Esto permite realizar la valoración de manera subjetiva u objetiva.

El método subjetivo utiliza expertos externos a la investigación para revisar primero la estrategia de búsqueda predefinida antes de pasar a la fase formal evaluativa. Luego, se comparan algunos estudios preseleccionados mediante búsquedas automatizadas para determinar su efectividad. El resultado de la evaluación depende principalmente de la experiencia, pericia, dominio, educación y conocimiento del evaluador, lo cual se puede medir a través de un mecanismo cuantitativo.

Ahora, el método objetivo se basa enteramente en resultados estadísticos y diversas fórmulas matemáticas. Estas están definidas en diferentes guías de aplicación en la comunidad, por lo tanto, se debe seleccionar la que mejor cumpla con los requisitos del ECO de antemano.

El factor de relevancia depende enteramente de los resultados de la evaluación. Por consiguiente, se puede optar por incluir una evaluación objetiva al proceso subjetivo, la cual define parámetros más cuantitativos para evaluar el rendimiento de la búsqueda de manera precisa, predecible, reproducible y medible.

Durante el desarrollo de este documento, se mencionan continuamente los parámetros de sensibilidad y precisión. Estos se definen a continuación, ya que ayudan a comprender en profundidad el funcionamiento de ECO.

La sensibilidad de un tema se define como la proporción de estudios relevantes que se obtienen durante la búsqueda. La precisión, por otro lado, se refiere a la proporción de los artículos obtenidos que son importantes o que pueden considerarse primarios.

En la Ilustración 6 se demuestra mediante un diagrama de Venn cómo el estándar casi oro se suma a la sensibilidad y a la precisión, demarcando los parámetros óptimos para una búsqueda.

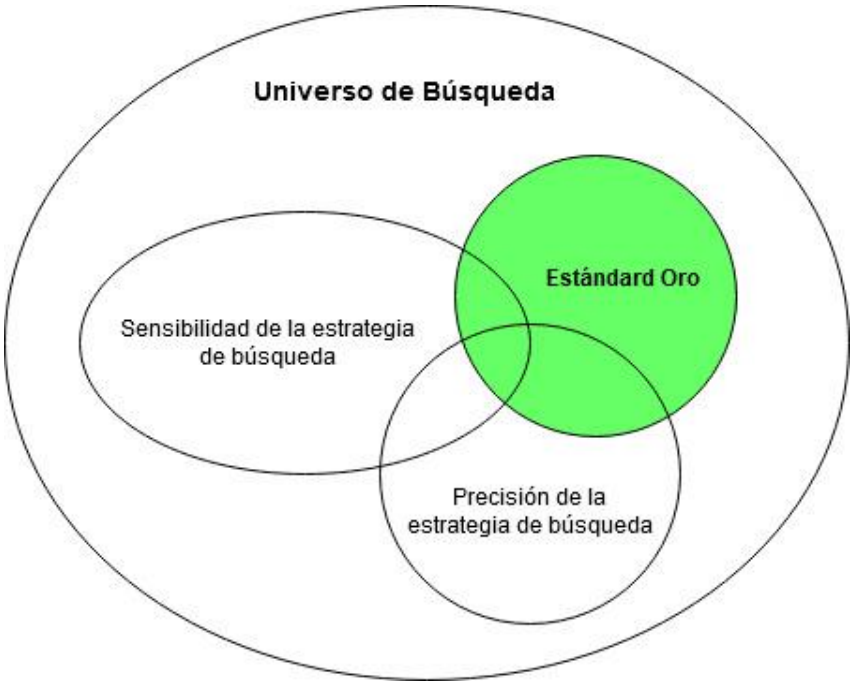


Ilustración 6: Universo de búsqueda

Fuente: Zhang y Ali Babar (s. f.), adaptación al español.

Mediante el proceso de búsqueda automatizada, la plataforma de búsqueda recibe una cadena de búsqueda específica. Esta cadena obtiene una cantidad

determinada de estudios, en los cuales se valoran la sensibilidad y la precisión utilizando las siguientes fórmulas:

Sensibilidad = Número de estudios relevantes que se obtienen/número total de estudios importantes * 100 %

Precisión = Número de estudios relevantes que se obtienen/número de estudios importantes * 100 %

Una estrategia de búsqueda con alto factor de sensibilidad dará como resultado muchos estudios dentro del estándar de oro, pero también incluye muchos artículos no deseados. Por otra parte, una estrategia de búsqueda con alto factor de precisión dará como resultado un menor número de estudios descartables, no obstante, puede dejar por fuera muchos artículos relevantes. La estrategia de búsqueda perfecta debe dar como resultado 100 % de sensibilidad y 100 % de exactitud, obteniendo el estándar de oro mientras se deja por fuera los estudios irrelevantes.

Según las estadísticas presentadas por Zhang y Ali Babar (2010) en la Ilustración 7, se puede notar una diferencia muy significativa en los dos primeros lugares de la tabla. IEEEXplore y ACM digital library obtuvieron una diferencia de al menos 23 puntos porcentuales hasta 34 puntos porcentuales. Esto implica que son los portales con mayor índice de reutilización como plataforma de búsqueda en los diferentes RSL.

Rank	Search engine	# of SLRs	% of SLRs
1	IEEE Xplore	24	92%
2	ACM digital library	21	81%
3	ScienceDirect	15	58%
4	ISI Web of Science	10	38%
5	EI Compendex	9	35%
6	SpringerLink	8	31%
6	Wiley InterScience	8	31%
6	Inspec	8	31%
9	Google Scholar	6	23%
10	SCOPUS	2	8%
10	Kluwer	2	8%

Ilustración 7: Tabla de frecuencias de ECO

Fuente: Zhang y Ali Babar (s. f.), adaptación al español.

Por consiguiente, se seleccionan ambos portales como principales fuentes de búsqueda de la RSL, tanto manual como automatizada. Además, ambas plataformas cuentan con un recurso de búsqueda que funciona con ECO.

ECO consiste principalmente en un grupo de estudios que provienen de distintas fuentes clave, como dominios específicos, periódicos y otras librerías digitales, reconocidos por la comunidad y sus expertos en la materia.

En comparación con el estándar *oro*, este solo cuenta con dos de las cuatro aristas de una estrategia de búsqueda óptima: el lugar y el cuándo. No obstante, según la manera en la que estas condiciones se presenten, puede determinarse como *oro* bajo la premisa de que se debe definir, probar e integrar un criterio más objetivo al proceso de RSL. A la vez, este criterio se apoya en el análisis de la información predefinida del ECO y no en la subjetividad de la percepción de la persona investigadora.

Otro aspecto importante por resaltar en el tema de la subjetividad es que se puede utilizar el ECO como mecanismo para evaluar los diferentes criterios y cadenas de búsqueda. Esto permite determinar la efectividad de la estrategia de búsqueda.

En la Ilustración 8 se puede observar cómo este mecanismo permite utilizar los resultados o estudios recolectados de las búsquedas manuales para establecer el ECO. Esto genera las cadenas de búsqueda para el proceso automatizado, el cual eventualmente puede usarse como criterio para evaluar la estrategia de búsqueda. Por otro lado, las búsquedas automatizadas ayudan a complementar la búsqueda manual, ya que expanden los alcances y mejoran la captura de los estudios más relevantes de manera relativamente rigurosa.

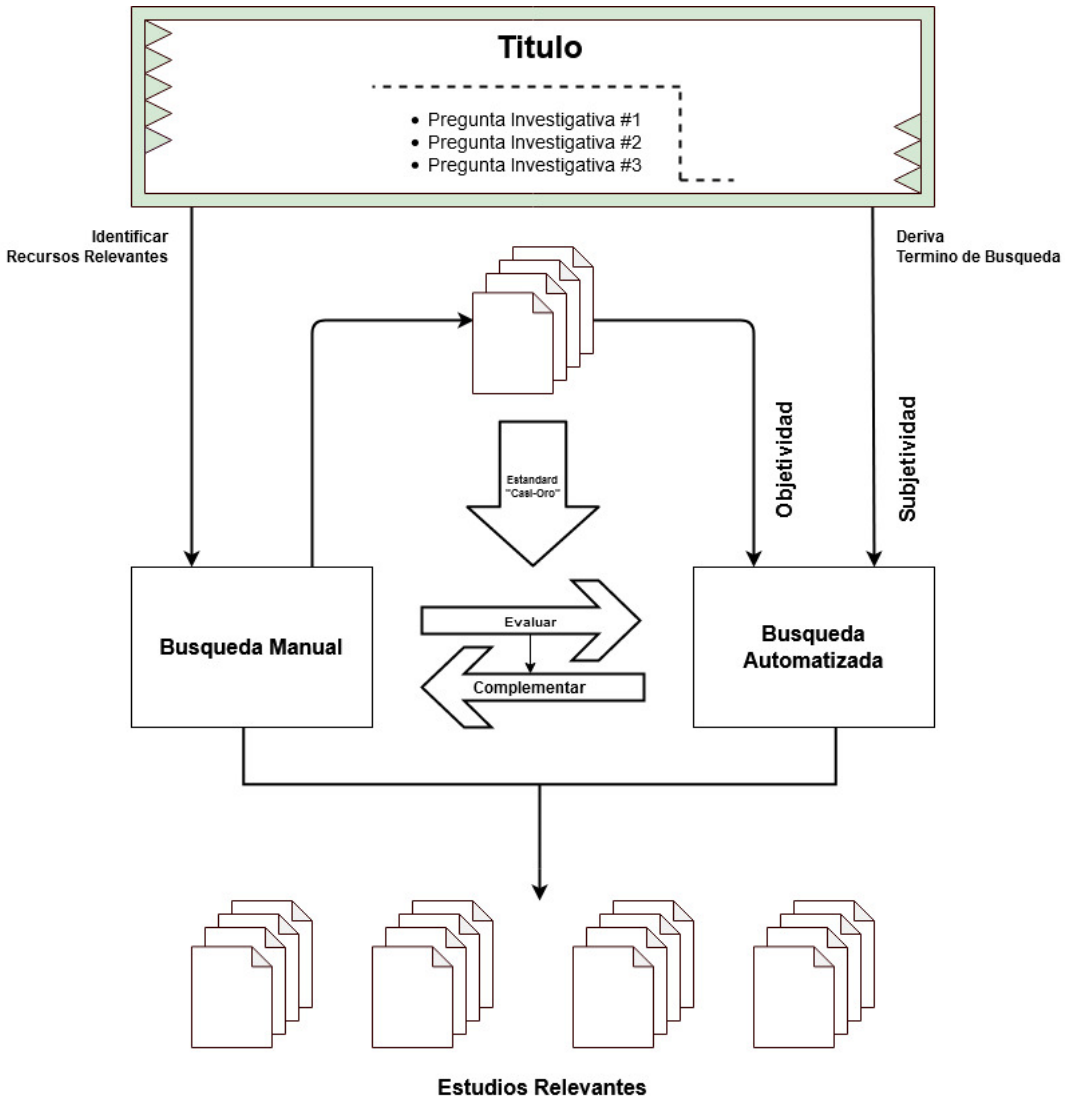


Ilustración 8: Mecanismo de operación de ECO

Fuente: Zhang y Ali Babar (s. f.), adaptación al español.

1.9.3 Proceso de aplicación del Estándar casi-oro

Como paso inicial en la aplicación, se identifican las fuentes para realizar búsquedas manuales. Para esto se utilizan diferentes plataformas y motores, como librerías y bases de datos.

El ECO se establece al realizar búsquedas manuales en las distintas fuentes definidas. Todos los resultados se agrupan utilizando como criterio las ubicaciones de los estudios extraídos.

El diseño de las cadenas de búsqueda puede ser subjetivo y objetivo. Las cadenas subjetivas las generan las personas investigadoras y, después, se evalúan con el ECO. Las cadenas objetivas se producen automáticamente usando como base los artículos predefinidos en el ECO.

Las cadenas que se crean objetivamente pueden utilizar parámetros como la frecuencia de las palabras o herramientas de contenido. Todos los resultados deben combinarse con el ECO y evaluarse. Por último, estos deben catalogarse y definirse como *aceptables* antes de poder utilizarse como criterios de búsqueda automatizada.

Debido a la relación de muchos a muchos entre las distintas fuentes, plataformas y motores, una búsqueda óptima debe cubrir la mayor cantidad de fuentes con la menor cantidad de recursos. Es decir, se busca eliminar la mayor duplicidad posible. La Ilustración 9 muestra el diagrama del proceso de una búsqueda.

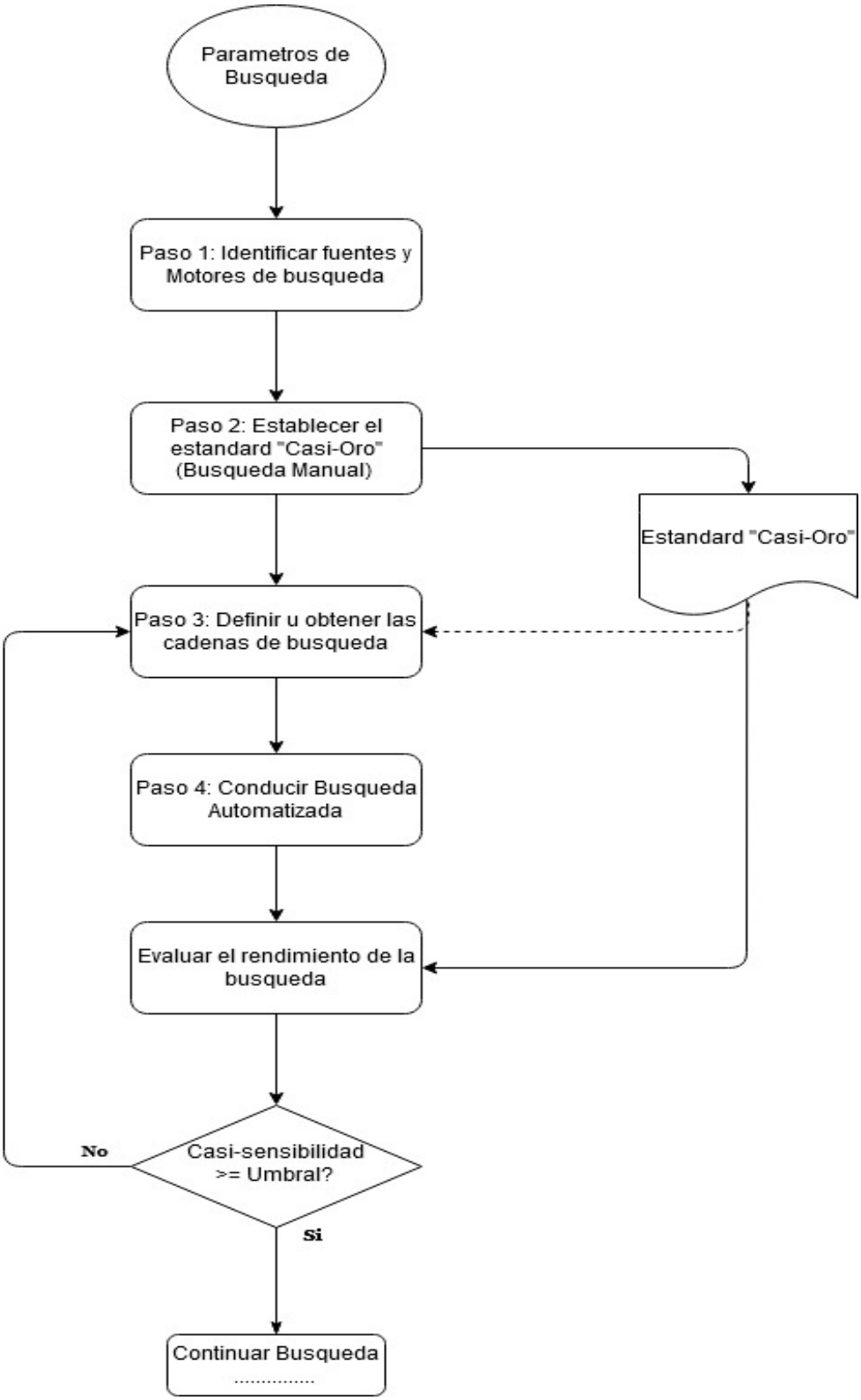


Ilustración 9: Proceso búsqueda de ECO

Fuente: Zhang y Ali Babar (s. f.), adaptación al español.

1.9.4 Implementación de la búsqueda

En la fase de búsqueda manual se seleccionan de manera empírica las distintas fuentes por consultar. Luego, se construyen las cadenas de búsqueda de forma subjetiva, con el objetivo de englobar conceptos de ciberseguridad e infraestructura, junto con sus respectivas intersecciones y vertientes. La Ilustración 10 ejemplifica una cadena de búsqueda que utiliza como parámetros o palabras clave: *ciberseguridad* e *infraestructura*.

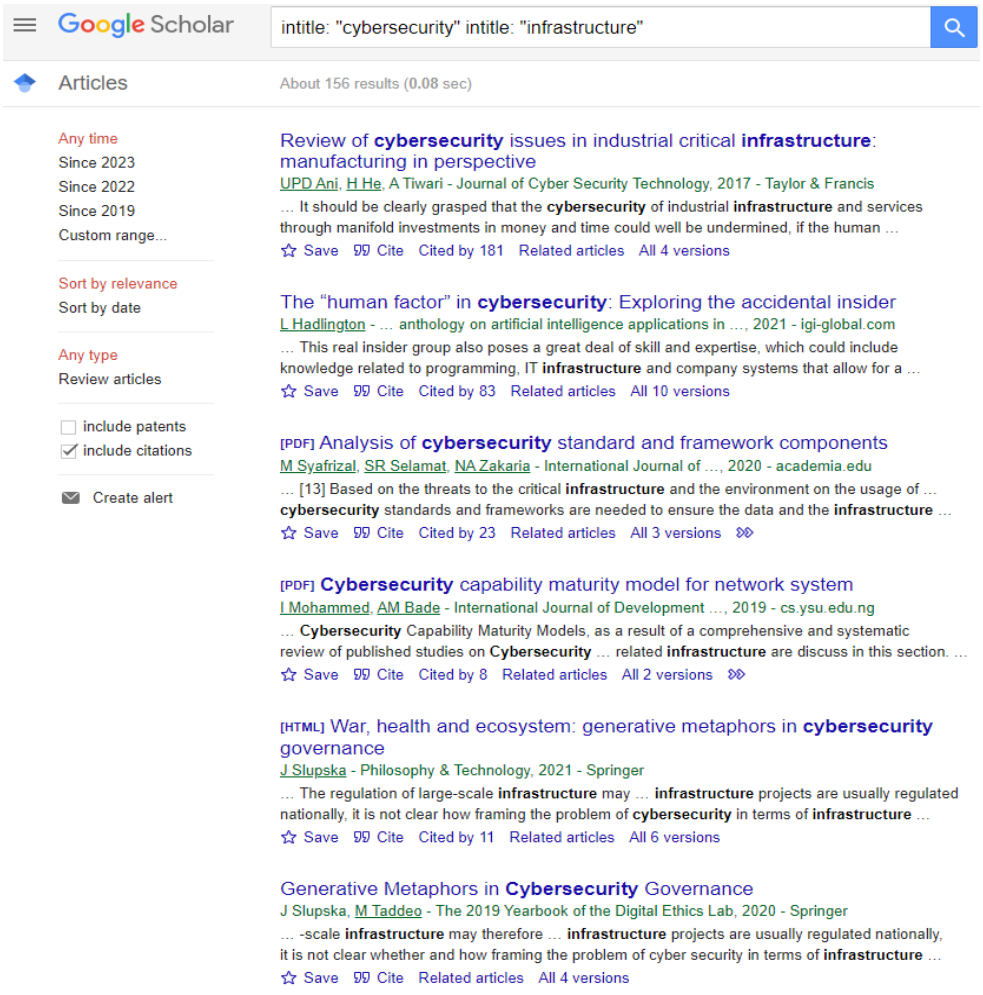


Ilustración 10: Cadena de búsqueda inicial

El resultado de esta búsqueda fue muy provechoso. La mayoría de los artículos que se encontraron engloban no solo el concepto, la afectación y sus características, sino que también abarcan componentes de gobierno digital y algunas recomendaciones o hallazgos que sirven como base de referencia.

Es importante destacar que esta búsqueda inicial revela mucha información referente al tema. Esta información debe ser refinada una vez que se tengan los puntos de datos del ecosistema sobre el que se desee trabajar específicamente. Esto se debe a que las diferentes industrias y necesidades de negocios dictan distintos requerimientos técnicos, financieros y regulatorios.

Durante el proceso investigativo aplicado al tema de infraestructura de ciberseguridad, se utilizó el método ECO, ya que este es inherente a la plataforma de búsqueda dentro de los repositorios de la AMC y IEEE. Esto aumentó considerablemente la precisión de la cadena de búsqueda. En la Ilustración 11 se muestra una rúbrica de referencia que cataloga la estrategia que se utiliza dentro de un estilo de alta *exactitud*.

Estrategia	Sensibilidad	Precisión	Comentarios
Alto Sensibilidad	85-90%	7-15%	Máxima sensibilidad a pesar de la baja precisión
Alto Precisión	40-58%	25-60%	Máxima precisión a pesar de la baja sensibilidad
Optimo	80-99%	20-25%	Maximizar ambas, Sensibilidad & Precisión
Aceptable	72-80%	15-25%	Sensibilidad y Precisión Justas (Promedio)

Ilustración 11: Categorización de estrategias de ECO
Fuente: Zhang y Ali Babar (s. f.), adaptación al español.

La cadena de búsqueda siguiente se definió con el objetivo de ajustar la perspectiva de la investigación dándole un enfoque más abierto y evaluativo a la

propuesta que, a la vez, reflejara la actualidad del estado global y las recomendaciones proporcionadas por la comunidad de ciberseguridad. Esta cadena de búsqueda también se incluyó como parte del ECO, al igual que los estudios que se obtienen como resultados (ver la Ilustración 12).

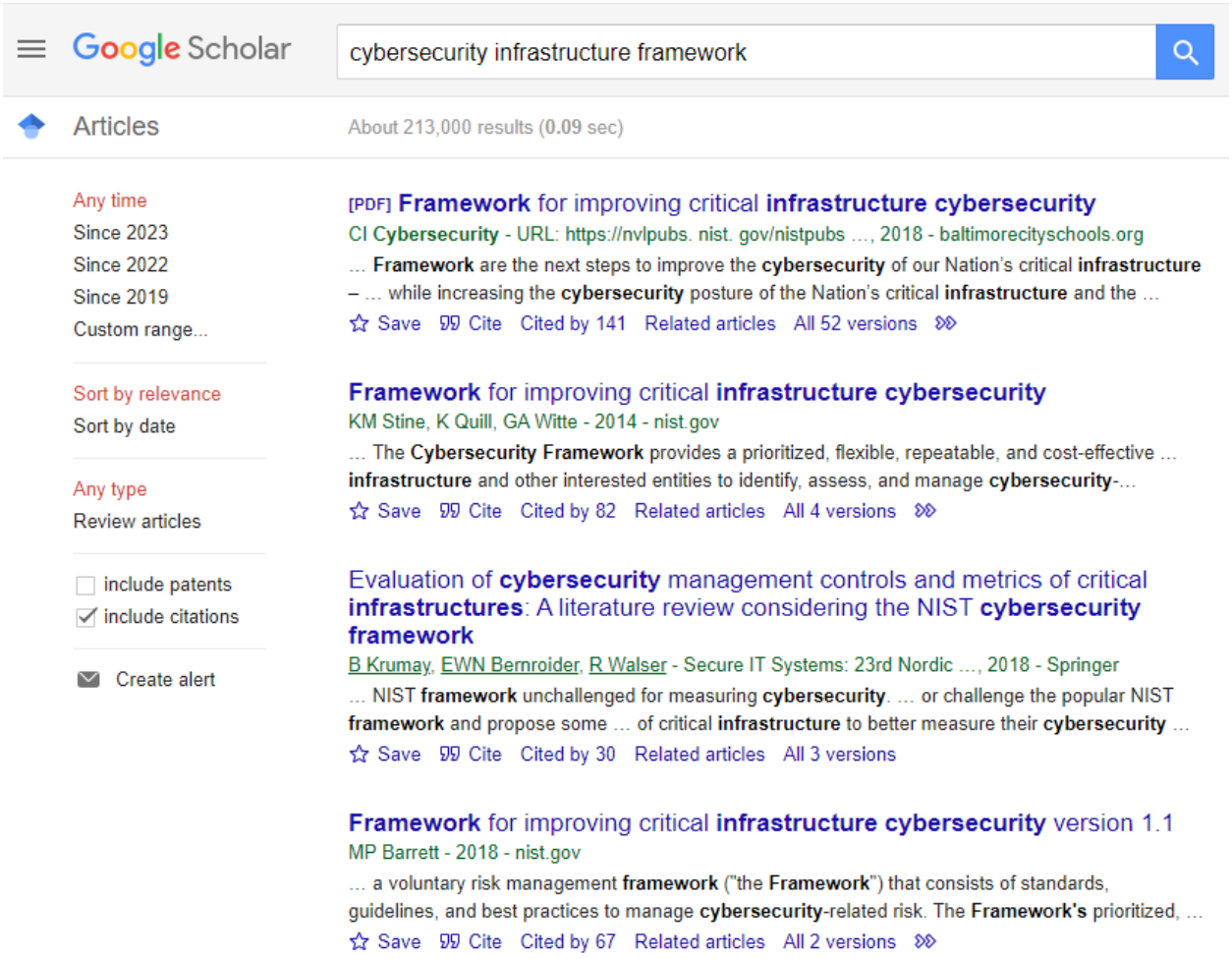


Ilustración 12: Cadena de búsqueda de ajuste a ECO

Con base en los resultados que se encontraron en el siguiente grupo de publicaciones, se realizó un ajuste a la cadena de búsqueda para centralizar los alcances

a un punto de enfoque más metodológico y sistemático (ver Ilustración 13 e Ilustración 14).

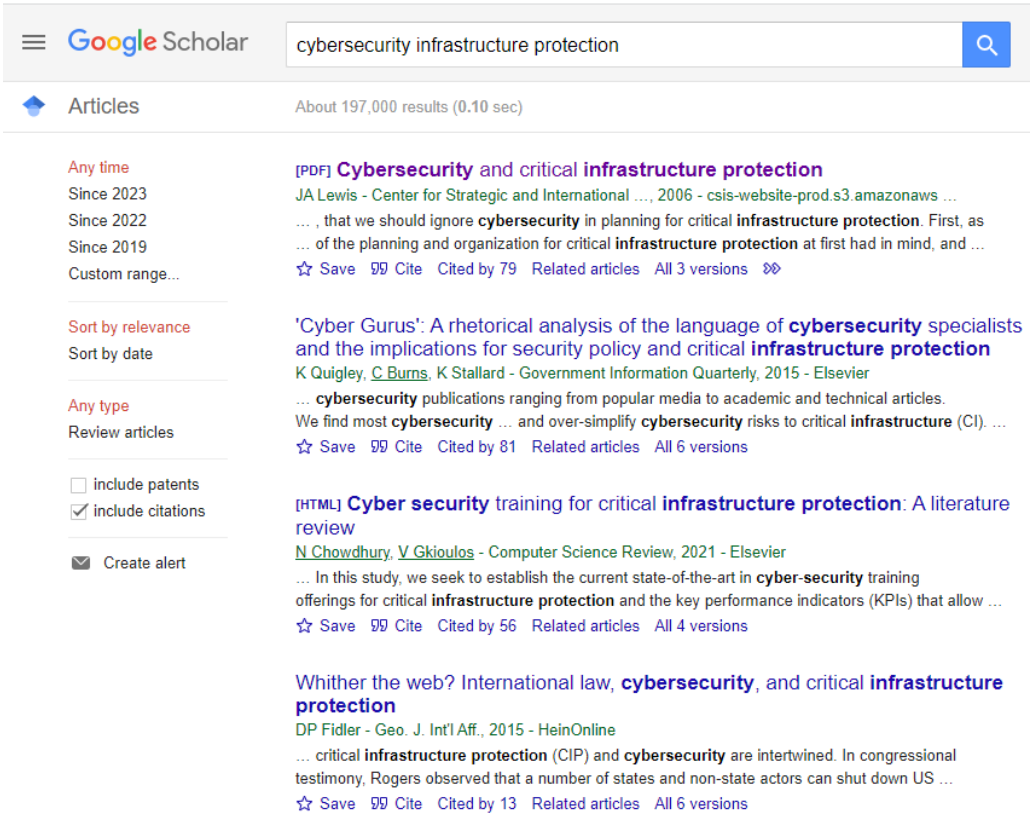


Ilustración 13: Cadena de búsqueda de ajuste a ECO #2

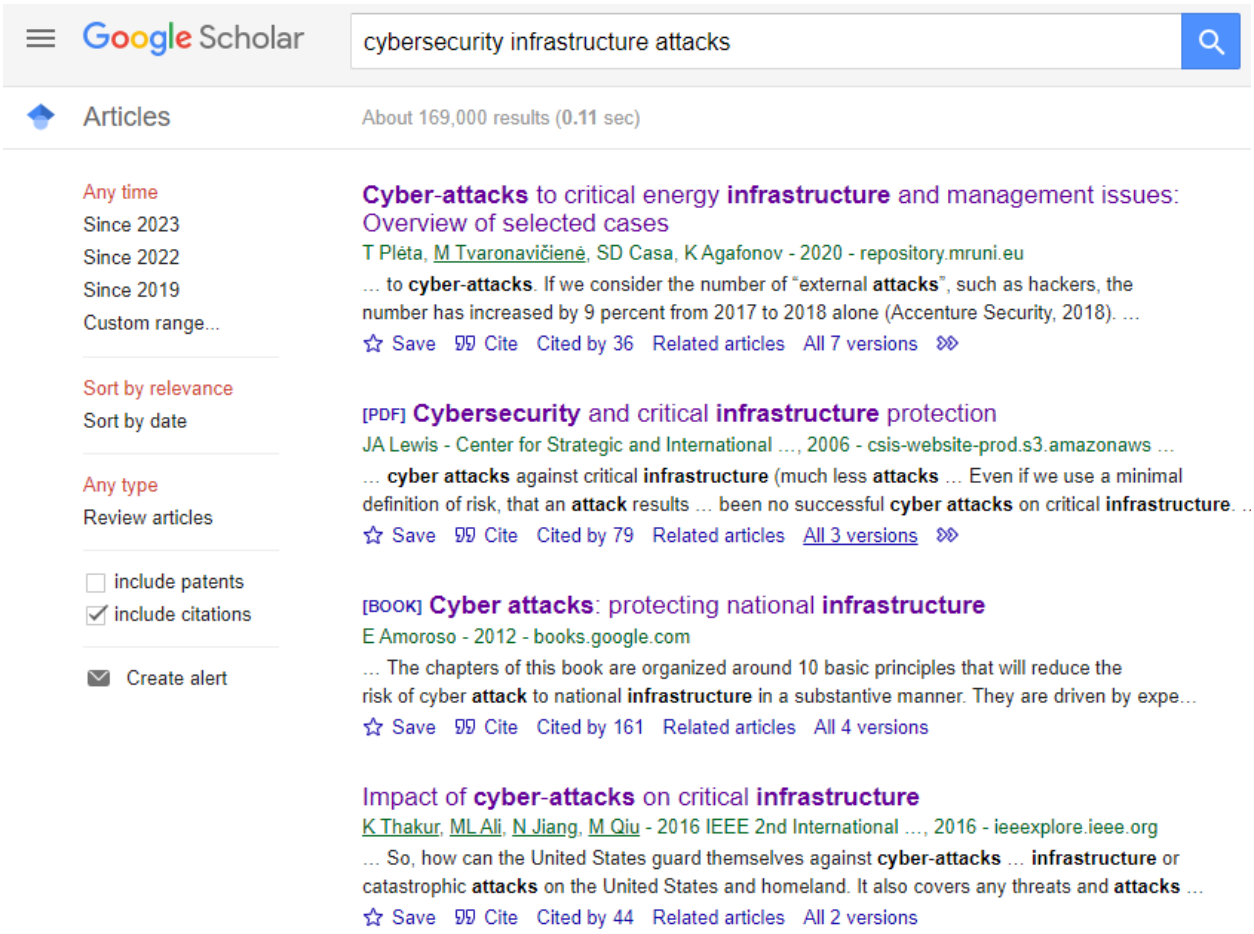


Ilustración 14: Cadena de búsqueda de ajuste a ECO #3

Durante la implementación del proceso de búsqueda se utilizan al menos tres cadenas de búsqueda. Los diversos estudios resultantes se emplearon como base para obtener y elaborar los criterios de búsqueda automatizada.

Cabe destacar que los resultados de las cadenas de búsqueda y procesos manuales no se enfocaron en obtener la mayor cantidad de resultados ni en capturar sus estudios relevantes, sino que se busca establecer el ECO. Además, los resultados importantes tampoco fueron excluidos.

Como resultado, se obtuvo una disminución muy significativa en los tiempos de búsqueda. Los factores de precisión aumentaron y la sensibilidad disminuyó, por lo tanto, el número de resultados también se redujo. Sin embargo, este ajuste a la estrategia de búsqueda mejoró considerablemente, impulsando el nivel de optimización de la RSL por encima del 90 %.

Durante el proceso de RSL se realizaron iteraciones adicionales, por ende, algunos de los componentes de la estrategia de búsqueda pueden cambiar, alterando los valores del criterio objetivo del ECO y acercando los resultados a un *estándar oro*. Ahora, desde un enfoque más subjetivo, el ECO puede mejorarse aún más al consultar diferentes comunidades y expertos en los distintos temas circundantes.

Capítulo 2: Marco conceptual

Como primer paso en la definición del marco conceptual de este proyecto se creó una nube de palabras utilizando la herramienta web. Esta nube fue alimentada con una concatenación del contenido de todos los estudios que se revisaron y catalogaron como relevantes o primarios para la estrategia de búsqueda, según el proceso descrito en el apartado del estado de la cuestión (ver la Ilustración 15).

Ilustración 15: Nube de palabras

Es importante resaltar que durante el proceso de definición de conceptos se utilizó la misma metodología del ECO. Por lo tanto, las palabras que resaltaron son el resultado de la optimización del criterio de diseño utilizando un combinado de factores objetivos, como el conteo de palabras y su respectivo peso estadístico y factores subjetivos, como el criterio experto de la persona investigadora y las tendencias de la comunidad.

El objetivo principal del ejercicio fue generar una conceptualización que permita a los lectores del documento un nivel base de entendimiento más allá de la experiencia, conocimiento y perfil. De esta manera, la información y los resultados pueden transmitirse de la forma más eficiente.

2.1 Guía metodológica

Inicialmente, se define que el objetivo principal del documento investigativo consiste en generar una guía de optimización. Por lo tanto, es de vital importancia profundizar en el detalle del método de elaboración de una guía para asegurar un resultado de calidad.

Según Cenet (2009), una guía metodológica consiste en sistematizar la reproducción conceptual y teórica de la experiencia práctica del objeto de estudio. Esta es una forma de elaboración intelectual cuyo resultado puede expresarse en formatos diferentes, los cuales se definen en las etapas iniciales como parte del método. De esta manera, procura hacer partícipes de los hallazgos a quienes no tuvieron la oportunidad de estar involucrados en la ejecución o elaboración de esta, pero que de una u otra forma buscan alcanzar objetivos o resultados similares.

En ciertas ocasiones es necesario compartir no solo el conocimiento de la práctica u objeto, sino también inducir, orientar o influenciar hacia una cierta forma de actuar.

Esta manera de actuar depende en su totalidad del conocimiento y la necesidad, sin embargo, demuestra efectividad en la práctica y, a través de la sistematización descubre, revalora y eleva su funcionalidad, poniéndola al servicio de otros interesados.

Las guías metodológicas, didácticas y operativas cumplen una función útil y contribuyen al mejoramiento de experiencias en marcha y su rendimiento. Esto facilita la realización de nuevos ejercicios, aumenta la eficiencia y, por consiguiente, su precisión, a partir del desarrollo metodológico alcanzado durante la experiencia precedente.

En la Ilustración 16 se presenta una propuesta del armazón o estructura que potencialmente puede llevar la guía junto con sus diferentes apartados. Para esto solo se tomaron en cuenta los componentes aplicables al caso de estudio.

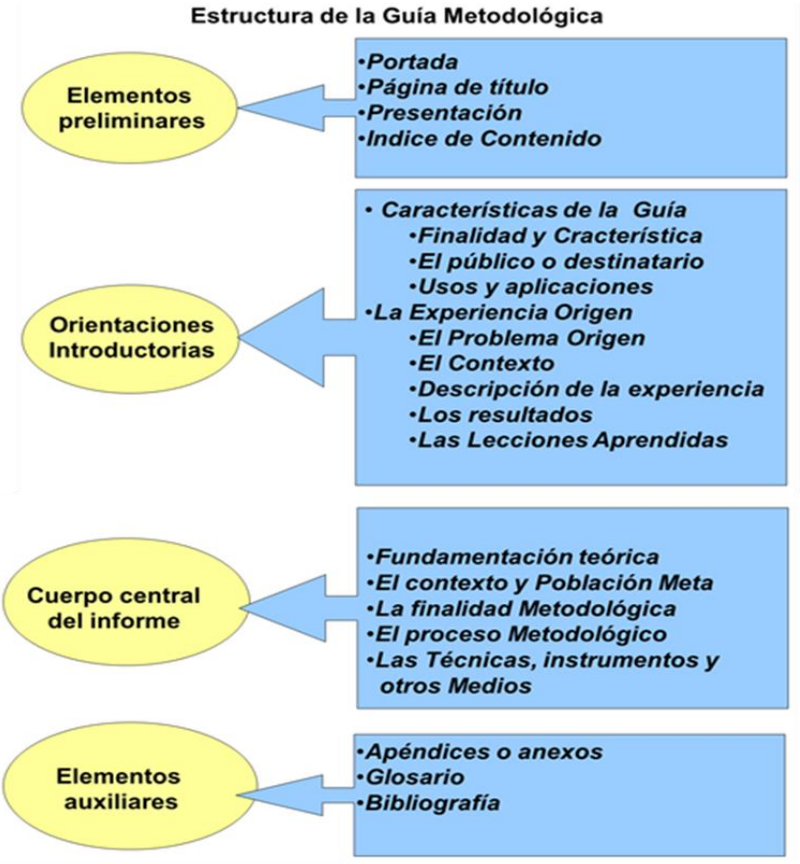


Ilustración 16: Estructura de una guía metodológica

Fuente: Cenet (2009).

La guía metodológica es un instrumento que permite unificar criterios en torno a la investigación. Por consiguiente, se propone utilizar como fuentes de origen de la guía metodológica los siguientes componentes:

- Experiencia sistematizada
- Vivencias del autor
- Fuentes secundarias

En referencia a la metodología como tal, en la imagen subsecuente se aprecia una estructura básica de planificación. Esta estructura permite encausar el esfuerzo y prevenir múltiples reiteraciones innecesarias (ver la Ilustración 17).

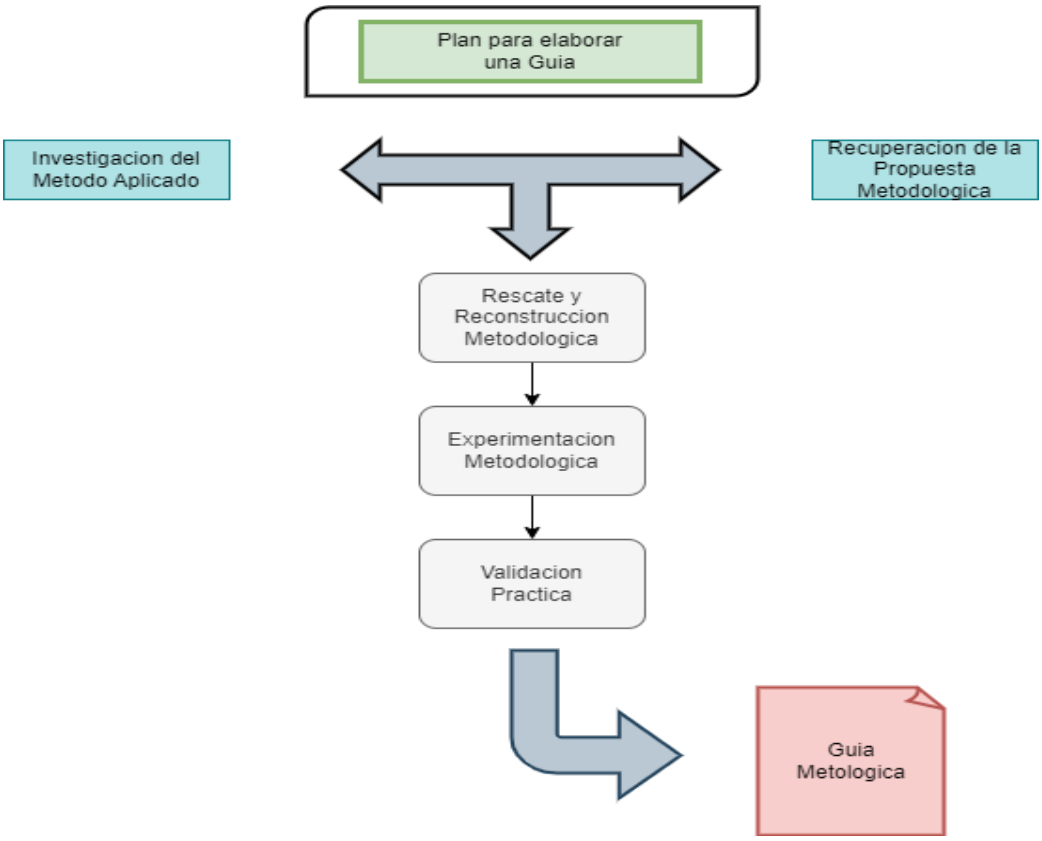


Ilustración 17: Plan de elaboración de una guía

Fuente: Cenet (2009).

Por último, una vez completadas las primeras versiones de la guía, se debe asignar un dueño o recurso que tenga como tarea obligatoria mantener el *documento vivo*, darle mantenimiento continuamente y responsabilizarse de que el contenido refleje la realidad de la organización sobre la cual se aplica.

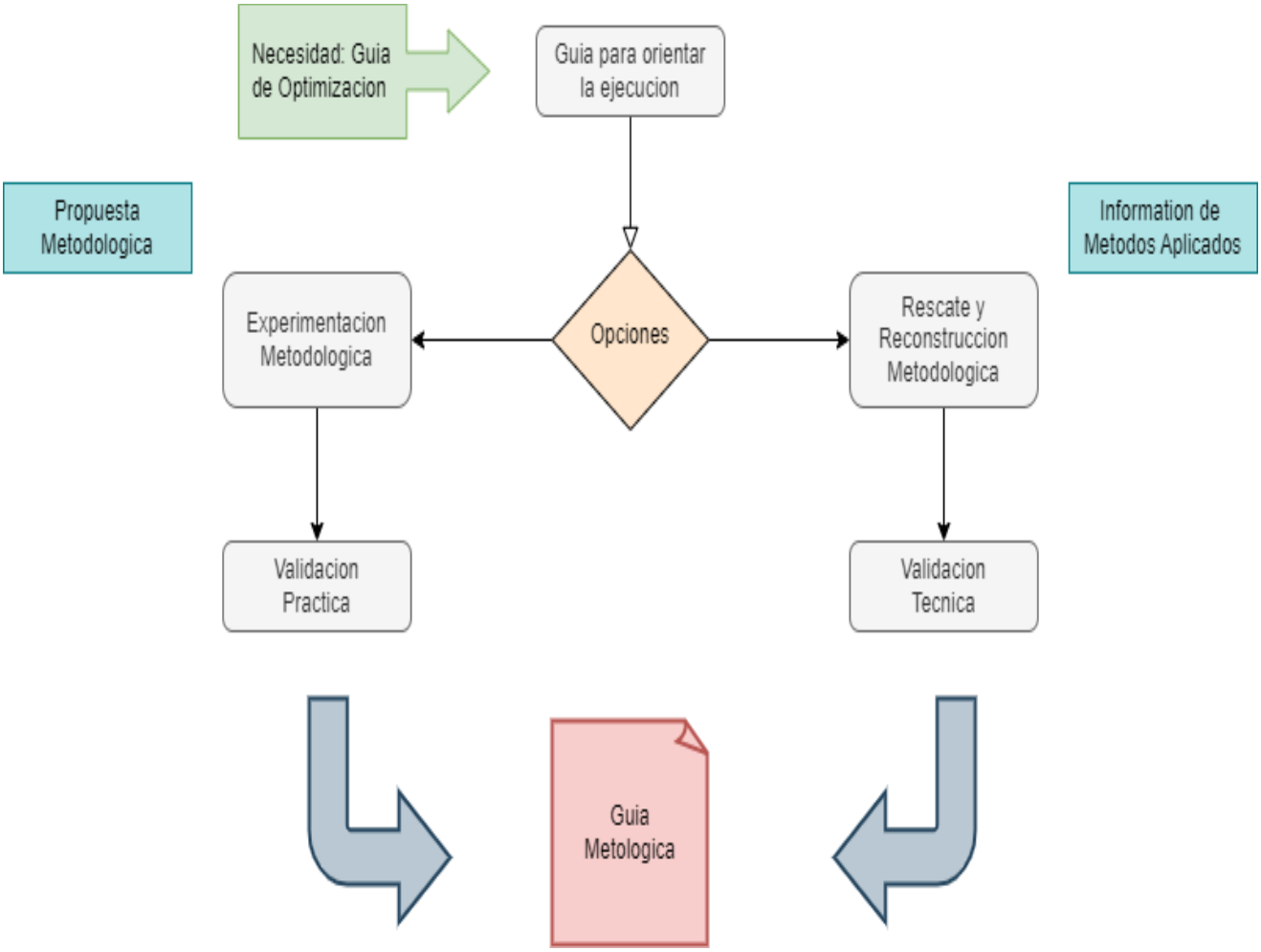


Ilustración 18: Proceso de elaboración de una guía

Fuente: Cenet (2009).

2.2 Conceptualización de referencia

Algunos de los términos más comunes dentro de la jerga de ciberseguridad son: activo, vulnerabilidad, amenaza y riesgo. Por lo tanto, siempre es relevante dedicar un momento para reforzar su concepto. Estos se utilizan de manera recurrente para explicar diferentes fenómenos, casos de estudio, materializaciones y técnicas.

Cualquier componente dentro del perímetro de la organización necesita ser protegido. Algunos ejemplos son:

- Datos.
- Infraestructura física y virtual.
- Personal o recursos.
- Herramientas propietarias.
- Procesos esenciales para el negocio.

Vulnerabilidad: una debilidad dentro del ecosistema que puede ser explotada por cualquier actor, como los defectos en los aplicativos o en sus procesos de desarrollo. Otro ejemplo pueden ser los activos que están fuera de servicio, fuera de soporte o sin los parches adecuados.

Amenaza: un fenómeno o acción que busca degradar, interrumpir, secuestrar o robar un activo. Estas engloban cualquier tipo de actor, desde los cibercriminales hasta los agentes internos.

Riesgo: la probabilidad de que una amenaza se materialice de manera efectiva dentro de los límites establecidos por las políticas de seguridad de la organización. El riesgo siempre debe considerar, el manejo y mitigación, y la posibilidad de pérdida total del activo. Un ejemplo de una fórmula para estimar el riesgo es la siguiente:

Riesgo = *Amenaza* x *Vulnerabilidad*.

2.3 Frameworks de referencia

La ciberseguridad define procesos, tecnologías, arquitecturas y diseños de *frameworks*. Estos se desarrollan con el fin de proteger a las organizaciones, programas, datos y demás activos de accesos no autorizados y ciberamenazas potenciales.

La comunidad de las tecnologías de la información siempre tiene la tendencia de crear compilados o *frameworks* de buenas prácticas, documentación de lecciones aprendidas, áreas de mejora, pros y contras. Estos incisos permiten reducir tiempos de investigación, implementación y mantenimiento, además de buscar aumentar índices de efectividad y accesibilidad a la información.

Algunos de los *frameworks* de trabajo más populares y reconocidos en el mercado son la Triada de CIA, NIST, ISO y SOC2. Estos se mencionan como referencia, ya que funcionan como insumo y punto de partida para la generación del documento investigativo final.

Se seleccionaron intencionalmente los *frameworks* anteriores, ya que son los que tienen la mayor relevancia para el objetivo que se busca alcanzar. Sin embargo, existen otros compilados reconocidos internacionalmente por la comunidad de ciberseguridad, como ITIL, Cobit, IASME, CIS, etc.

2.4 Triada de CIA

La definición de ciberseguridad puede variar mucho según la persona entrevistada, su nivel de conocimiento técnico y la frecuencia con la que se ocupa de temas del ámbito. Una de las definiciones más recurrentes o populares sostiene que la

ciberseguridad es la disciplina que previene que los *hackers* obtengan acceso a los sistemas. Por lo tanto, evita el robo de información y dinero. Esta definición subestima dramáticamente el papel que desempeña en el mantenimiento de los hogares modernos, los negocios e incluso los sistemas críticos que mueven el mundo, al mismo tiempo que busca mantener a los seres humanos seguros de posibles amenazas.

En el ámbito de Cyber, el acrónimo de CIA hace referencia a confidencialidad, integridad y disponibilidad. Estos se consideran por la comunidad como los pilares de la seguridad de la información que a la vez es un subsegmento del dominio de ciberseguridad. En adelante, se hace referencia a este campo de estudio como *InfoSec*.

La mejor manera de describir la CIA es enfocándola desde la perspectiva de un modelo que permite compilar varios elementos de seguridad fundamentales dentro de las tecnologías de información. Este modelo ayuda a desarrollar políticas de seguridad que permiten identificar problemas en las diferentes áreas del ecosistema mientras la empresa encuentra la respuesta o mitigación más apropiada a cada uno de los descubrimientos.

En la Ilustración 19 se muestra una gráfica que describe la tríada desde su punto integral o en su definición más aceptada por la comunidad de InfoSec. Además, se incluyen los conceptos antagónicos o contrapuestos de cada uno de sus pilares.

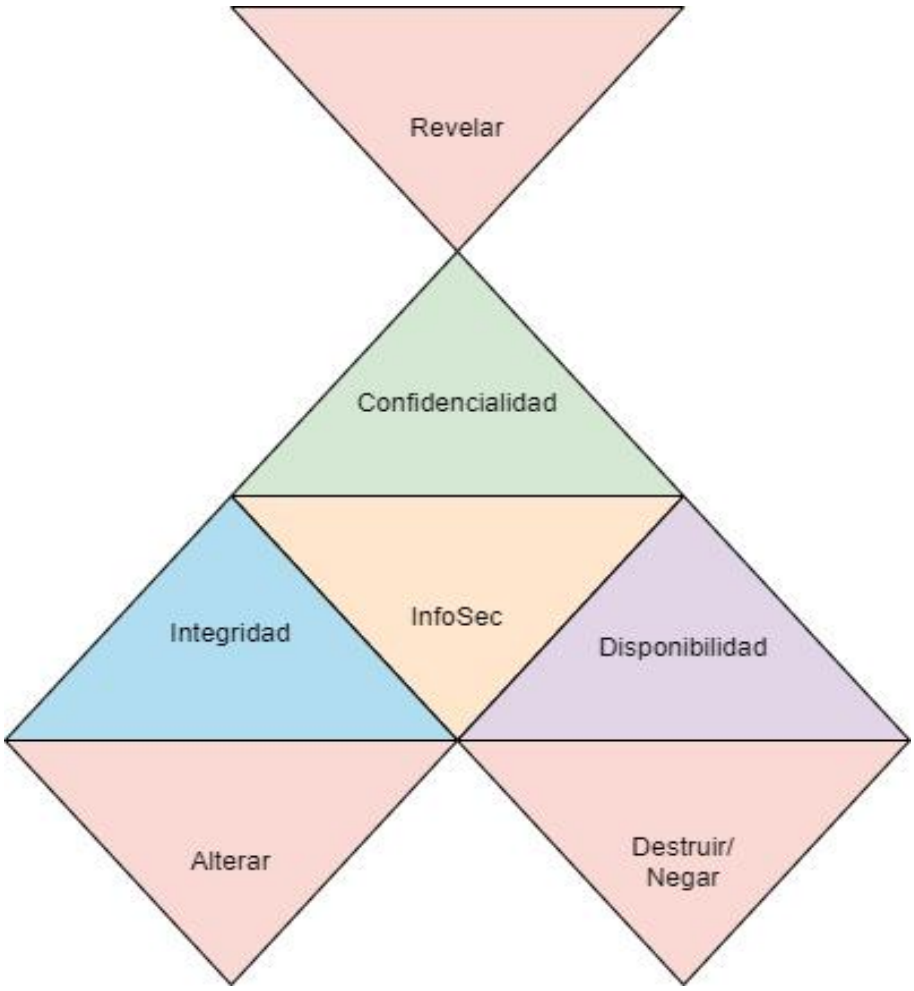


Ilustración 19: Triada extendida

Los temas referentes a infraestructura pueden variar ampliamente según la posición y el objetivo. Si se enfoca en su definición más conceptual, se puede analizar este componente con mayor fluidez y de manera agnóstica a sus diferentes sabores de implementación.

La tríada inicialmente habla de confidencialidad. Esta se refiere al aseguramiento de que la información no es compartida ni puesta a disposición de entidades o recursos

(personal interno/externo, organizaciones, procesos y demás) que no tengan una necesidad real para accederla, a pesar de que tengan o no un interés criminal.

Es importante mencionar que la confidencialidad no define ni abarca la totalidad de la privacidad, esta es solo un subsegmento del ámbito de la privacidad. La confidencialidad se enfoca en prevenir el acceso no autorizado a los datos, mientras que la privacidad abarca muchas más áreas de estudio y aplicación.

El concepto opuesto a la confidencialidad es la revelación. Los principales actores no solo buscan acceder o apoderarse de la información, sino también utilizarla como ventaja o apalancamiento para obtener beneficios de sus acciones. El proceso de revelar los datos no siempre es lineal o secuencial, sino que depende del objetivo detrás de la materialización. Un ejemplo muy claro es un *hacker* que rompe la seguridad perimetral y obtiene datos. Otro ejemplo puede ser un ataque de *ransomware*.

Subsecuentemente, el segundo pilar de la tríada es la integridad, el cual garantiza que los datos y la información sean exactos, precisos y completos. Por consiguiente, nunca se modificarán o alterarán de ninguna manera posible por agentes no autorizados o por algún desperfecto tecnológico, mientras mantienen su totalidad (ninguna parte o segmento ha sido removida).

La alterización de los datos o la información es uno de los paralelos más difíciles de analizar o estudiar. A menos que la detección haya sido en tiempo real, se convierte en un proceso muy manual y mecánico validar que hubo una manipulación o una alteración del objeto por estudiar. Un ejemplo muy común en esta área es un ataque de *man-in-the-middle*. Este consiste en interceptar o modificar los datos en el momento de transmitirse a su destinatario final.

Un detalle importante que engloba la integridad es el no repudio de la información. Esto significa que los datos se manipulan, de manera que nunca pueda ser cuestionada su autenticidad o precisión en ningún momento del proceso.

El último elemento de la tríada es la disponibilidad. A través del tiempo se ha mostrado en la comunidad informática y fuera del reino de la seguridad un sesgo de que este componente no es inherente al ámbito de Cyber. Se tiende a colocar como secundario o al menos no se le otorga el mismo grado de relevancia que sus conceptos subyacentes. No obstante, sin duda, es un elemento fundamental en la rama.

La disponibilidad asegura que la información, los sistemas que la almacenan, los respectivos procesos que la operan y los mecanismos que se utilizan para accederla y transmitirla, junto con sus controles de seguridad, funcionan apropiadamente. Usualmente, se usan puntos de referencia de mercado (*benchmarks*), como la cantidad de *nueves* (porcentaje de funcionamiento efectivo durante un periodo en forma de porcentaje) que la entidad necesita mantener para la operación efectiva del negocio o proveer para sus respectivos clientes.

Alcanzar y mantener estos niveles de servicio o de *uptime* tiene una tendencia a ser de una complejidad muy alta. Lo más normal es que se tenga la necesidad de abarcar muchas otras áreas que atraviesan el negocio y la organización, los mismos con diferentes ideas, enfoques, objetivos y métodos. Esto genera un fenómeno muy común: muchos cocineros en la misma cocina, especialmente en corporaciones de gran escala o globales y con proyectos que abarcan múltiples partes interesadas.

Para concluir, el paralelo de la disponibilidad puede definirse de diferentes maneras o tener un nombre diferente, según la superficie del impacto y del grupo en la

empresa que enfrenta la afectación. La negación o la destrucción de la disponibilidad puede retratarse utilizando como ejemplo un ataque distribuido de negación de servicio, cuyo objetivo principal es incapacitar o prevenir al usuario final o a la entidad de acceder a un servicio.

Se debe tener en cuenta que la mayoría de los ataques de esta índole cuentan con una amplia cantidad de recursos, como redes de equipos, servidores, ancho de banda y otros. En contraposición, los agentes de respuesta de incidentes suelen tener recursos limitados o predefinidos para mitigar los daños debido a las políticas de gobernanza.

2.5 National Institute of Standard and Technology

En adelante se hace referencia a este *framework* como NIST (según su acrónimo en inglés). El enfoque primordial radica en el desarrollo de controles organizacionales y la gestión del riesgo para los programas de seguridad de la información. Es imporante resaltar que este es un modelo complemente voluntario.

La metodología de trabajo se divide en tres áreas de interés: el núcleo del método, los niveles de implementación y los perfiles del método. La Ilustración 20 presenta, de manera gráfica, la categorización propuesta por la NIST en referencia a cómo se comparte la información, de qué forma se gestionan los riesgos y las decisiones y la integración dentro del amplio espectro del ambiente en estudio.

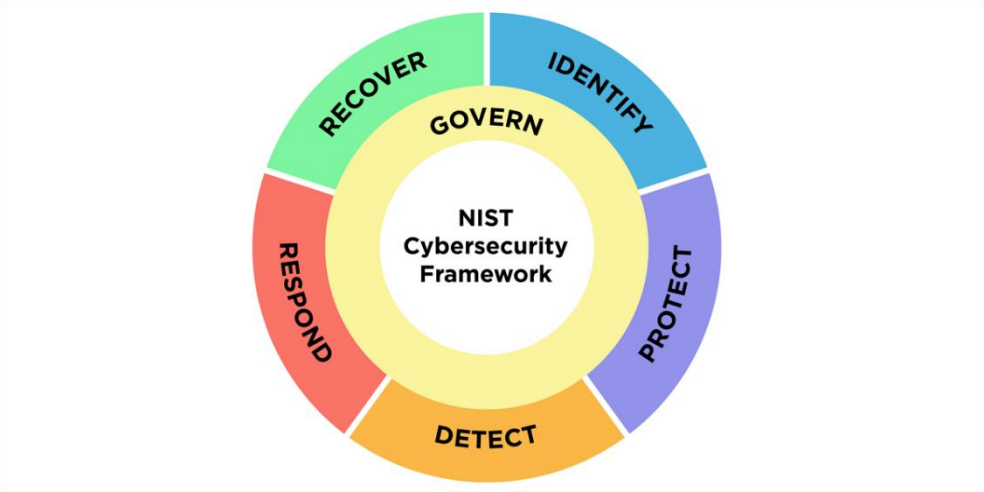


Ilustración 20: Framework de referencia de NIST

Fuente: Mahn et al. (2023).

El núcleo cubre principalmente seis funciones elementales para el negocio: identificar y proteger mientras la organización se prepara para tomar acciones como respuesta a una amenaza o ataque; detectar, responder y recuperar son todas las acciones o medidas que se realizan durante una materialización o incidente de ciberseguridad.

En la actualizacion 2.0 del framework de la NIST se agrega una sexta funcion que que abarca las otras cinco funciones. Determina como la organización puede alcanzar y priorizar los resultados que generan las otras funciones en el contexto de la mision de negocios y la expectativa que tienen los accionistas e inversores. Cada función se puede conceptualizar de la siguiente manera:

- **Identificar:** gestiona el riesgo entendiendo los activos, los datos y cualquier otro recurso que se encuentre en el alcance formulado.
- **Proteger:** protocolos y medidas que se implementan proactiva o reactivamente para proteger la infraestructura crítica.

- **Detectar:** define activa y, dinámicamente, que es un evento en contraste a la actividad normal de las operaciones del negocio.
- **Responder:** son las acciones y medidas específicas que se toman utilizando procesos predefinidos y manuales de operación.
- **Recuperar:** son todos los procesos que se utilizan para reparar o restaurar los servicios y las operaciones a un estado normal y óptimo.
- **Governanza:** Establace y monitorea la estratategia, las expectativas y las politicias de la gestion de riesgos organizacional.

Implementación de los niveles: la escala consta de cuatro niveles que varían, desde parcial hasta adaptativa. La Ilustracion 21, ejemplifica la estructuracion que plantea la NIST de los niveles de implementacion y su integracion en el proceso de gestions de riesgos.

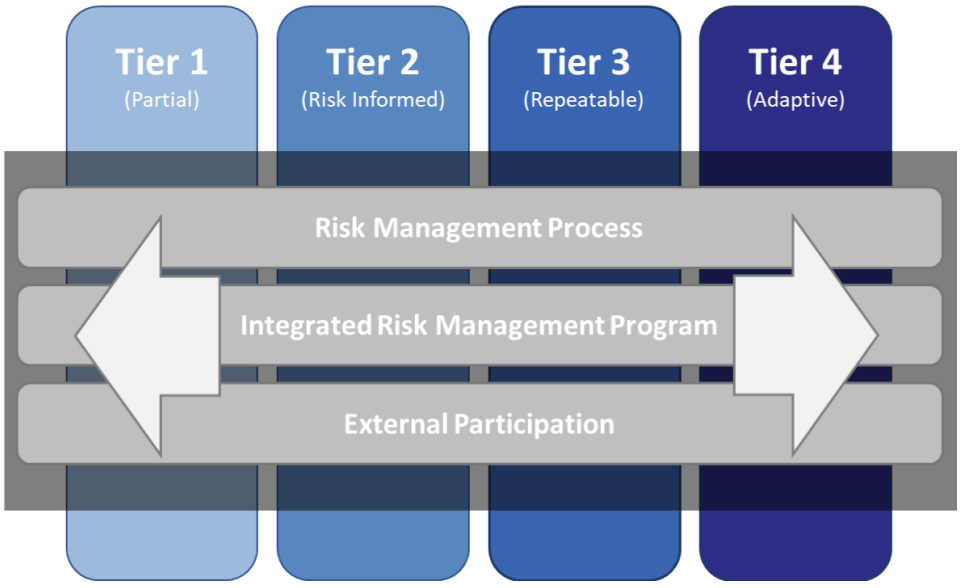


Ilustración 21: Implementación de los niveles basado en NIST

Fuente: Mahn et al. (2023).

Por último, los niveles se definen por los requerimientos y objetivos de negocios. La organización también es responsable de asignar la tolerancia al riesgo, los recursos y las herramientas que se utilizan para defenderse de las diferentes amenazas o materializaciones.

Perfiles del método: el último segmento del *framework* de trabajo de la NIST es opcional. No obstante, los profesionales en el área lo recomiendan altamente, ya que ayuda a la organización a definir una postura específica de seguridad de acuerdo con sus objetivos de negocios.

La creación de perfiles permite identificar oportunidades para refinar y mejorar la higiene de ciberseguridad. Las organizaciones pueden crear un perfil que retrate su estado actual y un segundo perfil que les permita proyectar en el futuro el estado que consideran que su negocio debe alcanzar. Otro caso de aplicación es elaborar perfiles asociados a cada una de sus áreas o divisiones de negocios, utilizando como base las necesidades de operación y las capacidades únicas de cada una.

Los procesos de actualización y perfilado de ciberseguridad deben ser previstos como un esfuerzo recurrente y de periodicidad indefinida. El perfil de la organización tiene la necesidad de mantenerse vigente y reinventarse continuamente para mejorar su postura de ciberseguridad.

2.6 International Organization for Standardization

La organización es también conocida por su acrónimo (ISO), la cual creó la norma 27001, que certifica que la empresa cumple con todos los requerimientos básicos de un programa de seguridad de la información. El estándar propuesto tiene un enfoque más de riesgos que técnico.

Las organizaciones reciben certificaciones de ISO, las cuales se reconocen y aplican en el ámbito internacional. En la actualidad, ISO cuenta con aproximadamente una docena de normas certificables que se centran en la administración segura de los activos.

Es importante resaltar que al hablar de riesgos en ciberseguridad se hace referencia a la probabilidad de exposición y pérdida que una organización puede sufrir mediante una afectación o ciberataque. Cuando una entidad adopta una postura que se enfoca en el riesgo, generalmente se basa en una metodología centrada en el análisis y gestión que en factores técnicos propios.

2.7 Service Organization Control Type 2

El *framework* de trabajo y de auditoría para ciberseguridad llamado SOC2 fue creado por el Instituto Americano de Contadores Públicos Certificados (Aicpa). Este tiene un enfoque muy específico en la administración de los datos de los clientes y los proveedores.

Tanto el *framework* de la NIST como el SOC2 se enfocan principalmente en los controles internos de la organización. Sin embargo, existen diferencias significativas en los lineamientos que cada uno ofrece. Por otro lado, la NIST proporciona una metodología para InfoSec y los controles de privacidad, SOC2 le permite a la empresa obtener certificaciones de cumplimiento.

2.8 Dominio de ciberseguridad y sus subdominios

La disciplina de ciberseguridad se encuentra actualmente dividida por subdominios o campos de aplicación. En la lista es posible encontrar los siguientes ejemplos:

- Asesoramiento o gestión de riesgos.
- Gobernanza.
- Inteligencia de amenazas.
- Operaciones de seguridad.
- Seguridad física.
- Arquitectura de seguridad.
- Aprendizaje.

En el Apéndice 2 se presenta un diagrama que recopila todos los subdominios que conforman la ciberseguridad actualmente. Se destaca que su definición y disciplinas pueden seguir experimentando cambios.

Asesoramiento o gestion de riesgos:

Dentro del primer subdominio, se deben tomar en cuenta dos componentes adicionales: la seguridad ofensiva y las pruebas de penetración.

Es posible definir el campo de la gestión de riesgo como la práctica que descubre y examina los riesgos asociados a la ciberseguridad. Estos riesgos pueden ocurrir o materializarse en la organización o el negocio.

El riesgo está presente en cada aspecto que se realiza, en cualquier lugar en el que estén y en cualquier momento. Un ejemplo muy elemental es el uso diario del Internet, este acarrea un riesgo inherente. La educación y el nivel técnico que tenga la persona usuaria pueden generar una variación en la probabilidad asociada al riesgo, pero en ningún instante deja de existir el riesgo.

Los riesgos asociados a una infección de un usuario independiente contra las implicaciones de que un recurso corporativo sea infectado varían muchísimo, tanto en el manejo de la situación como en las repercusiones que el mismo puede tener.

Un usuario final que ha perdido toda su información o dinero como resultado de una materialización tiene un criterio muy diferente al resto de la comunidad. En donde surgen naturalmente preguntas como: *¿Se puede confiar en los sistemas después de haber sido parcheados?, ¿Se puede encontrar un servicio que sea mejor, más estable y, por consiguiente, más seguro?, ¿Se puede confiar en una entidad financiera luego de haber perdido el dinero en sus cuentas?*

Estas son algunas de las potenciales justificantes a la necesidad de tener un proceso adecuado de gestión de riesgo. Idealmente, se pueden aplicar controles de seguridad para mitigar los riesgos y prevenir afectaciones que impacten o expongan de forma negativa la imagen de las diferentes organizaciones y sus respectivos clientes.

En ocasiones, los riesgos pueden mantenerse ocultos hasta el momento de la afectación, así como puede haber otros casos en los que los riesgos tienen la posibilidad de sobreevaluarse. Las compañías obtienen un beneficio directo y tangible de este campo, ya que les permite determinar cuántos controles de seguridad son necesarios y de cuáles tipos.

Las evaluaciones de seguridad se basan en factores como los costos del control, su implementación y su operación, la efectividad de los diferentes controles, el apetito y la tolerancia al riesgo, entre otros. El resultado de estas evaluaciones y su estudio a través del negocio generan políticas, métodos y servicios distintos e incluso pueden generar oportunidades de trabajo. Estas evaluaciones se aplican de manera individualizada y especializada a las organizaciones.

Tradicionalmente, las organizaciones tienen una estrategia más reactiva hacia las vulnerabilidades, por lo tanto, tienden a resolverlas o atenderlas después de su materialización. Esto puede ocurrir debido al desconocimiento, a una incorrecta priorización de las labores o incluso a la falta de personal y recursos.

La seguridad ofensiva cubre la necesidad de tener una estrategia proactiva. Diferentes profesionales de ciberseguridad aplican diversas técnicas para buscar e identificar activamente potenciales vulnerabilidades que puedan ser explotadas en el futuro. En el mercado es común que individuos o grupos dedicados al hackeo ético simulen potenciales acciones y ataques cibercriminales a ciertos segmentos o sistemas críticos. Esto les permite reconocer debilidades y tomar medidas preventivas antes de que los sistemas entren en producción. Se debe tener en cuenta que la seguridad ofensiva puede aplicarse a otras áreas de la infraestructura, como el *software*, los aplicativos, el equipo de redes, entre otros.

Es importante resaltar que los recursos que trabajen en esta área necesitan un permiso por parte de las organizaciones que los contratan, definiendo muy detalladamente el alcance de las pruebas, los sistemas o segmentos por probar, los

tiempos de pruebas y demás. Estos esfuerzos pueden considerarse ilegales de no ser así.

Los recursos que trabajan en la parte de pruebas se conocen como *Pentesters*. Estos tienen como objetivo generar diferentes tipos de ataques en busca de debilidades, puntos de acceso y demás. La única diferencia que tienen con respecto a los cibercriminales es que se dedican al hackeo ético (acciones legalmente aprobadas). Por lo tanto, su fin último es ayudar a las compañías a protegerse de los criminales.

El proceso estándar de testeo usualmente cuenta con los siguientes componentes:

- **Preexposición**:
    - Procesos de recolección de datos.
    - Entender y definir los alcances y limitaciones del proyecto.

- **Durante exposición**:
    - Procesos y pruebas de identificación de vulnerabilidades.
    - Explotación y materialización de las vulnerabilidades.

- **Posexposición**
    - Generación de reportes y resultados.
    - Creación de medidas de acción y respuesta.

Gobernanza:

Las organizaciones se rigen a través de diferentes regulaciones y prácticas, como se mencionó en los segmentos anteriores. Para asegurar el cumplimiento e implementación efectiva de estos, se necesita un esfuerzo organizado y significativo por parte de la organización. De hecho, construir, implementar y mantener un programa de ciberseguridad con sus respectivas políticas requiere la participación de la Gerencia, tanto táctica como operativa.

GRC:

El fundamento para crear políticas de ciberseguridad correctamente diseñadas consiste en combinar de manera efectiva y dinámica las áreas de gobernanza, gestión de riesgos y cumplimiento. Esto se conoce por sus siglas en inglés como GRC.

Componentes que integran las diferentes áreas de GRC:

a) **Gestión de riesgo**: es uno de los componentes más recurrentes dentro del subdominio de GRC, ya que estos son los insumos que los analistas utilizarán para proteger a la organización adecuadamente con base en sus necesidades de negocios. Estos son algunos elementos para considerar:
    a. Valoración de riesgos.
    b. Evaluación de riesgos.
    c. Monitoreo de riesgos.
    d. Mitigación de riesgos.

b) **Gobernanza**: está a cargo de supervisar el programa de ciberseguridad en conjunto para la organización. Desde el punto de vista del negocio este se enfoca

específicamente en la parte operativa y funcional de las regulaciones de ciberseguridad. Cada corporación tiene su propio compendio de ciberreglas que deben ser acatadas por todos los procesos y actividades en todo momento. Estos son algunos componentes que abarca:

a. Políticas.
b. Estándares.
c. Protocolos.
d. Cultura.
e. Políticas.

c) **Cumplimiento**: cada industria maneja diferentes requerimientos regulatorios y estas deben ser acatadas por las distintas corporaciones. Al igual que en los apartados anteriores, las organizaciones deben tener sus propias políticas de ciberseguridad que se ajusten específicamente a sus actividades de negocios.

Los recursos que trabajen en el área de GRC deben estar ampliamente informados de las regulaciones y de las leyes de ciberseguridad, tanto a nivel gubernamental como externas e internas. Esto les permite asegurar que las organizaciones cumplan con todos los estándares. Adicionalmente, deben mantenerse siempre vigentes y enterados de las nuevas tendencias cuando se amerite. Estas son las principales áreas que considerar:

a. Leyes.
b. Regulaciones.
c. Procedimientos.

d. Control de cambios.
e. Administración de configuración.

Los analistas de GRC típicamente deben mantenerse vigilantes y a la vanguardia cuando se habla de los pilares mencionados. Además, deben asegurarse de que todos los sistemas se mantengan seguros, funcionen al unísono y cumplan con los requisitos.

El analista de GRC no puede ni debe realizar su trabajo de manera aislada o independiente. Dentro de las organizaciones es necesario crear sinergias entre los diferentes recursos de seguridad para intercambiar datos, técnicas e información. Todo esto con el objetivo de generar e implementar los controles más adecuados de forma eficiente.

Por último, los encargados auditan las actividades de negocios contra la definición de seguridad. De esta manera, si alguna tarea o sistema no cumple los requerimientos deben trabajar con los demás recursos para alcanzar y asegurar el cumplimiento.

Inteligencia de amenazas:

Los cibercriminales trabajan alrededor del reloj. Continuamente, desarrollan diferentes tipos de ataques, optimizan sus técnicas y aumentan la cantidad de herramientas disponibles. Cada amenaza es más peligrosa y tiene un potencial nocivo cada vez más alto.

Habiendo dicho esto y al tomar en cuenta que la tendencia del mercado es hacia el aumento de incidencias en lugar de reducirse, los especialistas de ciberseguridad deben descubrir y eliminar cualquier indicio de un ataque en todo momento. La práctica

de mejorar la ciberseguridad salvaguardando a través de compartir, aprender, analizar y anticipar las ciberamenazas y sus respectivas complejidades se conoce como inteligencia de ciberamenazas.

Las organizaciones y los analistas de inteligencia de ciberamenazas deben mantenerse siempre un paso adelante durante el desarrollo de las estrategias corporativas. La información de ataques recientes, tendencias de negocios, noticias y anuncios de escala global son solo algunos de los recursos disponibles que sirven de apoyo en los procesos de analizar, proteger, predecir y prevenir potenciales ciberamenazas.

La inteligencia de ciberamenazas está compuesta por tres bloques principales:

1) Investigación.
2) Analítica.
3) Inteligencia.

Cuando se definen los tipos de inteligencia de ciberamenazas, se puede utilizar como punto de referencia el factor técnico de este. Por lo tanto, estas son las principales categorizaciones:

a) Insumos técnicos
b) Insumos no-técnicos

Existe también una categorización de la inteligencia de amenazas que se basa en el nivel de administración sobre el cual se trabaja y que se alinea con las líneas de mando organizacionales. Enseguida, se presenta su definición teórica:

a) **Inteligencia estratégica**: se enfoca primordialmente en los aspectos no-técnicos de una de las amenazas como los riesgos, el impacto y los efectos que pueden ejercer sobre las organizaciones. Su objetivo fundamental radica en apoyar la toma de decisiones a nivel ejecutivo; por ende, se apoya en la rama de GRC (explicado previamente), la cual provee la información necesaria para evaluar los riesgos y generar planes o medidas de mitigación.
b) **Inteligencia táctica**: este segmento tiene como objetivo analizar con detenimiento las tácticas que utilizan los actores y sus respectivas amenazas. Algunos ejemplos de este campo son: los procedimientos de los ataques y de los actores, los tipos de vulnerabilidades que pueden ser explotadas, cuáles pueden ser potenciales puntos de entrada y el análisis de las diferentes superficies de ataque que puedan tener las organizaciones.
c) **Inteligencia operativa**: se concentra en proveer información profunda y, altamente técnica referente a las amenazas. Por lo general, logra dar con los objetivos o las razones de las amenazas, las herramientas o técnicas que se utilizan en los ataques, indicadores de compromiso, nombres de archivos, diversidad de funcionalidades o productos, direcciones físicas y lógicas, entre otras.

En contraste con la inteligencia estratégica, la inteligencia táctica y la inteligencia operativa están ajustadas al personal y los recursos técnicos. Esto se debe a que analizan de cerca los diversos ataques y narran muchos aspectos que les permiten hacerlo.

Ahora, cuando se habla de la fuente de donde surge la información se tiene una subdivisión de referencia más que funcional, pero que al final define la relevancia y criticidad de esta. Ambas fuentes se detallan a continuación:

a) **Inteligencia de amenazas internas**: se genera principalmente de recursos internos de la organización como incidentes en progreso o investigación, incidentes pasados o resueltos, reportes de respuesta de incidentes, planes de respuesta, vulnerabilidades descubiertas, potenciales vulnerabilidades que se pueden tener, políticas de seguridad y mejores prácticas.
b) **Inteligencia de amenazas externas**: la contraparte del apartado anterior es la información proveniente de recursos externos o ajenos a la organización. Esta debe ser validada y referenciada por los diferentes recursos, de manera que no se conviertan en amenazas potenciales disfrazadas de soluciones. Estas son algunas fuentes que se consideran apropiadas para el proceso:
    - *Inteligencia de fuentes abiertas*:
        - Redes sociales.
        - Investigación pública.
        - Noticias globales, regionales y locales.
    - *Inteligencia técnica*:
        - Reportes gubernamentales.
        - Reportes y artículos de entidades avaladas.
        - *Feeds* y comunidades de seguridad.
    - *Otras*:

- *Dark* web
- Fuentes privadas o comerciales de pago.
- Entidades dedicadas a la investigación de ciberseguridad.

El conjunto o la combinación de estas aristas se conoce con el nombre de administración y operación de ciberinteligencia de amenazas. Los recursos que trabajan en esta área toman la información, la analizan y la consolidan con las herramientas y prácticas adoptadas por la empresa para determinar la severidad de las amenazas y los planes de mitigación respectivos.

Al igual que en otras áreas mencionadas, los recursos que trabajen en esta área deben mantener su conocimiento actualizado con las tendencias, tanto globales como locales. Asimismo, deben estar al tanto de áreas como ataques recientes, tecnologías emergentes, productos y servicios disponibles en el mercado, con el fin de encausar a la organización siempre en la dirección correcta.

Operaciones de seguridad

La disciplina se dedica a asegurar que la operación del negocio no se interrumpa, al detectar, prevenir, proteger y responder a las amenazas de seguridad y a los diferentes ataques. Por lo tanto, las operaciones de seguridad consisten en los planes que realizan los profesionales de ciberseguridad y los protocolos o procesos que se siguen para reaccionar a las amenazas.

Dentro de este subdominio existen algunos subsegmentos como Security Operations Center (SOC), Security Information and Event Management (SIEM) e Incident Response o respuesta de incidentes, sobre los cuales se trabaja en este apartado.

Respuesta de incidentes

Hasta esta fase del proceso, la mayor parte de las medidas tomadas y de los conceptos estudiados se han enfocado en la parte preventiva y en toda la planificación detrás. No obstante, la realidad del panorama actual dicta que no se puede tener un ecosistema 100 % seguro.

La disciplina de la respuesta de incidentes parte del peor escenario posible: la materialización de una amenaza y sus ramificaciones. Elaborar, aplicar y evaluar estrategias de respuesta y procedimientos de recuperación para el negocio es lo que define cada día de estos recursos.

La respuesta de incidentes puede ser dividida en tres bloques principales:

a) **Planificación**: responde a la fase de preparación o la fase preincidente.
    a. Preparación: los equipos de seguridad deben tener un aparato de seguridad estructurado y funcional, que le permita al personal reconocer y manejar potenciales incidentes.
    b. Identificación: el aparato de seguridad seleccionado envía y notifica al equipo de respuesta de incidentes de las alertas recolectadas, en donde estas se verifican, para determinar el tipo de amenaza y se determina que debe iniciar la fase de respuesta.

b) **Respuesta**: responde a la fase donde se toma acción o la fase durante-incidente.
    a. Contener: en esta fase se trata de limitar el impacto y el daño de la incidencia. Algunos ejemplos de acciones que se pueden tomar serían:
        i. Escaneo de la red de telecomunicaciones en busca de tráfico sospechoso.
        ii. Notificar a los diferentes grupos y empleados de actividades inusuales.
        iii. Retiro temporal de accesos y restricción entre segmentos del ecosistema.
    b. Erradicar: una vez que se determina que la materialización ha sido contenida se investiga la causa del problema. Lo más común es que en este punto se involucren los recursos de investigación forense.
    c. Recuperar: esta rama tiene una dependencia muy fuerte con los resultados de la investigación forense. Esto se debe a que la misma es el punto de partida para el proceso de recuperación de los sistemas comprometidos y la restauración de la operación normal de trabajo.
c) **Resultados/secuelas**: esta fase del proceso tiene muchas similitudes a la fase anterior, en donde el equipo de respuesta reexamina la incidencia, pero sin una variable definida de tiempo, mientras recolectan retroalimentación de todos los actores y recursos que se utilizan a ese momento.
    a. Evaluación: a pesar de que los incidentes han concluido, es de vital importancia analizar el proceso que se siguió, las acciones y los tiempos

de los equipos, de manera que se determine la efectividad de los planes o protocolos en vigencia.

b. Documentación: este puede ser uno de los pasos más simples de entender en todo el proceso, pero que implica un gran nivel de complejidad, ya que se deben capturar de manera muy minuciosa todos los detalles de la incidencia, los cuales se utilizan para presentar posteriormente los resultados a las jefaturas y para futuras referencias en la organización.
c. Mejora continua: este es el proceso de negocios, en donde se toman todas las lecciones aprendidas del procedimiento, se comparan contra los diferentes controles e indicadores para poder generar mejoras en los planes estratégicos, tácticos y operativos.

Arquitectura de seguridad

Hace referencia a la combinación de diferentes procesos de seguridad, los cuales son analizados desde una perspectiva de alto nivel y su propósito fundamental es producir una estructura de seguridad generalizada para la infraestructura de la organización.

En resumen, se podría definir como el rol o la disciplina que mezcla todos los subdominios que se han abarcado en los apartados anteriores y más. Las arquitecturas de seguridad varían de una organización a otra, por lo tanto, deben diseñarse teniendo en cuenta el tipo de negocio y los objetivos que se tienen. Estos objetivos deben analizarse y procesarse para producir objetivos de seguridad accionables.

El trabajo de los arquitectos de seguridad consiste en participar en el diseño e implementación de los programas de seguridad. Estos programas abarcan todas las verticales que pueden presentar los negocios. Además, los arquitectos de seguridad son responsables de diseñar arquitecturas de alto nivel para los datos, aplicativos, infraestructura y demás programas.

Al igual que otros recursos de seguridad mencionados, los arquitectos de seguridad deben trabajar con homónimos en otras áreas como redes, resiliencia, herramientas y demás para poder definir la estrategia a un nivel más macro del ecosistema sobre el que se trabaja. Por eso, los arquitectos de seguridad deben tener mucha experiencia, conocimientos avanzados y una clara noción del mercado y del negocio.

Existen muchas herramientas que ayudan a los arquitectos a realizar su trabajo de manera efectiva. Un ejemplo muy popular de un *framework* es Togaf, The Open Group Architecture Framework.

El ultimo subdominio que se planteo se basa en el aprendizaje, el cual es abordado como resultado del proceso investigativo y como parte de la propuesta de solucion.

2.9 Servicios y computación en la nube

El término computación en la nube toma cada vez más revuelo entre los profesionales en el Área de TI y el público general, ya que puede proporcionar soluciones más económicas, más flexibles y robustas en diversos casos de uso. Como respuesta a este fenómeno, los ataques y crímenes orientados a plataformas en la nube son cada vez más frecuentes y efectivos.

A pesar de los ataques que ha recibido, la computación en la nube sigue expandiéndose. Cada vez se observan mayores inversiones financieras y proveedores que ofrecen servicios y tecnologías de punta. Algunos sabores o categorizaciones principales en el mercado son:

- Plataforma como servicio (IaaS).
- Infraestructura como servicio (PaaS).
- Software como servicio (SaaS).

Existen otras categorizaciones según cómo se gestione, pero estos servicios sin duda traen beneficios en lo que respecta a accesibilidad y diversidad para los individuos y las organizaciones debido a sus modelos de responsabilidad compartida. Sin embargo, siempre se deben estipular tiempos y holguras razonables, ya que traen curvas de aprendizaje significativas para todas las partes.

En lo que respecta a los recursos que trabajan en el área de ciberseguridad y nube, aún hay muchas áreas por descubrir y oportunidades de crecimiento. La flexibilidad que aporta la nube a la infraestructura del negocio permite diseñar, desarrollar e implementar nuevas estrategias y arquitecturas. Sin embargo, también es necesario ser cauteloso con las nuevas superficies de ataque, los potenciales riesgos y las amenazas.

En conclusión, la arquitectura de seguridad es una combinación de los diferentes tipos de subdominios mencionados. Ahora, al incluir la computación en la nube, esta genera una sensación futurista que permite adoptarla en cualquier condición o experiencia. Además, muchas organizaciones se benefician de los procesos de adopción y transformación de infraestructura de nube.

En la ilustracion 22 se retrata de manera grafica algunos aspectos de seguridad que deben ser contemplados y analizados como fundamentales o nativos de la computaciones en la nube, mientras que se agregan otros aspectos de seguridad que podrian ser potencialmente integrados pero que varian dependiendo del nivel de adopcion que tenga el negocio.

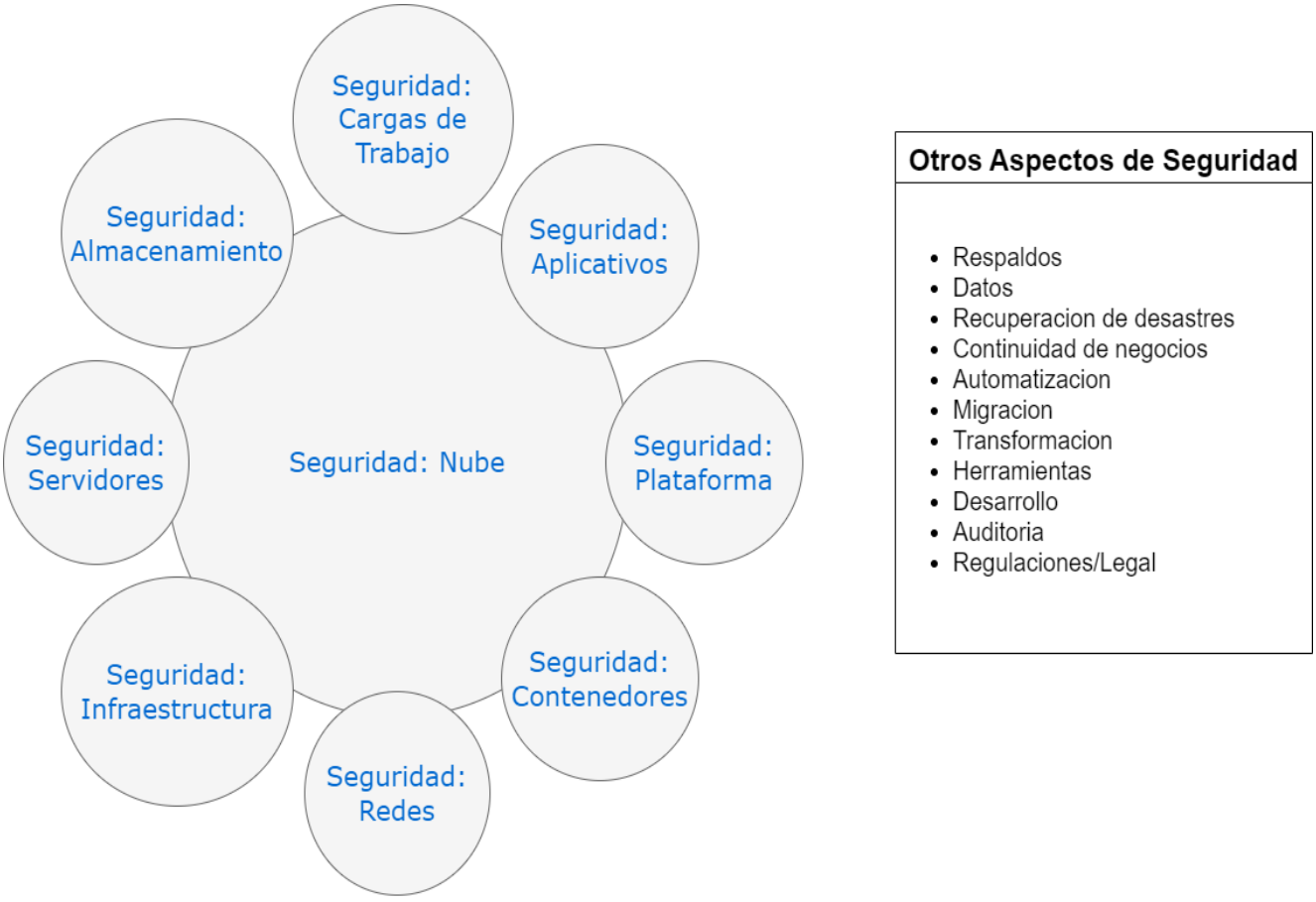


Ilustración 22: Aspectos de seguridad para computación en la nube

Capítulo 3: Marco metodológico

3.1 Tipo de investigación

Inicialmente, se define que la investigación realizada tiene un enfoque evaluativo, ya que se comparan distintos componentes de infraestructura y seguridad y se emite un criterio como resultado del proceso. Al mismo tiempo, se adicionan algunos tonos de investigación aplicada. Estos buscan utilizar la base de conocimientos que brinda la corporación y su cartera de clientes para resolver una tendencia de mercado en alza, mientras se genera la guía de referencia.

Kyndryl, como proveedor de servicios tercerizados, recibe un beneficio directo por parte de esta investigación. Esto no solo resuelve problemas potenciales con clientes existentes, sino que también mejora la calidad de los servicios que se ofrecen a través de toda su cartera.

Esta investigación se define como evaluativa y aplicada, ya que busca compilar información de primera mano de distintas fuentes. Además, se generan conocimientos y una herramienta nueva para los dueños del negocio y los usuarios finales (técnicos y no técnicos). Estos pueden tomar decisiones mejor fundamentadas como respuesta a los fenómenos analizados.

3.2 Alcance investigativo

Con base en la definición de los parámetros y requerimientos, se determina que la investigación en su fase inicial es de corte descriptiva. Este estudio puede ajustarse para incluir algunos rasgos exploratorios complementarios.

Desde el punto de vista descriptivo, se buscó determinar las características del fenómeno de afectación o, en este caso, la tendencia de mercado que presentaron los clientes y se recopilan detalles desde tres aristas. La primera arista es el estado actual del cliente y cuáles son sus necesidades, tanto técnicas como de negocios, sin dejar por fuera sus falencias o puntos de dolor.

La segunda arista evaluada es el estado actual de la legislación o de las buenas prácticas disponibles para la comunidad informática. Esto sirve como base de referencia durante el proceso de análisis, de manera que se evite trabajar sobre áreas que ya han sido estudiadas o evaluadas, al mismo tiempo que se solidifican los cimientos del criterio evaluativo.

Como última arista, se agrega el criterio y pericia de la persona investigadora. Esto tiene particular importancia, ya que la interpretación, análisis y calificación/descalificación de la información y de los diferentes casos de estudio son el punto de apoyo para elaborar la guía.

En referencia a los rasgos exploratorios complementarios, se puede acotar que el cliente no ha tenido contacto directo con los diferentes actores, tanto recursos técnicos como no técnicos. Además, se debe tomar en cuenta que durante el proceso investigativo, el investigador y los demás funcionarios de Kyndryl pueden incurrir en procesos o áreas desconocidas, por las cuales deben familiarizarse.

Como respuesta a ambos elementos, se define un proceso de documentación formal. Este procedimiento permite llevar un control del conocimiento revisado, adquirido y necesario para el contexto de la investigación. Dicho control se incluye como parte de la documentación entregable.

3.3 Enfoque

Se define que la investigación tiene un enfoque alternativo, ya que la naturaleza de esta y de la guía de referencia son elementos enteramente de negocios. Por lo tanto, es irreal tratar de generar un resultado con solo elementos cualitativos o cuantitativos, pues esto pintaría un panorama incompleto de los fenómenos en estudio.

A continuación, se definen las tres dimensiones (ontológica, epistemológica y axiológica) del enfoque de la investigación.

Inicialmente, se analiza la base epistemológica. El escenario ideal es que durante el proceso, el investigador y los demás funcionarios de Kyndryl tomen un papel de observadores, de manera que se pueda recolectar la información en su forma más pura y confiable. Ya sea que la información venga directamente de las personas colaboradoras o de las herramientas definidas, se debe asegurar que esta sea la más reciente y precisa, para que refleje la realidad de la condición del cliente y sus diferentes sistemas informáticos.

Eventualmente, se puede cambiar a un enfoque más participativo, ya que puede haber un desconocimiento procedimental o técnico por parte de los diferentes actores en primera instancia. Además, debido a los constantes ajustes del personal, el proceso puede requerir la participación de distintos miembros del proyecto en diversas calidades.

En relación con la base axiológica, en esta etapa del proceso se determinó que la información del cliente aún cuenta con una etiqueta corporativa confidencial y todavía no se comparte con el equipo del proyecto. Por lo tanto, no se puede

determinar exactamente los diferentes factores por evaluar, pero es posible definir de manera incipiente la rúbrica por utilizar de forma generalizada pero enfocada.

Desde el punto de vista ontológico, esta investigación no profundiza en ámbitos sociales, culturales ni ninguna otra rama afín en su defecto. Con el paso de los años, se demuestra en el ámbito de la seguridad informática que uno de los principales factores de la materialización de las amenazas es el error humano.

El motivo detrás de incluir esta dimensión radica en el hecho de que la disciplina de la informática ha dejado atrás a sus usuarios en todos los niveles de la escala, tanto técnicos como no técnicos. Este fenómeno aparece como resultado del crecimiento exponencial que ha sufrido la tecnología en todas sus ramas. De manera que un especialista, profesional o cualquier otra denominación o cargo ya no puede abarcar todo lo que comprenden estas ramas tecnológicas ni tampoco sus subsegmentos.

Si se mantiene esta misma línea de pensamiento y se extrapola este punto de análisis, es posible afirmar que ninguna persona es capaz de manejar cada concepto asociado a la ciberseguridad en la población actual.

Se toma en cuenta el desconocimiento de la disciplina y la falta de un método efectivo de aplicación como un fenómeno social que impacta la capacidad de proteger, optimizar y recuperar la infraestructura en cualquier escala. En donde, la infraestructura la implementa, opera y gestiona principalmente el recursos humanos.

3.4 Diseño

Se define que la investigación tiene un diseño secuencial mixto. Esto se debe a que el fenómeno se estudia de manera progresiva y desde diferentes perspectivas, lo que hace necesaria la aplicación de distintos métodos y técnicas de captura de datos.

Adicionalmente, el enfoque mixto permite manipular de manera flexible el foco y el proceso metodológico. Se realiza el análisis y la recolección de datos cuantitativos y cualitativos en dos etapas independientes. Se utilizan los datos cuantitativos como guía o referencia en el procedimiento de manipulación y operación de los datos cualitativos. Esto culmina en la correlación de ambos a través de la propuesta de solución como punto de cierre.

Definición de la metodología que se utiliza en el proceso investigativo:

- Recopilación inicial de información a lo interno, de manera que refleje la condición de la empresa, lo que establece un punto de partida o precedente para la metodología.
- Se realiza una investigación utilizando diferentes herramientas y cadenas de búsqueda que permiten definir el estado actual, las principales variables y demás factores referentes a la optimización y protección de la infraestructura, la seguridad informática y la prevención y recuperación de incidentes.
- Se establece una base conceptual de los componentes y elementos del dominio y los subdominios de ciberseguridad.
- Se realiza una investigación inicial para definir cuáles son las principales regulaciones, estándares y compendios de buenas prácticas asociados a la seguridad informática y más específicamente a la ciberseguridad. De estos se extraen los puntos por considerar como parte de la propuesta.
- Se define un fundamento teórico para el desarrollo, creación y aplicación de una guía metodológica que sirva como esqueleto o encuadre a los

componentes que se incluyen en la propuesta, de manera que tenga una estructura fundamentada.

- Desarrollo y aplicación de una encuesta, en diferentes fases con al menos dos métodos de aplicación. Lo anterior tiene el fin de hacer un sondeo inicial y fomentar el diálogo referente al fenómeno en estudio; concluyendo en un análisis social-cultural de las personas encuestadas y de la información que se recolectó en el proceso.
- Realizar un estudio de la aplicación y existencia de los sistemas expertos en el área de la ciberseguridad, que determine el estado de las herramientas disponibles para los diferentes actores. Esto permite utilizar la definición de la base y requerimientos para determinar los entregables de la investigación.
- Establecer los principales componentes y requerimientos de un *framework* de trabajo y su aplicabilidad a la ciberseguridad. Lo anterior tiene el fin de complementar e integrar la guía metodológica, lo que genera una definición teórica de la propuesta de solución y sus elementos mínimos.
- Elaboración de un diseño y propuesta con todos los componentes recopilados a lo largo del proceso investigativo.
- Cierre del proceso investigativo mediante un análisis de los resultados y conclusiones del fenómeno en estudio.

3.5 Población

En cuanto a la población, se debe considerar que no se trabajó sobre ningún grupo demográfico específico. Más bien, se buscó abarcar diferentes grupos para

retratar de manera representativa el fenómeno de estudio y su comportamiento a través de los distintos grupos demográficos.

En lo que respecta al muestreo, se utilizó el enfoque no probabilístico. Lo que se busca es recopilar respuestas y explicaciones a los distintos componentes técnicos y no-técnicos, por lo tanto, no se necesita demostrar de manera numérica los fenómenos, más bien retratar el panorama de ciberseguridad socialmente.

3.6 Instrumentos de recolección de datos

Inicialmente, se valoró la opción de utilizar el método de la entrevista del tipo mixto. En muchos casos, se necesitó evaluar los diferentes aspectos no técnicos de la organización, como procedimientos operativos, factores económicos, conocimientos base, toma de decisiones, gobernabilidad y demás.

Subsecuentemente, se amplió el alcance del proceso de entrevistas para abarcar un segmento demográfico más amplio, ya que los recursos internos no reflejaban la totalidad del caso de estudio. Esto funcionó como sondeo inicial y promovió el diálogo con los diferentes actores.

Se define un estilo mixto entre estructurado y no estructurado. Es necesario definir una base específica de la información mínima que se debe recopilar del entrevistado, pero también se necesita dejar un espacio para que el entrevistador tenga más libertad de explorar los diferentes aspectos descubiertos como resultado de la interacción. Por lo tanto, se generan distintos perfiles y entrevistas con base en la población detallada, de manera que la recolección de datos sea óptima.

A continuación, se elaboró la encuesta, la cual tuvo al menos tres iteraciones de prueba antes de ser extendida al público meta. El diseño de la encuesta utilizó preguntas tanto abiertas como cerradas.

Como mecanismo complementario opcional se utilizaron diferentes herramientas o mecanismos técnicos que manejan distintos enfoques y en su mayoría manejan sistemas de reporteo. Esto brinda gran flexibilidad en la recolección de datos, identificación de tendencias y presentación de los resultados. Por lo tanto, el investigador realizará una guía de utilización e interpretación de los reportes para evitar ambigüedades o situaciones confusas.

3.7 Técnicas de análisis de información

En primera instancia, se define que el proceso de análisis de información se basa primordialmente en los criterios técnicos de los diferentes actores de la investigación: investigador, recursos tecnicos, auditores y gerentes de los proyectos técnicos. En este caso siempre se toma en cuenta que las fuentes son diversas.

Una de las principales fuentes es el uso de herramientas técnicas, las cuales realizarán un análisis objetivo. Estas herramientas deben ser interpretadas, además, los resultados de las entrevistas son tabulados e interpretados manual y, subjetivamente, por parte de la persona investigadora.

Por último, se utiliza el mismo sistema de recolección de encuestas como herramienta de análisis, ya que este trae mecanismos de lógica y reporteo especializados. Estos instrumentos ayudaron a dar un vistazo inicial a los fenómenos de estudio, permitieron analizar las respuestas con controles cruzados y terminaron de generar potenciales ángulos de presentación de resultados.

Capítulo 4: Análisis de la situación

En este capítulo se exponen y analizan los resultados de todos los instrumentos de recolección de datos. Además, se presenta la metodología que se utiliza en cada uno y se plantean las conclusiones con base en los datos que se obtienen.

El objetivo principal de realizar estos estudios a los diferentes actores y público en general es profundizar en el comportamiento sociocultural del fenómeno en estudio para validar o desaprobar la hipótesis y los objetivos que plantea esta investigación. Indiferentemente del resultado, ya sea positivo o negativo, este sondeo se utiliza como cimiento para la solución que se desea proponer, los factores sociales para tomar en cuenta y las áreas de enfoque.

Por último, se busca demostrar la urgencia y la necesidad de implementar una solución de este tipo como respuesta a la falencia de conocimientos y cultura de la población. La tecnología se mueve de manera exponencial y ha dejado consistentemente atrás no solo a los usuarios finales, sino también a los recursos técnicos, los cuales carecen de las herramientas necesarias para responder de forma efectiva y segura.

4.1 Entrevista

Como parte del proceso investigativo y del sondeo inicial se llevó a cabo una entrevista aplicada a 15 personas con puestos profesionales que se relacionan con el campo informático, pero que no necesariamente desempeñan puestos de ciberseguridad.

Realizar este proceso tenía dos fines primordiales: someter a prueba las diferentes preguntas diseñadas para ser parte de la encuesta y fomentar el diálogo entre el investigador y las partes entrevistadas utilizando una metodología de pregunta abierta combinada con el formato de entrevista. A continuación, se detallan algunas variables que se analizaron:

- Claridad del texto de la pregunta.
- Alineación de la respuesta generada contra el objetivo buscado con la pregunta.
- Determinar la validez y efectividad de la pregunta en el contexto del análisis o estudio por realizar.
- Definición de los grupos demográficos más adecuados que iban a ser encuestados posteriormente.
- Análisis del tiempo de respuesta y la reacción de las personas entrevistadas a las preguntas. De manera que el diseño de la encuesta fuera lo más breve y efectivo, lo que aumenta el éxito en el proceso de recolección de datos.

A continuación, se presentan las preguntas que se utilizan en los procesos de entrevista mencionados:

1. ¿Cuál es su postura de seguridad como respuesta la actualidad del panorama global?
2. ¿Podría definir ciberseguridad y su campo de aplicación?
3. ¿Se ha capacitado en temas de seguridad, privacidad y protección?

4. ¿Entiende sus derechos, responsabilidades y riesgos respecto al tema de ciberseguridad?
5. ¿Entiende las implicaciones y riesgos de conectar un equipo propio a una red de datos ajena, compartida o pública?
6. ¿Entiende las implicaciones y riesgos de conectar un equipo ajeno, de fuente no confiable o incluso de agentes externos a un ambiente privado?
7. ¿Conoce el concepto de higiene de ciberseguridad?
8. ¿Ha tenido la oportunidad de utilizar algún servicio tercerizado?
   De ser positiva la respuesta puede compartir los detalles de este.
9. ¿Específicamente, utiliza algún servicio de seguridad o de protección? De ser positiva la respuesta puede compartir los detalles de este.
10. ¿Administra usted infraestructura o tiene alguna labor relacionada?
    De ser positiva la respuesta puede compartir los detalles de este.
11. ¿Podría listar las consideraciones más importantes dentro del esquema de protección de infraestructura?
12. ¿Cuáles son las variables de mayor relevancia en el proceso de optimización o modernización de la infraestructura?
13. ¿Podría definir efectivamente un plan o estrategia que le permita mantener seguro su ecosistema? ¿Cuánto tiempo considera que este plan o estrategia le tomaría en hacerse efectivo? ¿Cuánto tiempo considera que este plan o estrategia sería efectivo en la actualidad?
14. ¿Tiene claras cuáles serían sus opciones de acción en caso de ser víctima de una afectación de seguridad, en cualquiera de sus escalas?

15. ¿En caso de tener una afectación en su ecosistema puede recuperarse efectivamente y mantenerse en operación consistentemente? ¿Cuánto tiempo considera que le puede tomar recuperarse totalmente de una afectación?
16. ¿Sabe dónde puede obtener información o educación referente a ciberseguridad y cómo proteger, tanto a su persona como su ecosistema?

El segundo objetivo en el proceso de entrevista fue observar de manera incipiente y no estadísticamente hablando el comportamiento inicial del fenómeno por encuestar. Lo anterior tiene el fin de proveer la dirección hacia donde se inclinaba. Esto se logró haciendo las preguntas aún más efectivas y permite capturar información de mayor relevancia. Las siguientes son algunas de las perspectivas capturadas por parte de la persona investigadora:

- Los ejecutivos técnicos y no técnicos tienen consciencia de la relevancia de los temas de seguridad, pero no necesariamente entienden la definición técnica y su aplicación. Por lo tanto, sus aportes en el proceso son más reactivos o coaccionados por el contexto empresarial.
- Los profesionales informáticos al trabajar para empresas de grandes magnitudes o multidisciplinarias relegan mucha de la responsabilidad a los expertos en el área y no siempre logran correlacionar efectivamente su posición en la perspectiva de seguridad.
- La mayor parte de las personas entrevistadas obtuvieron su base de conocimientos a través de las empresas en las que trabajan. Los cursos

de actualización, las capacitaciones con base en web y las campañas de concientización fueron las respuestas más recurrentes. Por lo tanto, queda por descubrir si las personas que no manejan este contexto empresarial tienen el mismo desarrollo de conocimiento y si tienen a la mano alguna herramienta que les permita generar consciencia y conocimiento.

- Se valida que, en el ámbito social y disciplinario (informática, seguridad, ciberseguridad, etc.), no existen procesos ni campañas de concientización, educación y desarrollo para el público general.
- Hay un grado de incertidumbre, ignorancia y disconformidad muy elevado en el público general, debido al panorama mundial de seguridad, donde parte no entiende qué pasa, cómo pasa y por qué pasa; mucho menos entiende la relevancia de la ciberseguridad como resultado al clima tecnológico actual.
- Hay una respuesta generalizada del público, que indica que los temas de ciberseguridad son muy complejos, lo que genera una apatía hacia los tópicos asociados, agravando el fenómeno social en general.

4.2 Encuesta

El concepto de ciberseguridad se simplifica de manera consistente, pero su verdadera definición radica en las personas y su situación actual. Esto implica una gran variabilidad en temas de políticas, procedimientos y prácticas.

Algunos ejemplos que ilustran la necesidad de profundizar y encauzar los esfuerzos de manera efectiva son los siguientes:

a) Ciber para individuos puede significar que la información personal no sea accesible por otros, que sus equipos funcionen adecuadamente y que ninguno de los activos sea vulnerado.
b) Ciber para negocios pequeños o pymes puede incluir la protección de la información financiera (tarjetas de crédito, transacciones, datos personales de los clientes) y mantener estándares o regulaciones de protección de datos.
c) Ciber para firmas de negocios en-línea puede abarcar la protección de los activos que brindan los servicios a los usuarios finales o que se encuentran en los linderos del ecosistema, los cuales mantienen interacciones continuas con agentes exteriores.
d) Ciber para proveedores de servicios tercerizados como Kyndryl, usualmente tienen una diversa variedad de frentes que proteger como los data centers alrededor del mundo, redes de transmisión de datos, servidores con diferentes propósitos, tanto técnicos como de negocios, herramientas de monitoreo, mantenimiento y configuración, accesos a distintos clientes u organizaciones. Esto solo para ejemplificar.
e) Ciber para gobiernos implica las diferentes categorizaciones de datos, potencialmente pueden manejar sus propias regulaciones, leyes, procedimientos, políticas y tecnologías.

Por último, se tuvo en cuenta la entrevista de manera retroalimentativa para el proceso de diseño de la encuesta. En este procedimiento se consideraron las lecciones aprendidas y las perspectivas develadas, lo cual ocasionó el diseño que se incluye en el Apéndice 3. A continuación, se presentan las preguntas de forma textual para su estudio y análisis.

Definición de la situación social con respecto a la ciberseguridad

1. Análisis de población general

1. ¿Qué edad tiene actualmente?

- Menos de 19 años.
- De 20 años a 29.
- De 30 años a 39.
- De 40 años a 50.
- Mayor de 50.

2. ¿Qué grado académico posee?

- Bachiller (colegial o menor).
- Técnico, especialización o equivalente.
- Bachiller universitario o equivalente.
- Universitario con estudios superiores (licenciatura, maestría y demás).

3. ¿Cuál es el grado de conocimiento informático?

- Usuario normal (celular, laptop personal, Smart TV, etc.).
- Usuario corporativo (adicionalmente: celular de trabajo, laptop empresarial, Corp-Citizen).
- Usuario con conocimiento avanzado empírico.
- Usuario con conocimiento avanzado con educación formal (títulos universitarios o certificaciones afines).
- Usuario experto (administradores de sistemas.
- Empleado (informáticos, profesionales, etc.).

4. ¿Podría definir ciberseguridad y su campo de aplicación?

- Sí.
- No.
- Posee referencia, pero sin fundamento formal.
- Posee referencia, pero con fundamento formal.

5. ¿Se ha capacitado en temas de seguridad, privacidad y protección de datos?

- Sí, por cuenta propia.
- Sí, por obligación laboral.
- Sí, ambas.
- No.
- Otra.

6. ¿Entiende sus derechos, responsabilidades y riesgos alrededor de los temas de ciberseguridad?

- Sí.
- No.

7. ¿Conoce el concepto de higiene de ciberseguridad?

- Sí.
- No.

8. ¿Cuál es su postura de seguridad como respuesta a la actualidad del panorama global?

- No tiene una postura.
- Inseguro(a) por desconocimiento.
- Inseguro(a) por falta de recursos.
- Seguro(a) porque tomó pasos o acciones.
- Seguro(a) por tener acceso al conocimiento y los recursos.
- Seguro(a)/Inseguro(a) por desinterés.

9. ¿Entiende las implicaciones y riesgos de conectar un equipo propio a una red de datos ajena, compartida o pública?

- Sí.
- No.
- Parcialmente entiende.

10. ¿Ha tenido la oportunidad de utilizar algún servicio tercerizado u *outsourcing* de cualquier tipo?

- Sí.
- No.
- Entiende el concepto, pero no utiliza un servicio aún.

11. ¿Entiende las implicaciones y riesgos de conectar un equipo ajeno, de fuente no confiable o incluso de agentes externos a un ambiente privado?

- Sí.
- No.
- Parcialmente entiende.

12. ¿Específicamente, utiliza algún servicio de seguridad, ciberseguridad o de protección informática?

- Sí.
- No, por desconocimiento.
- No, por desinterés

2. Análisis de población técnica

13. ¿Administra usted infraestructura o tiene alguna labor relacionada?

- Sí, actualmente.
- No, pero sí he administrado.
- No, pero sí desempeño un rol técnico.

14. ¿En caso de tener una afectación de seguridad en su ecosistema, puede recuperarse efectivamente y mantenerse en operación consistentemente?

- Sí, puedo recuperarme y mantenerme operacional.
- Sí, puedo recuperarme, pero no mantenerme operacional.
- No puedo recuperarme ni tampoco mantenerme operacional.
- No tengo ninguna referencia.

15. ¿Podría definir efectivamente un plan o estrategia que le permita mantener seguro su ecosistema?

- Sí.
- No.

16. En caso de tener un plan o estrategia de seguridad ¿cuánto tiempo considera que este es efectivo en la actualidad?

- Menos de 3 meses.
- De 3 meses a 6 meses.
- De 6 meses a 12 meses.
- 12 meses hasta 24 meses.
- Más de 24 meses.

17. ¿Sabe dónde puede obtener información o educación sobre ciberseguridad y cómo proteger, tanto a su persona como a su ecosistema?

- Sí, tengo referencias vigentes.
- Sí, tengo referencias desactualizadas.
- No, desconozco del tema.
- No, pero me gustaría mejorar la condición actual.
- No tengo ningún interés

18. ¿Podría listar las consideraciones más importantes dentro del esquema de protección de infraestructura?

- Sí. ¿Cuáles serían?
- No. ¿Por qué?

19. ¿Cuáles son las variables de mayor relevancia en el proceso de optimización o modernización de la infraestructura?

20. ¿Tiene claras cuáles serían sus opciones de acción en caso de ser víctima de una afectación?

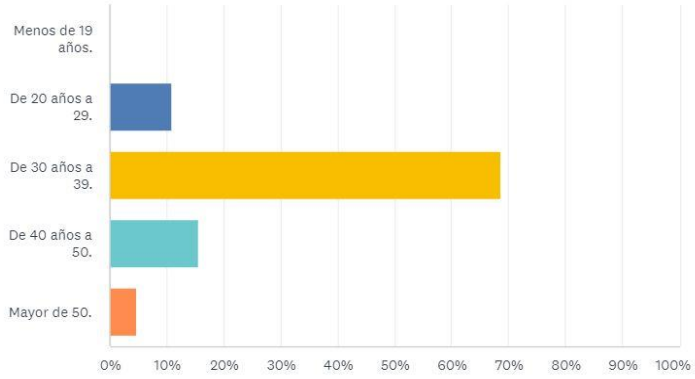
4.3 Resultado de las encuestas

Las primeras cinco preguntas de la encuesta se diseñaron para definir de manera inicial los diferentes grupos demográficos que abarcan la comunidad que actualmente engloba el contexto de la investigación, mientras retrata las primeras avenidas de análisis según escolarización y edad.

A continuación, se presentan las capturas de las diferentes preguntas que se utilizan como etiquetas, junto con sus respectivas respuestas. Debido a la cantidad de preguntas que tiene la encuesta, algunas se analizaron en conjunto o en asociación contextual.

¿Qué edad tiene actualmente?

Respondidas: 64 Omitidas: 0

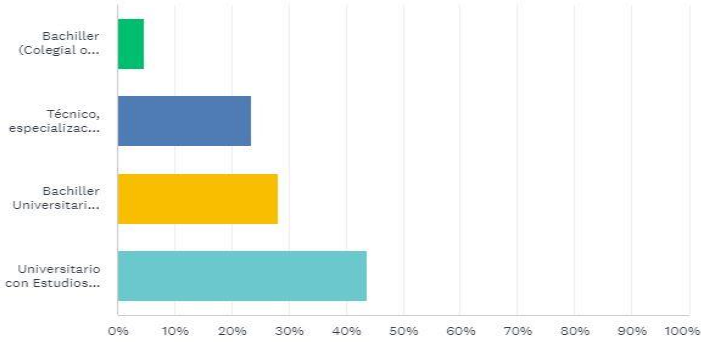


OPCIONES DE RESPUESTA	RESPUESTAS	
Menos de 19 años.	0,00 %	0
De 20 años a 29.	10,94 %	7
De 30 años a 39.	68,75 %	44
De 40 años a 50.	15,63 %	10
Mayor de 50.	4,69 %	3
TOTAL		64

Ilustración 23: Pregunta n.º 1 y sus respuestas

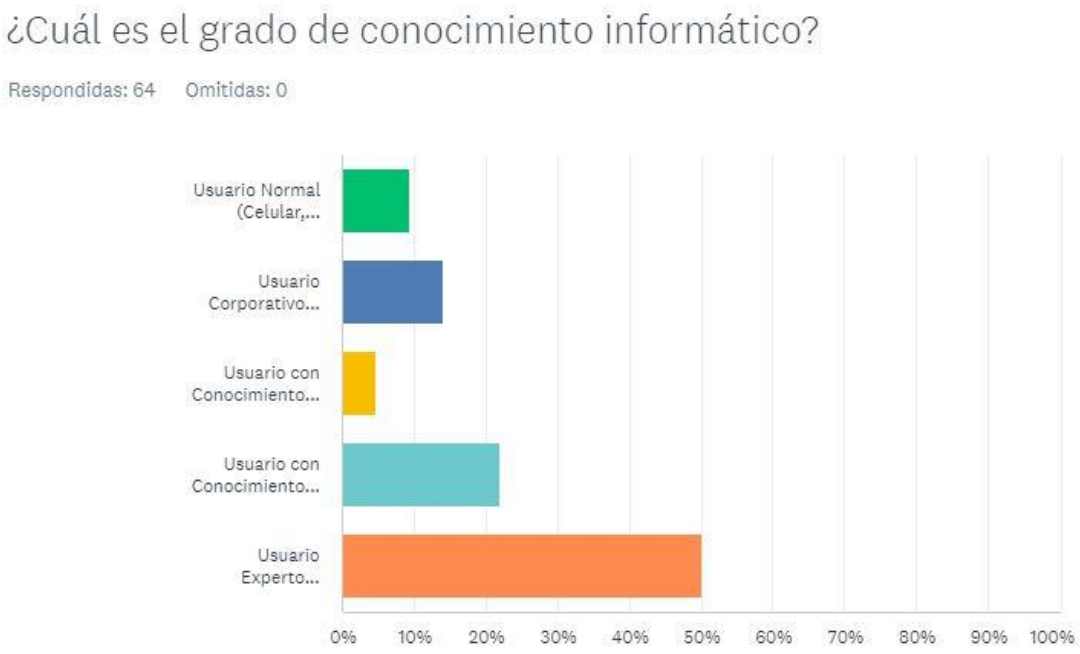
¿Qué grado académico posee?

Respondidas: 64 Omitidas: 0



OPCIONES DE RESPUESTA	RESPUESTAS	
Bachiller (Colegial o menor).	4,69 %	3
Técnico, especialización o equivalente.	23,44 %	15
Bachiller Universitario o equivalente.	28,13 %	18
Universitario con Estudios Superiores (Licenciatura, maestría, demás).	43,75 %	28
TOTAL		64

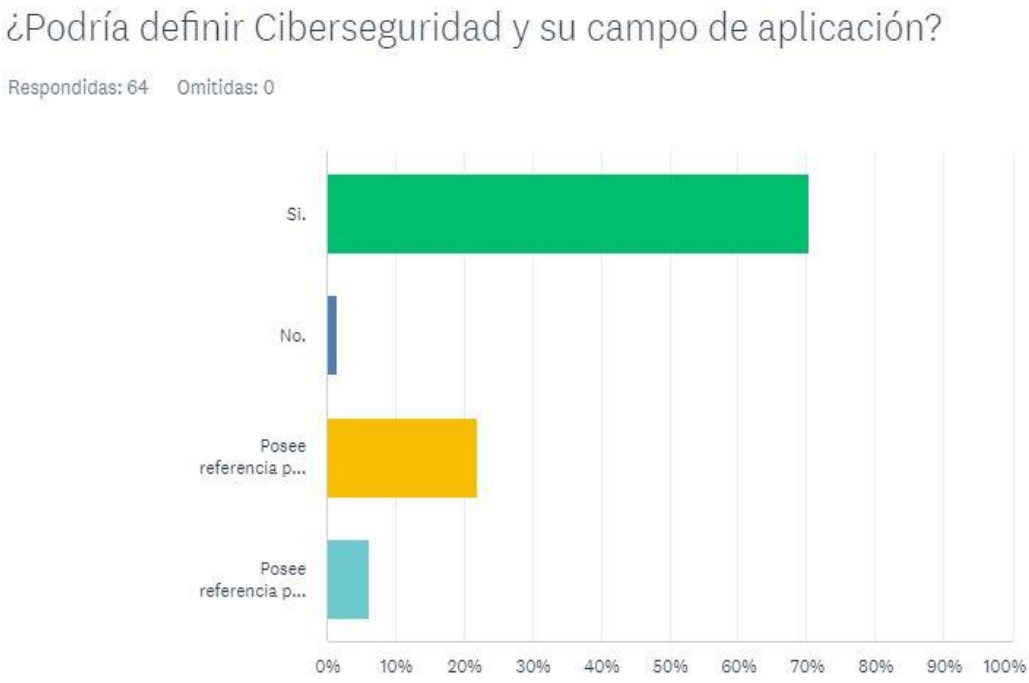
Ilustración 24: Pregunta n.º 2 y sus respuestas



OPCIONES DE RESPUESTA	RESPUESTAS	
Usuario Normal (Celular, Laptop Personal, Smart TV, etc).	9,38 %	6
Usuario Corporativo (Adicionalmente: Celular de trabajo, Laptop Empresarial, Corp-Citizen).	14,06 %	9
Usuario con Conocimiento Avanzado empírico.	4,69 %	3
Usuario con Conocimiento Avanzado con educación formal (Títulos universitarios o certificaciones afines).	21,88 %	14
Usuario Experto (Administradores de sistemas, Empleado Informáticos, Profesionales, etc).	50,00 %	32
TOTAL		64

Ilustración 25: Pregunta n.º 3 y sus respuestas

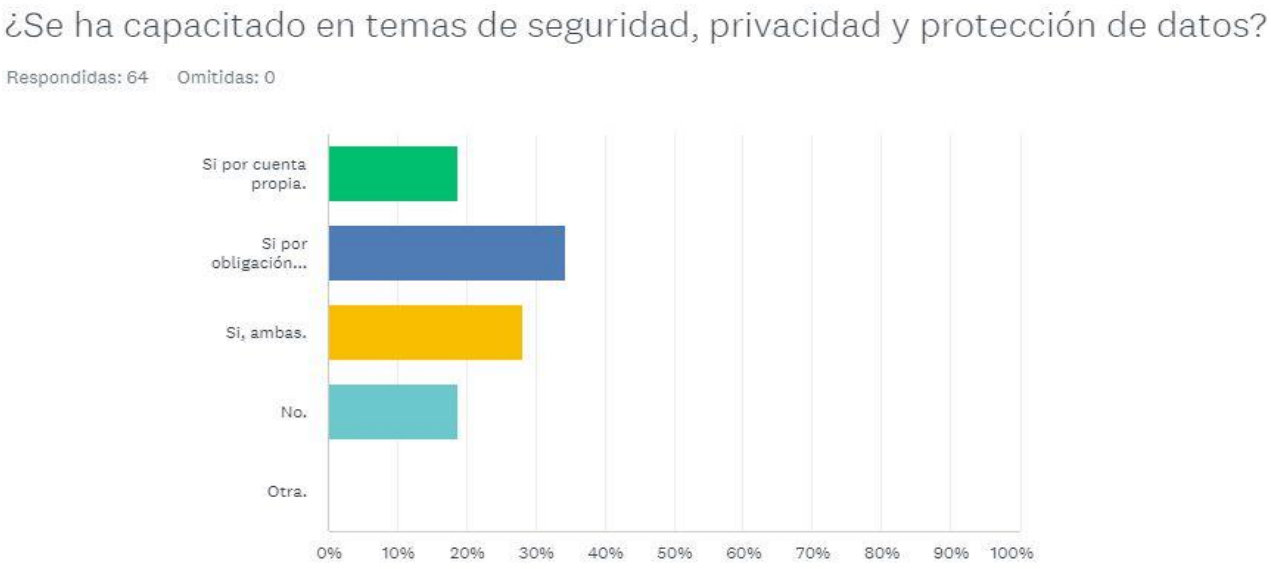
Como se refleja en las primeras tres preguntas, el grueso de la población investigada se encuentra en el rango de los 30 a 39 años, cubriendo el 68.75 % del total. Además, hay un alto grado de escolaridad, donde el 43.75 % tiene estudios de grado superior o universitario. Por último, el 50 % de la población tiene grado de experto o son profesionales en el área de la informática, mientras que el restante 50 % presenta una diversificación muy natural en cuanto al grado de conocimiento de las personas no técnicas.



OPCIONES DE RESPUESTA	RESPUESTAS	
Si.	70,31 %	45
No.	1,56 %	1
Posee referencia pero sin fundamento formal.	21,88 %	14
Posee referencia pero con fundamento formal.	6,25 %	4
TOTAL		64

Ilustración 26: Pregunta n.º 4 y sus respuestas

De toda la población encuestada, aproximadamente el 30 % no puede definir la ciberseguridad como disciplina ni referir su campo de aplicación de manera efectiva o fundamentada. Este dato es el más relevante para la investigación en curso. Además, cabe resaltar que aproximadamente un 22 % de la población ha escuchado el concepto, pero no puede ahondarlo.



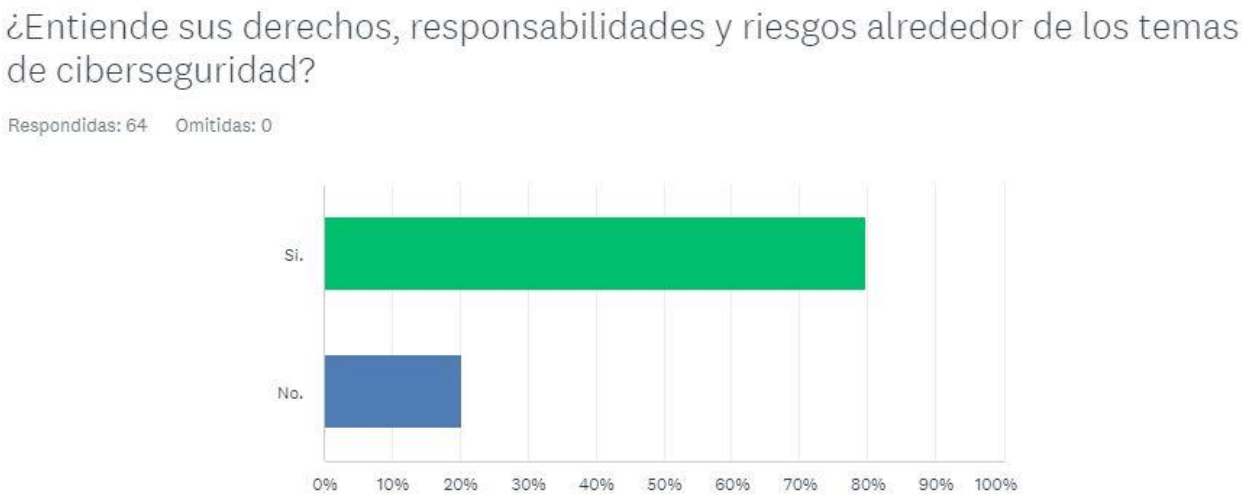
OPCIONES DE RESPUESTA	RESPUESTAS	
Si por cuenta propia.	18,75 %	12
Si por obligación laboral.	34,38 %	22
Si, ambas.	28,13 %	18
No.	18,75 %	12
Otra.	0,00 %	0
TOTAL		64

Ilustración 27: Pregunta n.º 5 y sus respuestas

Cuando se habla de conceptos, sin lugar a duda, los tópicos de seguridad, privacidad y protección de datos encabezan la lista de prioridades. En este caso, el 34.38 % de la población se ha capacitado en estos únicamente por obligación laboral.

Un indicador de relevancia también es el 46.88 % que representa la población que se ha capacitado de iniciativa propia. Este es una combinación entre interés propio (18.75 %) y obligación laboral (28.13 %). Queda por descubrir si la capacitación laboral incentivó la investigación más profunda o, de alguna manera, despertó el interés del encuestado.

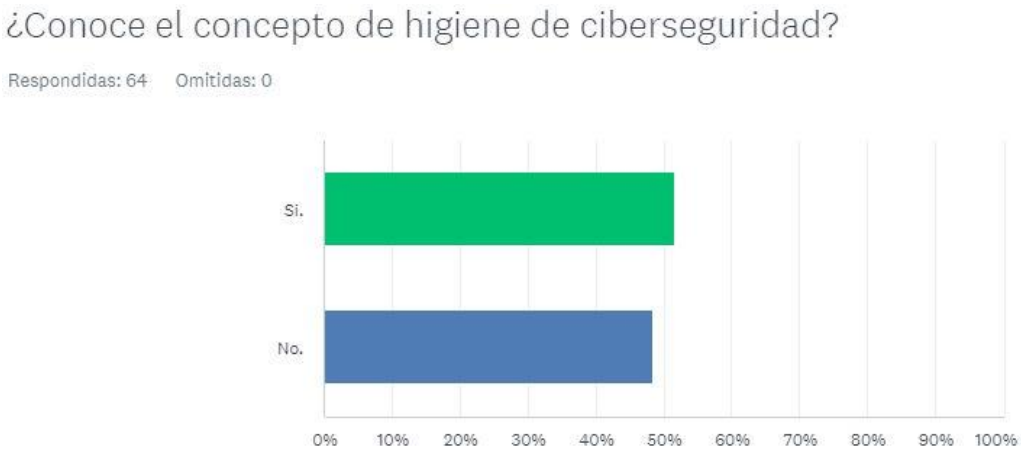
Las tres preguntas siguientes buscan dar un primer paso hacia comprender si la población entiende y maneja los detalles básicos de ciberseguridad y su gobernanza.



OPCIONES DE RESPUESTA	RESPUESTAS	
Si.	79,69 %	51
No.	20,31 %	13
TOTAL		64

Ilustración 28: Pregunta n.º 6 y sus respuestas

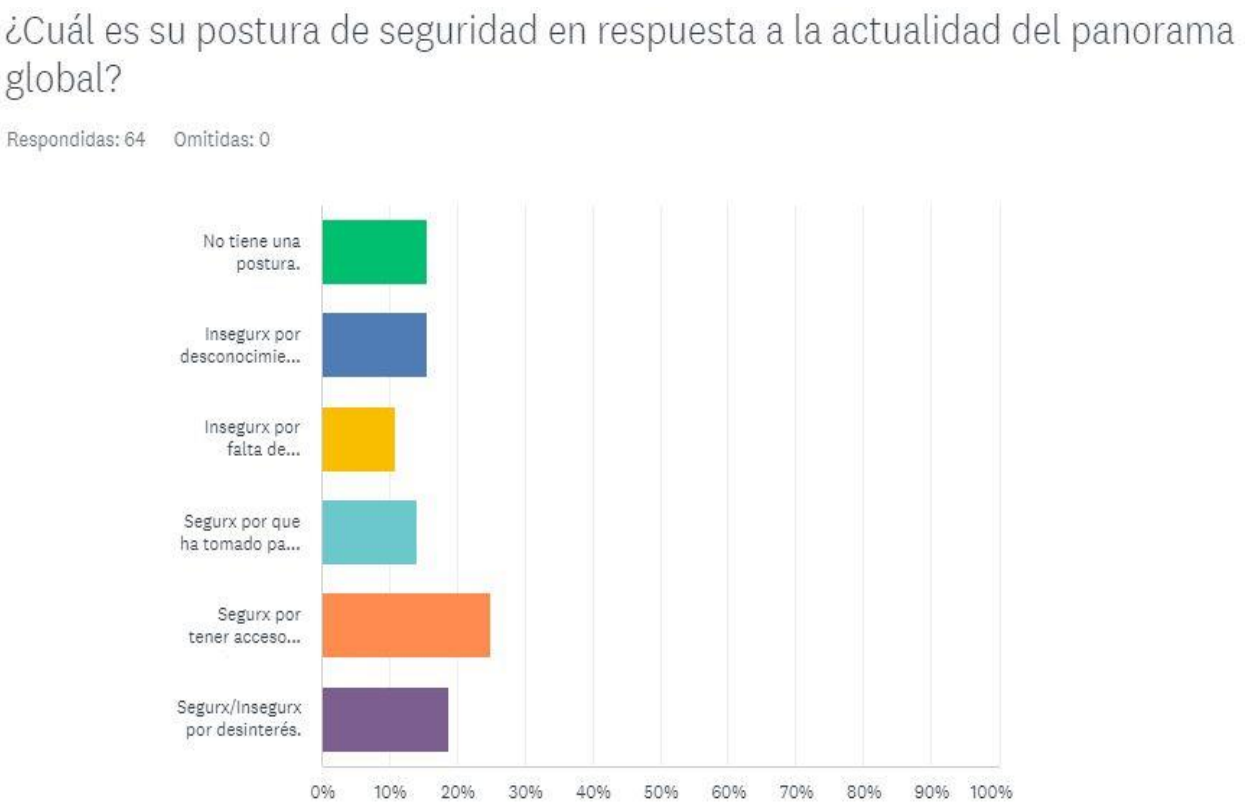
Cuando se hace una referencia cruzada entre los resultados de esta pregunta y la pregunta anterior se demarca un agravante a la situación. El 20 % de la población no tiene ningún conocimiento o capacitación. El resultado respalda que aproximadamente el 20 % de la población no entiende sus derechos, responsabilidades y riesgos.



OPCIONES DE RESPUESTA	RESPUESTAS	
Si.	51,56 %	33
No.	48,44 %	31
TOTAL		64

Ilustración 29: Pregunta n.º 7 y sus respuestas

En referencia, se mencionó un concepto formal, pero básico de la ciberseguridad, como la higiene. Se puede observar cómo el porcentaje de desconocimiento no solo disminuye aún más, sino que abarca un alarmante 48.44 % de la población total encuestada.



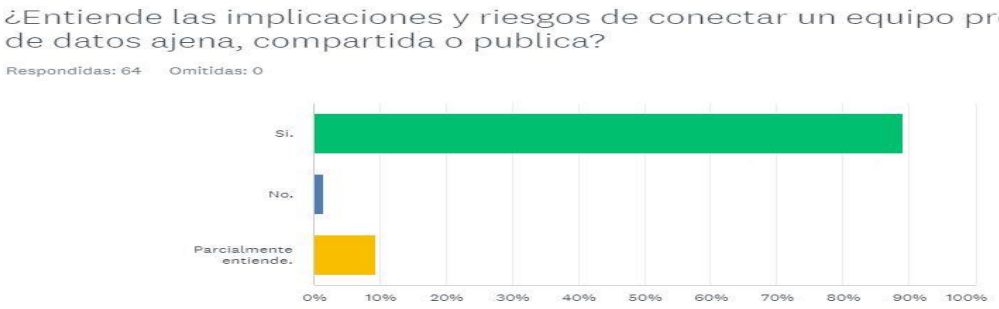
OPCIONES DE RESPUESTA	RESPUESTAS	
No tiene una postura.	15,63 %	10
Insegurx por desconocimiento.	15,63 %	10
Insegurx por falta de recursos.	10,94 %	7
Segurx por que ha tomado pasos o acciones.	14,06 %	9
Segurx por tener acceso al conocimiento y los recursos.	25,00 %	16
Segurx/Insegurx por desinterés.	18,75 %	12
TOTAL		64

Ilustración 30: Pregunta n.º 8 y sus respuestas

La pregunta anterior hace referencia a la postura de la población general con respecto a lo que se vive en la actualidad. Esta tiene dos ángulos de evaluación, los cuales se presentan subsecuentemente:

a) Primero, se analiza el factor social o el *sentir* generalizado de la población cuando se le cuestiona con respecto a su percepción de *sentirse protegidos y protegidas*. Se puede observar que solo el 39.06 % de las personas encuestadas se sienten seguras, indiferentemente de la circunstancia, del porqué o del cómo; como respuesta a eso, un 26.57 % de la población tiene un sentimiento de inseguridad generalizado.
b) La segunda arista radica en que se obtuvieron resultados alrededor del 15.63 % de la población, que ni siquiera tiene una postura y un 18.75 % que no presenta un interés por el tema. Esto los convierte en los blancos perfectos para una amenaza.

Con respecto a las siguientes cuatro preguntas, se enfocaron en personal no técnico para reflejar el entendimiento de los principios más básicos de ciberseguridad y determinar si existe alguna noción de la gobernanza.

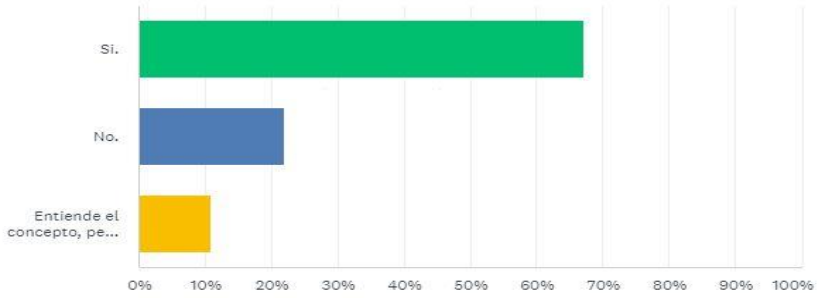


OPCIONES DE RESPUESTA	RESPUESTAS	
Si.	89,06 %	57
No.	1,56 %	1
Parcialmente entiende.	9,38 %	6
TOTAL		64

Ilustración 31: Pregunta n.º 9 y sus respuestas

¿Ha tenido la oportunidad de utilizar algún servicio tercerizado u outsourcing de cualquier tipo?

Respondidas: 64 Omitidas: 0

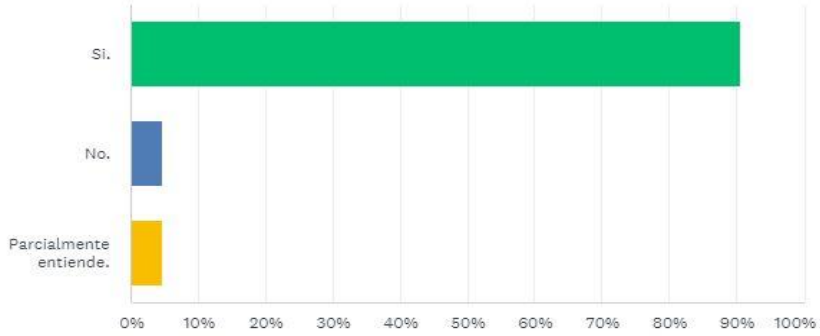


OPCIONES DE RESPUESTA	RESPUESTAS	
Si.	67,19 %	43
No.	21,88 %	14
Entiende el concepto, pero no ha utilizado un servicio aun.	10,94 %	7
TOTAL		64

Ilustración 32: Pregunta n.º 10 y sus respuestas

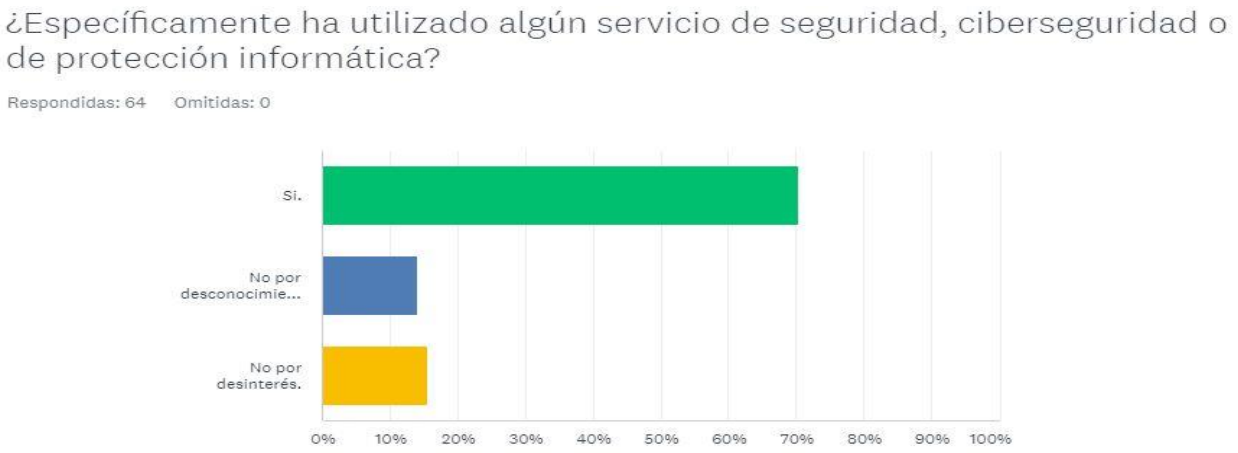
¿Entiende las implicaciones y riesgos de conectar un equipo ajeno, de fuente no confiable o inclusive de agentes externos a un ambiente privado?

Respondidas: 64 Omitidas: 0



OPCIONES DE RESPUESTA	RESPUESTAS	
Si.	90,63 %	58
No.	4,69 %	3
Parcialmente entiende.	4,69 %	3
TOTAL		64

Ilustración 33: Pregunta n.º 11 y sus respuestas



OPCIONES DE RESPUESTA	RESPUESTAS	
Si.	70,31 %	45
No por desconocimiento.	14,06 %	9
No por desinterés.	15,63 %	10
TOTAL		64

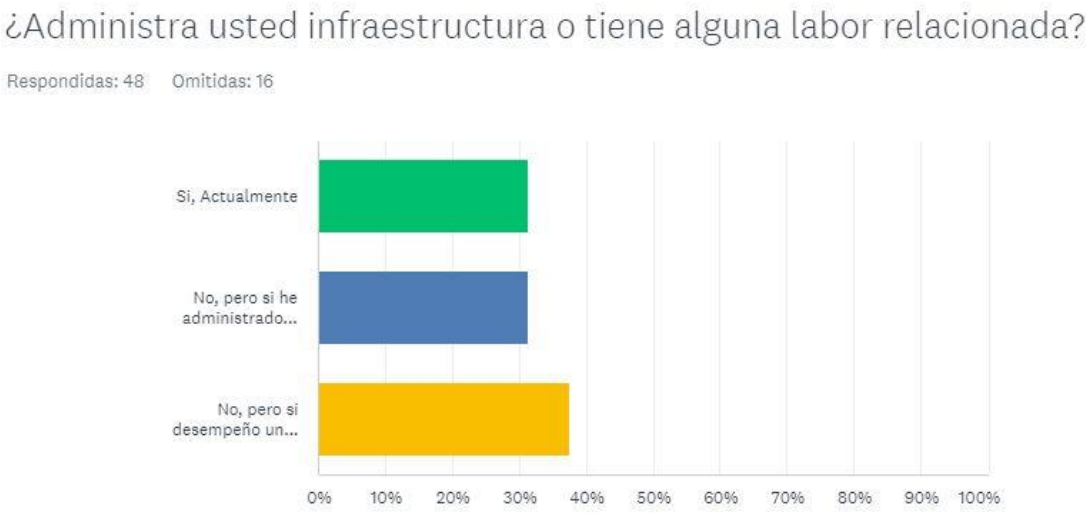
Ilustración 34: Pregunta n.º 12 y sus respuestas

Como respuesta a los conceptos técnicos básicos para personas no técnicas y técnicas, se puede denotar que al menos el 90 % de la población entiende el impacto de los diferentes ambientes seguros y la desconfianza que se debe tener de los terceros y los ambientes desconocidos o de poca confianza. Sin embargo, queda para futuras investigaciones estudiar la razón del porqué hay una incidencia tan alta a pesar del desconocimiento conceptual.

Para cerrar con la página #1 de la encuesta, se expone que en las preguntas referentes a servicios tercerizados, aproximadamente el 70 % de la población entiende y utiliza esta categorización. Además, un porcentaje similar consume servicios técnicos de seguridad.

A continuación, se presenta la segunda página de preguntas con sus respectivas respuestas. Este segmento se diseñó para recursos técnicos, por lo tanto, se agregó un

encabezado que permitiera a las personas encuestadas no técnicas terminar de manera inmediata y darles paso a los recursos con trabajos de administración de infraestructura o profesionales en el área informática. Esta segmentación aumentó la efectividad al recolectar datos y en el porcentaje de realización. Sin embargo, también introdujo una variabilidad mínima en la cantidad de respuestas, lo que demuestra una apatía por completar algunas preguntas.

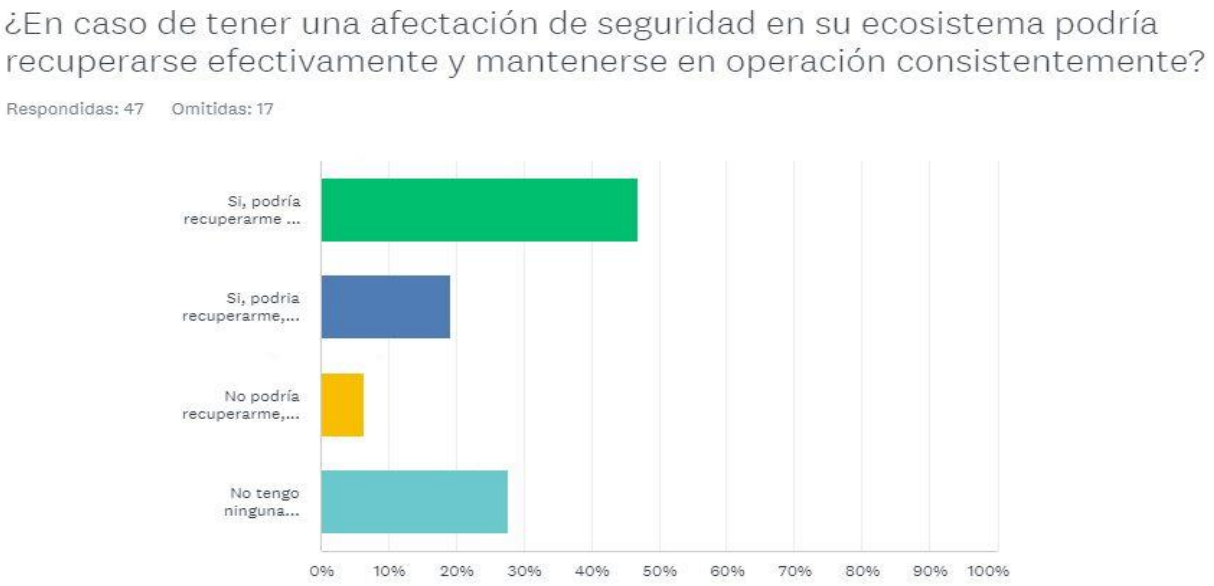


OPCIONES DE RESPUESTA	RESPUESTAS	
Si, Actualmente	31,25 %	15
No, pero si he administrado con anterioridad	31,25 %	15
No, pero si desempeño un rol técnico.	37,50 %	18
TOTAL		48

Ilustración 35: Pregunta n.º 13 y sus respuestas

En la primera pregunta del segmento técnico se delinea el tipo de población a la que se encuestó en el ámbito técnico. Se distribuyeron muy equitativamente los resultados entre las tres categorías predefinidas (a) Sí son profesionales con roles de

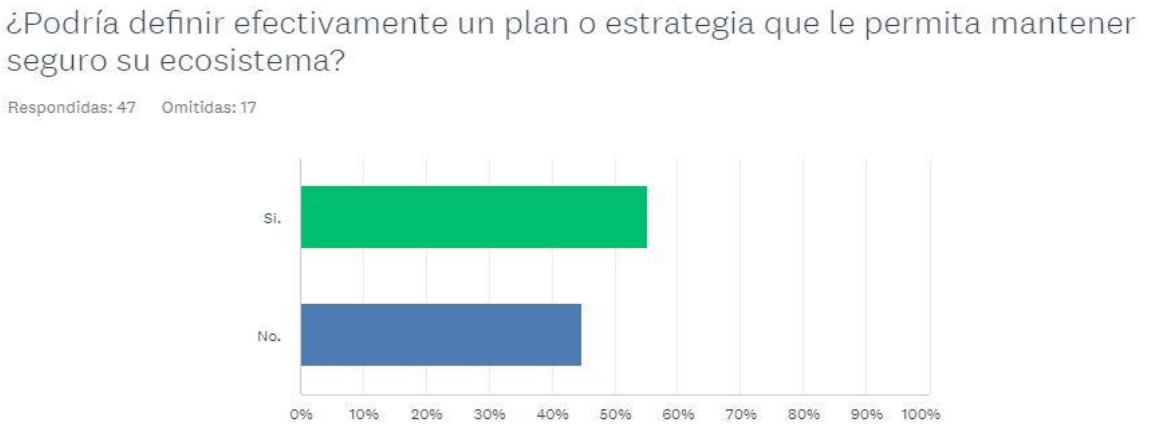
administración de infraestructura; b) No, pero sí administraron infraestructura en algún momento; por último; c) Sí, tienen roles de administración infraestructura actualmente). Para fines de la investigación es de interés combinar las opciones A y B, ya que demarcan la mayor cantidad de resultados de relevancia con un 62.50 %.



OPCIONES DE RESPUESTA	RESPUESTAS	
Si, podría recuperarme y mantenerme operacional.	46,81 %	22
Si, podría recuperarme, pero no mantenerme operacional.	19,15 %	9
No podría recuperarme, ni tampoco mantenerme operacional.	6,38 %	3
No tengo ninguna referencia.	27,66 %	13
TOTAL		47

Ilustración 36: Pregunta n.º 14 y sus respuestas

Como respuesta a una incidencia o una materialización, su recuperación y demás factores, al menos el 34.04 % de las personas encuestadas es capaz de recuperarse de una incidencia. Además, el 19.15 % puede restablecerse o recuperarse hasta el punto de BAU (*business as usual*), pero reconocen que no pueden mantenerse operacionales.



OPCIONES DE RESPUESTA	RESPUESTAS	
Si.	55,32 %	26
No.	44,68 %	21
TOTAL		47

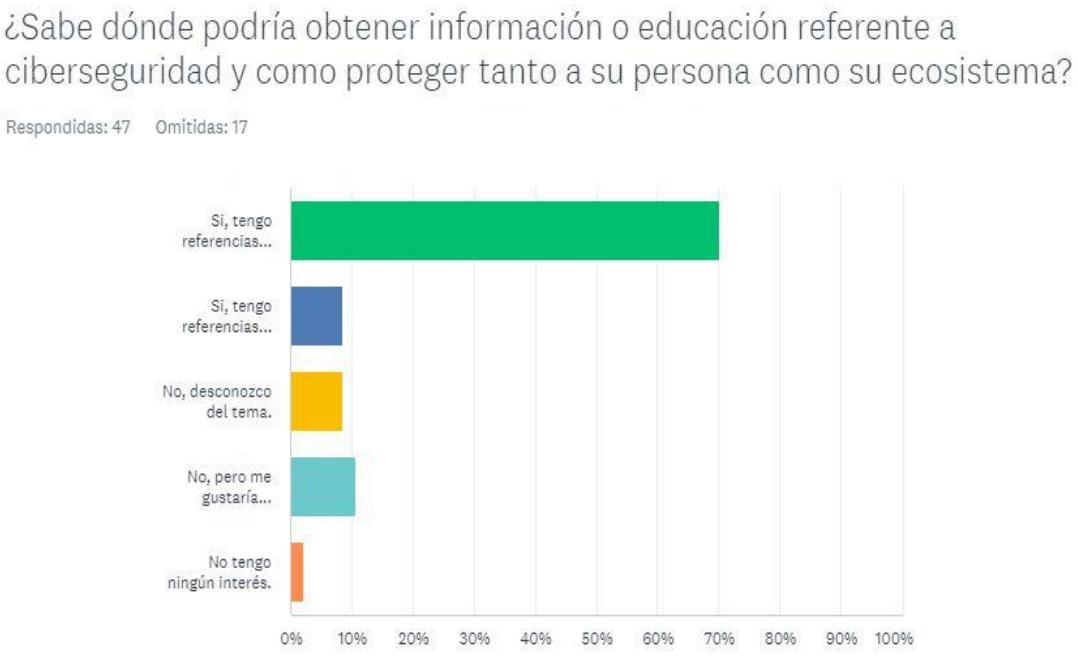
Ilustración 37: Pregunta n.º 15 y sus respuestas

De toda la población entrevistada, solo el 55 % puede elaborar efectivamente un plan de continuidad de negocios, una estrategia de seguridad o al menos alguna guía de aseguramiento del ecosistema. Queda para futuras investigaciones determinar la profundidad del conocimiento individual y los parámetros de efectividad que manejan.

OPCIONES DE RESPUESTA	RESPUESTAS	
Menos de 3 meses.	35,90 %	14
De 3 meses a 6 meses.	23,08 %	9
de 6 meses a 12 meses.	25,64 %	10
12 meses hasta 24 meses.	5,13 %	2
Más de 24 meses.	10,26 %	4
TOTAL		39

Ilustración 38: Pregunta n.º 16 y sus respuestas

Cuando se consultó por los tiempos de efectividad de los planes de seguridad y de continuidad de negocios, se nota un grado relevante de referencia. El 35.90 % reconoce la velocidad con que cambian los panoramas actuales. Además, hay un porcentaje muy sano combinado del 48.72 % de personas que reconocen que estos planes requieren mejoras y revisiones continuas. En contraste, se obtuvo un porcentaje bajo del 15.39 % de la población que no maneja planes efectivos o realistas.



OPCIONES DE RESPUESTA	RESPUESTAS	
Si, tengo referencias vigentes.	70,21 %	33
Si, tengo referencias desactualizadas.	8,51 %	4
No, desconozco del tema.	8,51 %	4
No, pero me gustaría mejorar la condición actual.	10,64 %	5
No tengo ningún interés.	2,13 %	1
TOTAL		47

Ilustración 39: Pregunta n.º 17 y sus respuestas

En temas de capacitación, se demarca que hay un porcentaje muy alto, aproximadamente el 78.72 %, de encuestados que pueden tomar acciones y capacitarse en tópicos de seguridad. Sin embargo, contrastando con las preguntas anteriores, se recalca que la población tiene un dejo de apatía por el tema. Desafortunadamente, también se muestra que al menos el 20.68 % reconoce el desconocimiento del tema.

El último segmento de la encuesta consta de tres preguntas en formato abierto. Esto permite analizar no solo la respuesta del encuestado, sino también ilustrar y

complementar la investigación con argumentos técnicos encausados. A estas respuestas, al no tener categorizaciones predefinidas, se les aplicó una técnica de etiquetado para agrupar los resultados de manera funcional.

¿Podría listar las consideraciones más importantes dentro del esquema de protección de infraestructura?

Respondidas: 37 Omitidas: 27

OPCIONES DE RESPUESTA		RESPUESTAS	
Sí. ¿Cuáles serían?	Respuestas	62,16 %	23
No. ¿Por qué?	Respuestas	43,24 %	16

Ilustración 40: Pregunta n.º 18 y sus respuestas

De primera mano, el 43.24 % de la población reconoce que es incapaz de listar las principales consideraciones en un contexto de protección de infraestructura. Al analizar el componente abierto de la pregunta mediante etiquetado, se obtuvieron los siguientes resultados:

Ilustración 41: Pregunta n.º 18 y análisis por etiquetas

Cuando se analiza de manera detenida las razones detrás de las respuestas es posible ver que el 43.75 % considera que no tiene el conocimiento y el 37.5 % piensa que no le corresponde como parte del rol técnico que ejerce.

A continuación, se analizaron las respuestas positivas utilizando un método de nube de palabras. El resultado fue el siguiente gráfico con su respectiva lista de incidencias.

Ilustración 42: Pregunta n.º 18 y análisis mediante nube de palabras

seguridad		26.09%	6
sistemas		17.39%	4
infraestructura		17.39%	4
datos		13.04%	3
Políticas		13.04%	3
monitoreo		13.04%	3
recursos		13.04%	3
red		13.04%	3
zero trust		13.04%	3

Ilustración 43: Pregunta n.º 18 y tabla estadística con respuestas positivas

En la pregunta n.º 19 se consultó a las personas encuestadas cuáles eran las variables de mayor relevancia en el proceso de optimización o modernización de la infraestructura. A todas las respuestas abiertas se les aplicó la misma técnica de nube de palabras y se agregó el listado de incidencias.

Ilustración 44: Pregunta n.º 19 y análisis mediante nube de palabras

Costos		12.12%	4
equipos		12.12%	4
seguridad		12.12%	4
datos		9.09%	3
Presupuesto		9.09%	3
infraestructura		9.09%	3

Ilustración 45: Pregunta n.º 19 y tabla estadística con respuestas positivas

Con base en la lista de incidencias obtenida, sobresalen los factores asociados al costo o presupuesto, el tipo de equipos o infraestructura, el valor de los datos y la seguridad requerida. Estos factores se toman en cuenta y se integran en el siguiente capítulo y en la respectiva propuesta de solución.

Por último, se realiza una referencia cruzada entre las respuestas positivas y negativas, la lista de incidencias y el componente abierto de la pregunta. Al completar el etiquetado, se obtiene un resultado consistente con el tono de la encuesta. En este sentido, el 51.52 % de la población considera que la variable de mayor peso es el requerimiento técnico que se debe cubrir.

En el segundo puesto de relevancia se obtuvo un 36.36 % de respuestas asociadas al elemento financiero o de costos. Por último, se obtuvo un 24.24 % de respuestas negativas de los encuestados técnicos de los cuales son incapaces de dar una referencia o que ni siquiera tienen respuesta para la pregunta.

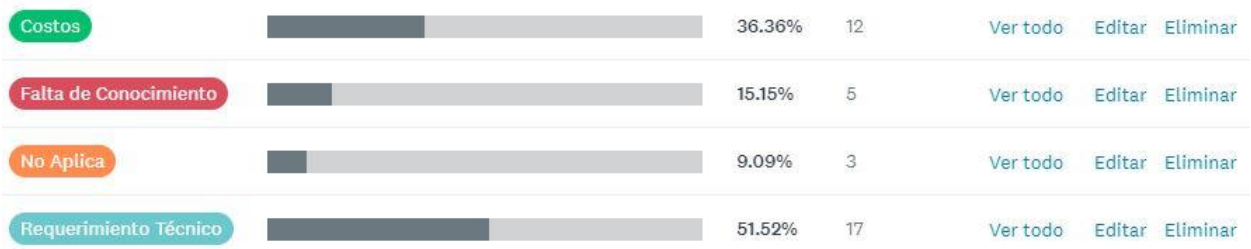


Ilustración 46: Pregunta n.º 19 y análisis por etiquetas

En la pregunta n.º 20 se consultó a las personas encuestadas si tienen claras cuáles serían sus opciones de acción en caso de ser víctimas de una afectación de seguridad, ya no en el ámbito personal, sino a un nivel más macro y profesional. El 57.89 % de las respuestas fue positivo, es decir, tienen idea de un plan de acción. Sin

embargo, sorprendentemente, el 42.11 % de las respuestas fueron negativas y, además, no poseen conocimiento al respecto.

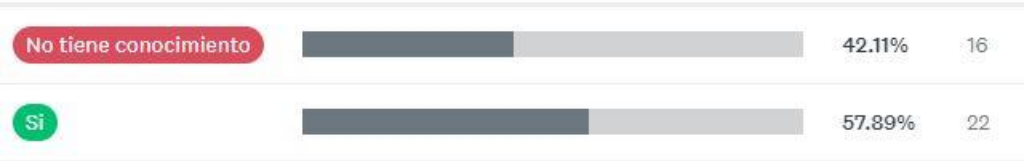


Ilustración 47: Pregunta n.º 20 y análisis por etiquetas

En el Apéndice 5 se presentan los resultados y las respuestas obtenidas por parte de la población en caso de que sea necesario el estudio de aristas subsecuentes. Con base en los resultados y las evidencias presentadas en la sección anterior, se concluyen los siguientes apartados:

a) Se parte desde la premisa que *los ejecutivos técnicos y no técnicos tienen consciencia de la relevancia de los temas de seguridad, pero no necesariamente entienden la definición técnica y su aplicación. Por lo tanto, sus aportes en el proceso son más reactivos o coaccionados*. Por este motivo, se expande el dominio de la premisa y se agrega una porción significativa de los profesionales, tanto técnicos como no-técnicos y se demuestra que en muchos segmentos de la población generalizada el fenómeno se confirma.
b) La mayor parte de la alfabetización ciberinformática de la población general y su concientización proviene de la implicación social de la existencia de grandes corporaciones y empresas globales. Esto demarca muy claramente la necesidad de establecer campañas de educación y fortalecimiento social que

sean independientes del ámbito laboral y que les permitan protegerse de una manera más efectiva y con base en su contexto de vida.

c) En el ámbito técnicoinformático, queda demostrado que los profesionales de su disciplina necesitan apoyo correlacionando los conceptos de la seguridad informática con sus roles laborales. Indiferentemente que la fuente sea motivada por el individuo o por las organizaciones en sí mismas.

d) A pesar de que la encuesta tuvo una alta incidencia en respuestas de individuos altamente técnicos queda claro que aún se debe trabajar en desmitificar la ciberseguridad y ponerla aún más al alcance de las personas, de manera que se pueda generar una capa de defensa adicional y que la superficie de los ataques se vea reducida todavía más independientemente del contexto de la infraestructura que se utilice.

e) Queda evidenciada la necesidad de generar herramientas de alto nivel y de alto rendimiento para la población, indiferentemente del contexto que manejen, de manera que se pueda producir fortaleza a través de la comunidad y la concientización social. Por consiguiente, queda validada la necesidad de la guía que se propone en el capítulo subsecuente.

Capítulo 5: Propuesta de solución

Los hallazgos y evidencias recopilados a través de este documento investigativo han recalcado la urgencia de establecer una base de conocimientos en la población general. Como respuesta a este fenómeno, se propone a continuación un segmento preliminar de aprendizaje que sirva como cimiento para mejorar la efectividad de la solución propuesta y que, a la vez, propicie un grado de adopción más elevado.

En la conceptualización de la metodología para elaborar una guía en el marco conceptual, se estableció que una de las bases en el proceso de sensibilización tecnológica y de ciberseguridad es la capacidad del lector o individuo para generar un marco de trabajo contextualizado en cada etapa del camino. Lo anterior tiene el fin de poder recopilar y estructurar el conocimiento.

5.1 Utilización de frameworks como una herramienta

Un *framework* de infraestructura en el contexto tecnológico hace referencia a un conjunto de herramientas, prácticas y lineamientos diseñados para facilitar los procesos de implementación, mantenimiento y administración de infraestructura de tecnologías de información.

En un principio, el término se utilizaba para definir y agilizar los procesos de desarrollo de *software*. Esto les permitía a los recursos generar módulos de código reutilizables y promover estandarización y consistencia en los procedimientos y resultados. De esta manera, se podían prever mejor los resultados y, a la vez, hacer cálculos más efectivos de los tiempos y esfuerzos de las tareas a lo largo del proceso.

En la línea del tiempo hacia la modernidad tecnológica, la terminología ha experimentado muchas variantes. Gracias a esa diversificación, hoy en día se aplica el término *framework* o marco de referencia en la mayoría de los ámbitos de la tecnología y su gestión.

Los componentes específicos y el diseño de un *framework* pueden variar ampliamente según el contexto y los objetivos que se busca alcanzar. Sin embargo, un *framework* bien construido tiene como objetivo proporcionar una hoja de ruta para experiencias o resultados que permitan reflejar la efectividad de este y que sean de índole cuantificable. Por ende, debe contar con las siguientes características o requerimientos en el ámbito conceptual:

a) **Abstracción**: permite abstraer las complejidades y los detalles de bajo nivel en los procesos y tareas, lo que da la posibilidad de enfocarse en la lógica de alto nivel y en el resultado. Además, proporciona un conjunto de funciones y clases predefinidas que se pueden ampliar o personalizar para cumplir requisitos específicos o técnicos.
b) **Reusabilidad**: fomenta la reutilización de los componentes y de los diferentes módulos disponibles, los cuales son prediseñados y pueden ser integrados fácilmente en otras soluciones o proyectos. El fin último es ahorrar tiempo, recursos y esfuerzo a los individuos o la organización; en contrapuesta de tener que fabricar todos los elementos siempre desde cero.
c) **Estructura**: impone estructuras o diseños específicos. Esto ayuda a mantener organizadas las tareas, promueve el uso de buenas prácticas y facilita la colaboración con otros recursos o componentes.

d) **Consistencia**: normalmente, los *frameworks* acatan o están asociados a diferentes estándares, convenciones o mejores prácticas. Por lo tanto, aseguran que los recursos mantengan un enfoque y una metodología consistentes. Esta coherencia mejora la legibilidad, la aplicabilidad y el mantenimiento.

e) **Productividad**: disminuye significativamente el tiempo que toma a los recursos alcanzar objetivos y cumplir sus tareas, ya que no invierten tiempo en reinventar la rueda, más bien pueden aprovechar las características y funcionalidades preexistentes del *framework.*

f) **Escalabilidad**: los *frameworks* deben estar diseñados para adaptarse al crecimiento. Por lo tanto, estos deben proporcionar mecanismos para manejar mayor complejidad y demanda de recursos, sin generar mayor impacto en el rendimiento.

g) **Comunidad/ecosistema**: algunos *frameworks* más populares cuentan con comunidades y ecosistemas activos. Esto implica que los recursos pueden acceder a una gran cantidad de documentación, tutoriales, complementos, lecciones aprendidas y demás materiales que se enfocan en las diferentes áreas de interés.

En conclusión, los *frameworks* son herramientas esenciales en el ámbito tecnológico, ya que simplifican, encausan y aceleran los diferentes procesos y tareas, lo que promueve la aplicación de buenas prácticas. Esto permite a los recursos que los

usan generar resultados o soluciones más robustas y escalables de manera consistentemente confiable.

5.2 Componentes fundamentales de un framework de ciberseguridad

Al tomar como referencia las tasas de éxito en el proceso de búsqueda, se utiliza la misma técnica aplicada en las cadenas de búsqueda anteriores y con el algoritmo de Quasi-Gold. Para esto se realiza una investigación estructurada con al menos tres niveles de anidación utilizando inteligencia artificial de dominio público, con el objetivo de definir cuáles son las principales características que debe tener un *framework* de seguridad.

Acontinuacion se detallan los componentes que se determinaron como fundamentales en el proceso de elaboracion de un Framework y que se alinean a la objetivos de la investigacion:

a) Definir objetivos y alcance

Comienza definiendo claramente los objetivos del marco de ciberseguridad. ¿Qué se está tratando de lograr? ¿Qué activos y datos se necesita proteger? Determina el alcance del marco, lo que incluye a los sistemas, redes y dispositivos que abarcará.

b) Comprender los requisitos legales y regulatorios

Identifica los requisitos legales y regulatorios que se aplican a la organización. Esto puede incluir regulaciones específicas de la industria, como GDPR, HIPAA, NIST e ISO 27001 y leyes regionales de protección de datos. Se debe asegurar de que el marco esté alineado con estos requerimientos.

c) Identificar las partes interesadas clave

Determina las partes interesadas clave y los tomadores de decisiones dentro de la organización que participarán en el desarrollo e implementación del marco de ciberseguridad. Esto puede incluir ejecutivos, equipos de TI, personal legal, de cumplimiento y de gestión de riesgos.

d) Evaluación y análisis de riesgos

Realiza una evaluación exhaustiva de riesgos para identificar y priorizar riesgos de ciberseguridad. Esta evaluación implica reconocer amenazas potenciales, vulnerabilidades y el impacto potencial de incidentes de seguridad en tu organización. Utiliza metodologías de evaluación de riesgos como ISO (*International Organization for Standarization*), FAIR (*factor analysis of information risk*) u OCTAVE (*operationally critical threat, asset, and vulnerability evaluation*).

e) Seleccionar un marco o estándar

Elige un marco o estándar de ciberseguridad establecido como base para el narco que se esta elaborando. Algunas elecciones comunes incluyen:

- Marco de ciberseguridad NIST: proporciona un conjunto ampliamente reconocido de pautas y mejores prácticas para gestionar el riesgo de ciberseguridad.
- ISO 27001: un estándar global para sistemas de gestión de seguridad de la información.
- Controles CIS: un conjunto priorizado de acciones diseñadas para mitigar las amenazas de ciberseguridad más comunes.

- Cobit: se centra en alinear TI y ciberseguridad con los objetivos empresariales.

f) Personalización y adaptación

Personaliza el marco elegido para satisfacer las necesidades específicas de la organización. Esto puede implicar agregar o modificar controles, políticas y procedimientos para abordar los riesgos y requisitos únicos.

g) Documentar políticas y procedimientos

Se desarrollan políticas, procedimientos y pautas de ciberseguridad exhaustivos con base en el marco. Se asegura de que estos documentos sean claros, concisos y accesibles para todo el personal relevante.

h) Implementar controles

Se establecen controles técnicos y procedimentales necesarios para proteger los activos y datos de la organización. Esto incluye seguridad de red, controles de acceso, cifrado, planes de respuesta a incidentes y otros.

i) Formación y concientización

Capacita a los empleados y crea consciencia sobre las mejores prácticas de ciberseguridad para asegurar de que todos los miembros del personal comprendan sus roles y responsabilidades en el mantenimiento de la seguridad.

j) Monitoreo y mejora continua

Implementa procesos de monitoreo continuo para detectar y responder a incidentes de seguridad de manera oportuna. Revisa y actualiza regularmente el marco para adaptarte a las amenazas y tecnologías en evolución.

k) Plan de respuesta a incidentes

Desarrolla un plan de respuesta a incidentes sólido que describa cómo la organización responderá a incidentes de seguridad. Prueba el plan a través de ejercicios y simulacros.

l) Cumplimiento y auditoría

Asegura el cumplimiento continuo de los requisitos legales y regulatorios. Audita y evalúa regularmente el programa de ciberseguridad para identificar áreas de mejora.

m) Reporte y comunicación de incidentes

Establece canales claros para reportar incidentes de seguridad, tanto interna como externamente si es necesario. Comunica de manera efectiva con las partes interesadas en caso de una violacion de seguridad.

n) Gestión de documentación y registros

Mantiene registros completos de las actividades de ciberseguridad, lo que incluye evaluaciones de riesgos, informes de incidentes y documentación de cumplimiento.

o) Concientización y formación en ciberseguridad

Educa y forma continuamente al personal sobre las mejores prácticas de ciberseguridad, asegura de que estén al tanto de las últimas amenazas y sobre cómo mitigarlas.

En conclucion, la ciberseguridad es un proceso continuo y el marco debe evolucionar para abordar amenazas emergentes y cambios dentro de la organización. Se debe evaluar y actualizar regularmente el marco para mantener la delantera en los riesgos cibernéticos. Además, es una buena práctica contar con expertos o consultores en ciberseguridad en caso de necesitar asistencia especializada durante el desarrollo e implementación del marco.

5.3 Fortalecimiento a través de la educación, capacitación y concientización: Social "Hardening"

La ciberseguridad siempre ha sido un tema importante y sigue ganando más atención y relevancia con el tiempo. Especialmente, después del fenómeno global de la COVID-19, se ha vuelto crítico y vital para los negocios. Muchos se vieron obligados a adoptar un enfoque más *en línea* y parte del mercado se volvió dependiente de Internet y la digitalización de los procesos de negocios.

La demanda en la educación sobre temas de ciberseguridad sigue en aumento. Por lo tanto, se propone que la alfabetización debe estructurarse de manera mandataria de la siguiente forma:

- Todos los usuarios deben tener consciencia del concepto de ciberseguridad y de sus principios básicos.
- Todos los profesionales, tanto técnicos como no técnicos deben recibir o tener capacitación en áreas relevantes a la ciberseguridad (relacionada con su cotidianidad y contextualizada a sus roles de trabajo).
- Tanto los especialistas en el área de ciberseguridad como profesionales informáticos deben recibir educación avanzada en el área de seguridad informática.

Ahora al tomar en cuenta la propuesta de solución de este documento, se plantea una resolución a la falta de consciencia y conocimiento social, recurriendo al subdominio de conocimiento de ciberseguridad y con las herramientas de *framework* mencionadas.

Educación: hace referencia a situaciones en las que los individuos toman acciones para realizar estudios centrados en ciberseguridad, con el objetivo de convertirse en especialistas. Por ejemplo, obtienen una certificación o grado académico formal.

Siempre es relativo al centro educativo, al grado y al objetivo que se busca obtener, pero los grados académicos formales son más enfocados en la teoría y tienen un porcentaje limitado de práctica. Por tanto las personas estudiantes deben haber obtenido el conocimiento estructurado y los fundamentos de ciberseguridad en el momento de graduarse, para luego orientarse hacia las diferentes áreas de interés.

Otra manera eficaz de aprender nuevas habilidades es tomar clases en línea, diplomados y talleres. Por lo general, tienen tiempos de aprendizaje más cortos en comparación con una universidad, pero son naturalmente más intensos, especializados, prácticos y, según el área, pueden complementar el trabajo de campo con la teoría de forma muy efectiva.

Capacitaciones: los individuos pueden adquirir nuevos conocimientos y habilidades a través de las empresas para las que laboran y sus respectivas formaciones, en lugar de utilizar medios educativos formales.

Las capacitaciones laborales se enfocan más en los roles y requerimientos del negocio. Al mismo tiempo, permiten a los profesionales exponerse a escenarios reales y situaciones prácticas. Como resultado, el conocimiento adquirido es muy concentrado y se centra en temas específicos, en lugar de proporcionar una visión holística.

Concientización: en contraste con las capacitaciones en el apartado anterior, la concientización se refiere a reforzar el conocimiento existente para arraigarlo en el individuo, pero, al mismo tiempo, busca expandirse hacia los demás.

Para generar y mantener un grado de sensibilidad hacia la ciberseguridad, se pueden aplicar mejores prácticas e integrarlas en la rutina. Por ejemplo, es importante tomar un *software* fundamental para el contexto del individuo y darle constantemente relevancia. Además, se debe estudiar el producto, anotar las características técnicas y validar de forma continua las actualizaciones y parches, entre otros. Idealmente, desde ahí se tiene la posibilidad de producir o mejorar los hábitos de seguridad.

Una manera de sensibilizar a otros es participar en actividades de la comunidad. Los proveedores de productos y servicios comparten conocimientos y refuerzan conceptos, tanto a individuos como a compañías a través de actividades públicas, redes sociales, noticiarios, *webcast* y *podcasts* o a veces de forma tan simple como conversaciones informales.

Aparte de los pilares expuestos anteriormente, existen muchos métodos alternativos para mantenerse educado y vigente en temas de ciberseguridad. Algunos ejemplos de estos son:

- Investigación tradicional.
- Atendiendo a competencias o *hackáthones*.
- Al tomar certificaciones y cursos de proveedores autorizados.
- Suscribiéndose a fuentes de información y de actualización que sean de interés.
- Integrándose a una comunidad.

Se realizó una investigación en paralelo para determinar el estado de la cuestión en referencia a programas de concientización social y temas de ciberseguridad. Donde se rescata un documento investigativo de un caso de estudio en el cual un grupo de investigadores diseñó, modeló e implementó en 2022 un *framework* de concientización de ciberseguridad aplicado a centros educativos en Catar y que se enfocó en grupos de niños de aproximadamente 12 años. La metodología del programa se alineó a muchas de las premisas de este documento, por lo tanto, se extraen los elementos de valor y se plantea una base de referencia que se ajusta para reflejar los objetivos del estudio.

En la siguiente figura se propone un esquema de concientización y sensibilización que permite generar una capa de defensa adicional mediante el proceso denominado *social hardening*.

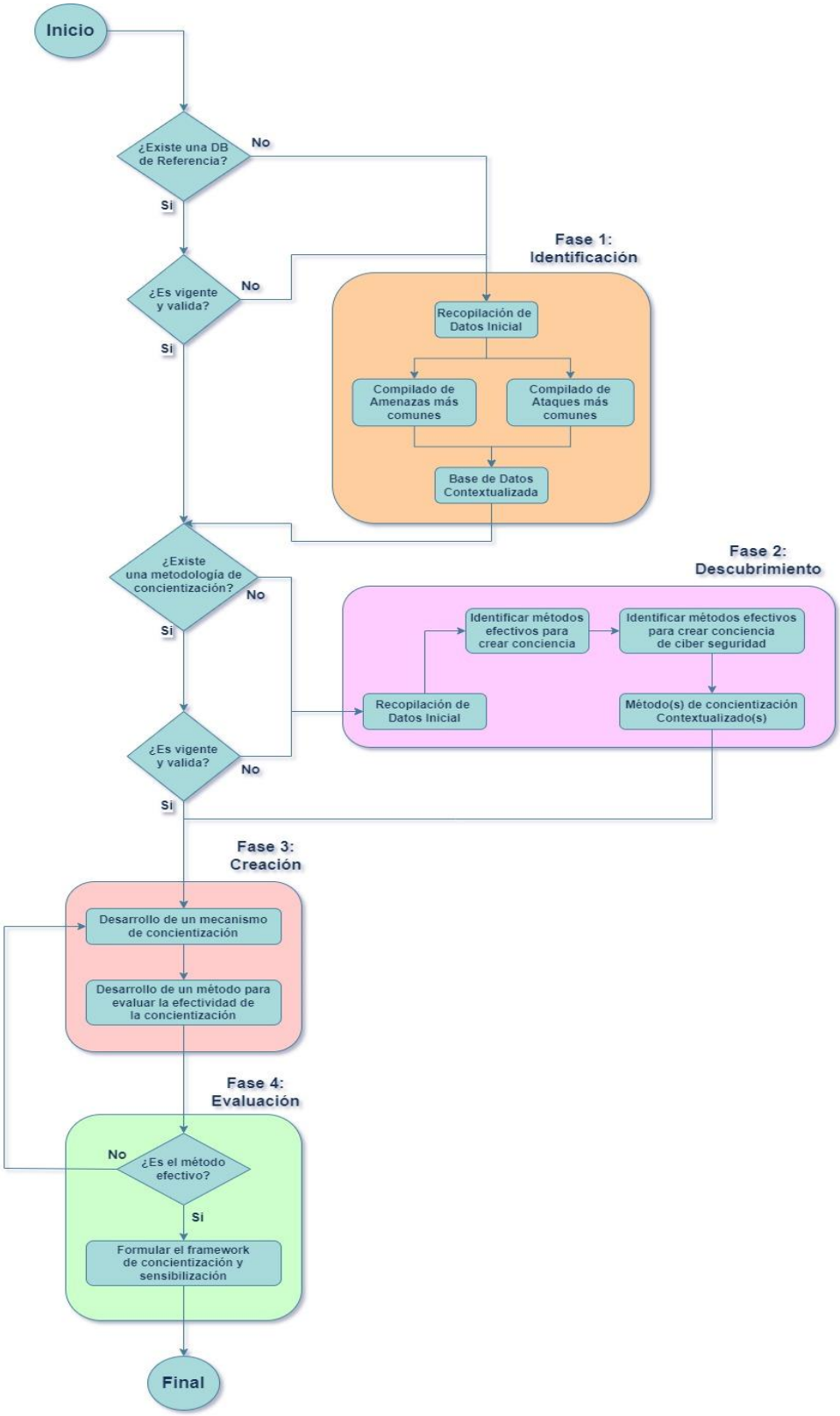


Ilustración 48: Diagrama de social hardening

Como se muestra en el estudio, para que un programa de concientización sea efectivo se debe crear un *framework* operacional que canalice los esfuerzos y los resultados del proyecto investigativo.

El modelo catarí presenta inicialmente cuatro fases de fundamentación y aplicación teórica. Sin embargo, al extrapolarlo a un nivel más macro, no se realiza ninguna validación. Por lo tanto, se agregan al modelo condicionales que permiten ahorrar recursos y tiempo en caso de tener referencias previas, sin afectar directamente el flujo que se planteó.

Fase 1: identificación

Se inicia el proceso de recolección de datos que genera una base de datos de las amenazas y ataques más comunes para el contexto del individuo. La organización y la categorización se pueden realizar mediante tablas que demuestren cada hallazgo de manera entendible. Se puede utilizar cualquier otro método disponible, siempre y cuando cumpla el mismo objetivo.

La categorización se basa en diferenciar los tipos de riesgos, tanto de los ataques como de las amenazas. Los riesgos asociados a los ataques ya han sido materializados y han generado un impacto, mientras que los riesgos asociados a las amenazas siguen sin generar una incidencia, pero pueden cambiar de estado si no se mitigan y contemplan.

Se deben agregar indicadores que permitan al individuo diferenciar el tipo de riesgo, como *phishing*, ingeniería social, *malware*, entre otros y su respectiva descripción detallada. Por último, es necesario incluir un segmento de implicaciones que permita

medir objetivamente el impacto de cada clase de ataque y amenaza. En el documento de la guía se agrega un artefacto con algunos ejemplos de referencia y que sirve como punto de partida.

Fase 2: descubrimiento

El enfoque consiste en encontrar los mejores métodos existentes para generar consciencia y sensibilización en el individuo dentro y fuera del contexto de ciberseguridad. Si durante el proceso se encuentran hallazgos específicamente beneficiosos para el contexto sobre el que se trabaja es de gran beneficio. Se incluyen dos validaciones que no necesariamente son secuenciales debido a la naturaleza de la investigación.

La tarea primordial de esta fase consiste en identificar técnicas o metodologías efectivas y aplicables al área de ciberseguridad. Se debe tener en cuenta que este proceso puede ayudar potencialmente durante los procesos de investigación forense.

Al final de esta fase se obtiene una base de datos categorizada en forma de tablas que muestran los resultados de manera comprensible. La categorización se basa en el tipo de método que se utiliza para propagar el mensaje, como videos, juegos, capacitaciones interactivas, entre otros. Esta tabla debe incluir los detalles de relevancia del método según el contexto. En el documento de la guía se agrega un artefacto con algunos ejemplos de referencia.

Fase 3: creación

Con base en ambos compilados de información o bases de datos contextualizadas, la fase tres da paso a crear un mecanismo de concientización. En este

punto, ya se tiene una fundamentación teórica más clara y profunda de los posibles ataques y amenazas que pueden afectar al individuo en sus diversos casos de uso y cuál es el método más efectivo para comunicar el conocimiento adquirido.

El último paso de esta fase consiste en desarrollar un método para evaluar la efectividad del mecanismo que se concretó y así poder validar si se utiliza la mejor opción disponible o si se puede mejorar aún más algún otro aspecto.

Fase 4: evaluación

Esta fase se inicia cuestionando si al realizar la evaluación el método que se desarrolló es efectivo o no. Si la respuesta es negativa, se regresa al inicio de la fase tres y se inicia nuevamente al proceso de creación de otro mecanismo de concientización o, en su defecto, al ajuste del existente de manera cíclica hasta que se obtenga un método satisfactorio y la respuesta del cuestionamiento sea positiva.

Una vez concluido el proceso de evaluación, se toma el método y se integra al *framework* operacional que se utiliza para desarrollar consciencia y sensibilidad en el individuo. Por lo tanto, al final de este procedimiento secuencial se obtiene un *framework* diseñado y enfocado en resultados precisos y un proceso orientado en confiabilidad.

La ciberseguridad no se basa solo en conocimiento teórico, sino también cubre un rol activo, el cual debe presentarse a los educandos. El resultado de la totalidad del proceso debe ser individuos *hardened* que pueden ser capaces de tomar decisiones, de una manera más informada, que pueden integrarse a cualquier organización de una forma fluida y segura, que pueden ser una capa adicional y confiable de ciberseguridad

y que idealmente son capaces de afrontar tecnologías presentes y futuras en beneficio de la comunidad.

Una vez definidos los componentes necesarios para generar de manera efectiva un *framework* de ciberseguridad, se combina con el estudio realizado sobre la conceptualización de una guía y con los procesos de *social hardening* propuestos anteriormente y se genera un documento adicional que sirve no solo como resultado de la premisa de investigación, sino que está en cumplimiento con los resultados del documento investigativo.

Conclusiones

- En estos tiempos modernos se ha hecho cada vez más difícil mantenerse al tanto de todo lo que engloba la seguridad informática debido a lo exponencial de la velocidad con la que avanza la tecnología. De esta manera, el asegurar que la ciberseguridad se convierta en un tema esencial para toda la población es crítico.

- La moderna manera de vivir obliga a depender del uso de la tecnología, la cual se ha extendido a todas las áreas y sectores que rodean a las personas, como la educación, la medicina, la comida, los servicios hasta los dispositivos en el hogar. Sin lugar a duda, la vida de las futuras generaciones depende de su correcta utilización y su aseguramiento. Por ende, se debe encontrar una forma de cerrar estas brechas como especialistas de ciberseguridad.

- Los requerimientos tecnológicos han aumentado y, por ende, la ciberseguridad que la rodea, el problema principal radica en la falta de educación, consciencia y sensibilidad. La tecnología se volvió tan inevitable, accesible y poderosa que ubica a la población general en condiciones globales y contextos diversos, exponiéndoles a situaciones de riesgo que muchas veces les sobrepasan.

- Se concluye que definir un solo método, protocolo o estándar que defina efectivamente un ecosistema como *seguro* o *protegido* es irreal y está documentado como *inalcanzable*. No obstante, el estudio confirma como resultado que la definición

de un *framework* contextualizado a la situación del usuario o la empresa es un requerimiento y, a la vez, lo recomiendan todos los materiales revisados para alcanzar un ecosistema de ciberseguridad efectivo.

Mediante la guía de optimización de infraestructura tecnológica para prevenir y recuperar incidentes de ciberseguridad, que se presentó como resultado de este documento investigativo, se demostraron diferentes adaptaciones y procesos extraídos de los distintos compendios disponibles en el mercado global. A continuación, se presentan algunos beneficios que se obtienen:

- Los individuos con un estado de *hardened*, que implica que son recursos que necesitan menos tiempo de integración en la empresa y que tienen una probabilidad mucho más baja de incurrir en incidencias, obtienen una mejor postura de seguridad. Esto ocasiona una menor superficie de ataque y una reducción en el índice del catalizador más común.

- El uso de *frameworks* como herramienta trae beneficios al individuo dentro y fuera del ámbito de los negocios. El documento puede usarse como puente o recurso para generar personal mejor calificado y resiliente, con capacidades más elevadas de análisis y resolución de problemas y, por consiguiente, con mejores perfiles laborales.

- Toma objetivos teóricos, necesidades de negocios, requerimientos técnicos, entre otros y los convierte en medidas accionables y planes estratégicos, los cuales, a la vez, implican métodos de evaluación y entregables efectivos y medibles.

- Este documento investigativo y la guía que lo acompaña con sus respectivos artefactos puede usarse, tanto a lo interno como externamente para fomentar conversaciones técnicas fundamentadas, con una dirección estratégica específica. Lo anterior permite revelar puntos de dolor, falta de controles o incluso falencias en los sistemas e infraestructura, lo que mejora los planes y estrategias de negocios y los tiempos necesarios para implementarlos.

- Tanto el documento investigativo como la guía de optimización sacrifican profundidad técnica, para abarcar más amplitud y diversidad en los temas, lo que genera un punto de convergencia teórico. Idealmente, incentiva la curiosidad del individuo al fomentar la investigación y el crecimiento en tópicos que no conozca en profundidad y revelar potenciales aristas no consideradas o analizadas dentro del esquema y contexto de seguridad.

En conclusión, se define como exitoso el estudio y se logra elaborar efectivamente una guía de cumplimientos con los objetivos generales y específicos que se plantearon al inicio del proceso investigativo.

Lecciones aprendidas

- Como profesional en el área de la gestión informática, el autor siempre tuvo como parte de las responsabilidades entender los diferentes estándares, regulaciones y demás compendios. Sin embargo, realizar este documento investigativo le cambió la perspectiva de la diferencia entre comprender un documento y lo que implica implementar un estándar.

- El autor tuvo la oportunidad de profundizar en los diferentes estándares y trascender de ser un lector más hasta ser capaz de utilizarlo como una herramienta de gestión, desde ahí llegar a un punto en que se pudieran evaluar, criticar, adaptar y hasta mejorar. Lo anterior lo ayudó a crecer como profesional en el área de la gestión de la ciberseguridad.

- Una de las cosas que más se cuestionaba el autor como profesional era la capacidad de moverse fuera de su zona de comodidad y por dónde podría siquiera empezar su carrera como máster en la ciberseguridad. Este documento le ayudó a encontrar una manera de cumplir su objetivo de dar ese primer paso en la dirección correcta y reconocer que no tenía por qué ser tortuoso; la integración siempre es un paso vital en los procesos informáticos.

- Laboralmente hablando, como especialista en infraestructura, desde la primera vez que se le pidió al autor crear un plan de aseguramiento hasta este momento que presenta este documento escrito se puede decir que ha habido un camino largo y

difícil, pero que no es imposible. Este documento es su conceptualización de lo que consideraría un ejemplo de un proceso de gestión y optimización de la ciberseguridad.

- Una de las cosas que más le afectó negativamente al autor en el proceso investigativo y también la parte filosófica es verse acorralado por la cantidad de sitios y librerías digitales de pago. Durante la fase de recolección de datos, tuvo la oportunidad de encontrarse con muchos materiales que no pudo acceder, de manera que se considera que debe haber mayor accesibilidad a los datos.

- A pesar de estar en el año 2024 se siguen teniendo limitaciones con el idioma. La cantidad de material que se encontró en los compendios y repositorios que solo estaba disponible en inglés es totalmente desproporcionada, lo que extiende la brecha de conocimiento y da una sensación de retraso tecnológico.

- Una característica que se encontró de manera consistente en todos los documentos fue la alta dificultad técnica y profundidad del contenido, definitivamente es algo necesario, pero se debe considerar una forma en la que se alcance los objetivos técnicos del documento pero que, al mismo tiempo, sea entendible y accionable. Lo anterior ya que este método hace que la información sea inaccesible e inentendible para la mayor parte de la población.

- Una consideración importante que reveló el estudio es que la mayor parte de las veces los individuos o los mismos profesionales son incapaces de cerrar la brecha

entre lo que necesitan, lo que tienen, lo que son capaces de costear y cómo llegar hasta ahí. Este comportamiento ya abarca muchas áreas dentro de esta disciplina informática, en donde siquiera entre los mismos profesionales son capaces de manejar todos los detalles técnicos. Por lo tanto, se debería tomar las medidas respectivas para lograr un alcance más eficiente y una sensibilización por parte de toda la comunidad en términos de seguridad de la información.

- Indiferentemente del nivel en el que se encuentre el individuo o la organización, solo con el hecho de leer el documento ya se genera una eficiencia financiera. Esto se debe a que una condición que caracteriza a los seres humanos es que una vez que vio, escuchó o aprendió algo nuevo es difícil no considerarlo. Por lo tanto, si durante el proceso de lectura el sujeto aprendió algo nuevo, inherentemente está ahorrando dinero, ya sea en planificación, mitigación, resolución o solo con el simple hecho de no incurrir en vulnerabilidades.

Referencias bibliográficas

Abu, M. S.; Selamat, S. R.; Ariffin, A. y Yusof, R. (2018). Cyber threat intelligence-issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science, 10*(1), 371-379. https://ijeecs.iaescore.com/index.php/IJEECS/article/view/11065

Accenture. (s. f.). *State of Cybersecurity Resilience 2023*. https://www.accenture.com/us-en/insights/security/state-cybersecurity

Analytics India Magazine. (2022, 16 de mayo). *What happened to IBM's spun off IT services firm Kyndryl?* https://analyticsindiamag.com/what-happened-to-ibms-spun-off-it-services-business-kyndryl/

Auger, G. y Scott, J. (2021, 13 de setiembre). *Cybersecurity: Career Master Plan*. Packt Publishing.

Beier, C. (2023a, 24 de octubre). *Ten Modern SIEM use cases*. Sumo Logic. https://www.sumologic.com/blog/why-modern-siem/

Beier, C. (2023b, 5 de octubre). *Securing IaaS, PaaS and SaaS with Cloud SIEM*. Sumo Logic. https://www.sumologic.com/blog/securing-iaas/

Benzoni, E. (2020, 07 de mayo). *The cost of cybersecurity solutions vs. the cost of cyber attacks*. Sumo Logic. https://www.sumologic.com/blog/the-cost-of-cybersecurity-solutions-vs-the-cost-of-cyber-attacks/

Boscán de Pacheco, G. (2016). Conocimiento, contexto y método. Aspectos que promueven una postura de investigador. *Compendium, 19*(36), 75-86. https://www.redalyc.org/comocitar.oa?id=88046587005

Castellanos Vela, D. y Renna, H. (s. f.). *Guía metodológica para educación en entornos no presenciales*. https://es.unesco.org/sites/default/files/guia-metodologica-para-educacion-en-entornos-no-presenciales.pdf

Centro Nacional de Educación para el Trabajo (Cenet). (2009). *Elaboración de una guía*. https://cenet.gob.hn/web16/?s=guias

Computer History Museum (CHM). (s. f.). *International Business Machines Corporation (IBM).* https://www.computerhistory.org/brochures/g-i/international-business-machines-corporation-ibm/

Creative Commons. (s. f.). *CC BY-SA 4.0 DEED, Attribution-ShareAlike 4.0 International, Determinar el diseño de la investigación*. https://creativecommons.org/licenses/by-sa/4.0/

El Confidencial. (2023, 10 de noviembre). *El mayor banco mundial sufre un ciberataque en EEUU y operó con USBs enviados por mensajeros*. https://www-elconfidencial-com.cdn.ampproject.org/c/s/www.elconfidencial.com/amp/empresas/2023-11-10/icbc-mayor-banco-ciberataque-usb-enviado-mensajeros_3771409/

Freeman, E. y Harvey, N. (2021, 12 de enero). *97 Things Every Cloud Engineer Should Know*. O'Reilly Media, 1st edition.

García de Soto, B.; Georgescu, A.; Mantha, B.; Turk, Ž.; Maciel, A. y Sonkor, M. S. (2022). Construction cybersecurity and critical infrastructure protection: new horizons for Construction 4.0. *ITcon 27*, 571-594. https://doi.org/10.36680/j.itcon.º 2022.028

GooBiz. (s. f.). *From BMM and TOGAF toward SOA - Capitalizing on the Business Capabilities*. https://goobiz.com/From_BMM_to_SOA.htm

Google Scholar. (s. f.). *Cadena: cybersecurity infrastructure attacks*. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=cybersecurity+infrastructure+attacks&oq=cybersecurity+infr

IDG Communications, Inc. (2023, 7 de noviembre). *What is Kyndryl? IBM's managed infrastructure services spin-off explained*. https://www.cio.com/article/189224/what-is-kyndryl-ibms-managed-infrastructure-services-spin-off-explained.html

Indeed Editorial Team. (2022, 24 de junio). *8 Steps To Help You Create a How-To Guide*. https://www.indeed.com/career-advice/career-development/how-to-create-a-how-to-guide

International Business Machines (IBM). (2021, 3 de noviembre). *IBM Completes the Separation of Kyndryl*. https://newsroom.ibm.com/2021-11-03-IBM-Completes-the-Separation-of-Kyndryl

International Business Machines (IBM). (s. f.a). *Frequently asked questions about the Kyndryl Holdings, Inc. Distribution*. https://www.ibm.com/investor/services/faqs-about-the-kyndryl-holdings-inc-distribution

International Business Machines (IBM). (s. f.b). *Mission and Vision Statement Analysis*. https://mission-statement.com/IBM/

Isaca. (s. f.). *Capability_Maturity_Model_Integration*. https://cmmiinstitute.com/

Islam, M.; Chowdhury, M.; Li, H. y Hu, H. (2018). Cybersecurity Attacks in Vehicle-to-Infrastructure Applications and Their Prevention. *Transportation Research Record, 2672*(19), 66-78. https://doi.org/10.1177/0361198118799012

Krishna, A. (2020). *My first day as CEO - our journey together*. https://www.linkedin.com/pulse/my-first-day-ceo-our-journey-together-arvind-krishna/

Kyndryl Inc. (s. f.a). *Corporate Citizenship*. https://www.kyndryl.com/us/en/about-us/corporate-responsibility

Kyndryl Inc. (s. f.b). *Spin-off Information*. https://investors.kyndryl.com/shareholder-resources/spinoff-information#:~:text=Kyndryl%20Holdings%2C%20Inc.,(the%20%E2%80%9CDistribution%E2%80%9D)

Kyndryl Inc. (s. f.c). *Investor relations*. https://investors.kyndryl.com/

Kyndryl Inc. (s. f.d). *The Heart of Progress™*. https://www.kyndryl.com/us/en?utm_content=SRCWW&p1=Search&p4=43700066035627636&p5=e&gclid=CjwKCAjwhJukBhBPEiwAniIcNU6afAt8ycvUNh7etSNL2jQx73LbTVjyZ59uuG56OgcnQ6nKIw_gqhoCgDQQAvD_BwE&gclsrc=aw.ds

Kyndryl Inc. (s. f.e). *Kyndryl Targets $47B Managed Security Services Market with End-to-End Security Capabilities*. https://www.kyndryl.com/us/en/about-us/news/2023/07/new-managed-cybersecurity-services

Kyndryl Inc. (s. f.f). *Industries*. https://www.kyndryl.com/us/en/industries

Kyndryl Inc. (s. f.g). *About us*. https://www.kyndryl.com/us/en/about-us.

Lewis, J. (2006). *Center for Strategic and International Studies. Cybersecurity and Critical Infrastructure Protection*. http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf

Mahn, A.; Marron, J.; Quinn, S. y Topper, D. (2021). *Primeros pasos de NIST Marco de ciberseguridad: Guía de inicio rápido*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf

Meeuwisse, R. (2019). *Is Effective Cybersecurity Expensive?* Info-Security Magazine. https://www.infosecurity-magazine.com/blogs/effective-cybersecurity-expensive

Moody's Analytics. (s. f.). *Kyndryl Luxembourg, S.À R.L. Company Information*. https://www.kompany.com/p/lu/b98800

Morillo, C. (2021, 19 de octubre). *97 Things Every Information Security Professional Should Know*. O'Reilly Media.

Muguira, A. (s. f.). *Diseño de investigación. Elementos y características*. QuestionPro. https://www.questionpro.com/blog/es/diseno-de-investigacion/#:~:text=El%20dise%C3%B1o%20de%20investigaci%C3%B3n%20se,sea%20manejado%20de%20manera%20eficiente

National Institute of Standards and Technology (NIST). (s. f.a). https://www.nist.gov/

National Institute of Standards and Technology (NIST). (s. f.b). *NIST Cybersecurity Framework 2.0*. https://www.nist.gov/cyberframework

National Institute of Standards and Technology. (2015, 12 de diciembre). *Views on the Framework for Improving Critical Infrastructure Cybersecurity*. https://www.federalregister.gov/documents/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity#print

Ocaña Delgado, R. (2010). Pasado y presente de la investigación educativa. *Revista Digital Universitaria [en línea], 11*(2). http://www.revista.unam.mx/vol.11/num2/art18/int18.htm

Ortega, C. *¿Qué es la investigación explicativa?* QuestionPro. https://www.questionpro.com/blog/es/investigacion-explicativa/

Ovrutsky, A. (s. f.). *How to execute an Azure Cloud purple team excercise*. Sumo Logic. https://www.sumologic.com/blog/azure-cloud-purple-team/

Pomanda. (s. f.). *Kyndryl UK Limited Company Information*. https://pomanda.com/company/13141201/kyndryl-uk-limited

Posada Ramírez, J. (2014). Ontología y Lenguaje de la Realidad Social. *Cinta de moebio, (50)*, 70-79. https://dx.doi.org/10.4067/S0717-554X2014000200003

Robles, F. (s. f.). *¿Qué es el diseño metodológico de una investigación? Características más importantes*. https://icecregiondecoquimbo.cl/wp-content/uploads/2019/12/9-EL-DISE%C3%91O-METODOL%C3%93GICO-DE-LA-INVESTIGACI%C3%93N.pdf

Rohloff, M. (2008). *Framework and Reference for Architecture Design*. https://aisel.aisnet.org/amcis2008/118

SlideServe. (s. f.). *La Guía Metodológica*. https://www.slideserve.com/file-download/895210

Steinberg, J. (2022, 8 de abril). *Cybersecurity For Dummies*. For Dummies; 2nd edition.

Stock Analysis. (s. f.a). *Kyndryl Holdings Employees*. https://stockanalysis.com/stocks/kd/employees/

Stock Analysis. (s. f.b). *Company Description*. https://stockanalysis.com/stocks/kd/company/

Ulrich, W. (s. f.). *Business Architecture 2008: Standards, Frameworks and Governance*. https://www.bainstitute.org/resources/articles/business-architecture-2008-standards-frameworks-and-governance

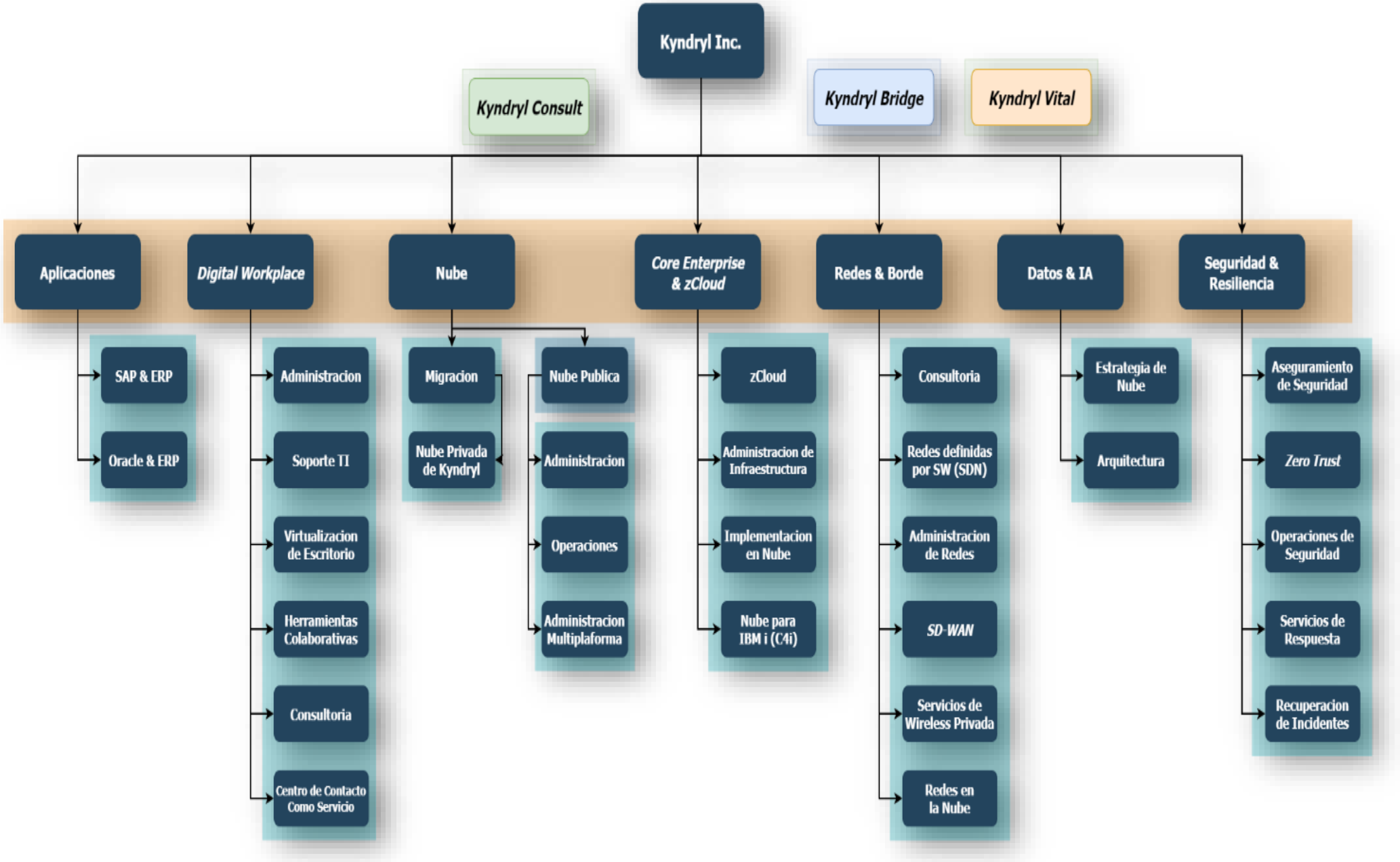
Ward, H. (2023, 06 de agosto). *History-computer, IBM: Complete Guide — History, Products, Founding, and More*. https://history-computer.com/ibm-history/

Zhang, H. y Ali Babar, M. (s. f.). *On Searching Relevant Studies in Software Engineering*. https://pdfs.semanticscholar.org/59d3/ec40b4f17ed94dc5ae510c316ac511915031.pdf

Apéndices

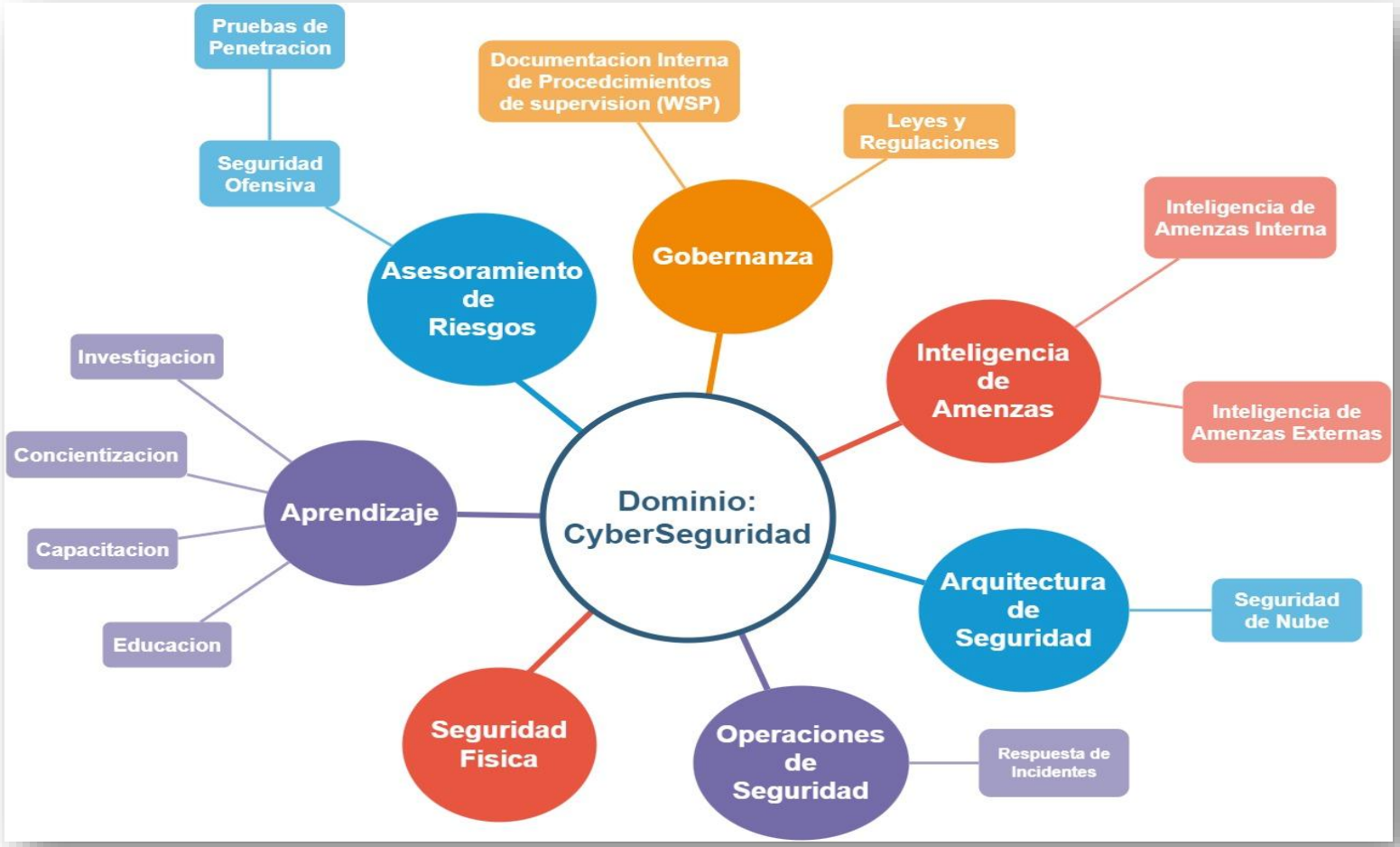
Apéndice 1

Diagrama representativo de todas las áreas tecnológicas y servicios sobre los que opera y ofrece Kyndryl Inc. (al momento en que se realizó el documento escrito. Estas pueden variar en futuras referencias).


Kyndryl Inc.
Kyndryl Consult
Kyndryl Bridge
Kyndryl Vital
Aplicaciones
Digital Workplace
Nube
Core Enterprise & zCloud
Redes & Borde
Datos & IA
Seguridad & Resiliencia
SAP & ERP
Oracle & ERP
Administracion
Soporte TI
Virtualizacion de Escritorio
Herramientas Colaborativas
Consultoria
Centro de Contacto Como Servicio
Migracion
Nube Privada de Kyndryl
Nube Publica
Administracion
Operaciones
Administracion Multiplaforma
zCloud
Administracion de Infraestructura
Implementacion en Nube
Nube para IBM i (C4i)
Consultoria
Redes definidas por SW (SDN)
Administracion de Redes
SD-WAN
Servicios de Wireless Privada
Redes en la Nube
Estrategia de Nube
Arquitectura
Aseguramiento de Seguridad
Zero Trust
Operaciones de Seguridad
Servicios de Respuesta
Recuperacion de Incidentes

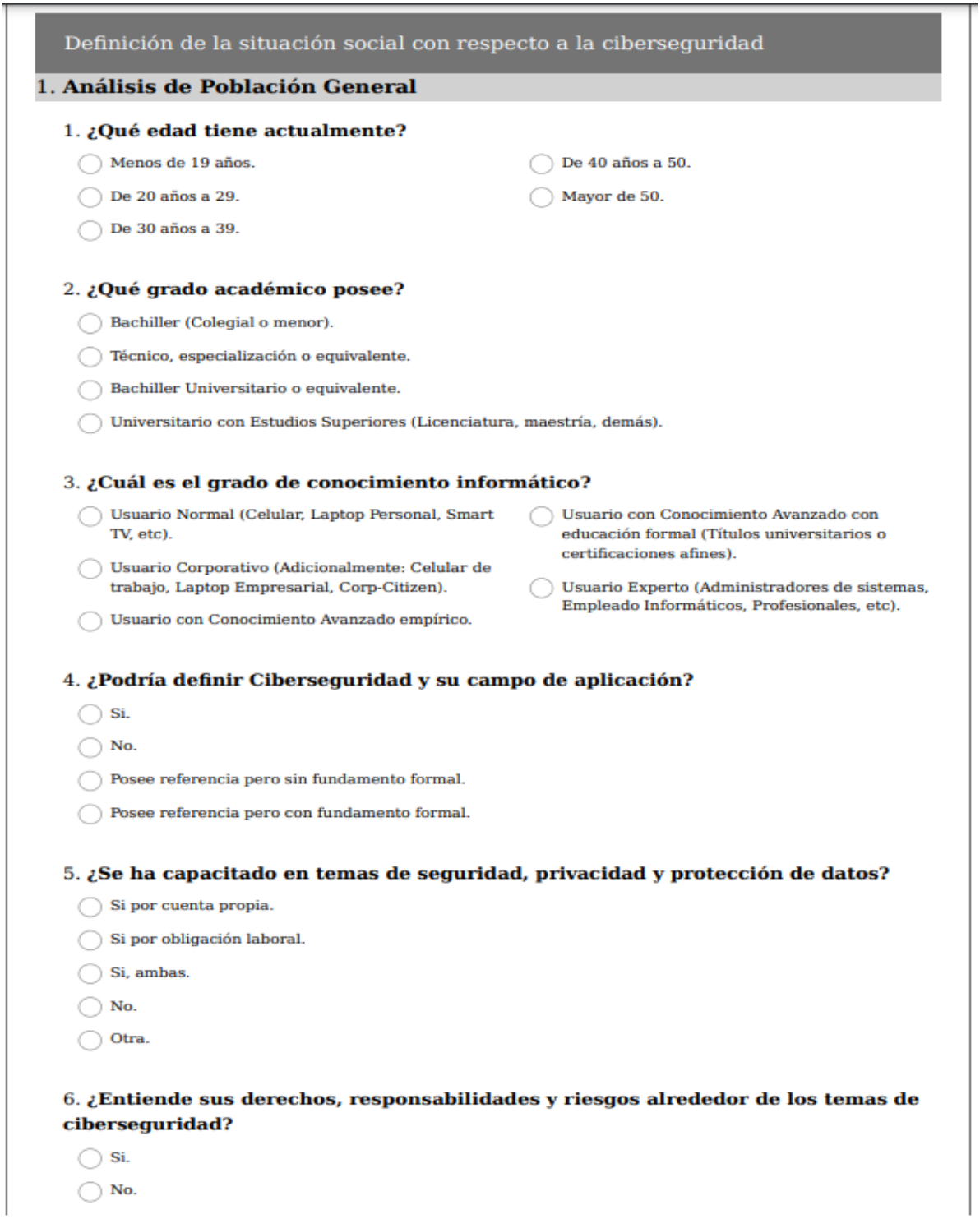
Apéndice 2

Diagrama representativo del dominio de ciberseguridad y los subdominios que lo componen (al momento en que se realizó el documento escrito, estos pueden variar en futuras referencias).



Apéndice 3

Capturas representativas del diseño de la encuesta aplicada a los diferentes actores sociales.



Definición de la situación social con respecto a la ciberseguridad

1. Análisis de Población General

1. **¿Qué edad tiene actualmente?**

- ◯ Menos de 19 años.
- ◯ De 20 años a 29.
- ◯ De 30 años a 39.
- ◯ De 40 años a 50.
- ◯ Mayor de 50.

2. **¿Qué grado académico posee?**

- ◯ Bachiller (Colegial o menor).
- ◯ Técnico, especialización o equivalente.
- ◯ Bachiller Universitario o equivalente.
- ◯ Universitario con Estudios Superiores (Licenciatura, maestría, demás).

3. **¿Cuál es el grado de conocimiento informático?**

- ◯ Usuario Normal (Celular, Laptop Personal, Smart TV, etc).
- ◯ Usuario Corporativo (Adicionalmente: Celular de trabajo, Laptop Empresarial, Corp-Citizen).
- ◯ Usuario con Conocimiento Avanzado empírico.
- ◯ Usuario con Conocimiento Avanzado con educación formal (Títulos universitarios o certificaciones afines).
- ◯ Usuario Experto (Administradores de sistemas, Empleado Informáticos, Profesionales, etc).

4. **¿Podría definir Ciberseguridad y su campo de aplicación?**

- ◯ Si.
- ◯ No.
- ◯ Posee referencia pero sin fundamento formal.
- ◯ Posee referencia pero con fundamento formal.

5. **¿Se ha capacitado en temas de seguridad, privacidad y protección de datos?**

- ◯ Si por cuenta propia.
- ◯ Si por obligación laboral.
- ◯ Si, ambas.
- ◯ No.
- ◯ Otra.

6. **¿Entiende sus derechos, responsabilidades y riesgos alrededor de los temas de ciberseguridad?**

- ◯ Si.
- ◯ No.

7. **¿Conoce el concepto de higiene de ciberseguridad?**

- ◯ Si.
- ◯ No.

8. **¿Cuál es su postura de seguridad en respuesta a la actualidad del panorama global?**

- ◯ No tiene una postura.
- ◯ Insegurx por desconocimiento.
- ◯ Insegurx por falta de recursos.
- ◯ Segurx por que ha tomado pasos o acciones.
- ◯ Segurx por tener acceso al conocimiento y los recursos.
- ◯ Segurx/Insegurx por desinterés.

9. **¿Entiende las implicaciones y riesgos de conectar un equipo propio a una red de datos ajena, compartida o publica?**

- ◯ Si.
- ◯ No.
- ◯ Parcialmente entiende.

10. **¿Ha tenido la oportunidad de utilizar algún servicio tercerizado u outsourcing de cualquier tipo?**

- ◯ Si.
- ◯ No.
- ◯ Entiende el concepto, pero no ha utilizado un servicio aun.

11. **¿Entiende las implicaciones y riesgos de conectar un equipo ajeno, de fuente no confiable o inclusive de agentes externos a un ambiente privado?**

- ◯ Si.
- ◯ No.
- ◯ Parcialmente entiende.

12. **¿Específicamente ha utilizado algún servicio de seguridad, ciberseguridad o de protección informática?**

- ◯ Si.
- ◯ No por desconocimiento.
- ◯ No por desinterés.

Definición de la situación social con respecto a la ciberseguridad

2. Análisis de Población Técnica

Si usted no posee un rol técnico o informático puede proceder al final de la pagina y completar la encuesta.

13. **¿Administra usted infraestructura o tiene alguna labor relacionada?**

- ◯ Si, Actualmente
- ◯ No, pero si desempeño un rol técnico.
- ◯ No, pero si he administrado con anterioridad

14. **¿En caso de tener una afectación de seguridad en su ecosistema podría recuperarse efectivamente y mantenerse en operación consistentemente?**

- ◯ Si, podría recuperarme y mantenerme operacional.
- ◯ Si, podria recuperarme, pero no mantenerme operacional.
- ◯ No podría recuperarme, ni tampoco mantenerme operacional.
- ◯ No tengo ninguna referencia.

15. **¿Podría definir efectivamente un plan o estrategia que le permita mantener seguro su ecosistema?**

- ◯ Si.
- ◯ No.

16. **En caso de tener un plan o estrategia de seguridad ¿Cuánto tiempo considera que este plan o estrategia seria efectivo en la actualidad?**

- ◯ Menos de 3 meses.
- ◯ De 3 meses a 6 meses.
- ◯ de 6 meses a 12 meses.
- ◯ 12 meses hasta 24 meses.
- ◯ Más de 24 meses.

17. **¿Sabe dónde podría obtener información o educación referente a ciberseguridad y como proteger tanto a su persona como su ecosistema?**

- ◯ Si, tengo referencias vigentes.
- ◯ Si, tengo referencias desactualizadas.
- ◯ No, desconozco del tema.
- ◯ No, pero me gustaría mejorar la condición actual.
- ◯ No tengo ningún interés.

18. **¿Podría listar las consideraciones más importantes dentro del esquema de protección de infraestructura?**

Si. ¿Cuáles serían?

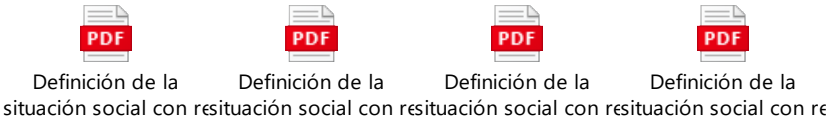
No. ¿Por qué?

19. **¿Cuáles son las variables de mayor relevancia en el proceso de optimización o modernización de la infraestructura?**

20. **¿Tiene claras cuales serían sus opciones de acción en caso de ser víctima de una afectación de seguridad, en cualquiera de sus escalas?**

Apéndice 4

Se adjuntan los documentos en formato pdf con todas las respuestas obtenidas durante la fase de encuestas. Todas las respuestas de la pregunta n.º 1 a la pregunta n.º 17 en formato cerrado se agregaron en un solo documento. Las preguntas subsecuentes tienen cada una su propio archivo para reflejar su condición de formato abierto.



Apéndice 5

Se adjunta el documento de aprobación de privacidad por parte de Kyndryl y su respectivo representante.

Apéndice 6

Se adjunta la Guia de Optimizacion & Incident Recovery y el artefacto que le complementa