Universidad Internacional de las Américas

Carrera de Relaciones Internacionales

Grado académico: Bachillerato

Análisis de la importancia de la ciberseguridad corporativa dentro de la dinámica internacional de la era digital: Caso Huawei (2018-2023) y su impacto internacional.

Sofía Cordero Gómez

Tutor: Bryan Acuña Obando

San José, octubre, 2023

Contenido

CAPÍTULO I

Introducción

En la era de la información y la conectividad global, marcada por la rápida expansión de las tecnologías de la información y la comunicación, el mundo empresarial ha experimentado una transformación sin precedentes. Sin embargo, esta era de avances tecnológicos también ha dado lugar a una nueva dimensión de riesgos: las amenazas cibernéticas. En este contexto, la ciberseguridad corporativa se ha erigido como una piedra angular en la protección de datos, la privacidad y la integridad de las operaciones empresariales a nivel global.

El presente estudio se enfoca en analizar la importancia de la ciberseguridad corporativa en el ámbito internacional, tomando como caso de estudio a Huawei, una de las empresas más influyentes en el sector de las tecnologías de la información y las comunicaciones, durante el período que abarca desde 2018 hasta 2023. Durante este tiempo, Huawei ha sido protagonista en un escenario internacional cargado de tensiones y desafíos relacionados con la seguridad cibernética y su presunta vinculación con el gobierno chino.

La relevancia de este análisis radica en que la seguridad cibernética se ha convertido en un tema central en la dinámica internacional de la era digital. Las implicaciones de las decisiones relacionadas con la ciberseguridad corporativa pueden extenderse mucho más allá de los confines de una empresa, afectando la seguridad nacional, las relaciones diplomáticas y el comercio internacional. En este contexto, comprender el caso de Huawei y su impacto en la escena global proporciona valiosas lecciones y perspectivas sobre cómo las organizaciones multinacionales navegan en un entorno digital cada vez más complejo y desafiante. Este estudio pretende arrojar luz sobre estos aspectos críticos y contribuir al entendimiento de la ciberseguridad corporativa en el contexto de la era digital.

Planteamiento

En la actualidad, la era digital ha transformado completamente la forma en que las empresas operan a nivel global. La creciente interconexión de sistemas y la dependencia de tecnologías digitales han generado numerosos beneficios económicos y sociales, pero también han comprometido a las organizaciones a riesgos cibernéticos significativos. En otras palabras, este entorno digital ofrece innumerables oportunidades, pero también está plagado de amenazas cibernéticas que pueden tener consecuencias devastadoras para las empresas a nivel global.

En este contexto, la ciberseguridad corporativa se ha convertido en un elemento crítico para garantizar la continuidad de las operaciones empresariales y la protección de datos sensibles. Sin embargo, el entorno internacional presenta desafíos únicos en cuanto a la gestión de la ciberseguridad corporativa. Estos van desde el robo de datos confidenciales, el espionaje industrial, hasta el sabotaje de operaciones. La magnitud de estos desafíos ha llevado a una reevaluación profunda de la forma en que las empresas abordan la seguridad cibernética.

Es importante hacer hincapié en la relación lineal: mientras más avance y expansión tecnológica haya, más aumentan las vulnerabilidades. Generalmente, las empresas manejan grandes cantidades de datos sensibles, incluyendo información personal y financiera de clientes y empleados. Por lo tanto, y entendiendo esa relación, la protección de estos datos se ha convertido en una prioridad crucial, ya que estos vulneran cada vez más.

En este punto es necesario mencionar sobre la ciberdelincuencia, que se puede definir como las prácticas por medio de la internet o tecnologías avanzadas que vulneran la seguridad ya sea de una empresa o entidad, hasta de un individuo. El problema aquí es que cuantas más herramientas tecnológicas y más progreso haya en ellas, más técnicas y estrategias sofisticadas utilizan para infiltrarse en sistemas corporativos y robar datos o interrumpir operaciones.

Aquí es donde nace la necesidad de un centro, es decir, un marco legal que contenga los debidos procesos ante estos desafíos que actualmente se presentan. Las regulaciones gubernamentales, como el Reglamento General de Protección de Datos (GDPR) en la Unión

Europea, obligan a las empresas a cumplir con estándares de seguridad cibernética, lo que aumenta la necesidad de una sólida ciberseguridad corporativa.

Las amenazas de ciberseguridad pueden implicar un impacto en las economías ya que las brechas de seguridad pueden tener un alto costo financiero, que incluye la pérdida de ingresos, gastos de recuperación y multas por incumplimiento de regulaciones de privacidad de datos. Por otro lado, los ciberataques exitosos pueden resultar en la pérdida de datos sensibles, dañando la reputación de la empresa y la confianza de los clientes.

La era digital sin duda ha generado un entorno propicio para el crecimiento y desarrollo de las empresas tecnológicas a nivel internacional. Huawei, una de las principales compañías de tecnología de la información y las comunicaciones (TIC), ha experimentado un rápido crecimiento y expansión global durante el período comprendido entre 2018 y 2023, el cual conduce a ser el caso de estudio de la presente investigación.

Durante el período de estudio, Huawei ha estado en el centro de controversias, debates y tensiones en particular con los Estados Unidos y otras potencias occidentales, que han cuestionado su relación con el gobierno chino y su capacidad para garantizar la seguridad de sus productos y servicios en el ámbito global. Estas controversias han generado preocupaciones significativas y han tenido un impacto profundo en varios aspectos de la dinámica internacional en la era digital. El problema que se plantea se centra en entender y analizar este impacto internacional del caso Huawei durante este período.

Por un lado, una de las principales causas del caso Huawei es la preocupación internacional sobre la seguridad cibernética relacionada con los productos y servicios de la empresa. Se ha argumentado que Huawei podría ser utilizada como una herramienta para el espionaje cibernético por parte del gobierno chino debido a su presunta relación cercana con el Partido Comunista Chino (BBC News Mundo, 2019).

Por otro lado, se puso en evidencia la competencia en tecnología 5G o carrera por el despliegue de redes 5G de próxima generación, lo cual desencadenó una intensa competencia entre empresas tecnológicas, incluida Huawei. Esto exacerbó las preocupaciones sobre la seguridad cibernética, ya que las redes 5G son fundamentales para la conectividad futura y la infraestructura crítica (BBC News Mundo, 2019).

Estos comportamientos por parte de esta empresa propician que posteriormente se tomen decisiones gubernamentales y regulaciones en las que varios gobiernos tomaron medidas para restringir o excluir a Huawei de sus mercados y proyectos de infraestructura crítica. Hay que entender que, al ser un fenómeno nuevo sobre estrategias de ataque, la manera de proceder es bastante drástica y por ello estas decisiones incluyeron prohibiciones de uso de equipos de Huawei en redes gubernamentales y la imposición de sanciones comerciales.

El caso Huawei sin duda tuvo un impacto significativo en la industria tecnológica, con la exclusión de la empresa de mercados clave, lo que llevó a cambios en las alianzas y en la competencia en el sector y ha tenido un impacto duradero en las decisiones comerciales, las relaciones internacionales y la seguridad cibernética. Ha destacado la necesidad de un enfoque más estratégico y cauteloso en la adopción de tecnologías críticas, y ha llevado a un mayor escrutinio de la seguridad en el ámbito tecnológico.

El caso de Huawei ha tenido un impacto importante en el ámbito diplomático, generando tensiones y desafíos en las relaciones internacionales. Las tensiones diplomáticas entre China y varios países, especialmente Estados Unidos, se intensificaron debido al caso Huawei. Esto afectó las relaciones bilaterales y la cooperación en cuestiones globales y repercute en la formación de alianzas y bloques.

Por otro lado, el caso Huawei ha tenido importantes consecuencias económicas a nivel global, afectando múltiples sectores y empresas en todo el mundo, la exclusión de Huawei de ciertos mercados y proyectos de infraestructura tuvo un impacto económico en la empresa y sus socios comerciales. Esto se pudo reflejar en las restricciones comerciales que suponen una gran cantidad y por consiguiente han afectado sus ingresos y ganancias. La empresa ha tenido que buscar mercados alternativos y ajustar sus estrategias comerciales.

En resumen, el caso Huawei entre 2018 y 2023 tuvo un impacto profundo en la tecnología, la geopolítica, la economía y la seguridad cibernética a nivel internacional. Las causas subyacentes y los efectos resultantes de este caso continúan siendo temas de debate y análisis en todo el mundo.

Interrogante científica:

- Las preocupaciones de seguridad cibernética en torno a Huawei han sido un tema candente en la escena internacional.
- Los gobiernos y las organizaciones internacionales han expresado temores acerca de posibles vulnerabilidades en los productos de Huawei.
- La relación de Huawei con el gobierno chino ha suscitado preocupaciones sobre la posible influencia estatal en la empresa.
- A raíz de estas preocupaciones, varios países han restringido o prohibido el uso de equipos de Huawei en infraestructuras críticas.
- Estas decisiones han desencadenado tensiones comerciales y diplomáticas a nivel global.
- Huawei, por su parte, ha buscado expandirse en nuevos mercados y reducir su dependencia de los países que le han impuesto restricciones.

Al terminar la presente investigación, se responde la siguiente interrogante científica: ¿Cuáles son las preocupaciones de seguridad cibernética planteadas por los gobiernos y las organizaciones internacionales en relación con Huawei, y de qué manera estas inquietudes han impactado en las decisiones de políticas y comerciales a nivel internacional en la época 2018-2023?

Este cuestionamiento profundiza en un tema que combina tecnología, geopolítica y economía, ofreciendo una visión integral de las implicaciones de seguridad cibernética relacionadas con esta empresa china de telecomunicaciones en el escenario global.

Objetivo General

Analizar de manera integral la importancia de la ciberseguridad corporativa en el contexto de la dinámica internacional de la era digital, utilizando el caso de Huawei (2018-2023) como estudio de caso, y examinar su impacto en las relaciones diplomáticas, la economía global y la seguridad cibernética a nivel internacional.

Objetivos Específicos

1. Investigar los retos y preocupaciones asociados con la seguridad cibernética en torno a Huawei, incluyendo su presunta vinculación con el gobierno chino y el impacto en las relaciones internacionales, la reputación empresarial y la posición en el mercado global.

2. Examinar las decisiones gubernamentales y regulatorias tomadas por varios países en relación con Huawei, como la exclusión de la empresa de proyectos de infraestructura crítica y la imposición de restricciones comerciales y sus implicaciones

3. Explicar las percepciones de expertos en ciberseguridad corporativa y gubernamental en Costa Rica sobre las prácticas, desafíos y tendencias actuales en el ámbito de la seguridad digital, con el fin de identificar áreas clave de mejora y fortalecer la colaboración entre el sector público y privado en la prevención y respuesta ante posibles riesgos cibernéticos.

4. Explorar el marco legal y regulador que aborde de manera efectiva los aspectos legales y jurídicos relacionados con la seguridad cibernética.

Justificación

El análisis de la importancia de la ciberseguridad corporativa dentro de la dinámica internacional de la era digital, con un enfoque en el caso de Huawei en el período de 2018 a 2023, tiene una justificación sólida debido a su relevancia en múltiples aspectos. Aquí están algunas razones que respaldan la importancia de este análisis:

Era digital y dependencia tecnológica: En la era digital, la dependencia de la tecnología y las redes de comunicación es crítica para la economía global. La infraestructura digital es la columna vertebral de las operaciones comerciales, la comunicación, la defensa nacional y más. Cualquier amenaza a la ciberseguridad corporativa en este contexto puede tener efectos devastadores a nivel nacional e internacional.

Caso Huawei y geopolítica: El caso Huawei no se limita a preocupaciones técnicas; tiene importantes implicaciones geopolíticas. Las acusaciones de espionaje y las restricciones comerciales relacionadas con Huawei han llevado a tensiones internacionales y han sido un punto focal en la competencia geopolítica entre Estados Unidos y China.

Seguridad nacional y privacidad de datos: La seguridad de las redes y equipos de telecomunicaciones es vital para la seguridad nacional y la privacidad de datos de los ciudadanos. Los gobiernos de todo el mundo están luchando por equilibrar la innovación tecnológica con la protección de datos sensibles y la seguridad de las comunicaciones.

Impacto en las empresas y la economía: El caso Huawei ha tenido un impacto significativo en la empresa y la economía global. Ha llevado a restricciones comerciales que afectan a empresas en todo el mundo que dependen de la cadena de suministro tecnológico global. También ha impulsado la inversión en la seguridad cibernética corporativa y la búsqueda de alternativas tecnológicas.

Lecciones aprendidas: El caso Huawei proporciona lecciones importantes sobre la necesidad de una ciberseguridad sólida, la evaluación de riesgos y la gestión de proveedores de tecnología en la era digital. Estas lecciones son relevantes para empresas y gobiernos en todo el mundo a medida que enfrentan desafíos similares.

Relevancia global de Huawei: Huawei es una de las empresas de tecnología más grandes y prominentes a nivel mundial, con una presencia significativa en el mercado de telecomunicaciones y tecnología de la información. Su impacto internacional y su papel como proveedor líder de equipos de red y tecnología 5G hacen que cualquier problema relacionado con su ciberseguridad tenga repercusiones globales.

Avances tecnológicos y vulnerabilidades: En la era digital, la tecnología está en constante evolución. Los avances como el despliegue de redes 5G presentan oportunidades emocionantes, pero también crean nuevas vulnerabilidades cibernéticas. Analizar la ciberseguridad de Huawei proporciona información vital sobre cómo las tecnologías emergentes están siendo manejadas en términos de seguridad.

Normas y regulaciones internacionales: La situación de Huawei ha llevado a debates sobre las normas y regulaciones internacionales en torno a la ciberseguridad corporativa. Examinar cómo diferentes países han respondido a las preocupaciones de seguridad puede proporcionar información valiosa sobre la necesidad de normativas globales más sólidas y coherentes en el ámbito de la ciberseguridad.

El análisis de la importancia de la ciberseguridad corporativa en el contexto de la era digital y el caso de Huawei durante el período de 2018 a 2023 es esencial para comprender cómo la seguridad cibernética se ha convertido en un tema clave en la geopolítica, la economía global y la seguridad nacional. El impacto internacional de este caso subraya la necesidad de abordar los desafíos de ciberseguridad de manera integral y colaborativa en el entorno digital actual.

Antecedentes

Desde hace unas décadas, el estudio de la ciberseguridad en general ha despertado el interés entre los investigadores. La ciberseguridad corporativa ha evolucionado significativamente en respuesta a una serie de amenazas y desafíos en la dinámica internacional a lo largo de los años. A continuación, se presentan algunos antecedentes clave sobre la ciberseguridad corporativa en el contexto internacional:

Al ser un término bastante reciente, no existían investigaciones específicas sobre el tema, pero se pueden encontrar algunas prácticas o esfuerzos de ciberseguridad en el mismo momento que se comenzaron a desarrollar las redes en las computadoras, ya que empezaron a surgir amenazas, pero solo se podían dar de manera física. No fue hasta finales de los años sesenta, posterior a la invención del internet, cuando ace el ciberespacio, que al mismo tiempo permitió que se dieran los ciberataques.

Es el 30 de noviembre de 1988 cuando la disciplina de la ciberseguridad se formaliza a través de la institución ACM (Association for Computing Machinery) (EuroInnova International Online Education, s.f.). (ACM (Association for Computing Machinery), 1988). Esta se creó con el fin de hacer conciencia acerca de los riesgos que pueden llegar a darse por causas de los ciberataques. Asimismo, otro objetivo de la ciberseguridad era generar la transformación digital en los sistemas informáticos, cosa que se logró con la protección de datos y sistemas requeridos.

Esta iniciativa evidenció la necesidad de abordar amenazas digitales emergentes. La creación de la ACM subrayó el papel crucial de la ciberseguridad en la transformación digital, destacando la importancia de proteger datos y sistemas para garantizar la seguridad y eficiencia de los sistemas informáticos. Este evento histórico refleja el reconocimiento oficial de los desafíos en la seguridad cibernética y la búsqueda activa de soluciones efectivas.

Entre los primeros antecedentes, se puede encontrar el trabajo titulado: ‘'La Industria 4.0: El Estado de la Cuestión ‘' por Raúl Blanco, Jordi Fontrodona y Carmen Poveda (2017). Aunque esta investigación no se refiera en su totalidad a cómo opera la ciberseguridad, y esto debido a la época en que se encuentra, es de bastante importancia, ya que sirve como referencia para señalar que, en esa época, la industria estaba pasando por una transformación digital.

Posteriormente, se plantea lo favorable que ha sido la incorporación de internet y cómo facilita los procesos necesarios en la industria: “Cada vez más dispositivos estarán enriquecidos con informática incrustada y conectados por medio de tecnologías estándar. Esto permite a los dispositivos de campo comunicarse e interactuar entre ellos y con los controladores centrales” (Blanco, 2017, p152)

El párrafo citado destaca una tendencia importante en la tecnología: la creciente integración de la informática en una amplia variedad de dispositivos y su interconexión mediante tecnologías estándar. Esto tiene varias implicaciones significativas: mayor interconexión, eficiencia y automatización, estándares tecnológicos, pero al mismo tiempo expone los desafíos de seguridad, ya que a medida que más dispositivos se conectan, la seguridad cibernética se convierte en una preocupación crítica.

Posteriormente, se plantean la necesidad de hacer frente a los desafíos de seguridad con lo siguiente:

> Ciberseguridad: el aumento de la conectividad que representa la Industria 4.0 incrementa dramáticamente la necesidad de proteger los sistemas industriales críticos y las líneas de producción contra las amenazas informáticas. También hay que mejorar la protección de la propiedad intelectual, los datos personales y la privacidad. (Raúl Blanco, 2017, p.153).

Es bastante importante lo indicado anteriormente, ya que es donde se hace mención sobre ciberseguridad en una época donde apenas venía surgiendo. Además, señala puntos clave que subrayan la importancia de proteger adecuadamente los sistemas industriales y la información en este entorno, tales como: datos personales y privacidad y el enfoque integral de la ciberseguridad.

Para resumir, el aumento de la conectividad en la industria 4.0 ofrece beneficios significativos en términos de eficiencia y automatización, pero también plantea desafíos sustanciales en términos de ciberseguridad. La protección de sistemas críticos, propiedad intelectual, datos personales y la privacidad deben ser prioridades para las organizaciones que operan en este entorno tecnológicamente avanzado.

Parte de lo que ahora corresponde a la disciplina de la ciberseguridad y toda su trayectoria se ha presentado como un reto, ya que los ciberataques se pueden concebir como fenómenos que atacan de diferentes formas, es necesario resaltar los avances en el conocimiento sobre cómo identificar y prevenir un eventual ciberataque y qué herramientas se posee en la actualidad con el fin de responder a ello sin poner en riesgo una compañía.

Para el año 2023, José M. González González en su trabajo de investigación "Uso de las técnicas del hacking ético para la reducción de amenazas de ciberseguridad", apunta que cuando se habla de un hacker, se tiende a asociarlo a una persona dañina, con malas intenciones que pretenden robar u obtener información de manera ilícita, pero se tiende a ignorar su fortaleza: habilidades avanzadas en el manejo de computadoras.

El conocimiento de cómo opera un hacker es importante, ya que las personas que conforman una empresa pueden responder de manera efectiva a estos ataques, es necesaria la aplicación de habilidades avanzadas en sistemas de computación y que utilicen su conocimiento por el bien común de la empresa (González). Falta poner el año

Según Luis Felipe Guillermo García Forero, en su trabajo "Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo", dentro de la ciberseguridad existen cuatro pasos fundamentales que fueron definidos en el marco de ciberseguridad del NIST (National Institute of Standards and Technology), que son fundamentales para el conocimiento de cualquier compañía:

1) Identificar: A nivel de organización es necesario tener una comprensión organizacional para poder llevar a cabo el riesgo de seguridad cibernética tanto para los sistemas como las personas, datos, etc. Esto también consiste en comprender el contexto empresarial, es decir, los recursos que respaldan las funciones críticas y los riesgos de seguridad cibernética relacionados dan paso a que una organización priorice sus esfuerzos de manera consistente con su estrategia de gestión de riesgos y sus necesidades empresariales.

2) Proteger: Se trata de desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos. Esta función admite la capacidad de limitar o contener el impacto de un posible evento de seguridad cibernética.

3) Detectar: Desarrollar e implementar patrones para identificar la ocurrencia de un evento de seguridad cibernética. La función Detectar permite el descubrimiento oportuno de eventos de seguridad cibernética para así tener el tiempo suficiente de prepararse. La detección oportuna de eventos de seguridad cibernética es fundamental para responder de manera efectiva a las amenazas. Cuanto antes se identifique un evento o una anomalía, más rápida y eficaz será la respuesta, lo que puede reducir el daño potencial.

4) Responder: Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad cibernética. La función Responder respalda la capacidad de contener el impacto de un posible incidente de seguridad cibernética. La función Responder en la gestión de seguridad cibernética es un componente crítico en la protección de una organización contra amenazas cibernéticas.

5) Recuperar: Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética. La función Recuperar en la gestión de seguridad cibernética desempeña un papel fundamental en la garantía de la continuidad de los negocios y la resiliencia de una organización frente a incidentes cibernéticos.

En el trabajo de Luis Felipe Guillermo García Forero se destaca la importancia de seguir los cuatro pasos fundamentales en el marco de ciberseguridad de la NIST para proteger las organizaciones. El proceso comienza con la identificación, que implica comprender el contexto empresarial y priorizar los esfuerzos de gestión de riesgos. Luego, la protección se centra en desarrollar e implementar medidas de seguridad para garantizar la entrega de servicios críticos y limitar el impacto de posibles eventos de seguridad cibernética.

La detección se vuelve crucial al desarrollar patrones para identificar oportunamente eventos cibernéticos, permitiendo una respuesta efectiva que reduzca el daño potencial. Por último, la respuesta y la recuperación son esenciales para contener incidentes y mantener la resiliencia, asegurando la continuidad de los negocios frente a amenazas cibernéticas. Este enfoque integral subraya la necesidad de una gestión proactiva y estratégica de la seguridad digital en las organizaciones.

Hasta ahora, se ha analizado los antecedentes y la evolución de la ciberseguridad corporativa, destacando la importancia de proteger los sistemas y datos en un mundo cada vez más digitalizado. Esta sólida base en ciberseguridad corporativa facilitará comprender mejor cómo se aplican estos principios en el caso de estudio: Huawei, una empresa líder en tecnología de telecomunicaciones y equipos de red que ha estado en el centro de la atención global en relación con la seguridad cibernética y la geopolítica. Para comprender completamente el contexto de este caso, es esencial considerar los antecedentes tanto de la empresa como de las preocupaciones de seguridad cibernética que la rodean.

Desde una perspectiva comercial, es importante destacar lo dicho por Oviedo Guachamin en su trabajo "Análisis de la guerra comercial China - Estados Unidos a partir del caso Huawei", el cual plantea que, en guerras comerciales, es un juego de suma 0 donde no hay ganador, pero que pone en evidencia sin duda la competencia comercial entre China y EE. UU. y su lucha por tener la hegemonía comercial a nivel mundial, que esto llevó a recorrer otros horizontes como la tecnología. (Oviedo Guachamín, 2021).

Sin duda esta relación que destaca la autora resalta la complejidad de las guerras comerciales y cómo estas pueden impactar la economía global. En un mundo interconectado, es fundamental reconocer que las decisiones económicas y comerciales tienen ramificaciones que trascienden las fronteras nacionales, y la cooperación internacional puede ser clave para evitar resultados perjudiciales para todas las partes involucradas.

Por otro lado, existe la relación entre el caso Huawei y la ciberseguridad. En este punto, es importante señalar el trabajo que se remonta a los años 2021-2022 bajo el nombre de: "Ciberseguridad y redes 5G en las relaciones internacionales: el caso de Huawei", de Mireia Martin Porras, el cual da más contexto en lo referente al caso de estudio e incorpora otro tema importante, que es la inclusión de las redes 5G como una de las estrategias comerciales de China (Porras, 2021-2022).

Proyecciones

Proyectar el análisis de la importancia de la ciberseguridad corporativa en el contexto de la era digital, específicamente a través del caso de Huawei (2018-2023) y su impacto internacional, implica considerar las tendencias y desafíos que podrían surgir en el futuro cercano.

Intensificación de la regulación y normativas: Es probable que las regulaciones y normativas internacionales en torno a la ciberseguridad corporativa se vuelvan más estrictas y específicas. Los gobiernos y las organizaciones podrían implementar estándares más rigurosos para garantizar la seguridad de las infraestructuras críticas y los datos sensibles del usuario (Maroto, 2009).

La intensificación de la regulación y normativas en ciberseguridad refleja la creciente conciencia sobre la importancia de proteger las infraestructuras críticas y los datos sensibles. Se espera que gobiernos y organizaciones adopten estándares más estrictos para fortalecer la seguridad cibernética. Este enfoque busca abordar las amenazas digitales de manera más específica y efectiva, garantizando la integridad y confidencialidad de la información. La adaptación a normativas más rigurosas no solo protege a las empresas, sino que también contribuye a la seguridad general de la sociedad en la era digital.

Mayor enfoque en la evaluación de riesgos de proveedores: Las empresas y los gobiernos podrían prestar más atención a la evaluación de riesgos de proveedores de tecnología, especialmente en el caso de empresas multinacionales como Huawei. Se podrían implementar procesos más detallados para asegurar que los productos y servicios de empresas tecnológicas sean seguros y no tengan vulnerabilidades explotables.

Lo anterior destaca la importancia de garantizar la seguridad en la cadena de suministro tecnológico. Este enfoque sugiere la posible implementación de procesos más detallados para asegurar que los productos y servicios tecnológicos sean seguros y estén libres de vulnerabilidades. La evaluación minuciosa de riesgos es esencial para mitigar amenazas y proteger la integridad de sistemas críticos. En un entorno digital cada vez más complejo, este mayor escrutinio de proveedores refleja la necesidad de robustecer las defensas contra posibles vulnerabilidades explotables.

Enfoque en la transparencia y auditorías independientes: Para recuperar la confianza perdida, las empresas tecnológicas podrían optar por ser más transparentes sobre sus prácticas de seguridad. Las auditorías independientes podrían convertirse en una norma para garantizar la integridad de los productos y servicios tecnológicos.

Mayor inversión en investigación y desarrollo en ciberseguridad: Ante la creciente sofisticación de las amenazas cibernéticas, se espera que las empresas inviertan más en investigación y desarrollo para crear soluciones de ciberseguridad avanzadas. Esto podría llevar a avances significativos en la detección y mitigación de amenazas cibernéticas.

Colaboración internacional en ciberseguridad: Los países y las organizaciones podrían aumentar la colaboración internacional en temas de ciberseguridad. La cooperación en el intercambio de información sobre amenazas y mejores prácticas podría ayudar a fortalecer las defensas cibernéticas en todo el mundo.

Mayor conciencia pública sobre ciberseguridad: A medida que la conciencia pública sobre la importancia de la ciberseguridad aumente, los consumidores podrían volverse más exigentes en cuanto a la seguridad de los productos y servicios que utilizan. Esto podría presionar a las empresas para que mejoren sus estándares de seguridad.

Protección de la privacidad y datos del usuario: La ciberseguridad corporativa también tiene un impacto directo en la privacidad y seguridad de los datos de los usuarios finales. Las vulnerabilidades en productos y servicios pueden llevar a la exposición y explotación de datos sensibles, lo que resalta la importancia de un análisis detenido de la ciberseguridad en empresas como Huawei.

Normas y regulaciones internacionales: La situación de Huawei ha llevado a debates sobre las normas y regulaciones internacionales en torno a la ciberseguridad corporativa. Examinar cómo diferentes países han respondido a las preocupaciones de seguridad puede proporcionar información valiosa sobre la necesidad de normativas globales más sólidas y coherentes en el ámbito de la ciberseguridad.

Avances tecnológicos y vulnerabilidades: En la era digital, la tecnología está en constante evolución. Los avances como el despliegue de redes 5G presentan oportunidades emocionantes, pero también crean nuevas vulnerabilidades cibernéticas. Analizar la ciberseguridad de Huawei proporciona información vital sobre cómo las tecnologías emergentes están siendo manejadas en términos de seguridad.

En los próximos años, se esperan desarrollos significativos en el ámbito de la ciberseguridad corporativa, especialmente en casos de empresas líderes como Huawei. La

industria y los gobiernos probablemente respondan a los desafíos emergentes con regulaciones más estrictas, tecnologías más avanzadas y una mayor colaboración internacional para proteger los sistemas y datos en la era digital.

CAPÍTULO II

Marco Histórico

La última década ha sido testigo de una rápida transformación global con la proliferación de la tecnología digital. Este es el momento de entrada de la era digital. En este contexto, la ciberseguridad corporativa se ha convertido en el bastión esencial para proteger la integridad, confidencialidad y disponibilidad de los datos. El presente análisis abordará el periodo 2018-2023 y se adentrará en la evolución de la ciberseguridad empresarial a nivel internacional, focalizándose en el caso de Huawei.

La ciberseguridad surgió con la interconexión de equipos y el desarrollo de redes de computadoras, un hito que tuvo lugar en la década de 1950 con la creación de las primeras redes informáticas y módems. Su consolidación como disciplina definida comenzó en la década de 1960, adoptando la forma que reconocemos en la actualidad (Prieto, 2023).

En otras palabras, la evolución de la ciberseguridad desde la interconexión de equipos en la década de 1950 hasta su consolidación como una disciplina definida en la década de 1960 refleja la creciente importancia de proteger la información en el entorno digital emergente. Este periodo inicial marcó el inicio de un proceso continuo de adaptación y desarrollo de medidas de seguridad, enfrentando los desafíos cambiantes de la tecnología y las amenazas cibernéticas.

La comprensión de estos hitos históricos es esencial para apreciar la complejidad actual de la ciberseguridad y su papel crucial en la protección de la integridad de datos en la era digital. La historia de la ciberseguridad no abarca tantos años como se podría imaginar; de hecho, se gesta a partir de la segunda mitad del siglo XX y ha experimentado diversas etapas hasta alcanzar su estado actual.

A lo largo de la historia, la digitalización ha sido un motor clave para el aumento de las amenazas cibernéticas. Desde la adopción generalizada de las tecnologías de la información hasta la interconexión global de sistemas, varias etapas históricas han contribuido al cambio en la naturaleza y la magnitud de las amenazas cibernéticas.

1) Era de las computadoras personales (1970-1980):

El surgimiento de las computadoras personales marcó el inicio de la digitalización. A medida que más individuos y empresas adoptaron estas tecnologías, la ciberdelincuencia tendría más oportunidades de desplegar sus garras. Comenzaron a surgir los primeros virus y malwares, al detectar vulnerabilidades en los sistemas operativos de los principiantes en internet y que no conocían el significado de ciberseguridad (S., 2002). Poner apellido completo

El párrafo destaca el impacto significativo del surgimiento de las computadoras personales en el inicio de la era de la digitalización. La adopción generalizada de estas tecnologías por parte de individuos y empresas se presenta como un catalizador para el crecimiento de la ciberdelincuencia. La metáfora "desplegar sus garras" sugiere la amenaza y la expansión de actividades maliciosas en este nuevo panorama tecnológico.

2) Expansión de internet (1990-2000):

La digitalización se generalizó en la década de 1990, abriendo un mundo de posibilidades, pero también exponiendo nuevas tácticas de ataque. El correo electrónico se convirtió en un vector común para ataques de phishing y los primeros ataques distribuidos de denegación de servicio (DDoS) demostraron la vulnerabilidad de las redes conectadas. (Medina Martínez, 2021)

Lo anterior resalta la paradoja de la década de 1990, donde la generalización de la digitalización ofreció un vasto panorama de oportunidades, pero también introdujo nuevos riesgos. Se destaca el papel crucial del correo electrónico como un vector frecuente para ataques de phishing, subrayando la amenaza a la seguridad cibernética. Además, la mención de los primeros ataques distribuidos de denegación de servicio (DDoS) subraya la vulnerabilidad inherente de las redes conectadas en esa época.

3) Era de la movilidad y la nube (2000-2010):

Hasta las últimas fechas se extiende más aún la digitalización, con la proliferación de dispositivos móviles y servicios en la nube. El robo de datos personales y la explotación de vulnerabilidades en aplicaciones móviles se convirtieron en amenazas comunes. Los

ciberdelincuentes también han comenzado a centrarse en el ransomware que cifra datos críticos para obtener rescates (Chacín, 2017).

Se destaca la expansión continua de la digitalización durante la era de la movilidad y la nube (2000-2010), con el auge de dispositivos móviles y servicios en la nube. Se subraya la amenaza persistente del robo de datos personales y la explotación de vulnerabilidades en aplicaciones móviles, evidenciando la complejidad de la seguridad en este entorno tecnológico.

4) Internet de las cosas (2010 en adelante):

La Internet de las cosas (IoT), también conocida como internet de los objetos, está destinada a transformar fundamentalmente la realidad, incluyéndonos a nosotros mismos. Aunque esta afirmación pueda parecer audaz, se puede reflexionar sobre el impacto que la Internet ha tenido en la educación, la comunicación, los negocios, la ciencia, el gobierno y la sociedad en general. Es innegable que la Internet se ha convertido en una de las creaciones más influyentes y poderosas en la historia de la humanidad.

La IoT representa la próxima fase evolutiva de la Internet, prometiendo un avance significativo en su capacidad para recopilar, analizar y distribuir datos que pueden ser transformados en información, conocimiento y, en última instancia, sabiduría. En este contexto, la importancia de la IoT se vuelve evidente.

Actualmente, ya se están implementando proyectos relacionados con la IoT que ofrecen la posibilidad de reducir las disparidades entre las clases sociales, mejorar la distribución de los recursos mundiales hacia aquellos que más los necesitan y permitir comprender el planeta de una manera que nos haga más proactivos y menos reactivos. Sin embargo, persisten diversos desafíos que podrían obstaculizar el desarrollo de la IoT, como la transición a IPv6, la necesidad de establecer estándares comunes y el desarrollo de fuentes de energía para millones, e incluso miles de millones, de sensores diminutos (Evans, 2011).

Lo anterior destaca la implementación actual de proyectos vinculados a la Internet de las cosas (IoT), que prometen abordar las disparidades sociales, mejorar la distribución de recursos y proporcionar una comprensión más proactiva de nuestro planeta. A pesar de estos avances, se mencionan desafíos persistentes que podrían obstaculizar el desarrollo de la IoT,

como la transición a IPv6, la necesidad de estándares comunes y el desarrollo de fuentes de energía para los numerosos sensores diminutos. Esta dualidad entre el potencial transformador y los desafíos pendientes destaca la complejidad y la importancia de la evolución de la IoT en la sociedad actual.

A pesar de estos obstáculos, a medida que empresas, gobiernos, entidades de normalización y universidades trabajen colaborativamente para superar estos desafíos, la IoT continuará progresando. En consecuencia, el propósito de este trabajo es proporcionar una comprensión clara y accesible sobre todo lo relacionado con la IoT, permitiéndole al lector estar bien informado y apreciar el potencial transformador que posee para alterar nuestra comprensión actual del mundo.

Ahora que todo tipo de dispositivos diarios se conectan con el Internet de las cosas (IoT), la superficie de ataque se ha vuelto extremadamente vasta. Ataques realizados contra dispositivos IoT, como cámaras de seguridad y electrodomésticos conectados, han hecho manifiestas las preocupaciones de seguridad en una sociedad interconectada (Díaz, 2019).

La creciente interconexión a través del Internet de las cosas (IoT) ha expandido de manera significativa la superficie de ataque, abarcando desde dispositivos cotidianos hasta electrodomésticos conectados. Este aumento en la conectividad ha llevado a una mayor exposición a amenazas de seguridad.

Ataques dirigidos contra dispositivos IoT, como cámaras de seguridad y electrodomésticos, han puesto de manifiesto las legítimas preocupaciones sobre la seguridad en una sociedad cada vez más interconectada. La necesidad de medidas robustas de ciberseguridad se vuelve evidente en un entorno donde la vulnerabilidad de estos dispositivos puede tener implicaciones directas en la privacidad y seguridad de los usuarios (Yancey, 2017).

Los ataques específicos contra dispositivos IoT, como cámaras de seguridad y electrodomésticos, subrayan preocupaciones legítimas sobre la seguridad en una sociedad cada vez más interconectada. Este escenario resalta la necesidad urgente de implementar medidas sólidas de ciberseguridad, ya que la vulnerabilidad de estos dispositivos podría tener consecuencias directas en la privacidad y seguridad de los usuarios. La referencia a Yancey

(2017) respalda la importancia de abordar estos riesgos emergentes y destaca la relevancia continua de la ciberseguridad en un entorno digital en constante evolución.

Marco Conceptual

La era digital representa un período histórico marcado por la omnipresencia y la influencia significativa de la tecnología digital en la sociedad y la economía a nivel mundial. Se caracteriza por la transición de sistemas analógicos a digitales en diversas áreas, como las comunicaciones, la información, el entretenimiento y la gestión de datos.

La relevancia global de la era digital radica en su capacidad para transformar fundamentalmente la forma en que se interactúa, comunica, trabaja y accede a la información. La digitalización ha acelerado el ritmo de la innovación, permitiendo avances tecnológicos rápidos y la creación de redes interconectadas a escala global. Esto ha dado lugar a nuevas oportunidades, pero también ha planteado desafíos relacionados con la privacidad, la seguridad cibernética y la brecha digital.

Contextualización de la Importancia de la Ciberseguridad Corporativa en la Dinámica Internacional de la Era Digital y su Impacto Internacional

La era digital ha marcado una transformación significativa en la forma como las empresas operan a nivel mundial. Con la rápida adopción de tecnologías de la información y comunicación (TIC), las organizaciones han experimentado un aumento exponencial en la interconexión global, lo que ha llevado a una mayor vulnerabilidad frente a amenazas cibernéticas.

Interconexión Global y Riesgos Cibernéticos

La interconexión global de empresas a través de redes digitales crea oportunidades sin precedentes, pero también expone a las organizaciones a riesgos cibernéticos que trascienden las fronteras nacionales. La seguridad de la información se convierte en un elemento esencial para proteger los activos digitales y mantener la confidencialidad, integridad y disponibilidad de la información en un entorno internacional donde las amenazas pueden originarse desde cualquier punto del globo (Yocupicio, 2020).

La creciente interconexión global de empresas a través de redes digitales ha generado oportunidades inéditas, pero conlleva riesgos cibernéticos que trascienden fronteras nacionales. En este contexto, la seguridad de la información emerge como un elemento esencial para salvaguardar activos digitales y preservar la confidencialidad, integridad y disponibilidad de la información.

La referencia a Emiko Yocupicio (2020) destaca la importancia de abordar las amenazas en un entorno internacional, donde los riesgos pueden surgir desde cualquier punto del globo. Este enfoque integral es fundamental para mantener la resiliencia en un mundo cada vez más interconectado digitalmente.

Impacto en la Economía Global

El impacto de incidentes cibernéticos en la economía global es significativo. La pérdida de datos confidenciales, interrupciones en la cadena de suministro y la desconfianza resultante pueden afectar no solo a la empresa afectada, sino también a sus socios comerciales y a la economía en general. La ciberseguridad corporativa se convierte así en un componente crítico para salvaguardar la estabilidad económica y la competitividad internacional.

Lo anterior destaca de manera acertada la magnitud del impacto de los incidentes cibernéticos en la economía global. La pérdida de datos confidenciales, las interrupciones en la cadena de suministro y la consecuente desconfianza no solo afectan a la empresa directamente involucrada, sino también reverberan en sus socios comerciales y tienen ramificaciones para la economía en su conjunto.

En este escenario, la ciberseguridad corporativa emerge como un componente crítico, no solo para proteger los activos digitales de una entidad, sino también para salvaguardar la estabilidad económica y preservar la competitividad internacional en un entorno empresarial cada vez más interconectado.

Confianza y Reputación Empresarial

En un mundo interconectado, la confianza es un activo invaluable. Incidentes de seguridad pueden socavar la confianza de los clientes, inversores y socios comerciales, afectando la reputación de una empresa a nivel mundial. La ciberseguridad corporativa se

posiciona como un elemento clave para mantener la confianza en un entorno digital donde la percepción de seguridad puede tener repercusiones inmediatas y duraderas.

Lo previamente destacado hace referencia a que la confianza se erige como un activo inestimable. Los incidentes de seguridad pueden minar la confianza de clientes, inversores y socios comerciales, impactando la reputación de una empresa a nivel global. En este contexto, la ciberseguridad corporativa se erige como un elemento crucial para preservar la confianza en un entorno digital donde la percepción de seguridad puede tener repercusiones inmediatas y duraderas. Es un recordatorio contundente de que la seguridad digital no solo protege activos, sino que también resguarda la piedra angular de relaciones comerciales exitosas: la confianza.

Regulación Internacional y Responsabilidad Corporativa

La dinámica internacional de la era digital también se ve influenciada por regulaciones y estándares internacionales en constante evolución. Las empresas se enfrentan a la responsabilidad de cumplir con normativas de ciberseguridad que buscan proteger los intereses nacionales y globales. La implementación efectiva de medidas de ciberseguridad no solo es una exigencia regulatoria, sino un acto de responsabilidad corporativa en la preservación de la estabilidad digital internacional.

Introducción al Caso Específico de Huawei y su Posición en el Ámbito Internacional

En la última década, Huawei, la gigante tecnológica con sede en China, ha emergido como una fuerza dominante en el panorama global de las telecomunicaciones y la tecnología. Su ascenso meteórico ha estado marcado por innovaciones tecnológicas, extensas inversiones en investigación y desarrollo, y una rápida expansión en mercados internacionales. Sin embargo, este éxito también ha venido acompañado de una creciente atención y escrutinio, especialmente en el ámbito de la ciberseguridad corporativa.

Historia y Trayectoria de Huawei

Huawei fue fundada en 1987 por Ren Zhengfei y ha experimentado una evolución extraordinaria desde sus humildes comienzos en Shenzhen, China. Inicialmente enfocada en la fabricación de equipos de telecomunicaciones, la compañía ha diversificado su cartera para abarcar una amplia gama de productos, desde *smartphones* hasta infraestructura de red y

soluciones de nube. Su ascenso ha sido impulsado por una estrategia agresiva de expansión global y una reputación por ofrecer tecnología de vanguardia a precios competitivos.

Posicionamiento Internacional

En la última década, Huawei ha logrado establecerse como un jugador clave en el mercado internacional de telecomunicaciones, compitiendo directamente con empresas occidentales establecidas. Su despliegue de tecnología 5G ha sido especialmente destacado, ganando contratos en múltiples países y consolidando su posición como uno de los principales proveedores de equipos de red a nivel mundial. Este rápido ascenso ha desafiado las dinámicas tradicionales del sector, generando tanto admiración como preocupación en diferentes partes del mundo.

Desafíos y Controversias en Ciberseguridad

A pesar de sus éxitos, Huawei ha enfrentado una serie de controversias relacionadas con la seguridad de sus productos y su presunta cercanía al gobierno chino. Varios países, liderados por Estados Unidos, han expresado preocupaciones sobre posibles riesgos de seguridad asociados con la participación de Huawei en el despliegue de infraestructuras críticas, argumentando que la empresa podría facilitar el espionaje cibernético por parte del gobierno chino. Estas preocupaciones han llevado a restricciones y prohibiciones en el uso de tecnología de Huawei en ciertos países.

Impacto Internacional y Reacciones

Las tensiones en torno a la seguridad cibernética han tenido un impacto significativo en la expansión global de Huawei. La empresa se ha visto envuelta en una compleja red geopolítica, con decisiones de países y operadores de telecomunicaciones que reflejan la delicada balanza entre la innovación tecnológica, la seguridad nacional y la competencia global. Las reacciones a las preocupaciones de ciberseguridad han variado, desde restricciones comerciales hasta acuerdos de seguridad y debates sobre la autonomía tecnológica.

Definición de la Era Digital y su Impacto en la Forma en que las Empresas Operan

La "era digital" se refiere a la época en la que la tecnología digital, la conectividad en red y la información electrónica han pasado a ser fundamentales en todas las facetas de la sociedad y la economía. Este periodo ha transformado radicalmente la manera en que las empresas operan, interactúan con sus clientes y competidores y gestionan sus procesos internos. El impacto de la era digital en el entorno empresarial es multifacético y abarca diversas áreas cruciales (Gates, 1999).

Este cambio ha provocado una transformación radical en la operación de las empresas, en su interacción con clientes y competidores, y en la gestión de procesos internos. El comentario destaca la multifacética influencia de la era digital en el entorno empresarial, subrayando su impacto significativo y omnipresente en diversas áreas cruciales.

Conectividad Ubicua

La era digital se caracteriza por la omnipresencia de la conectividad. La proliferación de internet y la expansión de las redes de comunicación han creado un entorno donde la información fluye sin restricciones, permitiendo una comunicación instantánea y un intercambio de datos en tiempo real. Las empresas se benefician al poder colaborar con socios en cualquier parte del mundo y acceder a mercados globales de manera más eficiente (Eduardo O. Sosa, 2014).

El concepto de conectividad ubicua, delineado por Eduardo O. Sosa (2014), resalta la omnipresencia de la conectividad en la era digital. La expansión de internet y las redes de comunicación ha creado un entorno donde la información fluye libremente, posibilitando una comunicación instantánea y un intercambio de datos en tiempo real. Este fenómeno no solo redefine la forma en que las empresas operan, sino que también les brinda la capacidad de colaborar con socios en cualquier lugar del mundo y acceder a mercados globales de manera más eficiente. La conectividad ubicua se presenta como un pilar fundamental en la dinámica actual de los negocios, permitiendo una interconexión global sin precedentes.

Big Data y Analítica Avanzada

La era digital ha generado una explosión de datos, conocida como *Big Data*. Las empresas ahora tienen acceso a cantidades masivas de información sobre el comportamiento

de los consumidores, tendencias del mercado y operaciones internas. La capacidad de recopilar, procesar y analizar estos datos ha permitido a las empresas tomar decisiones más informadas, personalizar sus estrategias y mejorar la eficiencia operativa (García, 2023).

La era digital ha desencadenado una explosión de datos, comúnmente denominada *Big Data*. Este fenómeno ha otorgado a las empresas acceso a vastas cantidades de información sobre el comportamiento de los consumidores, tendencias del mercado y operaciones internas. La capacidad para recopilar, procesar y analizar estos datos ha brindado a las empresas la oportunidad de tomar decisiones más informadas, personalizar estrategias y mejorar significativamente la eficiencia operativa. En este contexto, el *Big Data* se ha convertido en un recurso invaluable que potencia la toma de decisiones estratégicas en la dinámica empresarial actual.

Automatización y Transformación Digital

La digitalización ha impulsado la automatización de procesos empresariales. La transformación digital implica la integración de tecnologías digitales en todos los aspectos de una empresa, desde la gestión de la cadena de suministro hasta el servicio al cliente. La automatización de tareas repetitivas libera recursos humanos para actividades más estratégicas y creativas, mejorando la agilidad y la competitividad de las empresas (Guerra, 2017).

En un mundo cada vez más digital, la automatización se ha convertido en una especie de aliado empresarial. La transformación digital va más allá de adoptar tecnologías digitales; implica integrarlas en todos los rincones de una empresa. Este cambio no solo simplifica procesos, sino que también libera a las personas de tareas monótonas, permitiéndoles enfocarse en labores más estratégicas y creativas. Es como darles a las empresas un respiro digital que les permite ser más ágiles y competitivas. En definitiva, la automatización no solo es eficiencia, sino también la oportunidad de dar lo mejor de nosotros en lo que realmente importa.

Cambio en la Interacción con el Cliente

La era digital ha redefinido la forma en que las empresas se relacionan con sus clientes. Las redes sociales, plataformas de comercio electrónico y aplicaciones móviles han

creado canales directos de comunicación, permitiendo una interacción más personalizada. Las empresas deben adaptarse a las expectativas de los consumidores, ofreciendo experiencias digitales satisfactorias y utilizando datos para comprender y anticipar las necesidades de los clientes (Lalaleo-Analuisa, Bonilla-Jurado, & Robles-Salguero, 2021).

La investigación de Lalaleo-Analuisa, Bonilla-Jurado y Robles-Salguero (2021) respalda esta perspectiva, subrayando la importancia de la adaptación estratégica en un entorno empresarial cada vez más digitalizado. En la era digital, la relación entre empresas y clientes ha experimentado una metamorfosis significativa.

La presencia en redes sociales, plataformas de comercio electrónico y aplicaciones móviles ha trazado nuevos caminos para la comunicación directa, permitiendo una interacción más personalizada y cercana. En este contexto, la adaptación a las expectativas del consumidor se vuelve crucial. Las empresas deben ofrecer experiencias digitales satisfactorias y aprovechar los datos para comprender y anticipar las necesidades de sus clientes

Principales Avances Tecnológicos en la Era Digital:

Internet de las cosas (*Internet of things* (IoT))

La interconexión de dispositivos físicos a través de internet ha permitido la recopilación y el intercambio de datos en tiempo real. Esto ha llevado al desarrollo de soluciones inteligentes para hogares, ciudades y empresas.

Inteligencia Artificial (IA) y Aprendizaje Automático

Los avances en algoritmos de aprendizaje automático y la capacidad de procesamiento han impulsado la adopción de la inteligencia artificial. Esto se refleja en asistentes virtuales, sistemas de recomendación, automatización de procesos y aplicaciones más inteligentes.

Computación en la Nube

La computación en la nube ha revolucionado la forma en que las empresas almacenan, acceden y procesan datos. Proporciona flexibilidad, escalabilidad y acceso remoto a recursos informáticos, reduciendo la dependencia de infraestructuras físicas.

Blockchain y Tecnologías de Registro Distribuido (DLT)

La tecnología *blockchain* ha introducido un enfoque descentralizado y seguro para realizar transacciones y gestionar registros. Se ha aplicado en sectores como finanzas, logística y salud para garantizar la transparencia y la seguridad.

Realidad Aumentada (AR) y Realidad Virtual (VR)

La AR y la VR han transformado la experiencia del usuario al superponer información digital en el mundo real o sumergir a los usuarios en entornos virtuales. Se utilizan en juegos, educación, medicina y entrenamiento empresarial.

5G y Conectividad Ultrarrápida

La implementación de redes 5G ha llevado la conectividad a un nivel superior, ofreciendo velocidades de transmisión de datos más rápidas y una menor latencia. Esto habilita aplicaciones como vehículos autónomos, IoT a gran escala y servicios de transmisión de alta calidad.

Ciberseguridad Avanzada

El aumento de amenazas cibernéticas ha impulsado el desarrollo de tecnologías avanzadas de ciberseguridad. Esto incluye soluciones basadas en inteligencia artificial para la detección y prevención de ataques, así como encriptación y autenticación mejoradas.

Robótica Avanzada

La robótica ha evolucionado con robots más autónomos, capaces de realizar tareas complejas en entornos diversos. Desde la fabricación hasta la atención médica, los robots están desempeñando roles importantes en diversas industrias.

Biometría y Reconocimiento Facial

Avances en tecnologías biométricas, como el reconocimiento facial, han mejorado la autenticación y la seguridad. Se utiliza en sistemas de acceso, pagos móviles y aplicaciones de seguridad.

Impresión 3D

La impresión 3D ha cambiado la fabricación al permitir la creación de objetos tridimensionales a partir de modelos digitales. Se aplica en la producción de prototipos, piezas personalizadas y hasta en la construcción de viviendas.

Vehículos Autónomos

La combinación de sensores avanzados, inteligencia artificial y conectividad ha permitido el desarrollo de vehículos autónomos. Esto tiene implicaciones significativas en el transporte y la logística.

Edge Computing:

La computación en el borde (*edge computing*) lleva el procesamiento de datos más cerca de la fuente de origen, reduciendo la latencia y mejorando la eficiencia en entornos donde la velocidad de respuesta es crítica.

Identificación de las Oportunidades y Desafíos de la Era Digital

Oportunidades

Innovación Disruptiva

La era digital ofrece oportunidades para la innovación disruptiva, permitiendo a las empresas transformar modelos de negocio existentes y crear nuevos productos y servicios.

Acceso Global a Mercados

La conectividad digital facilita el acceso a mercados globales, permitiendo a las empresas expandirse internacionalmente y llegar a nuevos clientes de manera más eficiente.

Eficiencia Operativa

Las tecnologías digitales, como la automatización y la inteligencia artificial, permiten mejoras significativas en la eficiencia operativa, reduciendo costos y aumentando la productividad.

Personalización y Experiencia del Cliente

La era digital proporciona la capacidad de personalizar productos y servicios según las preferencias individuales de los clientes, mejorando la experiencia del cliente y fortaleciendo la lealtad.

Colaboración Remota

La digitalización facilita la colaboración remota, permitiendo a equipos de trabajo distribuidos trabajar de manera efectiva y superar barreras geográficas.

Desarrollo Sostenible

Las tecnologías digitales pueden utilizarse para abordar desafíos medioambientales y promover prácticas empresariales sostenibles, desde la gestión eficiente de recursos hasta la reducción de emisiones.

Desafíos

Ciberseguridad y Amenazas Digitales

El aumento de la conectividad también ha llevado a un aumento en las amenazas cibernéticas. Garantizar la seguridad de datos y sistemas se ha vuelto un desafío crítico para las empresas.

Brecha Digital

A pesar del avance digital, existe una brecha digital global donde algunas regiones o grupos de personas tienen un acceso limitado a la tecnología, creando disparidades económicas y sociales.

Privacidad de Datos

La recopilación masiva de datos plantea preocupaciones sobre la privacidad. Las empresas deben abordar la gestión ética de la información personal y cumplir con regulaciones de privacidad.

Desplazamiento Laboral

La automatización y la inteligencia artificial pueden conducir al desplazamiento de trabajadores en ciertos sectores, creando desafíos en la recualificación y adaptación de la fuerza laboral.

Dependencia Tecnológica

La dependencia excesiva de la tecnología puede hacer a las empresas vulnerables a interrupciones, ya sea por fallas técnicas, ciberataques u otros problemas.

Rápida Obsolescencia Tecnológica

La velocidad a la que evolucionan las tecnologías puede llevar a la obsolescencia rápida de infraestructuras y sistemas, requiriendo una adaptación constante.

Desafíos Regulatorios

La falta de regulaciones actualizadas puede dificultar la gestión de nuevas tecnologías, mientras que regulaciones excesivas pueden obstaculizar la innovación y el crecimiento.

Amenazas Geopolíticas

En un entorno globalizado, tensiones geopolíticas pueden afectar la colaboración internacional y la libre circulación de datos, creando incertidumbre para las empresas internacionales.

Riesgos Éticos y Sociales

La adopción de tecnologías como la inteligencia artificial plantea cuestiones éticas y sociales, desde la discriminación algorítmica hasta la pérdida de empleo en ciertos sectores.

Definición de Ciberseguridad Corporativa y su Papel en la Protección de la Información

La ciberseguridad corporativa se refiere al conjunto de prácticas, procesos, tecnologías y políticas diseñadas para proteger los sistemas, redes, datos y activos digitales de una organización contra amenazas cibernéticas. Estas amenazas pueden incluir ataques

maliciosos como el *malware*, el *phishing*, el *ransomware*, así como intrusiones y violaciones de seguridad. El objetivo principal de la ciberseguridad corporativa es garantizar la confidencialidad, integridad y disponibilidad de la información, mitigando los riesgos asociados con la creciente complejidad y sofisticación de las amenazas cibernéticas.

Papel en la Protección de la Información

Confidencialidad

La ciberseguridad corporativa se centra en preservar la confidencialidad de la información, asegurando que solo aquellos con autorización puedan acceder a datos sensibles. Esto se logra a través de prácticas como el cifrado de datos y el control de acceso.

Integridad

Garantizar la integridad de la información implica prevenir la alteración no autorizada de los datos. La ciberseguridad implementa medidas para detectar y prevenir cambios no deseados en la información, asegurando su exactitud y fiabilidad.

Disponibilidad

La disponibilidad de los sistemas y datos es esencial para el funcionamiento continuo de una organización. La ciberseguridad se ocupa de proteger contra ataques que buscan interrumpir o negar el acceso legítimo a servicios y recursos digitales.

Prevención de Ataques

La ciberseguridad busca prevenir una variedad de ataques cibernéticos, desde *malware* hasta ataques de denegación de servicio. Esto se logra mediante la implementación de *firewalls*, antivirus, sistemas de detección de intrusiones y otras herramientas especializadas.

Gestión de Identidad y Acceso

Controlar y gestionar de manera eficiente las identidades y los accesos es fundamental en ciberseguridad corporativa. Se establecen políticas y procedimientos para garantizar que solo personas autorizadas tengan acceso a sistemas y datos específicos.

Concientización y Capacitación

La ciberseguridad no solo se trata de tecnología, sino también de las personas. Programas de concientización y capacitación educan a los empleados sobre buenas prácticas de seguridad, reduciendo el riesgo de errores humanos que podrían comprometer la seguridad.

Respuesta ante Incidentes

A pesar de las medidas preventivas, los incidentes de seguridad pueden ocurrir. La ciberseguridad corporativa incluye planes de respuesta ante incidentes para minimizar el impacto de cualquier violación de seguridad y restaurar la normalidad operativa de manera rápida y efectiva.

Cumplimiento Normativo:

Las organizaciones están sujetas a regulaciones y normativas que exigen la implementación de medidas de seguridad. La ciberseguridad corporativa garantiza el cumplimiento de estos requisitos, lo que puede incluir normativas sobre privacidad de datos, protección de la información financiera, entre otros.

Enumeración de Amenazas Cibernéticas Comunes en Entornos Empresariales

Malware

Incluye virus, gusanos, troyanos y *ransomware* que infectan sistemas y redes, comprometiendo la integridad y confidencialidad de la información.

Phishing

Intentos fraudulentos de obtener información sensible, como contraseñas o datos financieros, haciéndose pasar por entidades confiables a través de correos electrónicos, mensajes de texto o sitios web falsos.

Ataques de Ingeniería Social

Manipulación psicológica de individuos para obtener información confidencial o persuadirlos a realizar acciones que comprometan la seguridad de la empresa.

Ataques de Denegación de Servicio (DDoS)

Sobrecargan sistemas, redes o servicios con tráfico falso, impidiendo el acceso legítimo y afectando la disponibilidad de los recursos.

Inyección de Código SQL

Ataques que aprovechan vulnerabilidades en las bases de datos al insertar código SQL malicioso, permitiendo a los atacantes acceder o manipular datos.

Ataques de Fuerza Bruta

Intentos repetidos y automatizados para adivinar contraseñas o claves de acceso, generalmente mediante la prueba de múltiples combinaciones.

Exploits de Vulnerabilidades:

Aprovechamiento de fallos de seguridad en sistemas operativos, aplicaciones o *software* para obtener acceso no autorizado o realizar acciones maliciosas.

Intercepción de Datos (*Sniffing*)

Monitorización no autorizada del tráfico de red para capturar información sensible, como contraseñas o datos confidenciales.

Secuestro de Sesiones (*Session Hijacking)*

Toma de control de una sesión de usuario activa para realizar acciones en nombre del usuario, comprometiendo su identidad.

***Backdoors* y Puertas Traseras**

Creación de accesos secretos no autorizados en sistemas, permitiendo a los atacantes ingresar y controlar sistemas sin ser detectados.

Rogue Software y Adware:

Instalación no autorizada de *software* malicioso o no deseado que puede afectar el rendimiento del sistema y recopilar datos sin consentimiento.

Ataques a Dispositivos Conectados (IoT)

Vulnerabilidades en dispositivos IoT pueden ser explotadas para acceder a redes empresariales, exponiendo datos y comprometiendo la seguridad.

Riesgos en la Nube

Problemas de configuración, accesos no autorizados o fallos de seguridad en servicios en la nube pueden resultar en la pérdida de datos o la exposición de información sensible.

Ransomware:

Encripta archivos o sistemas, exigiendo un rescate para restaurar el acceso. Puede causar pérdida de datos críticos y tiempo de inactividad.

Ataques a la Cadena de Suministro

Incluyen la manipulación de productos o servicios en la cadena de suministro para introducir *malware* o comprometer la seguridad de una organización.

La enumeración de estas amenazas cibernéticas destaca la diversidad y sofisticación de los riesgos a los que las empresas están expuestas en el entorno digital actual. La conciencia, la educación y la implementación de medidas de seguridad efectivas son fundamentales para mitigar estos riesgos y proteger la integridad de la información empresarial.

Marco referencial

Teoría Realista

En el contexto de la ciberseguridad corporativa de Huawei (2018-2023), una perspectiva realista se enfocaría en el poder y la competencia entre actores estatales y no estatales en el ámbito internacional (Blinder, 2021). Según la teoría realista, las empresas, en su búsqueda de maximizar el poder y la influencia, enfrentan amenazas y oportunidades en el ciberespacio. La importancia de la ciberseguridad para Huawei se analizaría en función de su capacidad para proteger sus intereses y datos sensibles frente a amenazas cibernéticas, ya

que cualquier vulnerabilidad podría ser explotada por competidores o actores estatales, afectando su posición en el mercado global.

Desde una perspectiva realista, según Blinder (2021), el análisis de la ciberseguridad de Huawei (2018-2023) se centra en el poder y la competencia a nivel internacional. Según esta teoría, las empresas, al buscar maximizar su poder, enfrentan amenazas y oportunidades en el ciberespacio. La importancia de la ciberseguridad para Huawei se evalúa en función de su capacidad para proteger sus datos frente a amenazas de competidores o actores estatales, lo que podría afectar su posición en el mercado global.

Teoría Constructivista

En una perspectiva constructivista, el análisis se centraría en cómo las percepciones, identidades y construcciones sociales influyen en la importancia atribuida a la ciberseguridad corporativa. En este caso, se exploraría cómo las acciones y declaraciones de Huawei respecto a la ciberseguridad contribuyen a la construcción de normas y valores compartidos en la comunidad internacional. La importancia de la ciberseguridad se entendería en términos de cómo las prácticas y discursos de Huawei afectan su reputación y la manera en que es percibida por otros actores internacionales, lo que a su vez impacta sus relaciones comerciales y su posición en el escenario global (Mg. Pedro J. Saldarriaga-Zambrano, 2026)

Desde una perspectiva constructivista, según Mg. Pedro J. Saldarriaga-Zambrano (2026), el análisis de la ciberseguridad de Huawei se adentraría en cómo las percepciones, identidades y construcciones sociales dan forma a la importancia otorgada a la seguridad digital corporativa. Este enfoque explora cómo las acciones y declaraciones de Huawei respecto a la ciberseguridad contribuyen a la formación de normas y valores compartidos a nivel internacional. La relevancia de la ciberseguridad se entendería en función de cómo las prácticas y discursos de Huawei moldean su reputación, afectando la manera en que es percibida por otros actores internacionales. En este marco, se sugiere que estas percepciones influyen en las relaciones comerciales y la posición de Huawei en el escenario global, destacando el papel de la construcción social en la dinámica de ciberseguridad.

Teoría de la Interdependencia Compleja

La teoría de la interdependencia compleja, desarrollada por Robert Keohane y Joseph Nye, se enfoca en las múltiples formas de interconexión entre actores internacionales y destaca la importancia de la cooperación en situaciones de interdependencia. En el caso de la ciberseguridad de Huawei (2018-2023), la teoría de la interdependencia compleja podría destacar cómo las acciones de la empresa afectan y son afectadas por otros actores, como gobiernos, competidores y consumidores, en un entorno altamente interconectado. La importancia de la ciberseguridad para Huawei se analizaría en términos de cómo sus decisiones y prácticas pueden tener ramificaciones en la estabilidad y la seguridad de la dinámica internacional en la era digital (Cordero, 2014).

La teoría de la interdependencia compleja, según Cordero (2014), destaca la conexión entre actores internacionales y resalta la importancia de la cooperación. En el caso de la ciberseguridad de Huawei (2018-2023), se enfocaría en cómo las acciones de la empresa impactan y son impactadas por otros actores en un entorno altamente interconectado. La relevancia de la ciberseguridad para Huawei se analizaría en términos de cómo sus decisiones pueden influir en la estabilidad y seguridad en la dinámica internacional de la era digital.

Teoría de Seguridad Corporativa

La teoría de seguridad corporativa aborda la seguridad en el ámbito empresarial, reconociendo que las empresas pueden ser actores significativos en asuntos de seguridad, tanto a nivel nacional como internacional. En el caso de Huawei, la teoría de seguridad corporativa podría analizar cómo la empresa se asegura contra amenazas cibernéticas, protege sus activos y datos, y cómo estas medidas afectan su posición en el escenario global (Rosete, 2020).

La importancia de la ciberseguridad para Huawei se comprendería en función de su capacidad para salvaguardar sus operaciones y proteger la integridad de la información, así como para mantener la confianza de los clientes y socios internacionales en un entorno digital complejo y potencialmente hostil.

CAPÍTULO III: MARCO METODOLÓGICO

El marco metodológico es una parte esencial de cualquier investigación, ya que proporciona la estructura y el enfoque que guiarán el estudio. En este contexto, el marco metodológico se encarga de definir las estrategias, métodos y técnicas que serán empleados para llevar a cabo la investigación de manera efectiva y alcanzar los objetivos planteados.

Enfoque de la investigación

Esta investigación se enmarca en el enfoque cualitativo, esto por su capacidad para explorar en profundidad las dimensiones humanas, sociales y políticas de las cuestiones de seguridad cibernética en el caso de Huawei, lo que es esencial para una comprensión completa de este tema complejo.

La utilización de entrevistas en profundidad con expertos en ciberseguridad, funcionarios gubernamentales y representantes de Huawei, junto con la incorporación de documentos y comunicados de prensa, es una estrategia integral para obtener una comprensión completa de las preocupaciones y acusaciones en torno a la seguridad cibernética de Huawei. Las decisiones gubernamentales y regulatorias a menudo involucran a múltiples partes interesadas, como legisladores, agencias gubernamentales, empresas, expertos en seguridad cibernética y grupos de defensa de la privacidad. Descubrir sobre cuáles son sus preocupaciones y argumentos es clave para la investigación

Por otro lado, las acusaciones y preocupaciones de seguridad cibernética suelen estar vinculadas a percepciones y opiniones. Un enfoque cualitativo es ideal para explorar estas percepciones y entender cómo impactan en la reputación y la percepción internacional de Huawei. El objetivo de evaluar cómo las lecciones aprendidas del caso Huawei pueden influir en las prácticas empresariales y gubernamentales relacionadas con la seguridad cibernética es intrínsecamente cualitativo. Este enfoque permitirá capturar las ideas, percepciones y recomendaciones de los expertos en ciberseguridad y de los actores involucrados.

Incorporar entrevistas en profundidad y análisis cualitativo para explorar cómo las lecciones del caso Huawei pueden influir en las prácticas empresariales y gubernamentales

relacionadas con la seguridad cibernética permitirá una comprensión más profunda de los aspectos cualitativos y las percepciones en juego.

Diseño

La presente investigación está basada en un diseño de investigación-acción, la cual se puede comprender como "el estudio de un contexto social donde mediante un proceso de investigación con pasos "en espiral", se investiga al mismo tiempo que se interviene" (León y Montero, 2002, citado en citado en Hernández, Fernández y Baptista, 2010, p. 509). "La investigación-acción construye el conocimiento por medio de la práctica" (p. 510).

En otras palabras, la investigación-acción es una metodología valiosa que, en lugar de realizar una investigación puramente teórica o abstracta, se centra en la comprensión y mejora de situaciones reales a través de la práctica. Por otro lado, busca comprender y mejorar situaciones sociales a través de la práctica activa y la adaptación continua. Al combinar la investigación y la intervención, se pueden lograr resultados más efectivos en la resolución de problemas y la generación de conocimiento práctico.

Un diseño de investigación-acción centrado en el análisis de la importancia de la ciberseguridad corporativa dentro de la dinámica internacional de la era digital, con un enfoque en el caso de Huawei (2018-2023) y su impacto internacional, podría abordarse de la siguiente manera:

Fase 1: Diagnóstico y Planificación

Identificación de los *stakeholders*: Se trata de determinar quiénes son los principales actores involucrados, como Huawei, gobiernos, organizaciones internacionales, competidores y otros interesados.

Definición de objetivos: Establecer los objetivos de la investigación, como comprender el impacto de las preocupaciones sobre ciberseguridad en Huawei y su influencia en la dinámica internacional.

Selección de métodos de recopilación de datos: Elegir los métodos de investigación, como entrevistas, análisis de documentos, encuestas y observación directa.

Recopilación de datos iniciales: Iniciar la recopilación de datos relevantes sobre el tema, incluyendo informes, noticias, declaraciones de la empresa, y regulaciones gubernamentales.

Fase 2: Análisis y Reflexión

Análisis de datos iniciales: Evaluar los datos recopilados para identificar patrones, tendencias y temas relacionados con la ciberseguridad en el caso de Huawei.

Identificación de problemas y desafíos: Identificar las preocupaciones y desafíos clave en relación con la ciberseguridad en Huawei y su impacto internacional.

Desarrollo de hipótesis: Desarrollo de hipótesis sobre cómo estas preocupaciones pueden haber afectado la posición de Huawei en el mercado internacional.

Fase 3: Intervención y acción diseño de intervenciones: Propuesta sobre posibles acciones o soluciones para abordar las preocupaciones de ciberseguridad en Huawei y su impacto en la dinámica internacional.

Implementación de Intervenciones: Llevar a cabo acciones específicas, como recomendar mejores prácticas de ciberseguridad a Huawei, o promover la cooperación internacional en cuestiones de ciberseguridad.

Fase 4: Evaluación y aprendizaje evaluación de resultados: Consiste en evaluar el impacto de las intervenciones en relación con la ciberseguridad en Huawei y su posición internacional.

Reflexión y aprendizaje: Reflexionar sobre las lecciones aprendidas durante el proceso de investigación-acción y cómo podrían aplicarse en futuros casos similares.

Fase 5: Comunicación y difusión informe y difusión: Comunicar los hallazgos de la investigación y las lecciones aprendidas a través de informes, presentaciones o publicaciones académicas.

Este diseño de investigación-acción permitirá una comprensión más profunda de la importancia de la ciberseguridad en el contexto de la era digital, con un enfoque específico

en Huawei y su impacto internacional. Además, se fomentará la acción y la toma de decisiones informadas para abordar los desafíos en este ámbito.

Fuentes

Una fuente de información es todo aquello que proporciona datos para reconstruir hechos y las bases del conocimiento (Rivera, 2015). En otras palabras, las fuentes de información proporcionan una comprensión fundamental sobre la importancia de las fuentes en la construcción del conocimiento y la reconstrucción de hechos. Las fuentes de información son los cimientos de la investigación y el aprendizaje, ya que brindan datos, evidencia y contexto necesarios para entender y analizar eventos pasados y actuales. Las fuentes se dividen en primarias y secundarias

Fuentes primarias

Son las que proporcionan datos e información original y directa sobre un tema en específico. En este caso, las fuentes primarias podrían incluir entrevistas con expertos en ciberseguridad, funcionarios gubernamentales y representantes de Huawei, documentos internos de la empresa, comunicados de prensa y declaraciones públicas de Huawei.

La incorporación de fuentes primarias en la investigación proporcionará información de primera mano y perspectivas únicas sobre el caso Huawei y la ciberseguridad corporativa en la era digital. Estas fuentes pueden enriquecer significativamente el estudio y darle una profundidad adicional.

Para esto, es necesario desarrollar un plan detallado que incluya la identificación de los entrevistados, la preparación de preguntas abiertas y específicas, y la logística para llevar a cabo las entrevistas. Es preciso obtener el consentimiento informado de los entrevistados y de respetar los protocolos éticos de investigación.

Por otro lado, intentar tener acceso a documentos internos de Huawei y establecer un proceso para recopilarlos. Esto podría implicar la colaboración directa con la empresa o la obtención de documentos a través de fuentes confiables, con el fin de poder tener más información que enriquece la investigación. Esto con el fin de poder examinar políticas, procedimientos, comunicaciones internas y cualquier otro documento que arroje luz sobre la ciberseguridad corporativa de la empresa.

Utilizar múltiples fuentes primarias en la investigación no solo fortalecerá la validez de los hallazgos, sino que también permitirá una comprensión más holística del tema. La triangulación, al cotejar los datos recopilados de diferentes fuentes, ayudará a identificar posibles discrepancias o puntos de convergencia en las evidencias. Al comparar las respuestas de las entrevistas con los documentos internos y las declaraciones públicas de Huawei, se podrá construir una narrativa coherente y sólida que respalde las conclusiones.

Fuentes secundarias

En lo que respecta a las fuentes secundarias, para utilizarlas en esta investigación es necesario tomar las siguientes pautas

Revisión de literatura: Utiliza libros, artículos académicos y revisiones de literatura para comprender las teorías existentes, los desarrollos históricos y los desafíos contemporáneos en ciberseguridad corporativa.

Artículos académicos y revistas especializadas: Busca artículos en revistas académicas de seguridad cibernética, relaciones internacionales y tecnología que aborden el caso de Huawei y la ciberseguridad corporativa. Estas fuentes suelen proporcionar un análisis profundo y actualizado.

Libros y monografías: Explorar libros académicos y monografías que se centren en la ciberseguridad corporativa en el contexto de la era digital y examinen el caso de Huawei. Pueden proporcionar una visión más completa y detallada.

Informes y documentos de organizaciones internacionales

Organizaciones como la ONU, la OTAN o la Unión Europea publican informes relacionados con la ciberseguridad y la dinámica internacional. Estos documentos pueden ofrecer una visión de alto nivel sobre las preocupaciones internacionales en torno a Huawei.

Artículos de prensa y medios de comunicación: Las principales publicaciones y medios de comunicación a menudo cubren cuestiones de seguridad cibernética y su impacto en Huawei. Estos artículos pueden proporcionar información actualizada y diversas perspectivas.

Documentos gubernamentales y regulaciones: Consulta los informes y regulaciones emitidos por gobiernos y agencias de seguridad cibernética en relación con Huawei. Estos documentos pueden reflejar las políticas y decisiones gubernamentales.

Bases de datos en línea: Utiliza bases de datos académicas y de investigación en línea, como Google Scholar, JSTOR o ProQuest, para buscar artículos y estudios relevantes relacionados con ciberseguridad y Huawei.

Entrevistas y discursos: Busca entrevistas y discursos de expertos en seguridad cibernética, funcionarios gubernamentales y líderes de la industria que puedan ofrecer ideas valiosas sobre el tema.

Población muestra:

La definición de la población muestra implica considerar a cada individuo como parte integrante de un conjunto de elementos que abarca personas, objetos y organismos involucrados en el problema de investigación. Es esencial delimitar claramente esta población en términos de su contenido, ubicación y período temporal, reconociendo así la singularidad de cada componente y su relevancia para el estudio.

Para los fines de la presente investigación, la población corresponde a personas expertas en tecnología con un nivel de conocimiento desde básico hasta avanzado en ciberseguridad, así como a personas abogadas con conocimientos sobre el marco legal pertinente.

Esta población incluye a todas aquellas personas físicas y jurídicas que participan activamente en las actividades relacionadas con la tecnología y la ciberseguridad, así como en la interpretación y aplicación del marco legal, durante el período comprendido entre 2018 y 2023.

Tabla 1:

Entrevistado	Puesto	Razon
#1: Silvia Hidalgo Barrantes	Seguridad Informática MICITT	Contexto sobre el marco legal informatico Importancia ciberseguridad
#2: David Meza Reyes	Seguridad Informatica	Importancia ciberseguridad
#3: Lic. Olman Mora Cruz	Abogado	Contexto sobre el marco legal informatico
#4: Mario Cordero Gomez	Experto en Informatica	Importancia ciberseguridad

Análisis Comparativo

Unidad de análisis

Importancia de la ciberseguridad corporativa en el contexto de la dinámica internacional de la era digital, en relación con el caso de Huawei.

Instrumentos

Los instrumentos se refieren a las herramientas, métodos, técnicas o dispositivos utilizados para recopilar datos y obtener información relevante para el estudio. Estos instrumentos son esenciales para llevar a cabo investigaciones de manera sistemática y obtener resultados válidos (Hernández, 2020).

En otras palabras, los instrumentos son herramientas esenciales en la caja de herramientas de un investigador, y su elección y uso adecuados desempeñan un papel fundamental en la calidad y la validez de la investigación. La comprensión de los instrumentos disponibles y su aplicación adecuada es esencial para llevar a cabo investigaciones efectivas y obtener resultados significativos.

Para efectos de esta investigación, con el objetivo 1, 2 y 3 se utilizará como instrumento la revisión bibliográfica, la cual consiste en la operación documental de recuperar un conjunto de documentos o referencias bibliográficas que se publican en el mundo sobre un tema, un autor, una publicación o un trabajo específico (Goris, 2015).

Para el objetivo 1, la revisión bibliográfica aportará de manera significativa en los siguientes aspectos:

Para investigar las preocupaciones y acusaciones relacionadas con la seguridad cibernética en torno a Huawei, incluyendo su presunta vinculación con el gobierno chino y su impacto en la percepción internacional de la empresa, es importante buscar fuentes académicas, informes de expertos y noticias actualizadas que aborden este tema desde diversas perspectivas.

Con el objetivo 2, la revisión bibliográfica será útil porque:

Se obtendrán fuentes que aborden este tema desde diferentes perspectivas y que incluyan información sobre las políticas y medidas adoptadas por los gobiernos, tales como:

Búsqueda de documentos oficiales emitidos por gobiernos, agencias de seguridad nacional y reguladores que detallen las decisiones y políticas relacionadas con Huawei.

Informes y análisis realizados por expertos en seguridad cibernética, relaciones internacionales y políticas de tecnología.

Artículos de noticias de fuentes confiables que informen sobre las decisiones gubernamentales y sus consecuencias en la industria de tecnología y las relaciones internacionales.

Informes y publicaciones de organizaciones internacionales como la Unión Internacional de Telecomunicaciones (UIT) y la Organización Mundial del Comercio (OMC) que aborden el tema de las restricciones comerciales y las políticas comerciales globales.

Estudios de caso específicos que describan cómo países individuales han abordado la cuestión de Huawei en sus redes de telecomunicaciones y proyectos de infraestructura crítica.

Todo ello ayuda a entender las bases legales y normativas que respaldan las acciones gubernamentales, lo que es fundamental para analizar la legitimidad de estas medidas.

La revisión bibliográfica permite identificar tendencias y patrones en la toma de decisiones en diferentes países, lo que puede arrojar luz sobre la dinámica global en torno a la seguridad cibernética y la participación de empresas como Huawei.

En lo que respecta al objetivo 3, la utilidad de la revisión bibliográfica conlleva una base integral y fundada para abordar el objetivo, permitiendo una evaluación informada del papel de la ciberseguridad corporativa en la era digital y la influencia de las lecciones aprendidas del caso Huawei en las prácticas empresariales y gubernamentales relacionadas con la seguridad cibernética.

Esto permite situar el tema de la ciberseguridad corporativa en el contexto más amplio de la era digital, ya que facilita la comprensión de las tendencias, desafíos y avances recientes en el ámbito de la seguridad cibernética. Por otro lado, ayuda a identificar y seleccionar las teorías, modelos y marcos conceptuales relevantes para analizar la ciberseguridad corporativa.

Asimismo, proporciona una base teórica sólida para fundamentar y respaldar las conclusiones de la investigación. Facilita la recopilación y análisis de estudios, informes y análisis relacionados con el caso Huawei y sus implicaciones en términos de seguridad cibernética. También permite identificar patrones, mejores prácticas y posibles áreas de mejora a partir de las experiencias de otras organizaciones.

También, posibilita la exploración de la literatura relacionada con las prácticas empresariales y gubernamentales en el ámbito de la ciberseguridad y facilita la identificación de políticas, regulaciones y estrategias que puedan influir en la implementación de medidas de seguridad cibernética.

De igual manera, permite sintetizar la información recopilada, identificando conexiones y relaciones entre diversos estudios y perspectivas. También facilita la elaboración de una argumentación sólida y la formulación de conclusiones respaldadas por la literatura existente.

Finalmente, para el objetivo 4, se utilizará el instrumento de la entrevista a profundidad, la cual consiste en un proceso que se divide en dos fases; la primera denominada de correspondencia, donde el encuentro con el entrevistado, la recopilación de datos y el registro, son la base para obtener la información de cada entrevista. En la segunda, considerada de análisis, se estudiará con detenimiento cada entrevista y se asignarán temas

por categorías, con esto, se podrá codificar de manera eficiente toda la información para su futuro análisis (Robles, 2011).

En otras palabras, la entrevista a profundidad puede aportar varios beneficios significativos para el objetivo de evaluar el papel de la ciberseguridad corporativa en la era digital y cómo las lecciones aprendidas del caso Huawei pueden influir en las prácticas empresariales y gubernamentales relacionadas con la seguridad cibernética.

Lo que la entrevista a profundidad aportaría al objetivo 3, es lo siguiente:

Las entrevistas permiten obtener perspectivas prácticas de expertos y profesionales que trabajan en el campo de la ciberseguridad corporativa y las políticas gubernamentales relacionadas. Puedes obtener información de primera mano sobre las estrategias, desafíos y éxitos en la implementación de medidas de ciberseguridad.

Los entrevistados pueden ofrecer información sobre tendencias emergentes y desafíos futuros en el campo de la ciberseguridad. Esto es especialmente relevante en un entorno en constante evolución como el de la ciberseguridad.

Las entrevistas pueden utilizarse para validar los datos y conclusiones obtenidos de otras fuentes, como investigaciones documentales. Esto aumenta la confiabilidad de los resultados.

La realización de entrevistas a profundidad en el contexto del objetivo 4 de explorar el marco legal y regulador relacionado con la seguridad cibernética puede aportar varios beneficios importantes:

Las entrevistas permiten aclarar y comprender mejor las políticas, regulaciones y leyes existentes relacionadas con la seguridad cibernética. Los entrevistados, que pueden ser expertos legales o funcionarios gubernamentales, pueden proporcionar información detallada sobre el contenido y el alcance de estas políticas.

Los entrevistados pueden señalar las lagunas o desafíos legales que existen en el marco regulatorio actual en relación con la seguridad cibernética. Esto puede ayudar a identificar áreas donde se necesitan reformas o mejoras.

Las entrevistas pueden proporcionar perspectivas de expertos en derecho cibernético, que pueden explicar los aspectos legales y jurídicos complejos relacionados con la seguridad cibernética, como la privacidad de los datos, la ciberdelincuencia, la responsabilidad legal y la normativa de protección de datos.

En ambos casos, la entrevista a profundidad ofrece la posibilidad de recopilar información detallada y contextual sobre la ciberseguridad corporativa y el marco legal y regulador en ciberseguridad. Estas entrevistas pueden enriquecer la comprensión de los desafíos y las oportunidades en estas áreas y ayudar a identificar mejores prácticas y áreas de mejora. Además, permiten adentrarse en las experiencias, percepciones y perspectivas de expertos y actores clave, lo que agrega una dimensión humana y práctica a la comprensión de estos complejos temas.

Recolección y procesamiento de datos

La recolección de datos es el proceso de búsqueda, recolección y medición de datos de diferentes fuentes para obtener información sobre los procesos, servicios y productos de la empresa o negocio y poder evaluar dichos resultados y así poder tomar mejores decisiones (Morales, 2023).

En otras palabras, la recolección de datos es un pilar fundamental para la gestión empresarial moderna, ya que proporciona la información necesaria para evaluar el rendimiento y tomar decisiones estratégicas. La recolección de datos es esencial para obtener información valiosa que puede ayudar a las organizaciones a comprender mejor sus operaciones, evaluar el desempeño de productos o servicios y, en última instancia, tomar decisiones informadas.

Paso 1: Diseño de la Investigación

Definición de los objetivos de la investigación, las preguntas de investigación y los temas clave por explorar en las entrevistas.

Selección de los participantes para las entrevistas, incluyendo expertos en ciberseguridad, representantes de Huawei, funcionarios gubernamentales, académicos y otros actores relevantes.

Paso 2: Entrevistas a Profundidad

Realización de las entrevistas a profundidad con los participantes seleccionados. Las entrevistas deben ser estructuradas de acuerdo con los temas clave de la investigación.

Grabación de las entrevistas para capturar la información de manera precisa.

Paso 3: Transcripción y Análisis de Entrevistas

Transcripción de las entrevistas para convertir las grabaciones en texto escrito.

Análisis de las entrevistas para identificar patrones, temas recurrentes y perspectivas clave relacionadas con la ciberseguridad corporativa y el caso Huawei.

Codificación de la información, agrupando datos similares en categorías y subcategorías.

Paso 4: Revisión Bibliográfica

Realización de una revisión bibliográfica exhaustiva para recopilar datos secundarios relevantes sobre ciberseguridad, regulaciones, el caso Huawei y su impacto internacional.

Resumen y síntesis de los hallazgos de la literatura existente.

Paso 5: Integración de Datos

Integración de los datos de las entrevistas a profundidad y de la revisión bibliográfica, identificando conexiones y contrastes entre las perspectivas de los participantes y la información de la literatura.

Paso 6: Análisis de Datos Integrados

Análisis comparativo de los datos integrados para responder a las preguntas de investigación y evaluar el impacto de la ciberseguridad corporativa en el caso Huawei y la dinámica internacional.

Paso 7: Conclusiones y Resultados

Elaboración de conclusiones basadas en el análisis de datos integrados y discusión de las implicaciones para la ciberseguridad corporativa y la dinámica internacional en la era digital.

Paso 8: Redacción del Informe de Investigación

Redacción de un informe de investigación que presente de manera clara y estructurada los hallazgos, conclusiones y recomendaciones.

Este enfoque combinado de entrevistas a profundidad y revisión bibliográfica permitirá obtener una comprensión completa y enriquecedora del tema de investigación, explorando tanto las perspectivas de los actores clave como la información disponible en la literatura académica y técnica.

Revisión bibliográfica

La revisión bibliográfica se puede definir como un resumen detallado de varios libros y estudios sobre el tema por investigar. En lugar de simplemente reunir información, se ha seleccionado cuidadosamente las partes más importantes de cada fuente. Al leer, se obtendrá una visión general de lo que otros expertos han dicho sobre el tema. Se intentó conectar estas ideas para crear un mapa que va a ser útil para a entender mejor el enfoque de investigación.

Según Romero (2013) se define la revisión bibliográfica como el proceso de revisión realizado que sigue una metodología sistemática en la que se busca identificar cómo se diferencian, se contraponen o son similares los diversos aportes académicos.

La aplicación de este proceso permite correlacionar los distintos enfoques, dando lugar a una síntesis exhaustiva de los variados aportes que muestra la evolución del concepto alrededor de áreas temáticas y tipologías diferentes.

Entrevista a profundidad

En esta tesina, cuando se menciona la entrevista a profundidad, se hace referencia a conversaciones más detalladas. Es como ir más allá de respuestas simples. En lugar de solo preguntas y respuestas, se pretende buscar y explorar experiencias importantes. Como

entrevistador, el trabajo es escuchar atentamente y obtener detalles que no son tan evidentes, contribuyendo así a entender mejor el tema que se está investigando.

De acuerdo con Izcara (2023), la entrevista es una conversación que se establece entre entrevistador y entrevistado con un propósito más o menos concreto. A diferencia de la conversación cotidiana, la entrevista, como instrumento de indagación en la realidad social, es un acto de interacción verbal asimétrico.

El entrevistador controla el intercambio verbal, a través de la formulación de preguntas; no obstante, recae sobre el entrevistado la mayor parte del peso de la participación en dicho intercambio conversacional, siendo el sujeto-objeto de la entrevista. Esta dinámica subraya la importancia del rol del entrevistado en proporcionar información relevante y enriquecer el diálogo con su experiencia y conocimientos.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

En esta sección, se abordará el análisis de resultados, una fase crítica en cualquier trabajo de investigación bibliográfica. Este capítulo reviste una importancia fundamental en el estudio realizado, ya que brinda la oportunidad de presentar los datos recopilados durante el período de investigación. Además, estos datos son sometidos a un exhaustivo análisis y estudio por parte del investigador, con el propósito de llevar a cabo posteriormente su interpretación de manera rigurosa.

Preocupaciones y acusaciones relacionadas con la seguridad cibernética en torno a Huawei, incluyendo la presunta vinculación con el gobierno chino y su impacto en la percepción internacional de la empresa

Investigar las preocupaciones y acusaciones relacionadas con la seguridad cibernética en torno a Huawei no solo aborda cuestiones técnicas de seguridad, sino que también tiene ramificaciones significativas en términos de relaciones internacionales, reputación empresarial y posición en el mercado global. La relevancia radica en comprender y gestionar eficazmente estos aspectos para garantizar la sostenibilidad y éxito de la empresa en un entorno cada vez más interconectado.

El análisis detenido del documento "China y el 5G: entre el recurso y el ejercicio del poder" de Esteban Actis (2023) proporciona una visión profunda de las preocupaciones y acusaciones relacionadas con la seguridad cibernética en torno a Huawei, considerando su presunta vinculación con el gobierno chino y el impacto resultante en la percepción internacional de la empresa.

En el anterior documento se destaca que, en la última década, China ha consolidado su capacidad para configurar y controlar agendas a nivel global, aunque este despliegue no ha estado exento de cuestionamientos. Las acusaciones de apropiación indebida de propiedad intelectual, especialmente relacionadas con filtraciones de ciberespionaje, han llevado a medidas concretas, como el acuerdo de seguridad cibernética firmado en 2015 entre China y la Administración Obama. Sin embargo, los servicios de inteligencia estadounidenses denunciaron en 2018 que China no cumplía con los términos acordados.

El documento conjunto del Parlamento, Comisión y Consejo Europeo en 2019 describe la relación entre la Unión Europea y China como una "rivalidad sistémica", resaltando la falta de transparencia del gobierno chino en compromisos internacionales. La creación del Trade and Technology Council (TTC) en 2021, formado por Estados Unidos y la Unión Europea, evidencia la preocupación compartida sobre la tecnología china.

En el contexto de la pandemia del COVID-19, la denominada "diplomacia de las mascarillas" y la rápida recuperación económica de China contrastan con cuestiones como la censura en el acceso a internet, el sistema de crédito social y la represión a minorías étnicas, generando recelos internacionales y afectando la credibilidad china. Este análisis señala que las intenciones de China en política exterior, incluida la expansión de la red 5G, han carecido de credibilidad, según destacan encuestas del Pew Research Center.

En términos de poder blando, se destaca la importancia de las narrativas en la expansión de la red 5G, donde la batalla por la percepción se vuelve tan crucial como las ventajas técnicas y económicas. La necesidad de *Reshaping Global Image* emerge como imperativo para consolidar la influencia tecnológica china, especialmente en Occidente. En este contexto, la diplomacia digital y las estrategias de comunicación se erigen como herramientas fundamentales, permitiendo moldear percepciones y construir una narrativa favorable que trascienda las fronteras tecnológicas y culturales.

En el presente análisis, se incorpora una tabla detallada (Tabla 1) que resume las preocupaciones y acusaciones relacionadas con la seguridad cibernética en torno a Huawei. Esta tabla proporciona una visión organizada y concisa de los hallazgos derivados del examen del documento "China y el 5G: entre el recurso y el ejercicio del poder" citado anteriormente y otros documentos clave.

A través de esta representación visual, se busca destacar las diversas dimensiones que rodean este tema, abordando aspectos técnicos, políticos y económicos que tienen un impacto significativo en la posición de Huawei en el mercado global. Al integrar estas perspectivas interrelacionadas, se pretende ofrecer una comprensión integral de los desafíos y oportunidades que definen el papel de Huawei en la actualidad, permitiendo así una toma de decisiones más informada tanto a nivel nacional como internacional.

Tabla 1

Preocupaciones y acusaciones relacionadas con la seguridad cibernética en torno a Huawei

Punto de Análisis	**Hallazgos/Información**
Documento de referencia	"China y el 5G: entre el recurso y el ejercicio del poder" de Esteban Actis (2023).
Aspectos considerados en el análisis	Vinculación con el gobierno chino Impacto en relaciones internacionales, reputación empresarial y posición en el mercado global.
Contexto histórico y político	Consolidación de China a nivel global. Acuerdo de seguridad cibernética (2015). Denuncias de incumplimiento por servicios de inteligencia estadounidenses (2018).
Relación Unión Europea-China	"Rivalidad sistémica" según el documento conjunto (2019). Creación del Trade and Technology Council (TTC) en 2021.

Impacto de la pandemia del COVID-19	"Diplomacia de las mascarillas". Recuperación económica de China versus cuestiones de censura y represión a minorías.
Evaluación de la credibilidad china en política exterior	Carencia de credibilidad según encuestas política exterior del Pew Research Center. Contraste entre intenciones y acciones.
Poder blando y narrativas	Importancia de las narrativas en la expansión de la red 5G. Diplomacia digital y estrategias de comunicación como herramientas fundamentales.

Como se indicó, la Tabla 1 resume de manera sistemática las principales preocupaciones y acusaciones en torno a la seguridad cibernética de Huawei, basándose en el exhaustivo análisis del documento "China y el 5G: entre el recurso y el ejercicio del poder" de Esteban Actis (2023) y otras fuentes clave. Cada punto en la tabla representa una faceta específica que contribuye al entendimiento global de la problemática.

Documento de referencia

El estudio de Actis se erige como piedra angular en esta revisión bibliográfica, proporcionando una visión profunda de las conexiones entre Huawei y las inquietudes de seguridad cibernética. Actis examina meticulosamente la posible vinculación de la empresa con el gobierno chino, destacando la complejidad de estas relaciones y la influencia que ejercen en el panorama internacional. Al incluir este documento en la Tabla 1, se subraya la necesidad de contemplar las dimensiones geopolíticas al abordar las cuestiones de seguridad cibernética.

Aspectos considerados en el análisis

La Tabla 1 resalta dos aspectos fundamentales: la presunta vinculación de Huawei con el gobierno chino y las repercusiones en las relaciones internacionales, la reputación

empresarial y la posición en el mercado global. Estos aspectos, analizados detalladamente, revelan que las preocupaciones de seguridad cibernética no se limitan a problemas técnicos, sino que también influyen en aspectos cruciales para la empresa.

La inclusión de estos elementos busca proporcionar una comprensión completa de los desafíos multidimensionales que enfrenta Huawei, desde la perspectiva técnica hasta las implicaciones políticas y comerciales. Esta aproximación holística pretende servir como una herramienta analítica integral, facilitando una evaluación exhaustiva de los factores que impactan la posición y estrategias de Huawei en el complejo escenario internacional de las telecomunicaciones.

Contexto histórico y político

Al explorar el contexto histórico y político, se destaca la consolidación de China a nivel global y eventos clave como el acuerdo de seguridad cibernética en 2015. Esta información contextualiza las acusaciones de seguridad cibernética al mostrar cómo eventos y políticas anteriores han dejado una marca indeleble en las percepciones actuales. Revela la complejidad del entorno en el que Huawei opera y la necesidad de considerar no solo los eventos recientes, sino también la evolución a lo largo del tiempo.

Continuando con los hallazgos, se encontró la noticia titulada "Ciberespionaje, vetos y robo de patentes: Huawei en el punto de mira de la balcanización de internet" de J. M. Sánchez (2019). Esta proporciona un punto de partida fundamental para investigar a fondo las preocupaciones y acusaciones relacionadas con la seguridad cibernética de Huawei, incluyendo su presunta vinculación con el gobierno chino y el consecuente impacto en la percepción internacional de la empresa.

En el contexto de la guerra tecnológica entre Estados Unidos y China por el dominio de internet y las redes 5G, Huawei se encuentra en una posición destacada. La noticia destaca que la guerra comercial entre ambas potencias ha llevado a acusaciones de ciberespionaje, vetos y robo de patentes, colocando a Huawei en el epicentro de un conflicto geopolítico.

Las acusaciones de fraude bancario, presunta violación de sanciones a Irán y espionaje industrial por parte del gobierno estadounidense contra Huawei han generado una serie de medidas, como la prohibición en departamentos de defensa y agencias de

inteligencia. Las tensiones comerciales y geopolíticas entre Estados Unidos y China se ven reflejadas en la situación de Huawei, cuya fundación por Ren Zhengfei, exoficial del Ejército Popular de Liberación chino, añade un componente adicional a las preocupaciones sobre su lealtad.

La noticia señala que la tecnología 5G, en la que Huawei lidera el desarrollo y despliegue, se ha convertido en un punto estratégico en esta guerra, y Estados Unidos, bajo el liderazgo de Donald Trump, reconoce la importancia de ganar esta "carrera del 5G". La medida de Google de vetar a Huawei tiene implicaciones económicas y comerciales más allá del consumidor final, evidenciando el impacto directo en la industria y en otras compañías dependientes.

El análisis de expertos citados en la noticia destaca la falta de pruebas demostradas de espionaje por parte de Huawei, pero la sospecha persistente, especialmente debido a la opacidad de la empresa y las acusaciones previas en relación con temas de propiedad intelectual. La guerra económica entre Estados Unidos y China, la dependencia europea de ambas potencias y la falta de músculo tecnológico propio sitúan a Europa en una posición vulnerable.

Grosso modo, la noticia de ABC Tecnología proporciona una base sólida para investigar las preocupaciones en torno a Huawei, explorando las complejidades de la guerra comercial y tecnológica entre Estados Unidos y China, y evaluando el impacto en la percepción internacional de la empresa en el contexto de la balcanización de internet y la carrera por el 5G.

En este contexto, el análisis de la Guerra Comercial China - Estados Unidos, focalizado en el caso de Huawei, se presenta como una perspectiva complementaria. Cabe destacar que la guerra comercial entre China y Estados Unidos, centrada en el caso de Huawei, es un fenómeno que ha impactado significativamente en la economía global, generando tensiones y acusaciones mutuas.

En el documento "Análisis de la Guerra Comercial China - Estados Unidos a partir del caso Huawei" (Oviedo Guachamín, 2021), se examinan las implicaciones de esta contienda en la seguridad cibernética, la percepción internacional de Huawei y las

acusaciones que han surgido durante este conflicto. Dicha investigación se complementa con la anterior y ofrece una comprensión más profunda de los diversos aspectos en juego en el enfrentamiento entre ambas potencias.

La autora destaca que las guerras comerciales históricamente han representado amenazas para las economías mundiales, generando un quiebre en la paz económica y afectando el comercio internacional. Subraya la importancia de las relaciones internacionales en el desarrollo económico, ya que estas permiten generar riqueza para las naciones, y su deterioro puede tener consecuencias adversas, como la disminución del crecimiento económico y el quiebre de relaciones entre países (BBC NEWS, 2018).

En el contexto de la guerra comercial, Estados Unidos ha adoptado medidas que han afectado directamente a China, imponiendo aranceles a productos chinos. El presidente Donald Trump ha justificado estas medidas acusando a China de prácticas comerciales desleales, robo de propiedad intelectual, piratería y supuestas amenazas a la seguridad estadounidense al vender equipos de telecomunicaciones a Irán. Como respuesta, China ha aplicado represalias, aumentando aranceles a productos estadounidenses, generando un caos en la actividad comercial mundial, con repercusiones en regiones como Europa (Hernández, 2019).

En el ámbito de la seguridad nacional de Estados Unidos, la empresa Huawei ha sido objeto de acusaciones difamatorias por parte del gobierno estadounidense. Se le ha señalado de intentar acceder a los sistemas de telecomunicaciones de Estados Unidos y otros países para robar información, así como de vulnerar sistemas relacionados con el comercio, tecnología de defensa y agencias gubernamentales en Washington. Huawei ha negado estas acusaciones, calificándolas como difamatorias y asegurando que no hay evidencia de sus intenciones maliciosas (López, 2019).

En cuanto a la propiedad intelectual, se destaca que Estados Unidos acusa a China de robo de propiedad intelectual, alegando que el gobierno chino favorece a las empresas locales en disputas relacionadas. La respuesta china niega rotundamente estas acusaciones, generando un punto de conflicto en el marco de esta guerra comercial (Vaswani, 2019). Este enfrentamiento en torno a la propiedad intelectual resalta la complejidad y la intensidad de

las disputas comerciales, evidenciando la tensión entre las dos potencias y sus repercusiones a nivel global.

Para concluir en este punto, la confrontación entre Estados Unidos y China, como se detalla en el documento "Confrontación Estados Unidos-China: De Geopolítica, Tecnología y Riesgos para Nuestra Región" de Levy, Meschoulam y Hernández (s.f.), revela una serie de preocupaciones y acusaciones centradas en la seguridad cibernética de Huawei. Este análisis exhaustivo abarca aspectos geopolíticos y tecnológicos, así como los riesgos que esta rivalidad plantea a nivel regional e internacional.

El documento destaca la percepción generalizada de una carrera acelerada entre las superpotencias, particularmente entre Estados Unidos y China. Desde la expansión china en los mares hasta las ventas de armas a Taiwán y las acusaciones de instigación a manifestaciones en Hong Kong, el panorama aborda diversas dimensiones de esta compleja relación.

En respuesta al discurso estadounidense sobre China, la agencia oficial de noticias china, Xinhua (s.f.), presenta un análisis crítico titulado "Las cinco falacias del discurso de Pence sobre China". Este contrargumento desacredita afirmaciones como la reconstrucción de China por parte de Estados Unidos, la inexistencia de un "expansionismo chino" y la percepción de prácticas comerciales injustas. Además, destaca las reformas políticas y económicas en China como elementos ignorados por el discurso de Pence (Xinhua, 2018).

Un aspecto adicional abordado en el documento es la carrera armamentista y el despliegue de misiles, particularmente la intención de Estados Unidos de desplegar misiles intermedios en áreas que podrían impactar a China. La salida de Washington del Tratado INF y la falta de compromiso por parte de Beijing generan inquietudes sobre una posible carrera nuclear de consecuencias imprevisibles (Levy et al., 2018).

Contexto: el enfrentamiento geopolítico EE. UU. - China

El enfrentamiento entre Estados Unidos y China se caracteriza no solo por la competencia material entre dos grandes potencias, sino también por la relación entre una potencia en crecimiento y expansión que se percibe a sí misma como fuerte, y otra que se ve rezagada y busca recuperar terreno. La interdependencia económica y tecnológica

históricamente construida entre ambas naciones complica la posibilidad de una desvinculación abrupta. A pesar de esta vinculación, surgen intereses diversos que no siempre convergen en una misma dirección.

La administración Trump ha redefinido la seguridad nacional estadounidense, reconociendo la "competencia estratégica" entre las potencias como la principal amenaza. China, con su capacidad económica, militar y tecnológica, es percibida como una amenaza mayor que Rusia. La rivalidad abarca diversos ámbitos, y la tecnología desempeña un papel fundamental en esta competencia.

La polémica en torno a las empresas tecnológicas chinas

El ascenso de China como potencia en tecnologías de la información, especialmente representado por Huawei, ha generado preocupaciones, acusaciones y bloqueos en Estados Unidos. La controversia se centra en aspectos como el apoyo financiero del gobierno chino, disputas sobre derechos de propiedad intelectual, vínculos estrechos con el ejército chino y amenazas a la seguridad nacional estadounidense.

La existencia de un "Comité del Partido Comunista" en Huawei y otras empresas chinas también ha generado polémica, ya que se percibe como un medio potencial para el espionaje o sabotaje impulsado por el gobierno chino. Estos temores se intensifican ante el auge de la tecnología 5G y plantean interrogantes sobre la seguridad y la intención detrás de la participación de estas empresas en los mercados internos de Estados Unidos.

Decisiones gubernamentales y regulatorias tomadas por varios países en relación con Huawei, como la exclusión de la empresa de proyectos de infraestructura crítica y la imposición de restricciones comerciales y sus implicaciones

Habiendo completado con éxito el análisis exhaustivo de los resultados relacionados con el primer objetivo, centrado en investigar las preocupaciones y acusaciones de seguridad cibernética en torno a Huawei, se va a proceder ahora hacia una nueva faceta crítica de la investigación. Con el objetivo 2, se explorará a fondo las decisiones gubernamentales y regulatorias adoptadas por diversos países en relación con Huawei.

Los resultados de este objetivo son cruciales en esta investigación debido a su impacto significativo en la geopolítica, la seguridad nacional y la economía global, punto clave en el desenvolvimiento de las relaciones internacionales. El seguimiento de estas decisiones proporciona información valiosa sobre la dinámica internacional, las alianzas estratégicas y las percepciones de seguridad. Además, puede influir en la toma de decisiones empresariales y estratégicas a nivel mundial, afectando el desarrollo de tecnologías clave y las relaciones comerciales.

En este análisis de la ciberseguridad y su relación con las decisiones gubernamentales respecto a Huawei, se ha utilizado como base el documento "Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos" escrito por Germán Alejandro Patiño Orozco del Instituto Tecnológico y de Estudios Superiores de Monterrey (Patiño Orozco).

El autor destaca la importancia de la ciberseguridad como una prioridad estatal en el siglo XXI y analiza las estrategias de ciberseguridad de China y Estados Unidos, enfocándose en aspectos sociopolíticos y técnicos, respectivamente debido a la creciente dependencia de los sistemas digitales e informáticos en la sociedad.

El documento resalta la necesidad de salvaguardar la integridad y continuidad de estos sistemas para garantizar la confidencialidad de la información, la integridad en el intercambio seguro de datos y la operatividad de la infraestructura tecnológica. En este sentido, se subraya la importancia de implementar medidas proactivas de ciberseguridad, tales como protocolos de encriptación robustos, sistemas de detección temprana de amenazas y una sólida gestión de acceso.

El análisis se centra en la comparación de los enfoques de ciberseguridad adoptados por dos potencias globales: Estados Unidos y China. Ambos países han elevado la ciberseguridad como una herramienta estratégica para proyectar su posición de dominio en una competencia intermodal a largo plazo. Se abordan las diferencias en la conceptualización de la ciberseguridad, donde el gobierno chino enfatiza aspectos sociopolíticos, mientras que el estadounidense se centra más en consideraciones técnicas.

Además, se resalta que la ciberseguridad se ha convertido en un terreno de cooperación y conflicto entre estas potencias, reflejado en sus prácticas antitéticas sobre el orden global de seguridad. La revisión identifica similitudes y diferencias en las estrategias de ciberseguridad implementadas por ambos gobiernos, haciendo hincapié en la importancia de la seguridad del espacio cibernético como un factor clave en la relación chino-estadounidense.

En este contexto de intensa competencia interestatal, la ciberseguridad emerge como una herramienta estratégica fundamental para la apuesta competitiva internacional. Históricamente, las sociedades han presenciado la confrontación de conjuntos de ideas en competencia, donde la dominancia de una ortodoxia se convierte en esencial para la acción efectiva (Legro, 2000, p. 258).

En la escala internacional, estas ideas se materializan en normas, regímenes e instituciones, lideradas comúnmente por una potencia hegemónica, aunque actualmente nos encontramos en un periodo de interregno hegemónico, caracterizado por intensas competencias y reconfiguraciones a nivel global (Morales, 2018, p. 482).

En este escenario, el gobierno chino, liderado por Xi Jinping, busca consolidar una posición dominante a través de iniciativas ambiciosas como el Cinturón Económico de la Ruta de la Seda y la Ruta Marítima de la Seda del Siglo XXI. La ciberseguridad desempeña un papel crucial en esta estrategia, ya que la protección de la infraestructura de información y comunicación se convierte en un activo esencial para el impacto y la configuración del orden internacional que China busca lograr (Berger, 2014).

La protección de cables de fibra óptica, redes de comunicación y el establecimiento de ciudades inteligentes se convierten en elementos centrales para alcanzar estos objetivos. En este contexto, la implementación de tecnologías de inteligencia artificial y aprendizaje automático se revela como un catalizador esencial para optimizar la gestión de infraestructuras críticas, anticipar posibles amenazas y fortalecer la respuesta ante incidentes.

En paralelo, el gobierno estadounidense aborda la ciberseguridad desde una perspectiva que busca mantener la estructura de gobernabilidad del ciberespacio, enfocándose en la colaboración con diversas empresas tecnológicas globales. Estados

Unidos, al aprovechar su posición temprana en el diseño del ciberespacio, busca liderar la evolución y el desarrollo de este ámbito (Segal, 2018).

No obstante, sus acciones han generado inquietudes sobre la militarización de los asuntos cibernéticos y su efecto en la estabilidad y funcionalidad de la estructura digital global (Valeriano, Jensen & Maness, 2019, p. 171). En este contexto, la comunidad internacional se encuentra desafiada a desarrollar normas y protocolos que regulen las actividades cibernéticas militares, promoviendo la transparencia y la cooperación para mitigar posibles tensiones y conflictos en el ciberespacio.

Ambos enfoques, el chino y el estadounidense, suscitan preocupaciones entre diversos actores estatales y no estatales. Las acciones en el ciberespacio se perciben como un "teatro para el espionaje, el sabotaje y el conflicto" (Valeriano, Jensen & Maness, 2019, p. 171). La militarización de los asuntos cibernéticos y la intervención constante en sistemas informáticos plantean desafíos para la estabilidad global. Además, la capacidad de los gobiernos para intervenir en los sistemas informáticos y el desarrollo de tecnologías para la censura y vigilancia generan preocupaciones sobre la limitación de derechos y libertades (Kaplan, 2016; Zuboff, 2019).

En este entorno, la ciberseguridad no solo es una cuestión técnica, sino una herramienta estratégica que influye en la configuración del orden internacional. Las acciones y políticas en este ámbito reflejan la intensa competencia entre potencias, la búsqueda de dominio en el escenario mundial y las implicaciones para la libertad y estabilidad global. En este sentido, la ciberseguridad se convierte en un elemento crucial en la apuesta competitiva internacional de las naciones.

En el artículo "La Unión Africana estrecha relaciones con Huawei y define su lugar en la 'cortina de acero digital'" de Vienna Acosta (2019), se aborda la compleja interacción entre la Unión Africana y Huawei en el contexto de la guerra comercial entre Estados Unidos y China. Este documento proporciona una visión detallada de las decisiones gubernamentales y regulatorias adoptadas por varios países respecto a Huawei, explorando las implicaciones de excluir a la empresa de proyectos críticos de infraestructura y la imposición de restricciones comerciales.

El autor destaca la importancia de la competencia global entre las empresas de telecomunicaciones y tecnología, subrayando la ausencia de un marco normativo en el ciberespacio, lo que conduce a una intensa lucha por la supremacía sin reglas claras. La disputa entre Estados Unidos y China se refleja en la acusación de robo de información contra Huawei, colocándola en una "lista negra".

Este acto limita su capacidad para establecer relaciones comerciales con empresas estadounidenses y adquirir tecnología esencial para su funcionamiento, incluyendo chips electrónicos y el sistema operativo Android (Acosta, 2019). Esta restricción ha generado un impacto significativo en la cadena de suministro y la competitividad global de Huawei, obligándola a replantear estrategias y diversificar sus fuentes de aprovisionamiento para mitigar las consecuencias a largo plazo.

En el escenario de tensión entre Estados Unidos y China, el autor destaca el papel crucial de la Unión Africana al estrechar lazos con Huawei. Se señala que, más allá del obsequio del edificio de la Unión Africana por parte del gobierno chino en 2012, se firma un Memorando de Entendimiento para fortalecer la colaboración en áreas clave como banda ancha, internet de las cosas, computación en la nube, 5G e inteligencia artificial (Acosta, 2019).

La noción de la "Cortina de Acero Digital" se presenta como un dilema para los Estados, quienes deben elegir entre adquirir tecnología y *software* de empresas estadounidenses o chinas. Se destaca que la Unión Africana ha optado por alinearse con Huawei, mostrando el potencial mercado africano para las nuevas tecnologías y la importancia de las decisiones políticas en medio de la competencia global por el dominio del ciberespacio (Acosta, 2019).

El artículo explora las medidas tomadas por Estados Unidos, incluyendo aranceles y la detención de la directora financiera de Huawei, Meng Wanzhou, bajo acusaciones de eludir sanciones a Irán. También aborda la inclusión de Huawei en una lista de entidades que "atentan contra los intereses norteamericanos", afectando sus relaciones con empresas como Google y otras proveedoras de *hardware*.

Esta restricción ha generado un impacto significativo en la cadena de suministro y la competitividad global de Huawei, obligándola a replantear estrategias y diversificar sus fuentes de aprovisionamiento para mitigar las consecuencias a largo plazo. Se evidencia la complejidad de las acusaciones de espionaje, vinculando las acciones contra Huawei a la sospecha de una conexión estrecha entre las empresas chinas y el Partido Comunista (Acosta, 2019).

La Unión Africana emerge como un actor estratégico al decidir aliarse con Huawei, aprovechando su presencia en África desde la década de 1990. La empresa ha contribuido significativamente al desarrollo de infraestructura de comunicación en el continente, implementando tecnologías avanzadas como 4G y 5G. A pesar de las acusaciones de espionaje, la Unión Africana refuerza su confianza en Huawei mediante la firma de acuerdos que buscan mejorar la experiencia técnica y capacidades tecnológicas en diversos sectores (Acosta, 2019).

La obra concluye destacando las necesidades de la Unión Africana en tecnologías de la información y comunicación, subrayando la importancia de acceder a tecnologías asequibles. Se cuestiona la viabilidad de que los estados africanos desarrollen sus propias capacidades tecnológicas en competencia con gigantes como Huawei. La "Cortina de Acero Digital" se presenta como una realidad en la que la Unión Africana, por el momento, ha optado por el lado chino en su búsqueda de conectividad y avances tecnológicos (Acosta, 2019).

En resumen, el artículo de Vienna Acosta ofrece una visión detallada y crítica de la relación entre la Unión Africana y Huawei, contextualizada en la guerra comercial entre Estados Unidos y China. Proporciona una base sólida para entender las decisiones gubernamentales y regulatorias relacionadas con Huawei, destacando el papel clave de la Unión Africana en medio de la competencia por el liderazgo en el ciberespacio. Este análisis contribuye significativamente a la comprensión de las complejidades geopolíticas y tecnológicas en el panorama actual.

La cibergeopolítica emerge como un componente fundamental en el escenario global, donde la competencia por el control de la información y la distribución de datos entre las potencias se intensifica. Tomando como base el análisis de Silvia Marina Rivas en su artículo

"El ciberespacio como zona de control geopolítico y papel de las potencias por la supremacía cibernética: China y Estados Unidos" (2019), se examinan las decisiones gubernamentales y regulatorias que afectan a empresas clave como Huawei.

En el documento, Rivas destaca la ausencia de un marco normativo global en el ciberespacio, lo que ha generado tensiones entre Estados Unidos y China. Este conflicto se refleja en la exclusión de Huawei de proyectos de infraestructura crítica y la imposición de restricciones comerciales. La acusación de robo de información contra Huawei la sitúa en una "lista negra", limitando sus relaciones comerciales con empresas estadounidenses y su acceso a tecnologías esenciales como chips electrónicos y el sistema operativo Android.

La carrera tecnológica y cibernética entre Estados Unidos y China, delineada en el artículo de Rivas, se manifiesta en la lucha por la supremacía en el mercado de dispositivos y la transmisión de datos a nivel mundial. La ciberseguridad y la ciberdefensa se presentan como elementos cruciales para preservar la integridad territorial, la seguridad ciudadana y las infraestructuras críticas, abordando las amenazas de ciberataques, espionaje y manipulación de información en el ciberespacio.

En este contexto, las decisiones gubernamentales y regulatorias de varios países respecto a Huawei adquieren relevancia. Estados Unidos, bajo la administración Trump, implementó políticas restrictivas, prohibiendo a empresas tecnológicas estadounidenses colaborar con Huawei. La inclusión de Huawei en la lista de empresas de riesgo para la seguridad nacional generó tensiones comerciales y tecnológicas.

La Unión Europea, consciente de su dependencia tecnológica, busca desarrollar protocolos de defensa y regulaciones para garantizar la seguridad cibernética en sus estados miembros (Rivas, 2019). En este contexto, se destaca la importancia de la colaboración entre los países miembros para abordar amenazas cibernéticas transfronterizas y promover la resiliencia en el espacio digital.

La competencia por el dominio en el ciberespacio se revela como una "carrera" estratégica entre países, especialmente aquellos con capacidades de investigación y desarrollo avanzadas. Desde sus inicios, la gestión y desarrollo de Internet, originalmente

diseñado para uso militar y académico por Estados Unidos, ha otorgado a este país ventajas significativas en ciberespionaje.

Este contexto político amplifica la magnitud de los desafíos que enfrenta Huawei en el escenario internacional. La expansión de internet como herramienta cotidiana ha permitido estrategias más amplias e innovadoras en este ámbito, incluso llegando al punto de violar *hardware* audiovisual para espiar a posibles sospechosos y aliados.

El desarrollo de internet ha evolucionado y, actualmente, diversos países compiten en el mercado de desarrollo, distribución y procesamiento de información, especialmente en el ámbito de dispositivos móviles y la tecnología 5G. Empresas líderes como Huawei y Google se destacan en este panorama, representando no solo avances tecnológicos, sino también un espacio estratégico para el dominio tecnológico y geopolítico.

La innovación y el dominio tecnológico en el ciberespacio se asemejan a la importancia que tenía el dominio aeroespacial durante la Guerra Fría. Actualmente, este nuevo frente tecnológico otorga ventajas significativas a un estado sobre los demás, pero también plantea amenazas en términos de capacidades y oportunidades de ciberespionaje.

En este escenario, la capacidad de adaptación y la agilidad en el desarrollo de estrategias cibernéticas se convierten en elementos esenciales para mantener una posición competitiva y garantizar la seguridad en la era digital. La colaboración entre sectores público y privado emerge como un pilar fundamental, promoviendo el intercambio de información y la creación de estándares comunes para fortalecer la resiliencia ante amenazas cibernéticas en constante evolución.

La prohibición por parte del gobierno estadounidense, bajo la administración del expresidente Trump, de vender partes a empresas chinas como Huawei y ZTE, y la sugerencia de crear una red de última generación propia, reflejan la preocupación por posibles riesgos a la seguridad nacional. Este enfoque defensivo subraya la importancia de mantener un equilibrio entre la innovación tecnológica y las medidas de seguridad para salvaguardar los intereses estratégicos del país.

En este contexto, la tensión entre la protección de intereses nacionales y la colaboración global en el ámbito tecnológico se intensifica, subrayando la necesidad de

equilibrar la seguridad cibernética con la promoción de la innovación y la competencia justa. En este contexto, la cibergeopolítica se manifiesta como un terreno estratégico donde las decisiones gubernamentales y regulatorias, como las implementadas por Estados Unidos, impactan no solo en las relaciones comerciales sino también en la seguridad nacional.

Esta situación evidencia la complejidad de la competencia entre las principales empresas fabricantes de dispositivos 5G y la necesidad de estrategias nacionales para salvaguardar intereses críticos. En este escenario, la cooperación internacional también se presenta como un elemento crucial para abordar de manera efectiva los desafíos globales y fomentar estándares comunes que impulsen el desarrollo sostenible de la tecnología 5G.

Papel de la ciberseguridad corporativa en la era digital y cómo las lecciones aprendidas del caso Huawei pueden influir en las prácticas empresariales y gubernamentales relacionadas con la seguridad cibernética

En la entrevista a profundidad con el primer entrevistado, se exploraron aspectos cruciales relacionados con su experiencia en el ámbito de la ciberseguridad corporativa. Con dos años de dedicación al área de seguridad informática, su perspectiva ofrece una visión valiosa sobre las prácticas y desafíos actuales en este campo.

El primer entrevistado destacó su enfoque en la seguridad de la información de la compañía, evidenciado por sus responsabilidades, que van desde la atención al usuario final hasta la administración de accesos y el control de seguridad de servidores mediante *firewalls*. Su mención del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) como entidad clave en Costa Rica subraya la importancia de las instituciones gubernamentales en la regulación y promoción de la seguridad cibernética. (Barrantes Hidalgo Silvia, Seguridad Informática, 11 Marzo, 2024)

En relación con el estado actual de la ciberseguridad en el entorno empresarial, el entrevistado describió la participación y alerta menos restrictiva en comparación con épocas anteriores. La implementación de herramientas de seguridad, como la aplicación Umbrella de CISCO, y el llamado de la Contraloría General de la República a fortalecer los marcos de referencia indican un ambiente dinámico, donde la seguridad es una obligación más que una opción. .(Barrantes Hidalgo Silvia, Seguridad Informática, 11 Marzo, 2024)

Desde la perspectiva del entrevistado, las lecciones aprendidas del caso Huawei resaltan la importancia de la gestión de contratos con proveedores, la vigilancia constante y la regulación de accesos físicos y lógicos. Además, enfatiza la necesidad de estar alerta ante amenazas en constante evolución y la importancia de la capacitación constante y campañas de concientización para abordar el eslabón humano, a menudo impredecible y vulnerable. .(Barrantes Hidalgo Silvia, Seguridad Informática, 11 Marzo, 2024)

Las implicaciones de estas lecciones en las prácticas empresariales y gubernamentales incluyen un aumento en la atención a los proveedores, una selección más cuidadosa de socios y estrategias comerciales, y la implementación de métodos que permitan una respuesta y recuperación más eficientes en caso de afectación. .(Barrantes Hidalgo Silvia, Seguridad Informática, 11 Marzo, 2024)

Respecto a las tendencias emergentes en ciberseguridad, el entrevistado resalta el aumento de métodos de doble autenticación, la adopción del enfoque Zero Trust, el almacenamiento en la nube y el uso de inteligencia artificial. Estas tendencias reflejan la adaptación continua a las amenazas cambiantes y la búsqueda de soluciones avanzadas. .(Barrantes Hidalgo Silvia, Seguridad Informática, 11 Marzo, 2024)

Los mayores desafíos para las organizaciones, según el entrevistado 1, incluyen amenazas más desarrolladas, la implementación de normas que requieren inversión en herramientas y equipos, y la carencia de profesionales certificados y capacitados. .(Barrantes Hidalgo Silvia, Seguridad Informática, 11 Marzo, 2024)

En cuanto a la colaboración empresarial y gubernamental, el entrevistado considera crucial establecer parámetros generalizados del tratamiento de la información y mejorar la regulación, a pesar de las diferencias iniciales de opiniones y parámetros. Además, destaca la importancia de la cooperación público-privada para actualizar y fortalecer las defensas contra amenazas cibernéticas. (Barrantes Hidalgo Silvia, Seguridad Informática, 11 marzo, 2024)

Por otra parte, el entrevistado 2 aporta más de dos años de experiencia en el campo de la ciberseguridad, centrándose específicamente en seguridad e infraestructura. Con más de ocho años de experiencia en soporte técnico e infraestructura, su perspectiva abarca tanto

la tecnología como el soporte operativo. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

Desde su punto de vista, a nivel privado e internacional, la ciberseguridad se considera prioritaria en la mayoría de las empresas, con avances notables en la madurez de este ámbito. No obstante, señala que la diferencia en la prioridad dada a la ciberseguridad varía según el tamaño y la función de la empresa, así como el presupuesto disponible. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

En contraste, a nivel gubernamental en Costa Rica, el entrevistado describe una situación preocupante. Se percibe una falta de avance, lentitud e incluso negligencia en ciberseguridad. Menciona casos notorios de ataques, como los sufridos por la CCSS y el Ministerio de Hacienda, destacando la desactualización del personal de TI y las deficiencias en las aplicaciones disponibles para garantizar la seguridad de la información. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

A pesar de estas carencias, el entrevistado señala que Costa Rica no es un desastre cibernético, siendo uno de los países más seguros para trabajadores remotos. Sin embargo, atribuye esta seguridad relativa a las empresas transnacionales que implementan protocolos y sistemas de seguridad más avanzados. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

Al abordar las lecciones del caso Huawei, el entrevistado destaca la importancia de otorgar relevancia a la ciberseguridad y comprender las regulaciones legales, que pueden variar de un país a otro. Subraya que la ciberseguridad no debe trivializarse, ya que las implicaciones pueden ser significativas y duraderas. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

En cuanto a la percepción de las lecciones de Huawei en las prácticas empresariales y gubernamentales, el entrevistado destaca la existencia de protocolos establecidos, especialmente en empresas estadounidenses y del Reino Unido. Estos protocolos abarcan desde manipulación de dispositivos hasta cambios en cuentas empresariales y son llevados a cabo de manera estandarizada, con un enfoque específico para diferentes países y situaciones. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

En cuanto a las tendencias emergentes, el entrevistado identifica inversiones en soluciones de seguridad y cifrado extremo a extremo, así como campañas y ejercicios frecuentes de concientización sobre ingeniería social y seguridad cibernética en general. Destaca mejoras en sistemas de autenticación (MFA) para controlar y delimitar accesos a recursos privados. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

Sin embargo, al abordar los mayores desafíos para las organizaciones en términos de seguridad cibernética, el entrevistado destaca la escasez de profesionales en el ámbito a nivel nacional. Aunque reconoce los esfuerzos de instituciones académicas para formar profesionales en ciberseguridad, señala que la demanda actual exige respuestas más rápidas. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

Sobre la colaboración entre empresas y entidades gubernamentales en materia de ciberseguridad, el entrevistado considera que es necesaria para lograr un desarrollo rápido y efectivo. Sin embargo, en Costa Rica, describe la colaboración como casi nula, atribuyéndolo a la lentitud del aparato estatal y la burocracia asociada. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

Aunque no puede proporcionar ejemplos específicos de buenas prácticas de colaboración, destaca los esfuerzos en España, donde la colaboración entre el Estado y las empresas privadas ha impulsado la educación en ciberseguridad y posicionado al país como líder en el continente. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

En relación con la innovación tecnológica, el entrevistado enfatiza su influencia significativa en las estrategias de ciberseguridad corporativa. La inteligencia artificial y el internet de las cosas (IoT) permiten acelerar y automatizar mecanismos de detección, prevención y defensa. No obstante, subraya que la consciencia y el presupuesto siguen siendo factores clave, ya que la adopción efectiva de nuevas tecnologías depende de estos elementos. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

En pocas palabras, el entrevistado destaca que, para muchas empresas en América Latina, el presupuesto sigue siendo el diferenciador principal en la adopción efectiva de nuevas tecnologías para fortalecer la postura de ciberseguridad. Sin embargo, enfatiza que la conciencia y la educación sobre las amenazas cibernéticas son igualmente cruciales para

impulsar la seguridad digital, instando a un equilibrio adecuado entre la inversión financiera y la capacitación de personal en la prevención y respuesta ante posibles riesgos. (Meza Reyes David, Seguridad Informática, 10 de marzo, 2024)

Por otro lado, el entrevistado #3, experto en geopolítica, inteligencia y contrainteligencia, aclara que, aunque no es un experto en ciberseguridad, ha estudiado a fondo este ámbito. Su perspectiva multidisciplinaria resalta la interconexión entre la seguridad digital y los aspectos geopolíticos, subrayando la necesidad de enfoques integrales que aborden las complejidades interrelacionadas de la ciberseguridad en el contexto global actual. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

En el contexto empresarial y gubernamental, destaca la importancia crucial de la seguridad digital en el siglo XXI. La era digital ofrece oportunidades significativas, pero también presenta retos considerables en términos de seguridad. Según el informe "Panorama de Amenazas 2023" de Kaspersky, América Latina enfrenta una creciente amenaza de ciberdelincuencia, siendo el *ransomware* una de las formas más preocupantes de ataques digitales. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

En relación con el caso Huawei, el entrevistado subraya la naturaleza política de la guerra comercial entre China y los EE. UU. Considera que la demonización de China en la esfera académica es sesgada y aboga por comprender la totalidad del problema. Estas lecciones deberían influir en la adopción de estrategias más realistas y en la comprensión de las complejidades de la ciberseguridad. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

En cuanto a las tendencias emergentes, destaca la creación de *war rooms* de ciberseguridad, equipos especializados en la defensa digital de empresas e instituciones. Identifica el mayor desafío actual como la protección de la información más sensible y valiosa de las organizaciones en esta era digital. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

En el ámbito de la colaboración público-privada, el entrevistado reconoce su importancia como un paso en la dirección correcta. Menciona un ejemplo de alianza entre empresas españolas e israelíes como un modelo de cooperación para mejorar prácticas y

fortalecer las defensas contra posibles ataques. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

Tambien, destacó la influencia de la innovación tecnológica, especialmente la inteligencia artificial y el *machine learning*, en el perfeccionamiento de los sistemas de ciberseguridad. La próxima generación de defensa cibernética podría centrarse en la robótica, lo que refleja la continua evolución en este campo. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

El último entrevistado, aunque posee un conocimiento básico/intermedio en ciberseguridad, ofrece valiosas percepciones sobre este campo en los ámbitos empresarial y gubernamental. Reconoce la sensibilidad inherente al tema y destaca la necesidad apremiante de implementar medidas sólidas para evitar incidentes, haciendo referencia al notorio caso de la CCSS en 2022.(Cordero Gomez Mario, informática, 9 de marzo, 2024)

En relación con las lecciones extraídas del caso Huawei, el entrevistado enfatiza que la seguridad informática trasciende la mera protección de dispositivos, abarca aspectos legales, culturales y éticos. Aboga por fomentar valores y ética para impulsar la colaboración y avanzar tecnológicamente. Advierte sobre el riesgo de enfrentamientos en lugar de colaboración si se rompen contratos con grandes empresas, subrayando la importancia de la cooperación en la era digital. .(Cordero Gomez Mario, informática, 9 de marzo, 2024)

En el contexto de las tendencias emergentes, el entrevistado destaca la implementación del segundo factor de autenticación y dispositivos con *firewalls* o VPN como medidas clave en ciberseguridad corporativa, reflejando la evolución constante de las estrategias de protección. .(Cordero Gomez Mario, informática, 9 de marzo, 2024)

Identifica al usuario final como el principal desafío actual, resaltando la importancia crucial de la conciencia y el instinto del usuario para detectar posibles amenazas, como el *phishing* o estafas. Considera que la educación y la concientización son fundamentales para fortalecer la postura de las organizaciones frente a estos desafíos. .(Cordero Gomez Mario, informática, 9 de marzo, 2024)

En cuanto a la colaboración entre empresas y entidades gubernamentales, el entrevistado reconoce mejoras, pero señala la necesidad imperante de sistemas y

capacitaciones más eficientes en Costa Rica para prevenir incidentes de seguridad informática, destacando la importancia de una colaboración efectiva entre sectores público y privado. .(Cordero Gomez Mario, informática, 9 de marzo, 2024)

El entrevistado destaca prácticas exitosas de colaboración en sistemas bancarios que emplean estándares de seguridad avanzados de terceros como Microsoft (Azure) o Amazon Web Services, ilustrando la importancia de asociaciones sólidas para fortalecer la ciberseguridad. .(Cordero Gomez Mario, informática, 9 de marzo, 2024)

En el ámbito de la innovación tecnológica, el entrevistado reconoce su impacto tanto positivo como negativo. Destaca la necesidad constante de actualizar protocolos y sistemas de seguridad ante las nuevas amenazas que surgen con la innovación tecnológica, subrayando la importancia de mantenerse al tanto de los avances para garantizar la eficacia de las estrategias de ciberseguridad. .(Cordero Gomez Mario, informática, 9 de marzo, 2024)

Finalmente, el entrevistado considera que las empresas están adoptando efectivamente nuevas tecnologías para fortalecer su postura de ciberseguridad, pero señala que algunas instituciones gubernamentales aún dependen de métodos de acceso menos seguros, como simples usuarios y contraseñas. .(Cordero Gomez Mario, informática, 9 de marzo, 2024)

En el contexto de las entrevistas sobre ciberseguridad, emerge una preocupación compartida acerca de la importancia crítica de abordar la seguridad digital tanto en el ámbito empresarial como gubernamental. Se destaca la necesidad de salvaguardar la información sensible y se subraya la relevancia de la concientización del usuario final como una capa esencial de defensa en el complejo entorno digital actual.

En relación con las amenazas, se reconoce la existencia de desafíos avanzados, siendo el *ransomware* señalado específicamente como una creciente inquietud. La colaboración entre empresas y entidades gubernamentales se plantea como un componente esencial para hacer frente a estas amenazas, aunque algunos entrevistados expresan críticas sobre la eficiencia del sector gubernamental en este aspecto clave.

De los casos emblemáticos, como el incidente de la CCSS y las preocupaciones asociadas a Huawei, se extraen lecciones valiosas. Se resalta la importancia de la gestión de

contratos, la vigilancia constante y la comprensión de las implicaciones políticas y legales vinculadas a las decisiones en ciberseguridad, evidenciando la necesidad de un enfoque integral en la protección de la infraestructura digital.

En cuanto a las tendencias emergentes, se observa un aumento en la implementación de medidas como la doble autenticación, el enfoque Zero Trust, la adopción de almacenamiento en la nube y la integración de inteligencia artificial en los sistemas de seguridad. Estos cambios reflejan la adaptación constante frente a las amenazas en evolución y la necesidad de estrategias más sofisticadas.

Entre los desafíos identificados, se menciona la persistencia de amenazas en constante evolución, la escasez de personal capacitado en ciberseguridad y la falta de profesionales a nivel nacional. Estos factores resaltan la necesidad urgente de invertir en la formación de especialistas para hacer frente a las complejidades de la seguridad digital en un entorno dinámico.

La innovación tecnológica, especialmente la inteligencia artificial y el *machine learning*, se destaca como una herramienta valiosa para mejorar continuamente las estrategias de ciberseguridad. Sin embargo, se enfatiza la importancia de mantenerse actualizado en términos de protocolos y sistemas de seguridad, ya que la innovación tecnológica también conlleva nuevos desafíos y riesgos.

En relación con la adopción de nuevas tecnologías, se observa una adaptación gradual en las empresas, aunque se reconoce que el presupuesto sigue siendo un factor determinante. Aunque algunas instituciones gubernamentales avanzan hacia prácticas más seguras, persiste la percepción de que aún hay espacio para mejoras en la seguridad digital a nivel estatal.

En resumen, las entrevistas reflejan una creciente conciencia sobre la importancia crítica de la ciberseguridad tanto a nivel local como a nivel global. Existe un llamado claro a fortalecer la colaboración, invertir en la formación de profesionales y mantenerse al tanto de las tendencias y amenazas emergentes en el ámbito de la seguridad digital para construir un entorno digital más seguro y resiliente.

Marco legal y regulador que aborde de manera efectiva los aspectos legales y jurídicos relacionados con la seguridad cibernética

Este segmento se adentrará en el análisis de los resultados derivados de las entrevistas a profundidad centradas en el objetivo específico de explorar el marco legal y regulador que aborda de manera efectiva los aspectos legales y jurídicos asociados con la seguridad cibernética. A través de las perspectivas y experiencias compartidas por expertos en el campo, se revelarán *insights* cruciales que permitirán evaluar la eficacia y pertinencia de las normativas existentes en este ámbito particular.

Como punto de partida, el entrevistado #1 destacó de manera contundente la percepción de debilidad en el marco legal actual de Costa Rica en relación con la seguridad cibernética. Subrayó la carencia de herramientas institucionales sólidas y la falta de estrategia y visión clara, evidenciadas de manera crítica durante el ataque cibernético a varias instituciones en 2022. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

Aunque el entrevistado #1 no especificó lagunas o áreas de mejora en la legislación, la generalidad de sus comentarios sugiere la necesidad urgente de fortalecer el marco legal para hacer frente a los desafíos de la seguridad cibernética. Además, enfatizó la importancia de una mayor colaboración entre los sectores público y privado, así como la participación activa de la sociedad civil, para construir un enfoque integral y efectivo en la protección de la ciberseguridad a nivel nacional. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

La falta de respuesta del entrevistado en cuanto a comparaciones con otras regiones podría indicar una limitada conciencia o conocimiento sobre buenas prácticas aplicables en el contexto abordado. Esta omisión destaca la importancia de una mayor investigación y análisis comparativo para enriquecer las perspectivas locales. Al profundizar en experiencias internacionales, cualquier país podría beneficiarse al adoptar estrategias exitosas implementadas en otras jurisdicciones, contribuyendo así a fortalecer su postura en materia de ciberseguridad de manera más efectiva. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

A pesar de no proporcionar detalles específicos sobre los desafíos en la aplicación de las leyes de seguridad cibernética, la realidad comúnmente experimentada en muchos lugares

sugiere obstáculos relacionados con la capacidad técnica y los recursos necesarios para la ejecución efectiva de la legislación. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

El entrevistado subrayó las tensiones entre las regulaciones de seguridad cibernética y las operaciones empresariales, destacando áreas críticas como la privacidad de la información, el control de datos y la competencia entre empresas y países. Esta observación resalta la complejidad del entorno empresarial en relación con la legislación de ciberseguridad. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

En términos del futuro del marco legal y regulatorio, el entrevistado expresó una visión clara de la ciberseguridad como uno de los problemas más apremiantes en la región. Destacó la necesidad de legisladores más informados y de legislación detallada para hacer frente a las crecientes amenazas cibernéticas que acompañan al avance de la economía digital y los negocios en línea. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

Aunque el entrevistado no proporcionó sugerencias específicas para cambios o mejoras en la protección legal, la falta de respuesta podría señalar la necesidad de un diálogo más profundo y colaborativo entre las partes interesadas, incluido el sector empresarial, para fortalecer el marco legal de seguridad cibernética en Costa Rica. (Lic. Mora Olman, Derecho, 10 de marzo, 2024)

Para obtener una visión más completa de las percepciones y experiencias en relación con el marco legal actual de seguridad cibernética a nivel local, se procede con el análisis del segundo entrevistado, el cual reveló una perspectiva informada sobre el marco legal actual en Costa Rica en relación con la seguridad cibernética.

El segundo entrevistado destacó la función del MICITT como un ente regulador y mencionó leyes específicas, como la Ley 8968 de protección de datos personales y la Ley 8204 contra la delincuencia organizada, que abordan los delitos informáticos. Sin embargo, identificó áreas de mejora, incluyendo la necesidad de una educación continua para la población y una mayor coordinación entre los sectores privado y público. (Barrantes Hidalgo Silvia, Seguridad Informática, 11 marzo, 2024)

Al comparar el marco legal con otras regiones, el entrevistado señaló avances positivos, pero resaltó la importancia de mejorar el alcance y enfoques de los recursos

dedicados a la ciberseguridad. Además, identificó buenas prácticas en otras jurisdicciones, como la investigación enfocada en la protección de la información y la apertura a otras compañías en procesos de licitación. (Barrantes Hidalgo Silvia, Seguridad Informática, 11 marzo, 2024)

En cuanto a los desafíos en la aplicación legal, el entrevistado mencionó la falta de legislación específica para el sector y la necesidad de capacitación en diferentes sectores. Propuso fortalecer las leyes de información pública y otorgar a una entidad la capacidad de velar por la concientización de la población. (Barrantes Hidalgo Silvia, Seguridad Informática, 11 marzo, 2024)

En el ámbito empresarial, el entrevistado resaltó que las regulaciones afectan las estrategias y operaciones, imponiendo medidas adicionales de protección y generando costos adicionales. También señaló tensiones entre los requisitos legales y las necesidades operativas, pero destacó que el cumplimiento efectivo puede fortalecer la resiliencia de la empresa. (Barrantes Hidalgo Silvia, Seguridad Informática, 11 marzo, 2024)

Mirando hacia el futuro, el entrevistado visualiza la necesidad de normativas internacionales estandarizadas y un enfoque en la protección de servicios esenciales. Propuso mejoras como auditorías obligatorias, coordinación internacional, fortalecimiento de medidas de protección y leyes actualizadas y claras. (Barrantes Hidalgo Silvia, Seguridad Informática, 11 marzo, 2024)

En el análisis global del marco legal y regulatorio relacionado con la seguridad cibernética en Costa Rica, se evidencia una percepción general de debilidad en la legislación por parte del primer entrevistado. Se destaca la falta de estrategias claras y un marco legal sólido, ejemplificado por los ataques cibernéticos sufridos en 2022, revelando la necesidad de una visión más clara y herramientas institucionales más robustas.

El segundo entrevistado, en cambio, reconoce avances positivos en la jurisdicción costarricense, especialmente a través del MICITT, que ha desempeñado un papel regulador en el fortalecimiento de las estructuras de seguridad de TI. Se mencionan leyes específicas, como la Ley 8968 de protección de datos personales y la Ley 8204 contra la delincuencia organizada, que abordan aspectos cruciales de la ciberseguridad.

Ambos entrevistados coinciden en señalar la necesidad de mejorar la educación continua a la población, la concientización pública y la coordinación entre el sector público y privado. Además, se destacan desafíos comunes, como la falta de legislación específica, la necesidad de capacitación en diversos sectores y la importancia de fortalecer las leyes de información pública.

En cuanto a las implicaciones empresariales, se subraya la exigencia de medidas adicionales para proteger la información, lo que implica costos adicionales y la implementación de planes de gestión de riesgos. Se reconoce la existencia de tensiones entre los requisitos legales y las necesidades operativas de las organizaciones, pero se destaca que el cumplimiento efectivo puede fortalecer la resiliencia empresarial.

En términos de jurisdicciones comparativas, se mencionan buenas prácticas observadas en la Unión Europea y Oceanía, enfocadas en la protección de la información y la apertura a diversas compañías en procesos de licitación para tecnología 5G. Esta referencia destaca la relevancia de explorar experiencias internacionales para enriquecer la estrategia local, adaptando enfoques exitosos a la realidad específica del país en cuestión.

Las tensiones percibidas entre estándares, cumplimientos y costos pueden generar un clima desafiante para las empresas, donde la implementación efectiva de medidas de seguridad cibernética no solo se convierte en una cuestión de cumplimiento normativo, sino también en un factor clave para preservar la integridad y reputación empresarial en un entorno digital en constante evolución. En este escenario, la anticipación de cambios regulatorios y la colaboración activa entre el sector público y privado se perfilan como elementos esenciales para el éxito futuro en la gestión de riesgos cibernéticos a nivel empresarial.

Finalmente, al proyectar el futuro del marco legal y regulatorio, se vislumbra la importancia de buscar normativas internacionales y estandarizadas. Se destaca la necesidad de un enfoque prioritario en la protección de servicios esenciales y la mejora de la capacitación y concientización para enfrentar amenazas cibernéticas en constante evolución. Además, se sugieren cambios como auditorías obligatorias, mayor coordinación internacional, fortalecimiento de medidas de protección y la actualización de leyes para garantizar transparencia en la privacidad y seguridad de la información.

Capítulo V: Conclusiones y recomendaciones

Conclusiones

En conclusión, este trabajo ha explorado de manera integral los desafíos y complejidades de la seguridad cibernética, focalizándose en el caso paradigmático de Huawei. A lo largo de este análisis, se han alcanzado los objetivos planteados, revelando aspectos cruciales que afectan tanto a la ciberseguridad global como a la dinámica específica de esta empresa.

Uno de los puntos centrales ha sido la evaluación de las acusaciones contra Huawei, marcadas por la controversia y la disputa. Las afirmaciones de ciberespionaje, recurrentes a lo largo del tiempo, han sido refutadas por la compañía, generando un debate en torno a la veracidad de dichas alegaciones. Esta controversia se vuelve aún más compleja al involucrar a gobiernos, como el chino, que niegan cualquier vínculo indebido con Huawei.

En este contexto, resulta evidente que la evaluación de las acusaciones contra Huawei no solo representa un desafío técnico, sino también político y diplomático. La disputa en torno a estas afirmaciones de ciberespionaje subraya la importancia de una mayor transparencia y cooperación internacional en el ámbito de la seguridad cibernética. Es fundamental que los países y las empresas trabajen juntos para abordar las preocupaciones legítimas sobre la privacidad y la seguridad de los datos, al tiempo que se evitan interpretaciones sesgadas o motivadas políticamente.

Asimismo, este conflicto no solo impacta en la esfera tecnológica, sino que tiene implicaciones políticas y económicas significativas. Las decisiones gubernamentales, como la exclusión de Huawei de proyectos críticos de infraestructura, reflejan la preocupación por posibles riesgos y han transformado el panorama del mercado tecnológico global. Se revela así la intersección entre seguridad nacional, la competencia global y las relaciones internacionales.

La exclusión de Huawei de proyectos críticos de infraestructura y las tensiones políticas y económicas resultantes subrayan la complejidad de este conflicto y sus ramificaciones más allá del ámbito tecnológico. Estas decisiones gubernamentales no solo

buscan mitigar posibles riesgos de seguridad cibernética, sino que también tienen el potencial de reconfigurar el panorama del mercado tecnológico global y afectar las relaciones internacionales.

Dentro de este análisis, se extraen lecciones valiosas para la ciberseguridad corporativa, enfatizando la importancia de la gestión de contratos y la necesidad de inversiones prioritarias. Este aprendizaje no solo impacta en las estrategias empresariales, sino que resalta la urgencia de una mayor sincronización entre el sector privado y las instituciones gubernamentales en Costa Rica, donde se identifican brechas que deben ser superadas mediante una colaboración más estrecha.

Estas lecciones no solo afectan las estrategias empresariales, sino que también subrayan la necesidad de una mayor coordinación entre el sector privado y las instituciones gubernamentales en Costa Rica. Es crucial superar las brechas identificadas a través de una colaboración más estrecha para fortalecer la ciberseguridad en todos los niveles y proteger los activos digitales de manera más efectiva.

A nivel legal, se reconocen avances notables en Costa Rica, respaldados por la actuación del MICITT y leyes específicas como la 8968 y la 8204. Sin embargo, se señalan áreas críticas de mejora, como la necesidad de educación continua y una mayor colaboración público-privada. La comparación internacional muestra avances positivos, especialmente en la Contraloría General de la República, pero resalta la necesidad de una mayor dedicación de recursos para abordar la ciberseguridad de manera integral.

Las regulaciones, si bien imponen costos adicionales y cambios en las estrategias empresariales, fortalecen la resiliencia y mejoran la reputación. Al mirar hacia el futuro, se vislumbra una búsqueda de normativas internacionales, la protección de servicios críticos y mejoras legislativas. Se plantean sugerencias clave, como auditorías obligatorias, coordinación internacional, entes reguladores constantes y leyes actualizadas, para fortalecer la protección legal y promover la seguridad de la información.

A pesar de las conclusiones significativas obtenidas, es esencial interpretarlas considerando las limitaciones inherentes al estudio. Entre estas limitaciones se encuentran las tensiones políticas y las complejas relaciones internacionales, las cuales podrían haber

afectado la disponibilidad de información precisa y objetiva. Estos factores podrían haber introducido posibles sesgos o limitaciones en la interpretación de los datos recopilados. Sin embargo, es crucial destacar que este trabajo representa una contribución valiosa al campo de las Relaciones Internacionales.

Al ofrecer un análisis detallado de la ciberseguridad corporativa en un contexto global y tecnológico en constante evolución, proporciona una base sólida para futuras investigaciones y acciones en el ámbito de la seguridad cibernética. La comprensión de las interrelaciones entre la ciberseguridad, la política y las relaciones internacionales es fundamental para abordar los desafíos emergentes en un mundo cada vez más digitalizado y conectado.

Finalmente, se concluye que durante el período de 2018 a 2023, las preocupaciones de seguridad cibernética relacionadas con Huawei han ejercido un impacto significativo en las decisiones de políticas y comerciales a nivel internacional. Estas preocupaciones, centradas en posibles actividades de ciberespionaje y la seguridad de las infraestructuras críticas, han llevado a medidas restrictivas por parte de varios países, así como a tensiones comerciales y diplomáticas entre naciones. Es crucial abordar estas preocupaciones de manera colaborativa y buscar soluciones que equilibren la seguridad cibernética con la innovación y la cooperación internacional.

Recomendaciones

Esta investigación ha explorado diversos aspectos de la seguridad cibernética en el contexto de Huawei, logrando cumplir con los objetivos planteados. Los resultados obtenidos arrojan luz sobre la compleja dinámica del ciberespacio entre potencias, destacando la importancia de fortalecer la ciberseguridad como mecanismo de defensa ante amenazas en constante evolución.

La evaluación de las acusaciones contra Huawei revela una situación controvertida, donde las afirmaciones de ciberespionaje son objeto de disputa. Aunque la empresa ha negado cualquier conexión indebida con el gobierno chino, estas disputas generan tensiones políticas y económicas a nivel internacional.

El análisis de decisiones gubernamentales y regulatorias relacionadas con Huawei subraya la intersección entre seguridad nacional, competencia global y relaciones internacionales. Las medidas adoptadas por varios países han tenido implicaciones significativas en el mercado tecnológico, destacando la complejidad política y económica de la presencia de Huawei a nivel mundial.

En el ámbito de la ciberseguridad corporativa, se extraen lecciones valiosas del caso Huawei, enfocándose en la gestión de contratos y la constante vigilancia ante amenazas. Estos aprendizajes resaltan la necesidad prioritaria de inversiones en ciberseguridad, influyendo en decisiones estratégicas y alianzas comerciales.

La brecha entre el sector privado y las instituciones gubernamentales en Costa Rica en términos de ciberseguridad destaca la importancia de una colaboración más estrecha. Aunque se reconoce la necesidad de la colaboración público-privada, persisten brechas que requieren una sincronización más efectiva entre ambos sectores.

En cuanto a tendencias y desafíos emergentes, se observa una efectiva adopción de nuevas tecnologías, pero los desafíos persisten frente a la evolución constante de amenazas y la necesidad crítica de contar con personal capacitado. Se evidencia la necesidad de adaptarse rápidamente a estas tendencias para garantizar una ciberseguridad robusta.

La evaluación del marco legal de ciberseguridad en Costa Rica destaca avances notables respaldados por el MICITT y leyes específicas. Sin embargo, áreas críticas de mejora incluyen la necesidad de educación continua y una mayor colaboración público-privada.

Comparativamente, se observan avances positivos, especialmente en la Contraloría General de la República. A pesar de ello, se destaca la necesidad de dedicar mayores recursos para abordar la ciberseguridad de manera integral. Desafíos identificados, como la falta de legislación específica y la necesidad de capacitación, podrían superarse mediante el fortalecimiento de leyes de información pública y la designación de una entidad responsable.

En el ámbito empresarial, las regulaciones imponen costos adicionales y cambios en las estrategias, pero el cumplimiento efectivo fortalece la resiliencia y mejora la reputación de las empresas. Mirando hacia el futuro, se visualiza la búsqueda de normativas internacionales, la protección de servicios críticos y mejoras legislativas. Sugerencias clave incluyen auditorías obligatorias, coordinación internacional, entes reguladores constantes y leyes actualizadas para fortalecer la protección legal y promover la seguridad de la información.

Estas recomendaciones, aunque significativas, deben interpretarse considerando las limitaciones inherentes a este estudio, tales como las tensiones políticas y las relaciones internacionales, especialmente aquellas relacionadas con Huawei y China, podrían haber influido en la disponibilidad de información precisa y objetiva. Esto podría haber introducido sesgos o limitaciones en la interpretación de los datos recopilados.

A pesar de estas limitaciones, el presente trabajo aporta significativamente al campo de estudio de las Relaciones Internacionales, al ofrecer un análisis detallado de la ciberseguridad corporativa, centrándose específicamente en el caso de Huawei. En el contexto de un nuevo panorama internacional y las crecientes herramientas tecnológicas que moldean las dinámicas globales, este estudio proporciona una visión clave sobre la intersección entre la ciberseguridad corporativa y las relaciones internacionales.

Bibliografía

Association for Computing Machinery (ACM). (30 de noviembre de 1988). *Formalización de la Disciplina de Ciberseguridad.* EuroInnova International Online Education. https://www.euroinnova.edu.es/cuando-se-creo-la-ciberseguridad

BBC News Mundo. (7 de junio de 2019). *Huawei: ¿qué empresas compiten con la compañía china en el desarrollo de la tecnología 5G?* https://www.bbc.com/mundo/noticias-48556359

BBC News Mundo. (12 de enero de 2019). *Huawei: el nuevo escándalo por espionaje que sacude al gigante tecnológico chino tras la detención de uno de sus directivos en Polonia*. https://www.bbc.com/mundo/noticias-internacional-46853250

Blanco, E., Fontrodona, J., & Poveda, C. (1999). *El marco conceptual.* Paidotribo.

Blanco, E., Fontrodona, J., & Poveda, C. (2017). La industria 4.0: el estado de la cuestión. *Economía Industrial.* https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/406/BLANCO,%20FONTRODONA%20Y%20POVEDA.pdf

Blinder, D. (Abril de 2021). *Realismo y Relaciones Internacionales: una observación desde la historia de la ciencia y la epistemología.* https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100119

Chacín, R. B. (24 de mayo de 2017). *La nueva era de los negocios: computación en la nube*. Venezuela. https://dialnet.unirioja.es/servlet/articulo?codigo=8577212

Cordero, J. L. (2014). *Interdependencia compleja. Cuatro enfoques teóricos.* https://www.scielo.org.mx/pdf/rcsl/v4n7/v4n7a12.pdf

Díaz, J. M. (1 de octubre de 2019). *Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas.* https://scielo.isciii.es/scielo.php?pid=S1886-58872019000200006&script=sci_arttext

EuroInnova International Online Education. (s. f.). *Cuándo se creó la ciberseguridad*. https://www.euroinnova.edu.es/cuando-se-creo-la-ciberseguridad#iquestcuaacutendo-se-creoacute-la-ciberseguridad-y-por-queacute-es-una-buena-opcioacuten-profesional

Evans, D. (Abril de 2011). *Internet of Things. La próxima evolución del internet lo está cambiando todo*. https://media.telefonicatech.com/telefonicatech/uploads/2021/1/126528_Internet_of_Things_IoT_IBSG_0411FINAL.pdf

García, O. A. (5 de mayo de 2023). *Impacto de las capacidades de análisis de big data en la innovación empresarial.* http://www.scielo.org.co/scielo.php?pid=S0123-30332023000200010&script=sci_arttext

Gates, B. (1999). *Los negocios en la era digital*. http://tecnologiasemergentesnegocios2012.pbworks.com/w/file/fetch/53892566/los-negocios-en-la-era-digital.pdf

González, J. M. (s. f.). *Uso de las Técnicas Del Hacking Ético para la Reducción de Amenazas de Ciberseguridad.* https://prcrepository.org/bitstream/handle/20.500.12475/1939/PUPR_CEAH_SJU_SP23_MCpE_Jos%c3%a9%20M.%20Gonz%c3%a1lez%20Gonz%c3%a1lez_Article.pdf?sequence=1&isAllowed=y

Goris, S. J. (2015). *Utilidad y tipos de revisión de literatura.* https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1988-348X2015000200002#:~:text=La%20revisi%C3%B3n%20bibliogr%C3%A1fica%20se%20ha,publicaci%C3%B3n%20o%20un%20trabajo%20espec%C3%ADfico.

Guerra, I. A. (Septiembre de 2017). *La transformación digital de la empresa.* (Trabajo de fin de grado). Universidad de Cantabria. https://repositorio.unican.es/xmlui/bitstream/handle/10902/13402/ALONSOGUERRAIVAN.pdf?sequence=1&isAllowed=y

Hernández Mendoza, S. (5 de diciembre de 2020). Técnicas e instrumentos de recolección de datos. *Boletín Científico de las Ciencias Económico Administrativas del ICEA.*

Vol.9, No. 17 (2020) 51-53. https://repository.uaeh.edu.mx/revistas/index.php/icea/article/view/6019/7678

Instituto Nacional de Aprendizaje (INA) (s. f.). *Generaciones de las computadoras.* https://www.inavirtual.ed.cr/pluginfile.php/35937/mod_resource/content/1/Generaciones%20de%20las%20computadoras.pdf

Izcara P, S. y Andrade R., K. L. (2003). *La entrevista en profundidad: teoría y práctica.* https://www.researchgate.net/profile/Simon-Izcara-Palacios/publication/271516834_LA_ENTREVISTA_EN_PROFUNDIDAD_TEORIA_Y_PRACTICA/links/58949701a6fdcc45530efb32/LA-ENTREVISTA-EN-PROFUNDIDAD-TEORIA-Y-PRACTICA.pdf

Lalaleo-Analuisa, F. R., Bonilla-Jurado, D. M., & Robles-Salguero, R. E. (Septiembre de 2021). Tecnologías de la Información y Comunicación exclusivo para el comportamiento del consumidor desde una perspectiva teórica. *Retos* vol.11 no.21 Cuenca abr./sep. 2021. http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-86182021000100147&script=sci_arttext

Levy, I., Meschoulam, M., & Hernández, M. *Confrontación Estados Unidos-China: de geopolítica, tecnología y riesgos para nuestra región.*, s.f, https://interactivo.eluniversal.com.mx/online/pdf-19/PDF-china-eu.pdf

Maranto R., M. y González F., M. E. (Febrero de 2015). *Fuentes de Información.* Universidad Autónoma del Estado de Hidalgo. https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/16700/LECT132.pdf

Maroto, J. P. (2009). *El ciberespionaje y la ciberseguridad*. file:///C:/Users/Mario/Downloads/Dialnet-ElCiberespionajeYLaCiberseguridad-4549946%20(1).pdf

Medina Martínez, J. J. (2021). *Análisis del phishing y la ley de delitos.* file:///C:/Users/Mario/Downloads/1948-Texto%20del%20art%C3%ADculo-4640-2-10-20230529.pdf

Morales, L. E. (21 de marzo de 2023). *Recolección de datos: qué es, ventajas y consejos para usarlos.* Tecnológico de Monterrey. https://blog.maestriasydiplomados.tec.mx/recoleccion-de-datos-que-es-ventajas-y-consejos-para-usarlos

Romero, J., Matamoros, S. y Campo, C. A. (2013*). Sobre el cambio organizacional. Una revisión bibliográfica. Innovar* vol.23 no.50 Bogotá Oct./Dec. 2013. http://www.scielo.org.co/scielo.php?pid=S0121-50512013000400004&script=sci_arttext

Oviedo Guachamín, L. S. (2021). *Análisis de la guerra comercial China - Estados Unidos a partir del caso Huawei.* (Tesis de licenciatura). Pontificia Universidad Católica de Ecuador.https://repositorio.pucese.edu.ec/bitstream/123456789/2592/1/OVIEDO%20GUACHAM%c3%8dN%20LAYS%20STEFAN%c3%8dA%20.pdf

Porras, M. M. (2021-2022). *Ciberseguridad y redes 5G en las relaciones internacionales: el caso de Huawei.* https://ddd.uab.cat/pub/trerecpro/2022/266102/TFM_MireiaMartinPorras.pdf

Prieto, E. (7 de noviembre de 2023). *¿Cuál es la historia de la ciberseguridad?* https://worldcampus.saintleo.edu/noticias/historia-de-la-ciberseguridad#:~:text=La%20ciberseguridad%20no%20naci%C3%B3%20hasta,que%20conocemos%20en%20la%20actualidad.

Saldarriaga-Zambrano, P. J., Bravo-Cedeño, G. y Loor Rivadeneira, M. R. (25 de octubre de 2026). La teoría constructivista de Jean Piaget y su significación para la pedagogía contemporánea. *Revista Científica Dominio de las Ciencias.* Vol. 2, núm. esp., dic., 2016, pp. 127-137 https://dominiodelasciencias.com/ojs/index.php/es/article/view/298/355

Sosa O, E. y Godoy, D. (Junio de 2014). Internet del futuro. Desafíos y perspectivas. *Revista de Ciencia y Tecnología versión On-line* ISSN 1851-7587 http://www.scielo.org.ar/scielo.php?pid=S1851-75872014000100007&script=sci_arttext

Robles, B. (Septiembre-Diciembre de 2011). *La entrevista en profundidad: una técnica útil dentro del campo antropofísico.* https://www.redalyc.org/pdf/351/35124304004.pdf

Rosete, A. G. (24 de diciembre de 2020). *Adaptación del modelo de Inteligencia de Seguridad Corporativa en un mundo en disrupción.* https://www.segurilatam.com/tecnologias-y-servicios/seguridad-corporativa-integral/adaptacion-del-modelo-de-inteligencia-de-seguridad-corporativa-en-un-mundo-en-disrupcion_20201224.html

Vicarra, F. (2002). VIRUS INFORMATICO: Entre el negocio y el temor. *Chasqui: Revista Latinoamericana de Comunicacion*, Nº. 78, 2002, págs. 62-69. https://dialnet.unirioja.es/servlet/articulo?codigo=5791601

Yancey, J. (Abril de 2017). *Los ataques cibernéticos y sus repercusiones políticos.*https://repositorio.utdt.edu/bitstream/handle/20.500.13098/6596/MEI_2017_Yancey.pdf?sequence=1

Yocupicio, E. (Agosto de 2020). *Riesgos ciberneticos a un click de distancia* . https://universidadmundial.edu.mx/wp-content/uploads/2020/04/riesgos-ciberneticos-a-un-clicl-de-distancia.pdf