Plan de gestión de riesgos asociados a IoT para proteger la información en la Secretaría Distrital de Desarrollo Económico

Joe Alexander Nuñez Yaguna

Asesor

Mariano Esteban Romero Torres

Universidad Nacional Abierta y a Distancia

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Maestría en Gestión de Tecnología de Información

2024

Dedicatoria

Este, otro de los logros en mi vida como profesional lo dedico especialmente a DIOS, fuente de poder y conocimiento que me llevo a obtener este resultado como el cumplimiento de mis sueños.

Esta pasión de convertirme en Magister en Gestión de Tecnología de Información a través de una Universidad no ha sido solo, está acompañado de todos mis seres queridos como mis padres Silvio Núñez y Yasira Yaguna, mi esposa Julieta Vicioso y mi hija Julieth Valentina quien con su amor y confianza han sido una gran motivación para conseguir este nuevo objetivo.

Gracias a todas las personas que participaron en que este sueño se convirtiera en realidad.

Agradecimientos

Mi agradecimiento superior a Dios por permitirme tener vida y salud para conseguir mis logros profesionales y personales.

Es mi deseo como sencillo gesto de agradecimiento, reconocer por su apoyo, paciencia y dedicación como asesor de este proyecto de grado al Ingeniero Especialista en Seguridad Informática Mariano Esteban Romero Torres su forma de guiarme con su conocimiento para el desarrollo de este trabajo de grado.

Finalmente, un agradecimiento especial a la UNAD y al grupo de docentes de la Escuela de Ciencias Básicas, Tecnología e Ingeniería por su orientación, acompañamiento y gestión en este proceso de aprendizaje muy enriquecedor en adelante para mi vida profesional y laboral.

Resumen

El presente documento de investigación se enfoca en la seguridad y privacidad de la información, un aspecto crucial para las organizaciones en la era del Internet de las Cosas (IoT), proteger la información es esencial para garantizar la disponibilidad, confidencialidad e integridad de los datos.

En este contexto, la gestión de los riesgos con los activos IoT se ha convertido en un desafío fundamental para las empresas, uno de los mayores obstáculos en el uso de dispositivos IoT es la falta de conciencia de los usuarios respecto a los riesgos potenciales. Por ello, este proyecto de investigación tiene como objetivo principal diseñar un plan de gestión de riesgos que aborde este problema y las herramientas necesarias para proteger la información generada.

Entre los principales hallazgos de este proyecto aplicado de investigación, se dilucidó la situación actual de la seguridad de los datos que se transmiten con los dispositivos IoT. Además, en el análisis exhaustivo de los activos de información se encuentra que la SDDE cuenta con elementos como equipos de comunicaciones, seguridad perimetral y bases de datos con funciones autónomas asociados a IoT, los cuales al realizar la respectiva evaluación del nivel de riesgos se detectan las posibles amenazas o vulnerabilidades que los afectan.

Posteriormente, acorde con los resultados se propone un plan de gestión de riesgos para mejorar la seguridad aplicando los controles recomendados por la norma ISO/IEC 27001.

Para desarrollar esta investigación aplicada, se empleó una metodología basada en la búsqueda, recolección, análisis y articulación de datos cuantitativos y cualitativos, con el fin de responder a la problemática identificada y como referente de buenas prácticas en la administración de riesgos y oportunidades asociadas a la TI, se utilizó la norma ISO/IEC 27001.

Palabras Clave: Seguridad digital, administración de riesgos, confianza digital.

Abstract

This research document focuses on information security and privacy, a crucial aspect for organizations in the era of the Internet of Things (IoT), protecting information is essential to guarantee the availability, confidentiality and integrity of data.

In this context, risk management with IoT assets has become a fundamental challenge for companies; one of the biggest obstacles in the use of IoT devices is the lack of user awareness regarding potential risks. Therefore, the main objective of this research project is to design a risk management plan that addresses this problem and the necessary tools to protect the information generated.

Among the main findings of this applied research project, the current situation of the security of data transmitted with IoT devices was elucidated. Furthermore, in the exhaustive analysis of the information assets it is found that the SDDE has elements such as communications equipment, perimeter security and databases with autonomous functions associated with IoT, which when carrying out the respective risk level evaluation are detected. the possible threats or vulnerabilities that affect them.

Subsequently, according to the results, a risk management plan is proposed to improve security by applying the controls recommended by the ISO/IEC 27001 standard.

To develop this applied research, a methodology was used based on the search, collection, analysis and articulation of quantitative and qualitative data, in order to respond to the identified problems and as a reference for good practices in the management of risks and opportunities associated with IT, the ISO/IEC 27001 standard was used.

***Keywords**:* Digital security, risk management, digital trust.

Introducción

La Secretaría Distrital de Desarrollo Económico, se encarga de liderar y ejecutar las políticas públicas de desarrollo económico para mejorar la competitividad empresarial, la productividad de la ciudad y la seguridad alimentaria de los ciudadanos del distrito de Bogotá, y como parte de sus estrategias debe cumplir con el componente de seguridad y privacidad de la información, eje principal de la investigación que se detalla en este documento, buscando mantener los principios de confidencialidad, integridad, disponibilidad de la información.

En el presente libro de proyecto de investigación, se muestran datos fundamentados y las evidencias necesarias para obtener los resultados esperados, cuyo objetivo principal fue diseñar un plan de gestión de riesgos apuntando a minimizar los riesgos que se presentan con el uso del IoT apoyado en la norma ISO/IEC 27001 para fortalecer el enfoque en la seguridad de la información y proteger la información en la Secretaría Distrital de Desarrollo Económico, que se derivó de un diagnóstico previo de la situación de la entidad.

La investigación se llevó a cabo usando una metodología bajo el paradigma empírico-analítico adecuado para estudiar los riesgos en IoT, combinando encuestas, revisión documental y matriz DOFA, con una confiabilidad de los datos robustecida por la evaluación de los instrumentos cuantitativos de investigación por parte del Juicio de Expertos, y, para el diseño del plan se aplicó los lineamientos de la norma ISO 27001 empleando el ciclo de Deming, también conocido como ciclo PHVA.

Este documento está organizado por capítulos, en el primero se aborda el problema de investigación donde se describe la naturaleza y magnitud del problema que se espera resolver con el logro de cada uno de los objetivos planteados en el proyecto. En el segundo capítulo y tercer capítulo el libro se esboza la fundamentación teórica de conocimientos, metodología de

investigación y las técnicas existentes para desarrollar proyecto aplicado. En el cuarto apartado se plasman los resultados de cada una de las fases de investigación; se muestra el diagnóstico de la situación actual en la empresa, los activos de información identificados asociados con IoT, las posibles amenazas o vulnerabilidades que puedan afectarles y la propuesta de plan de acción para que la SDDE fortalezca su Modelo de Seguridad y Privacidad de la Información (MSPI), y proteger sus recursos digitales buscando asegurar la continuidad de los procesos brindados a la ciudadanía en general.

Tabla de Contenido

Listas de Tablas

Listas de Figuras

Listas de Apéndices

El Problema

Descripción del Problema

La tecnología ha impulsado transformaciones significativas en diversos ámbitos sociales mediante la invención del internet, el desarrollo de dispositivos móviles y la expansión de la comunicación electrónica, cuyos procesos han facilitado la interacción entre personas a nivel global. En la actualidad, existen objetos capaces de transmitir, compilar y distribuir datos a la red, cuyo fenómeno es conocido como Internet de las Cosas (IoT). Esta tecnología se basa en una conexión de objetos articulados que, utilizando protocolos comunicativos estandarizados, permiten la conexión de cualquier dispositivo a internet, posibilitando el procesamiento de datos y la comunicación entre ellos, ya sea con o sin intervención humana. En tal sentido, los dispositivos inteligentes conectados a una red IoT contienen diversos tipos de datos cuya medición está integrada a protocolos de comunicación que, son enviados posteriormente, a una base de datos para analizar sistemas inteligentes con funciones específicas como la apertura de puertas, activación de cámaras y puesta en alerta al usuario mediante el uso de aplicaciones. Por ello, todo dispositivo o sistema que esté conectado a una red, sea por cable, de forma inalámbrica y que tenga como función principal la comunicación y/o interconexión a través de la nube o internet, denominado Internet de las Cosas (IoT). No obstante, los riesgos que pueden tener dichos dispositivos conectados a internet, ya sean de uso personal o corporativo son inminentes, pues la distorsión del suministro de datos de carácter empresarial y estrictamente confidenciales, pueden poner en riesgo las dinámicas entre los usuarios y actores corporativos. Empero, esto puede evadirse realizando una adecuada gestión de riesgos que salvaguarde la disponibilidad, la compactibilidad y la privacidad de la información provenientes de los actores antes mencionados respecto al IoT. En este contexto, el documento CONPES 3995, vigente en Colombia desde el 1

de julio de 2020 y emitido por el Departamento Nacional de Planeación (DNP), busca establecer una política nacional orientada a fortalecer la confianza y seguridad digital. Su objetivo es promover una sociedad más inclusiva y competitiva a nivel nacional. En consonancia con esto, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC) ha comenzado a divulgar las guías para la Cuarta Revolución Industrial 4.0. Esta iniciativa, enmarcada en la estrategia "Hablemos de Gobierno Digital", asume temáticas de inteligencia artificial, Big Data, Blockchain, Cloud Computing, IoT y obsolescencia tecnológica.

Dado lo anterior, resulta crucial atender la seguridad digital de los dispositivos empleados en las organizaciones, cuya información es esencial para su funcionamiento diario (Nurse et al., 2017). Estos autores exploran metodologías para evaluar el riesgo, teniendo en cuenta la interactividad y particularidad del IoT, mientras se conservan alineados con las mejores prácticas evaluativas en gestión de riesgos. En su análisis, destacan la transferencia de varios métodos, pautas y recursos para valorar riesgos, como:

- NIST SP800-30 (National Institute of Standards and Technology)
- ISO/IEC 27001 (International Organization for Standardization)
- OCTAVE (Operational Critical, Threat, Asset and Vulnerability Evaluation)
- CRAMM (CCTA Risk Analysis and Management Method)
- EBIOS (Expression of Needs and Identification of Security Objectives)

Además, los autores describen los componentes y la arquitectura del IoT, elementos fundamentales en la gestión de riesgos, puesto que permiten identificar y evaluar los dispositivos IoT dentro de las empresas, facilitando una gestión adecuada de los riesgos potenciales. Es importante resaltar que el uso de dispositivos IoT en las organizaciones presenta desafíos significativos en la implementación de la seguridad digital, como lo mencionan los autores

citados. Asimismo, Brous et al. (2020) señalan que el IoT genera un gran flujo de información que, de manera reiterativa, son mejores que los producidos por métodos tradicionales debido a su mayor granularidad y precisión, así como por su heterogeneidad derivada de múltiples fuentes, y por su oportunidad en tiempo real o diferido y los volúmenes significativamente más grandes que manejan.

Por otro lado, siguiendo a Alsharif et al., (2022), aluden que los dispositivos de IoT son más eficaces, aun cuando la cantidad de dispositivos conectados a la red es mayoritaria, razón por la cual los gobiernos y empresas están disponiendo de estas tecnologías para el desarrollo de actividades comerciales de forma segura. No obstante, el creciente uso de las tecnologías también incrementa significativamente los riesgos, como ataques a contraseñas, Phishing y vulnerabilidades en la ingeniería social. Por esta razón, es fundamental concienciar a los usuarios sobre los peligros a los que se expone la información cuando no se utilizan correctamente los dispositivos IoT. De acuerdo con Alsharif et al. (2022), los seres humanos juegan un papel fundamental en la ciberseguridad, puesto que más del 39% de las amenazas a la seguridad informática están vinculadas a factores humanos, y el 95% de los ciberataques se originan por fallos cometidos por personas, lo que indica que muchas amenazas provienen del interior. Por otro lado, las empresas deben implementar mejores prácticas de seguridad para mitigar los posibles riesgos generados por su personal. Además, para constatar uso correcto de los recursos dentro de las organizaciones, es esencial evaluar cómo interactúan estos recursos con el entorno externo. Se debe ofrecer a los usuarios un entorno seguro que proteja los preceptos esenciales de la seguridad informática como la disponibilidad, integridad y confidencialidad, siendo esta última considerada la base esencial de la seguridad de la información.

Teniendo en cuenta el entramado problémico de la presente investigación desde el ámbito empresarial educativo, es necesario señalar que el Foro Nacional de Estadísticas Educativas de los Estados Unidos desarrollado el presente año, reportó qué el 100% del suministro de datos de los estudiantes y sus familias se deberán considerar confidenciales y no ser susceptibles de manipulación. No obstante, pese a lo antes mencionado, un artículo publicado por Aguirre (2022), indicó que el 67% de los establecimientos educativos latinoamericanos, han sido víctimas de ataques cibernéticos y, que el 44%de las empresas encuestadas, no le prestan atención a la seguridad informática. De igual manera, una publicación titulada *"Panorama actual sobre la seguridad de la información en establecimientos educativos oficiales de educación básica y media en Colombia"*, expresó que Colombia había sido uno de los países latinoamericanos con más ataques cibernéticos en el año 2018 y que, dos de cada tres encuestados habían sufrido ataques cibernéticos.

Remitiéndonos al entramado problémico del escenario objeto de investigación, es necesario señalar que este se centra en la vulnerabilidad de la seguridad y confidencialidad de datos registrados en los dispositivos de IoT de la SDDE, cuya probabilidad de riesgo de seguridad de la información de dichos dispositivos es alta en términos de cualificación del recurso humano, pues el personal no está preparado para prevenir correctamente la seguridad de los dispositivos IoT. Otra de las causas corresponde a que la entidad no posee herramientas de manejo de incidentes para dispositivos IoT y la SDDE no es consciente de cómo el uso de IoT afecta la gestión de riesgos de ciberseguridad. Otro aspecto a señalar es que los equipos no proporcionan parches o actualizaciones para sus software y firmwares, además de que algunos dispositivos IoT no pueden ser gestionados por la entidad, tampoco se gestionan los activos ni los accesos asociados a IoT.

En cuanto a materiales, métodos y política de riesgos, los dispositivos asociados a IoT corresponden a modelos muy antiguos y de los cuales no se poseen manuales de uso o técnicos, además de que a SDDE no cuenta con procedimientos orientados a la gestión de riesgos asociados a IoT y, consecuentemente, las directrices de riesgos de seguridad y privacidad de la información no ha sido divulgada y compartida a toda la comunidad organizativa. Respecto a los efectos causados por el problema investigado, se encuentran la pérdida de la información provocada por incidentes de ciberseguridad, robo de la información, información no confiable pérdida de la imagen y credibilidad institucional por información fraudulenta.

Por todo lo antes mencionado y para efectos de mitigar el panorama de riesgos conforme a ciberseguridad y, en tal caso, dar solución a la problemática anteriormente descrita, surge la siguiente pregunta problémica.

Formulación del Problema

¿De qué manera el diseño de un plan de gestión de riesgos para el IoT, puede contribuir a la seguridad de la información en la Secretaría de Desarrollo Económico?

Subpreguntas

Para identificar oportunidades de mejoramiento y asumir medidas para la mejora continua del SGSI de la SDDE:

¿Cuáles son los activos de información asociados al IoT en la SDDE?

¿De qué manera puede determinarse la magnitud de riesgos asociados a los activos de información del IoT a partir de lo que consigna la norma ISO 27001?

¿De qué manera puede protegerse la seguridad de la información en IoT y que ello se rija como principio en la SDDE conforme a la norma ISO 27001?

Objetivos

Objetivo General

Diseñar un plan de gestión de riesgos de IoT apoyado en la norma ISO/IEC 27001 para proteger la información en la Secretaría Distrital de Desarrollo Económico.

Objetivos Específicos

Identificar mediante un análisis diagnóstico los activos de información asociados a IoT en la SDDE, a partir de aplicación de encuestas y la revisión del inventario de información de la entidad.

Evaluar el nivel de riesgos para identificar las amenazas y vulnerabilidades de los activos de información asociados a IoT, alineados con la norma ISO 27001.

Proponer un plan de acción con un enfoque basado en el ciclo de mejora continua para que la seguridad de la información en IoT se convierta en cultura organizacional de acuerdo con lo establecido en la norma ISO 27001.

Justificación

La innovación es un gran beneficio para las empresas, puesto que la automatización con dispositivos de conexión a internet les ofrece un control masivo de la información para la óptima toma de decisiones. cuando se recopilan datos se crean nuevas ideas para el incremento de la productividad, oferta y demanda de productos, así como el aumento de la seguridad por la supervisión rigurosa de la infraestructura. con ello se propende por la eficiencia y eficacia, se reducen los márgenes de error en la productividad por carencias de mantenimiento o desconocimiento de los procesos productivos y, en tal caso, se aumenta el nivel de satisfacción de los consumidores.

Teniendo en cuenta lo anterior, en la era digital las empresas buscan incrementar sus inversiones en herramientas cuyos procesos emergentes de sistemas de cómputo, recurso humano y productos, se vinculen a una sola cadena de análisis y recolección de datos. Entre tanto, la base fundamental de la digitalización de una empresa son las redes de los dispositivos, cuyo apelativo es el Internet de las Cosas (IoT).

En la actualidad, la seguridad de la información ha cobrado gran relevancia en las empresas, ya que resulta esencial cumplir con los objetivos clave de salvaguardar y proteger la información, garantizando la disponibilidad, confidencialidad e integridad de los datos. Por tanto, es fundamental implementar estrategias adecuadas para gestionar eficazmente los riesgos, particularmente aquellos asociados al uso de dispositivos IoT en las organizaciones. Según Malik y Singh (2020), los dispositivos IoT anticipan un futuro en el que estos sistemas, interoperables, eficientes y efectivos, se comunican entre sí mediante tecnologías avanzadas, generando un alto volumen de datos a una gran velocidad de procesamiento. Esta información es valiosa para optimizar la experiencia de los usuarios, aunque conlleva riesgos como el uso indebido o la

pérdida de datos. Por ello, a medida que la tecnología avanza, es crucial considerar un plan adecuado de gestión de riesgos. En este sentido, Nurse et al. (2017) destacan que los mecanismos de evaluación de riesgos para la seguridad informática han sido de gran importancia en las últimas dos décadas.

Se han propuesto diversas alternativas para que los gobiernos y organizaciones puedan protegerse de riesgos emergentes. En este contexto, el incremento de metodologías para la evaluación de los sistemas IoT plantea un reto importante, ya que los nuevos riesgos inherentes a estos ecosistemas podrían estar vinculados al alto nivel de conectividad o al acoplamiento de los sistemas digitales, ciberfísicos y sociales. En consecuencia, es fundamental destacar que numerosas entidades públicas han avanzado en la aplicación del Modelo de Seguridad y Protección de la Información (MSPI), promulgado por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC). Este modelo consta de 21 guías específicas, cuyo objetivo principal es fomentar la adopción de un conjunto de procedimientos para garantizar la seguridad y protección de la información en las instituciones estatales.

No obstante, es importante señalar que conforme a las pautas del MSPI no existe una enfocada específicamente en la gestión de riesgos relacionados con dispositivos IoT. Es precisamente aquí donde este trabajo cobra relevancia, ya que busca responder a esa necesidad identificada, aportando desde el ámbito académico hacia el empresarial. De esta manera, se espera generar un beneficio para los grupos de interés de la organización que implementen la guía de gestión de riesgos aplicada a dispositivos IoT, siguiendo los lineamientos establecidos por la norma ISO 27001.

El proyecto de investigación en curso tiene como propósito principal proponer una guía de gestión de riesgos para el Internet de las Cosas (IoT) dentro de la Secretaría Distrital de

Desarrollo Económico. Esto facilitará el perfeccionamiento de las directrices de seguridad y la protección de la información, lo que contribuirá al fortalecimiento de la gestión de riesgos dentro de la organización. De igual manera, la investigación busca apoyar a las instituciones en la alineación, revisión, análisis, creación y optimización de herramientas como planes, procedimientos, manuales, guías, formatos e instructivos, en conformidad con la política de gobierno digital, así como con el modelo de seguridad y protección de la información. Un objetivo notable es fomentar las prácticas óptimas en la seguridad de la información, apoyando la mejora en los procesos de intercambio de información pública, optimizando la gestión de la seguridad de la información dentro de las organizaciones y contribuyendo al desarrollo del plan estratégico institucional. Asimismo, se busca la elaboración del plan estratégico de información y comunicaciones, cuyas acciones constituirán la base para la implementación del concepto de seguridad digital.

Entre tanto, este trabajo tiene como propósito contribuir al cumplimiento del CONPES 3995 (DNP, 2020) por parte de la SDDE. Dicho documento tiene como misión implementar acciones orientadas a fortalecer la confianza y seguridad digital, con el fin de que Colombia se convierta en una sociedad inclusiva y competitiva en el entorno digital futuro. De esta manera, se propone diseñar un plan que evalúe los riesgos considerando las particularidades del Internet de las Cosas (IoT), sin dejar de aplicar las mejores prácticas de evaluación de riesgos con el rigor necesario.

También es necesario precisar que, conforme a la trazabilidad de los objetivos específicos, el alcance del primero permitirá conocer en el más amplio sentido los activos de información asociados a IoT en el contexto investigativo, con el segundo se prevendrán los riesgos de los activos de información asociados a IoT desde la norma ISO 31000, para el caso del

tercero, se tomarán las medidas necesarias para que la seguridad de la información en IoT se constituya en un principio ineludible que fomente y fortalezca la cultura organizacional conforme a la normatividad establecida.

Alcance

El presente proyecto investigativo se basa en el diseño de un plan apoyado en las normas ISO 27001 e ISO 31000, las cuales establecen los requerimientos para la implementación, seguimiento, control y mejora continua del Sistema de Gestión de la Seguridad de la Información, además de regir las normas necesarias para que las organizaciones efectúen un análisis y evaluación de riesgos de manera eficiente y eficaz. Con ello se busca que la SDDE proteja la confluencia de datos emergentes que, como organización, gestiona y ejecuta políticas de desarrollo económico, competitividad y economía rural, enfocadas a la promoción y fortalecimiento de pequeñas y medianas las empresas, así como el abastecimiento alimenticio, la promoción de empleo y nuevos ingresos para los ciudadanos en Bogotá. Esto indicará los procedimientos y controles de seguridad que deben tener en cuenta los encargados del área de tecnología, con el fin de mejorar la seguridad de la información por las vulnerabilidades contenidas en los activos asociados al IoT.

También, el lector final entenderá cuales son los riesgos a los que se enfrenta cuando hace uso de hardware y software de IoT, ayudando a concebir la problemática que presenta la tecnología y sus vulnerabilidades.

Delimitaciones

Ahora bien, dentro de las principales limitaciones del proyecto se contempla la ejecución de dicho plan, dado que la disponibilidad del tiempo y espacio para su aplicabilidad es poca, cuya práctica de seguridad informática se constituye en una restricción operacional.

Otra de las posibles limitaciones del estudio es la indisponibilidad del personal de la empresa para participar en el estudio, los posibles sesgos muestrales y las probables intermitencias de la red para la conformación y desarrollo de actividades mediante el trabajo colaborativo.

Además, factores externos que están fuera del control de este proyecto aplicado, como los generados por movilización laboral de los directivos y subdirectivos encargados de cada una de las áreas que conforman de la SDDE, podrían influir en los resultados esperados de esta investigación, debido a los cambios en la toma de decisiones de las personas que ocupan estos cargos administrativos de naturaleza provisional.

Otra de las posibles limitaciones del estudio es la indisponibilidad del personal de la empresa para participar en el estudio porque si no se encuentran disponibles para responder las encuestas que hacen parte de las actividades que el investigador debe ejecutar podría verse afectada la recopilación de datos necesarias para determinar el diagnóstico de la situación actual de la SDDE; los posibles sesgos muestrales y las probables intermitencias de la red para la conformación y desarrollo de actividades mediante el trabajo colaborativo dado que se afectaria la comunicación entre los participantes e incluso impedir que se lleven a cabo el trabajo de la manera deseada.

El continuo crecimiento de la industria encargada de producir componentes IoT genera una limitación práctica en cuanto a la implementación de controles y soluciones viables para enfrentar los ataques a dispositivos que han sido instalados sin las medidas de seguridad adecuadas, razón por la que este documento no aborda de manera detallada, los procedimientos específicos para la implementación de herramientas de seguridad informática, lo que constituye una restricción práctica. Tampoco contempla la creación de dispositivos ni la elaboración de

entornos de prueba para identificar las vulnerabilidades de seguridad en los activos relacionados con IoT. Por lo tanto, el proyecto es de carácter documental y se enfoca exclusivamente en definir los elementos teóricos sobre la seguridad que debe aplicarse a los activos de información IoT utilizados en la entidad acorde con el estándar de la norma ISO/IEC 27001.

Marco de Referencia

En esta sección se efectúa un análisis exhaustivo de la literatura global, que abarca tanto los estudios realizados a nivel internacional como aquellos desarrollados en los contextos nacionales y locales. De igual manera, se consigna información de los aspectos espacio-temporales del escenario objeto de investigación, posteriormente, se desarrolla la revisión de la literatura universal y, de manera secuencial, los trayectos teóricos, conceptuales y legales que fundamentan el objeto de estudio. La presente recopilación documental expone cómo se han descrito tanto el contexto como los actores emergentes, además de ilustrar las diversas aproximaciones con las que los investigadores han desarrollado sus estudios, arquetipos onto-epistémicos y legislativos que atañen el estudio, es decir, es un proceso que consta del rastreo, el análisis, la lectura y el contraste de la bibliografía encontrada del tema en cuestión, así como de las tendencias desarrolladas desde los diferentes contextos y miradas de los investigadores, sus hallazgos y problemas estudiados en el campo. A continuación, se expone la interrelación de los aspectos previamente mencionados dentro de este contexto.

Alshurideh et al. (2023) llevaron a cabo una investigación titulada "The effect of information security on e-supply chain in the UAE logistics and distribution industry", cuyo objetivo fue analizar el rol mediador del riesgo en la cadena de suministro dentro de la industria logística y de distribución. Este estudio proporciona datos relevantes para investigaciones futuras y sectores especializados. El modelo propuesto empleó un diseño descriptivo, causal y analítico basado en un enfoque cuantitativo. Se utilizó una muestra de 301 encuestas aplicadas a gerentes de 176 empresas de logística y distribución ubicadas en Dubai y Abu Dhabi, con el fin de evaluar las variables implicadas en la investigación. Los resultados indicaron que los sistemas de información ejercen un impacto positivo en la cadena de suministro electrónica. Además, el

riesgo asociado a la cadena de suministro también mostró un efecto indirecto positivo significativo en la misma. Este hallazgo es clave para la toma de decisiones relacionadas con la seguridad de la información en cadenas de suministro electrónicas, sugiriendo la implementación de políticas internas que mejoren tanto el rendimiento como la gestión del riesgo informático.

Por su parte, Ming-Lang et al. (2023), en su estudio "Cyber supply chain risk management and performance in industry 4.0 era: information system security practices", buscaron identificar las influencias directas e indirectas de las prácticas de seguridad de los sistemas de información en la relación entre la gestión de riesgos en la cadena de suministro cibernética y su desempeño. Mediante encuestas en línea a 105 empresas en Malasia y utilizando el modelado de ecuaciones estructurales de mínimos cuadrados parciales, se evaluaron tanto la idoneidad del modelo como las hipótesis planteadas. Los resultados demostraron que las operaciones inciden directa e indirectamente en el rendimiento de la cadena de suministro a través de mediadores, mientras que la gobernanza influye directamente en la flexibilidad de esta y, de manera indirecta, en su desempeño. Sin embargo, la integración de sistemas no mostró efectos ni directos ni indirectos, lo cual sugiere que las empresas manufactureras y sus asociados han alcanzado una mayor comprensión de la gestión de riesgos en la cadena de suministro cibernética.

En la investigación realizada por Geethamanikanta et al. (2022), titulada "Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management", se exploraron diversas áreas en las que la inteligencia artificial (IA) ha desempeñado un rol crucial en la mitigación de riesgos cibernéticos dentro del ámbito de la seguridad y gestión de información. Este estudio examinó el creciente número de ataques cibernéticos y el papel de la IA en la seguridad de la información en los sectores financiero y administrativo. Se adoptó un

enfoque mixto basado en la revisión de literatura existente y encuestas a 50 empleados del sector industrial, logrando obtener una visión integral sobre el tema. La principal conclusión fue que el uso de IA ha acelerado significativamente las estrategias de gestión de riesgos cibernéticos.

Atif et al. (2022), en su estudio "Smartphone Security Hardening: Threats to Organizational Security and Risk Mitigation", identificaron los principales riesgos de seguridad que las organizaciones enfrentan por el uso de dispositivos móviles personales en el entorno laboral. También se destacaron medidas de mitigación, como configuraciones seguras y herramientas específicas, para fortalecer la seguridad organizacional. Se concluyó que la revisión periódica de la seguridad en dispositivos personales incrementa la conciencia entre empleados y empleadores sobre la protección de información confidencial.

En el estudio de Raghuvanshi et al. (2022), "Intrusion Detection Using Machine Learning for Risk Mitigation in IoT-Enabled Smart Irrigation in Smart Farming", se desarrolló un marco para detectar intrusiones en redes IoT utilizadas en la agricultura inteligente. El estudio abordó la importancia de la seguridad en este tipo de redes y propuso el uso de algoritmos de aprendizaje automático como máquinas de vectores soporte y bosques aleatorios para clasificar y analizar las amenazas. Los resultados permitieron evaluar el rendimiento de los algoritmos basados en parámetros como precisión y recuperación, subrayando la relevancia de la seguridad en el IoT agrícola.

Lo expuesto evidencia que las tecnologías de la información en corporaciones e instituciones públicas y privadas son esenciales para la calidad de los servicios, con las TIC jugando un papel central en la gestión de la seguridad informativa. No obstante, la aparición de amenazas cibernéticas interfiere en los procesos comerciales, haciendo imprescindible una gestión de riesgos eficaz que reduzca dichas amenazas. El análisis de la gestión de riesgos debe

centrarse en evaluar el contexto, identificar posibles riesgos y aplicar medidas correctivas que fomenten una gestión segura y responsable de la información.

En el contexto peruano, Landaeta-Arcentales et al. (2021) implementaron un estudio titulado "Diseño e implementación de un sistema de registro de accesos utilizando IoT", cuyo objetivo fue mejorar la seguridad física en un datacenter mediante el uso de tecnologías IoT. El estudio, que empleó un diseño pre-experimental, mostró que la implementación de un sistema integral de registro de accesos mediante IoT mejoró la seguridad del datacenter y optimizó el uso de recursos en la institución.

Por otro lado, Angulo-Montenegro (2023), en su investigación en Ecuador, desarrolló un sistema de monitoreo contínuo basado en IoT para medir la contaminación atmosférica. Este estudio implementó un controlador Esp8266 y sensores para recopilar datos en tiempo real, permitiendo el monitoreo remoto a través de una plataforma web. Los resultados destacaron el potencial del IoT para mejorar la calidad del aire y proporcionar información accesible sobre condiciones ambientales.

En Colombia, Contreras-Hernández et al. (2022) llevaron a cabo una investigación titulada "Propuesta Integral de gobierno de la información para la Secretaría Jurídica Distrital", la cual se centró en la gestión de la información en una entidad gubernamental mediante un enfoque estratégico. Esta propuesta incluyó políticas y procedimientos destinados a mejorar la transparencia y la gestión documental a través de las TIC.

Finalmente, Ramos-Guzmán et al. (2023) desarrollaron una propuesta de consultoría para la implementación del WAF en AWS, un servicio diseñado para proteger aplicaciones web de ataques maliciosos. La consultoría incluyó fases de análisis, diseño, implementación y

capacitación, concluyendo que la correcta implementación del WAF mejoró la seguridad de las aplicaciones web y generó mayor confianza entre los usuarios.

Marco Teórico Conceptual

En este acápite se describe el arquetipo teórico y conceptual del presente estudio, cuyas consideraciones soportan las variables que subyacen de diversos autores, por lo tanto, esta sección comprende el sustento de la investigación cuya compilación informativa, busca exponer el criterio de innovación que el proyecto investigativo tiene en un área específica del conocimiento (Ñaupas, 2018).

Lo anterior precisa el fenómeno de interés, sus conceptos relevantes y lo que se quiere ahondar a lo largo del estudio, además de justificar, comprobar e interpretar la hipótesis y los hallazgos de una investigación, esto de manera coherente y sistemática. Asimismo, busca formular, con la debida confiabilidad, las conclusiones o el replanteamiento de una pregunta problematizadora con mayor exhaustividad, por ello, se hace necesario destacar las dimensiones y/o categorías donde subyace, a la luz del estudio, el acervo conceptual donde se circunscribe la formulación del problema.

Por lo anteriormente expuesto, vale precisar la perspectiva teórica del conectivismo expuesta por George Siemens, quién explica cómo la tecnología ha influido, significativamente, en el mundo en el que los individuos viven, dentro del que se comunican e intercomunican. Esta perspectiva onto-epistémica se basa en una mirada tecnológica que busca desde el intercambio informativo de roles. En esta teoría, el apoyo en los libros de texto es fundamental, sin embargo, la búsqueda de información en la red es compartida entre grupos de apoyo donde se fomentan foros de discusión para dinamizar los saberes de los participantes (Juliao et al., 2021).

Lo anterior también contribuye a la apropiación y la ejecución de las competencias tecnológicas de las personas en todo escenario social, por ello, familiarizarse con el uso de la tecnología es una herramienta fundamental que no solo fortalece las habilidades y las destrezas de los sujetos sociales, sino que propende la interacción significativa para que, desde el ciberespacio, se agencien con el uso adecuado del internet, haciendo uso responsable de la red.

Sociedad de la Información, Era Digital y Sociedad del Conocimiento

El concepto de Sociedad de la Información tuvo su origen en la década de los años sesenta, y su significado ha evolucionado con el paso del tiempo. Sin embargo, debido al acelerado progreso tecnológico, hoy en día se la concibe como un proceso sociotecnológico donde los grupos humanos adquieren y comparten simultáneamente contenido informativo (Alonso-Sánchez, 2016).

Según Mendoza (2021), la sociedad de la información junto con las TIC constituye el marco para el diseño, la transmisión, distribución y gestión de la información, influyendo directamente en los procesos económicos, sociales y culturales de la humanidad. Desde su perspectiva, estas dinámicas se establecen como un fundamento clave para que las sociedades mejoren su calidad de vida. Por otro lado, Basadre (2021) plantea que esta esfera se caracteriza por la interconexión constante entre las personas, impulsada por la búsqueda y desarrollo de innovaciones tecnológicas a través del uso de las TIC. Esto posibilita la difusión simultánea de la información, promoviendo la expansión del conocimiento en cualquier tiempo y lugar.

Competencias Digitales

Las transformaciones impulsadas por la tecnología han dado lugar a que la sociedad del siglo XXI sea conocida como la "sociedad del conocimiento y la transformación". Este nuevo contexto es el resultado de factores como la globalización, el notable impacto de las TIC y la

gestión del conocimiento, los cuales han promovido el desarrollo de competencias digitales. Estas competencias se refieren al uso crítico, creativo y fiable de las tecnologías digitales con el propósito de mejorar la empleabilidad, gestionar el tiempo libre y fomentar la inclusión social (Rivas et al., 2021). Según Amador-Alarcón et al. (2021), las competencias digitales abarcan las habilidades y destrezas que permiten a las personas utilizar dispositivos digitales, herramientas de comunicación y redes informáticas para acceder a la información y gestionarla de manera eficiente. La capacidad de adaptarse y apropiarse de dichas competencias contribuye a la creación, comunicación y colaboración en entornos digitales, facilitando un desarrollo eficiente, efectivo y creativo tanto en la vida personal como en el ámbito laboral y en las actividades diarias.

Las personas que utilizan la tecnología no son solo espectadores o consumidores de contenidos informativos en internet, pues las necesidades que demanda la incursión en el ciberespacio requieren de buenos niveles de pericia. Ante esto, los seres humanos han pasado de espectadores a actores, convirtiéndose en protagonistas de su conocimiento a pasos agigantados, donde han de convertirse en sujetos activos que crean, publican y difunden la información adquirida.

Sociedad de la Información

Este vocablo tiene sus inicios en la década de los años sesenta, así, a través del tiempo, ha reconfigurado sus significados, sin embargo, por el surgimiento de avances tecnológicos a gran escala, esta es definida como un proceso tecnológico y social dentro del que el desarrollo de grupos humanos está direccionado a la obtención y la difusión instantánea de todo contenido informativo (Amador-Alarcón et al., 2021).

Para Pin-Hsiang et al., (2020), en la sociedad de la información y la colectividad social, las TIC constituyen el diseño, la distribución y el manejo de la información, lo que influye en las dinámicas económicas y socioculturales de los seres humanos, pues su perspectiva integradora se enfoca en el desarrollo y la difusión de la información y el conocimiento, una premisa clave para que los pueblos y las comunidades ejerzan, plenamente, su desarrollo sostenible y la mejora de su calidad de vida. Por otra parte, Muhammad et al., (2021) definieron esta categoría como el proceso de permanente interconexión de los seres humanos, cuya búsqueda de innovaciones tecnológicas y

sociales, a través del uso responsable de las TIC, permite que la información fluya simultáneamente, con el fin de crear y difundir el conocimiento en todo tiempo y espacio.

Internet de las Cosas (Internet of Things-IoT)

El Internet de las cosas es un tópico cuya importancia de índole social, técnico y económico, tiene vital relevancia en los ámbitos corporativo e industrial, gracias a la gama de bienes y servicios que ofrece en términos de tecnología y seguridad de la información. No obstante, el IoT también consta de desafíos que preponderan en la prevención de ciberataques que dificultan sus beneficios potenciales, los cuales representan riesgos y factores de riesgo relacionados con la confidencialidad de los datos.

En consecuencia, resulta esencial realizar un análisis histórico sobre la etimología del IoT, su evolución conceptual y su principal exponente. En este marco, es pertinente referirse a Kevin Ashton, quien en 1999 se desempeñaba como gerente en la empresa Procter & Gamble (PyG). Ashton intentaba solucionar un inconveniente relacionado con la disponibilidad de los productos más demandados de PyG, los cuales no siempre se encontraban en stock en las tiendas. Al observar que un aumento en la publicidad de un producto generaba un agotamiento

más rápido del inventario, propuso una solución innovadora: integrar sensores conectados a la red en los productos de PyG con el propósito de supervisar su disponibilidad en tiempo real. El concepto de Internet de las Cosas (IoT) fue introducido por Ashton para referirse a dispositivos o "entidades" que emplean internet como medio de comunicación dentro de un entorno tecnológico interconectado. Según el Instituto Europeo de Normas de Telecomunicaciones (ETSI, 2010), el IoT se describe como una infraestructura global de red de naturaleza dinámica y con capacidad de autoconfiguración, en la cual los objetos, tanto físicos como virtuales, poseen identidades únicas, características físicas y personalidades virtuales, interactuando entre ellos y con las redes de datos a través de interfaces inteligentes.

Según lo expuesto, la definición de Internet de las Cosas (IoT) puede adaptarse según el enfoque, sin embargo, de manera formal se entiende como una infraestructura de red global y dinámica, cuya principal característica es la capacidad de autoconfiguración y de establecer comunicaciones interoperables (Aguilar, 2021). En términos sencillos, IoT implica la posibilidad de conectar a internet todos los elementos que nos rodean, desde máquinas, dispositivos, teléfonos móviles y automóviles, hasta ciudades y carreteras, proyectando un entorno completamente interconectado.

Características de IoT

En el ámbito de la seguridad informática las directrices que las rigen están ligadas a los retos que atañen la óptima distribución de bienes y servicios cuyo indicador es la satisfacción de los usuarios. Los dispositivos del IoT poco seguros pueden convertirse en objeto de amenazas y ciberataques, al dejar flujos de información vulnerable. Entre tanto, la premisa de interconexión de los dispositivos IoT manifiesta que el despliegue significativo de artefactos tecnológicos homogéneos cuenta con la capacidad de conectarse de manera automática y simultánea a otros

cuyas características sean similares. En principio, quienes ejecutan el sistema y usan los dispositivos del IoT, tienen el deber de asegurar los datos de los usuarios, por ello, se requiere de un abordaje colaborativo para optar soluciones eficaces y ante los desafíos concernientes a distribución, procesamiento, control y protección de la información, con el objeto de resolver con eficiencia complejidad emergente de los problemas de ciberseguridad.

De acuerdo con lo expuesto, Aguilar (2021) menciona otras características clave del Internet de las Cosas (IoT):

- Interconectividad: En el entorno del IoT, cualquier dispositivo puede estar vinculado con la infraestructura global de información y comunicaciones.
- Servicios basados en objetos: El IoT tiene la capacidad de ofrecer servicios relacionados con los objetos, considerando sus limitaciones, como la protección de la privacidad y la coherencia semántica entre los objetos físicos y sus versiones virtuales. Para que estos servicios sean viables, es fundamental que tanto las tecnologías físicas como las digitales sigan evolucionando continuamente.
- Heterogeneidad: Los dispositivos que forman parte del IoT presentan una gran diversidad, ya que operan con diferentes plataformas de hardware y redes. A pesar de estas diferencias, pueden interactuar y comunicarse entre sí o con otros servicios a través de redes distintas.
- Variabilidad dinámica: Los estados de los dispositivos cambian de forma continua, como de modo de reposo a activo, o de estar conectados a desconectados, junto con aspectos contextuales como la ubicación o la velocidad. Además, el número de dispositivos conectados puede experimentar variaciones dinámicas.

- Gran escala: La cantidad de dispositivos que requerirán ser gestionados y establecerán comunicación entre ellos podría exceder con creces el número presente de equipos conectados a la red global.

La demanda de comunicación entre estos dispositivos será notablemente superior a la comunicación entre personas, lo que hará fundamental la gestión eficiente e interpretación de los datos generados, en especial en relación con la semántica y su procesamiento.

Las proyecciones y tendencias del IoT son una realidad indiscutida, por ello, es necesario un cambio de pensamiento para sumirse en un mundo interactivo e hiperconectado con dispositivos que suelen potenciar las redes comunicacionales de manera exponencial. Esto constituye desde la arquitectura del internet, la posibilidad de tener acceso abierto a los servicios y aplicaciones que promueven el uso responsable de la tecnología. Todo ello destaca la flexibilidad en la manera que los dispositivos del IoT pueden conectarse e interconectarse para proporcionar un valor significativo para el usuario.

Gestión de Riesgos en IoT

De acuerdo con lo señalado por Lee (2020), el estudio de la literatura sobre los enfoques cualitativos y cuantitativos en la gestión de riesgos en ciberseguridad revela que los primeros tienden a concentrarse en marcos conceptuales más amplios. Los enfoques cualitativos resaltan la relevancia de estos marcos, compartiendo un proceso común en la gestión de riesgos de ciberseguridad. Un ejemplo de ello es que el Marco de Ciberseguridad del NIST incorpora normas de la ISO 27001, cuyo objetivo es la certificación de los requisitos de seguridad de la información. De forma similar, la Plataforma de Ciberseguridad CMMI está alineada con marcos clave como la ISO 27001 y el Marco de Ciberseguridad del NIST. Sin embargo, ninguno de

estos marcos aborda explícitamente el ecosistema de ciberseguridad del Internet de las Cosas (IoT) ni los retos específicos que este plantea para la gestión de riesgos.

Tras el análisis exhaustivo de la literatura disponible, se ha determinado que la gestión de los riesgos asociados a los dispositivos IoT no ha sido objeto de suficiente atención para controlar o reducir sus efectos. Esto se debe a que los marcos actuales para la evaluación de riesgos no han logrado responder de manera integral a esta cuestión, que resulta ser de gran complejidad. En consecuencia, dichos marcos resultan insuficientes para cubrir de manera efectiva estas necesidades. Asimismo, esto incluye mecanismos que consideran las expectativas emergentes en torno a la privacidad. En este sentido, los flujos de información generados por los dispositivos IoT otorgan un nivel de exclusividad a los usuarios; sin embargo, es esencial implementar principios que protejan la privacidad de los datos con el fin de evitar los riesgos potenciales que puedan afectar el funcionamiento óptimo de dichos dispositivos.

Activos de Información

Este término se refiere a todos los elementos que una entidad emplea para almacenar, gestionar o transmitir datos (García & Moreta, 2019). Estos recursos pueden abarcar desde bases de datos y documentos hasta correos electrónicos, software, y hardware, entre otros. Es fundamental resguardar dichos activos para asegurar la confidencialidad, integridad y disponibilidad de la información contenida en ellos.

De acuerdo con Guevara-Vega et al., (2023), los activos informativos constituyen recursos clave en los Sistemas de Seguridad de la Información, cuya misión es facilitar que las empresas logren sus metas en términos de ciberseguridad. Marreros y Mendoza (2024) señalan que los activos de información poseen características específicas que los hacen valiosos y merecedores de protección. Algunas de estas particularidades incluyen:

1. Confidencialidad: La información puede ser confidencial y requerir protección para evitar su divulgación no autorizada.

2. Integridad: Es importante que la información se mantenga precisa, completa y fiable a lo largo del tiempo.

3. Disponibilidad: Los activos de información deben estar disponibles para aquellos que tienen autorización para acceder a ellos cuando sea necesario.

4. Autenticidad: La información debe ser veraz y provenir de fuentes fidedignas.

5. No repudio: Se refiere a la capacidad de demostrar que una acción o transacción ha tenido lugar, de manera que no pueda ser negada posteriormente por ninguna de las partes involucradas.

Estas características son fundamentales para comprender la importancia de proteger los activos de información en cualquier organización, por tanto, la toma de decisiones efectivas en todos los niveles de la misma puede constituirse en una ventaja competitiva al permitir acciones más acertadas ante las necesidades del mercado. Otro aspecto a señalar es el cumplimiento normativo organizacional, dentro del cual se reglamenta la protección y gestión adecuada de la información, razón por la que los activos de información son fundamentales para el desempeño de normas reguladoras.

En cuanto a la continuidad el negocio, la disponibilidad de la información es crucial para mantener su sistematicidad en situaciones adversas, además de la protección de la reputación, puesto que la pérdida o divulgación no autorizada de información sensible puede perjudicar la reputación y la confianza de la organización. Por estas razones, es fundamental proteger y gestionar adecuadamente los activos de información, asegurando sus tres principios básicos: confidencialidad, integridad y disponibilidad.

Siguiendo a Berrones-Paguay (2020), los activos de información pueden clasificarse en diferentes categorías, y atributos, entre las cuales se incluyen:

1. Datos: Incluyendo bases de datos, archivos digitales, registros de clientes, información financiera, entre otros.

2. Hardware: Equipos informáticos como servidores, computadoras, dispositivos de almacenamiento, redes, entre otros.

3. Software: Sistemas operativos, aplicaciones, programas informáticos y cualquier software utilizado para el procesamiento y gestión de la información.

4. Recursos humanos: El conocimiento y la experiencia del personal de la organización también son considerados activos de información.

5. Documentación: Cualquier tipo de documentos físicos o electrónicos que contengan información relevante para la organización.

6. Infraestructura física: Edificios, centros de datos, sistemas de climatización y cualquier infraestructura física que soporte la operación y protección de los activos de información. Para el caso de los atributos estos se denominan en cuantitativos y cualitativos. Los primeros se basan en el valor del cambio que se emplea para ciertos activos cuya utilidad es específica, en cambio, el atributo cualitativo sostiene la clasificación de los tipos de activos debido a su naturaleza.

Finalmente, vale señalar que, para la prevención de riesgos y aseguramiento de la seguridad informática, es necesario abordar procesos de automatización y control mediante aplicaciones que contengan requerimientos organizativos, cuyas configuraciones del software permitan el óptimo abordaje del Sistema de Gestión de Seguridad de la Información.

Vulnerabilidades y Amenazas

Las vulnerabilidades informáticas representan deficiencias en los sistemas, redes o procesos que exponen los activos de información a posibles riesgos en cuanto a su confidencialidad, integridad o disponibilidad (Álava-Zambrano et al., 2022). Estas debilidades pueden ser ocasionadas por configuraciones deficientes, la falta de actualizaciones, errores en el software o diversos factores adicionales. En contraste, las amenazas informáticas se refieren a cualquier elemento que pueda predisponer los activos tecnológicos a sufrir daños, tales como ciberataques, malware, extravío de dispositivos o acciones intencionales de personal interno, así como desastres naturales (Balseca-Chávez et al., 2021).

De acuerdo con Chacón et al. (2020), una vulnerabilidad informática es la fragilidad de un activo o control susceptible a una o varias amenazas. Por su parte, una amenaza es una posible causa de un incidente que podría generar perjuicios en un sistema o en una organización.

En este sentido, Guevara-Vega et al., (2023) indican que las vulnerabilidades informáticas precisan la inconsistencia de los sistemas, dado que pueden incrementar el riesgo de un ciberataque y afectar los activos de información. Todo ello puede ocasionar daños al software, hardware y a la red corporativa, hasta fragilizar las fortalezas del sistema de seguridad informática por amenazas latentes que propicien consecuencias irreversibles a los activos de información de una organización.

Metodologías de Análisis y Gestión de Riesgos

En la actualidad, se emplean diversas metodologías para el análisis y gestión de riesgos, siendo algunas de las más reconocidas las siguientes:

- Evaluación Operacional de Amenazas, Activos y Vulnerabilidades Críticas (OCTAVE).

Según Alberts et al. (1999), OCTAVE constituye un marco que facilita la identificación y administración de los riesgos vinculados con la seguridad de la información. Este enfoque holístico permite a las organizaciones identificar sus activos de información críticos, detectar amenazas potenciales a dichos activos y evaluar las vulnerabilidades que podrían comprometer su integridad. El objetivo principal de este proceso es reconocer los factores de riesgo para prevenir situaciones que puedan poner en peligro la seguridad de los activos informáticos, lo que, a su vez, afecta la gestión de la seguridad dentro de la organización. En este contexto, la entidad puede desarrollar e implementar estrategias que reduzcan la exposición a los riesgos relacionados con sus activos de información.

- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT).

Esta metodología fue desarrollada por el Consejo Superior de Administración Electrónica (CSAE) de España, un órgano dependiente del Ministerio de Hacienda y Administraciones Públicas, encargado de formular y aplicar políticas y estrategias gubernamentales en el ámbito de las tecnologías de la información y la comunicación. MAGERIT sigue la terminología de la norma ISO 31000, enfocada en la gestión del riesgo. Su estructura se basa en los principios del "Proceso de Gestión de Riesgos", descritos en la sección 4.4, "Implementación de la Gestión de Riesgos", dentro del "Marco de Gestión de Riesgos". Este marco ofrece las bases para que los órganos de gobierno tomen decisiones informadas respecto a los riesgos asociados al uso de tecnologías de la información.

En el análisis de riesgos, MAGERIT establece un procedimiento sistemático que incluye las siguientes fases:

1. Identificación de los activos más relevantes para la organización, analizando su interrelación y valor, así como el costo asociado a su degradación.

2. Detección de las amenazas a las que dichos activos están expuestos.

3. Evaluación de las medidas de protección existentes y su capacidad para mitigar los riesgos.

4. Estimación del impacto potencial, es decir, el daño que sufriría el activo si la amenaza se materializara.

5. Valoración del riesgo, que se determina a partir de la combinación del impacto y la probabilidad de ocurrencia de la amenaza.

- Metodología del DAFP

Esta guía, desarrollada por el Departamento Administrativo de la Función Pública de Colombia, tiene como objetivo orientar a las entidades públicas en la gestión de riesgos y la implementación de controles. Durante la evolución de esta metodología, se tomaron en cuenta una serie de procesos en un orden cronológico específico.

2009: Presentación de la primera versión.

2011: Actualización a la versión 2.

2014: Publicación de la versión 3.

2018: Lanzamiento de la versión 4.

2020: Implementación de la versión 5.

2022: Versión actual, la versión número 6.

Entre las ventajas que ofrece esta metodología, se destacan los siguientes aspectos:

- Facilita una mejor toma de decisiones: posibilita la identificación, análisis y mitigación de los riesgos que podrían obstaculizar el cumplimiento de los objetivos institucionales.
- Optimización de los recursos disponibles: ayuda a priorizar las inversiones dirigidas a la gestión de riesgos.
- Refuerza la transparencia y la rendición de cuentas: establece un marco normativo para la gestión transparente de riesgos.
- Fomenta la cultura del control interno: impulsa la adopción de una cultura de control dentro de las instituciones públicas.

Un aspecto relevante de esta metodología es su capacidad para integrarse en todos los niveles organizativos. Según el Departamento Administrativo de la Función Pública (DAFP, 2022), cada entidad, acorde con su estructura estratégica, procesos, procedimientos, políticas operativas y sistemas de información, cuenta con los insumos fundamentales para implementar la metodología propuesta en la gestión de riesgos. Es crucial resaltar que para una adecuada implementación de esta metodología, es necesario comprender detalladamente el entorno organizacional. A partir de dicha comprensión, se podrán ejecutar de manera eficaz los siguientes pasos:

1. Comprensión del entorno organizacional:

- Conocer a fondo la misión, visión, objetivos y valores de la entidad.
- Identificar los principales procesos y actividades que se desarrollan.
- Reconocer a los actores clave que participan en la gestión de la entidad.

2. Implementación de los pasos metodológicos:

- Identificación de riesgos:

- Determinar los tipos de riesgos que pueden influir en la entidad.
- Analizar las causas y posibles efectos de cada riesgo.

3. Evaluación de riesgos:

- Estimar la probabilidad y el impacto de cada riesgo.
- Priorizar los riesgos según su nivel de gravedad.

4. Diseño de controles:

- Definir las medidas para prevenir, mitigar o transferir los riesgos.
- Seleccionar los controles más apropiados para cada riesgo identificado.

5. Ejecución y evaluación de controles:

- Implementar los controles establecidos.
- Monitorear y evaluar la eficacia de dichos controles.

6. Monitoreo y mejora continua:

- Llevar a cabo un seguimiento constante de la gestión de riesgos.
- Detectar oportunidades de mejora en la metodología aplicada.

Este enfoque asegura una gestión integral del riesgo, adaptable y eficiente en función de las características y necesidades de cada entidad.

Marco Contextual

La Secretaría Distrital de Desarrollo Económico es una entidad central de la Alcaldía Mayor de Bogotá, creada en el año 2006 tras la promulgación de las disposiciones por parte del Concejo de Bogotá, las cuales regulan la estructura, organización y funcionamiento de las instituciones y organismos de la ciudad.

A través del Acuerdo 257 de 2006, en su artículo 75, se estableció la Secretaría Distrital de Desarrollo Económico, dotándola de autonomía administrativa y financiera. Su función

principal es dirigir y liderar la formulación de políticas orientadas al desarrollo económico, así como a las actividades comerciales, empresariales y turísticas del Distrito Capital.

Dentro de su mapa de procesos se identifican diecisiete (17) procesos, distribuidos en 4 tipos de procesos así:

Tabla 1

Procesos de la SDDE

Tipo de proceso	Proceso
Misional	Estudio de Desarrollo Económico
	Gestión de Competitividad
	Desarrollo Rural y Abastecimiento
	Gestión de Empleo
	Desarrollo Empresarial
Apoyo	Gestión Contractual
	Gestión de Talento Humano
	Gestión Documental
	Gestión Jurídica
	Control Disciplinario
	Bienes y Servicios generales
	Gestión Financiera
	Gestión de TIC
Estratégico	Gestión de Comunicaciones
	Atención al Ciudadano
	Planeación Estratégica
Evaluación	Control Interno

Nota. Procesos del sistema de gestión de la SDDE. Tomado de https://intranet.desarrolloeconomico.gov.co/sistemaintegrado/

Marco Legal

En esta sección se presentan los fundamentos éticos y legales clave, así como los principios, normativas y criterios que resultan indispensables para el desarrollo adecuado de un proyecto de investigación desde una óptica jurídica, cuyo objetivo es facilitar el logro de las metas establecidas (Ñaupas et al., 2018). En el contexto de las políticas públicas dirigidas a

fomentar el acceso y la utilización de las tecnologías de la información y la comunicación (TIC) en América, la VI "Cumbre de las Américas", realizada en Cartagena de Indias, Colombia, en 2012, adoptó como lema principal "Conectando las Américas: Socios para la Prosperidad". La cumbre centró su atención en la integración y la cooperación regional, consideradas pilares esenciales para alcanzar un mayor desarrollo y enfrentar los retos comunes de la región. Entre los temas más relevantes discutidos estuvieron la pobreza, la desigualdad, la seguridad ciudadana, los desastres naturales y el acceso y uso de tecnologías. En este evento, se definieron directrices concretas sobre el acceso y empleo de las TIC, subrayando su potencial para reducir las desigualdades sociales, económicas y regionales, así como para facilitar el acceso equitativo a la información y al conocimiento.

En la construcción de los consensos políticos alcanzados, se tomaron en cuenta los siguientes elementos para la creación de estatutos: 1. Las TIC han adquirido un rol esencial en la modernización empresarial de pequeñas y medianas empresas, generando un entorno innovador que incrementa la productividad y competitividad, además de facilitar el acceso a oportunidades en la economía globalizada; 2. Las TIC permiten a los gobiernos de la región avanzar en sus programas de modernización estatal, incrementando el acceso a servicios electrónicos como trámites en línea, educación a distancia, salud, capacitación laboral, empleo y seguridad pública; 3. Las TIC son un recurso fundamental para el desarrollo ciudadano, posibilitando la participación a través del acceso a nuevos servicios y herramientas en línea, tales como el voto electrónico, la búsqueda de empleo, el teletrabajo, el pago de impuestos, los servicios educativos y de salud a distancia, entre otros trámites.

La aplicación de este llamado a los líderes sobre el acceso y utilización de las tecnologías de la información y la comunicación (TIC) ha facilitado un avance notable en la integración de

las naciones del continente americano dentro de la sociedad de la información. En este marco, la Comisión Interamericana de Telecomunicaciones (CITEL), que actúa como órgano consultivo especializado de la Organización de los Estados Americanos (OEA), continúa abordando de manera constante los temas vinculados a las telecomunicaciones y se encuentra capacitada para respaldar a los distintos países en la ejecución de estos mandatos, colaborando con otras entidades interamericanas e internacionales afines. A nivel nacional, resulta relevante mencionar la Ley 1341 del 30 de julio de 2009, que establece los principios y directrices sobre la sociedad de la información y la regulación de las TIC, teniendo como objetivo primordial incentivar el acceso y la utilización masiva de las TIC, promover la competencia libre, garantizar el uso eficiente de la infraestructura, así como salvaguardar los derechos de los usuarios.

ISO/IEC 27001 de 2022

La normativa actual, ampliamente reconocida, establece los lineamientos esenciales para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Aunque existen múltiples estándares dentro de la familia ISO/IEC 27000, su aplicación permite a las organizaciones, sin importar su naturaleza, gestionar de manera eficaz la seguridad de sus activos, como información financiera, propiedad intelectual, datos de empleados o información confidencial suministrada por terceros.

La norma ISO/IEC 27001:2013 detalla los requerimientos necesarios para desarrollar, implementar, mantener y mejorar continuamente un SGSI en el contexto de cada organización. Asimismo, aborda la identificación y gestión de riesgos asociados a la seguridad de la información, ajustando estas estrategias a las necesidades particulares de cada entidad.

Por su parte, los requisitos establecidos en la ISO/IEC 27001:2022 son aplicables de forma general a cualquier tipo de organización, sin importar su tamaño o sector. Paralelamente,

la Organización Internacional de Normalización (ISO) se encuentra elaborando un estándar dirigido a los controles de seguridad y privacidad para los participantes en sistemas de IoT, lo cual facilitará su implementación a lo largo del ciclo de vida de estos sistemas. Es igualmente crucial actualizar y revisar la literatura más reciente durante el desarrollo de las actividades, asegurando que los objetivos propuestos se alineen con un plan actualizado de gestión de riesgos para la tecnología IoT.

El Internet de las Cosas (IoT) se posiciona como una de las tecnologías más relevantes en el ámbito de las redes, ya que permite que diversos dispositivos recojan e intercambien datos de manera constante. Las aplicaciones actuales de IoT están enfocadas en la informatización de objetos inanimados, permitiendo su operación autónoma sin supervisión humana. Esta autonomía hace que los servicios de IoT, tanto actuales como futuros, sean altamente eficientes, requiriendo, sin embargo, elevados niveles de seguridad, protección, verificación y recuperación ante posibles ciberamenazas. En este contexto, la incorporación de mejoras en la ingeniería de sistemas de IoT es fundamental para asegurar una estabilidad integral en todos sus niveles.

Norma ISO/IEC 27001 y Norma ISO/IEC 27002

Esta norma integra un estándar internacional optando como referente los seguimientos y controles para ejecutar un SGSI incorporando inspecciones para el acceso a datos, e intervención criptográfica de los mismos de modo confidencial gracias a la administración de credenciales de acceso (Vásquez, 2023). La norma ISO/IEC 27002 proporciona directrices que facilitan la protección de la información en consonancia con las necesidades empresariales y las normativas legales aplicables. Este marco incluye la formulación de políticas destinadas a gestionar la seguridad de la información, las cuales deben ser aprobadas, divulgadas y comunicadas tanto a los empleados como a los agentes externos. Según Moya (2023), esta normativa se estructura en

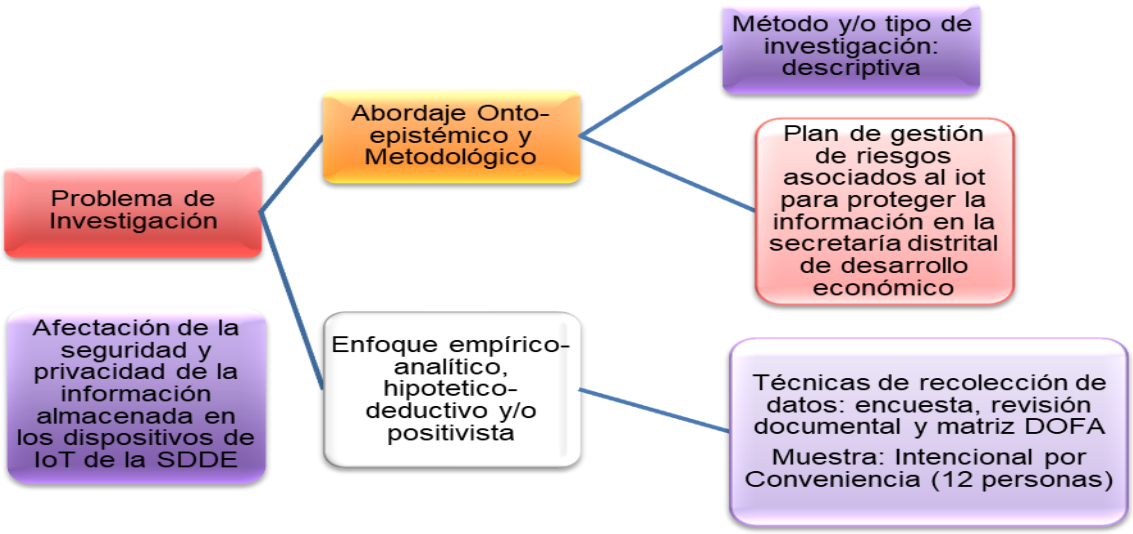
varios niveles: inventario de activos, asignación de propiedad sobre dichos activos, uso adecuado de los mismos y su devolución cuando corresponda. El primer nivel identifica los activos de información que sustentan el negocio, clasifica los activos según su importancia, información y sus propietarios. El segundo nivel propende la gestión, transferencia y almacenamiento del activo para ser asignado como propietario. El tercer nivel se refiere la documentación y uso adecuado del flujo de información, así como su descripción requisitos de seguridad de los activos de información y la comunicación a los empleados de una empresa respecto al uso indebido de datos. El último nivel respecta un control riguroso para que actores corporativos devuelvan los activos de información, una vez culminado su periodo de uso, acuerdos laborales o aspectos contractuales.

Es de mencionar que para implementar este control es importante concluir de manera formal el tiempo de uso, haciendo hincapié en la devolución de activos físicos y/o electrónicos. Todo ello con el objeto de establecer un proceso de transferencia y supresión informativa de manera eficaz, en caso de que sea pertinente; en tal sentido, vale resaltar que el propietario del activo bajo ninguna circunstancia es el dueño del activo, más bien le corresponde abordar una serie de responsabilidades sobre el mismo antes de su fecha de caducidad.

Metodología

Figura 1

Engranaje Metodológico de la Investigación



Nota. Descripción gráfica de la metodología de investigación usada

Trayectos Metodológicos

Este apartado integra el arquetipo metodológico de la investigación, cuyo constructo es definido según Ñaupas et al., (2018), como el engranaje de aspectos que direccionan el trabajo de campo mediante la definición del objeto de estudio, enfoque paradigmático, tipología investigativa y técnicas de recolección de datos. Siguiendo a Ortiz (2015), la metodología de un proyecto investigativo es el camino que se optará para abordar la problemática que subyace en el contexto, mediante la información proveniente de diversas técnicas de recolección de datos, cuya serie de procesos y/o mecanismos que se desarrollan sistemáticamente dan consistencia a la investigación científica.

Es de mencionar que la importancia de la metodología parte del análisis crítico-reflexivo de las variables y/o categorías del entramado teórico, ya que su articulación dilucida y fortalece

los hallazgos y la discusión del estudio en cuestión. En este contexto, el trabajo de grado que se presenta fue realizado con empleados de la Secretaria Distrital de Desarrollo Económico de Bogotá D.C., lo que implicó la necesidad de llevar a cabo diversas actividades orientadas a cumplir con los objetivos establecidos.

Enfoque Investigativo

Esta sección se define como una serie de procesos que, de manera lógica, sistemática y empírica, son aplicables para el estudio de un problema que subyace en un campo estudio (Hernández et al., 2016). En tal sentido, estos aspectos denotan el objeto de estudio desde la definición del tema, problema investigativo, aspectos teórico-conceptuales, arquetipo metodológico, selección de técnicas de recolección datos, análisis e interpretación de los mismos. En esta perspectiva, el estudio se contextualiza bajo el enfoque cuantitativo o también conocido como empírico-analítico, dado que buscó desde la objetividad del problema el abordaje investigativo desde su especificidad y delimitación. Además, se estableció una hipótesis previa a la implementación del trabajo de campo y, una vez fueron recolectados los datos, se fundamentaron en la medición y análisis de procedimientos estadísticos.

Paradigma

El modelo que sustenta el presente estudio es el empírico-analítico, también conocido como hipotético deductivo, positivista, racionalista o naturalista, tiene por objeto de interés la comprobación del conocimiento mediante la predicción desde el planteamiento de una serie de hipótesis para determinar algo por suceder y, posteriormente, verificarlo y/o comprobarlo (Sánchez-Bayón, 2022).

Este arquetipo suele emplear el cálculo numérico y el uso del análisis estadístico para establecer con eficacia modelos de comportamiento en una población determinada.

Otro aspecto para señalar es que este enfoque paradigmático concibe como conocimiento verdadero aquél basado en la objetividad y verificabilidad, negando otras perspectivas metodológicas para la concepción de la realidad; lo que implica la cuantificación y medición repetitiva del objeto a estudiar hasta constituirse en tendencias y, por tal efecto, su premisa parte de que el conocimiento científico es el resultado de la experiencia de los sentidos, de lo observable y absolutamente objetivo. Otra de las características de esta perspectiva epistemológica es que la realidad está dada y es conocida por el sujeto cognoscente y, por tal motivo, es de hallar el mecanismo propicio y válido para descubrirla.

En consecuencia, asume la existencia de un método para concebir esa realidad y estipula su aplicación como garante de legitimidad para la construcción del conocimiento. Todo ello preponderó la ruta que se discurrió para el abordaje del problema, cuyo proceso comprende las técnicas y métodos de recolección de datos desde una perspectiva no experimental y corte transversal.

Tipo de Investigación

El estudio es de tipo descriptivo, ya que recopila información que además de ser cuantificable es empleada para el análisis estadístico de la muestra poblacional, cuya perspectiva no experimental evalúa determinantemente el objeto de estudio según la trazabilidad de objetivos Jiménez (2020). De este modo, el investigador no emplea un mecanismo formal para alterar los factores que están de acuerdo o en desacuerdo con una temática establecida; en tal sentido quien investiga se limita a describir el estado de una o más variables identificadas.

De acuerdo con lo anterior, para concebir los compendios metodológicos se hizo necesaria la trazabilidad de unos propósitos investigativos orientados en la cuya operacionalización del conocimiento se efectuó mediante el diagnóstico de un problema en el

campo de estudio, la evaluación de sus riesgos potenciales, la proposición de un plan de acción planificar y establecer con estamentos teóricos el plan de acción y la identificación de acciones de mejora.

Población y Muestra

Este acápite es entendido como el grupo de personas que integran la investigación para las cuales se aplican procedimientos de los que se desea obtener información, cuyas actividades subyacen de los objetivos (Cisneros-Caicedo, 2022). Dentro de las clasificaciones de la población objeto de estudio se puede tener una población finita o infinita. Según Rodríguez (2019), una población finita es aquella cuyos elementos en su totalidad son identificables por el investigador, dado a que se conoce la cantidad total.

Con base en lo anterior, la presente investigación constituye una población finita y accesible, dado que el investigador cuenta con los registros de los elementos que lo conforman. En este caso la población objeto de estudio está conformada por 12 personas que laboran en el escenario objeto de investigación. El muestreo utilizado fue el Intencional por Conveniencia, dado que se tuvo en cuenta aspectos espacio-temporales como la disponibilidad horaria de los actores corporativos para participar en el estudio, su convergencia horaria y confianza con el investigador, y la proximidad geográfica con el escenario laboral para acceder al uso de artefactos técnicos, tecnológicos e información cibernética de vital importancia.

Técnicas e Instrumentos de Recolección de Datos

Las técnicas utilizadas para la obtención de información en este proyecto incluyeron la aplicación de encuestas, el análisis de documentos y la elaboración de una matriz DOFA. Como afirman Caicedo et al. (2022), la encuesta se considera una herramienta muy común en estudios cuantitativos, ya que permite al investigador recolectar información objetiva a través de un

cuestionario previamente estructurado, sin intervenir en el entorno o fenómeno analizado, lo cual facilita la representación de los datos en tablas o gráficos. Asimismo, según Losada y Marmo (2022), la encuesta constituye un método de recopilación de datos que se implementa mediante un cuestionario sistemático, sin posibilidad de cambios durante su ejecución; posteriormente, los datos obtenidos se organizan en tablas o gráficos para su respectivo análisis.

Para la recolección de datos a través de encuestas, se empleó un cuestionario con preguntas de opción única, lo cual permitió obtener información objetiva y relevante para cumplir con los objetivos específicos del estudio. En paralelo, la revisión documental se reconoce como un método fundamental en la investigación científica, al proporcionar acceso a fuentes referenciadas que luego son codificadas en unidades de análisis.

Por otro lado, la matriz DOFA es una herramienta analítica que facilita la identificación de Debilidades, Oportunidades, Fortalezas y Amenazas en una organización o entidad, con el propósito de implementar acciones correctivas y gestionar riesgos organizacionales (Salgado & Awad, 2022). Según Losada y Marmo (2022), los instrumentos de recolección de datos son herramientas indispensables para registrar y almacenar información sobre los fenómenos observados en el trabajo de campo. En este caso, se utilizó un cuestionario como el principal medio de recolección de datos. Velasco (2022) resalta que las encuestas, debido a su flexibilidad, permiten estructurar preguntas claras y organizarlas secuencialmente para asegurar su comprensión.

El cuestionario diseñado en esta investigación, de acuerdo con su enfoque, contenía preguntas cerradas dirigidas a los empleados participantes, utilizando una escala Likert con las siguientes opciones: Siempre (4), Casi siempre (3), A veces (2) y Nunca (1). Es importante señalar que el diseño del instrumento se elaboró de manera precisa para alinearse con los

objetivos de la investigación, los cuales orientaron su formulación. A continuación, se detalla la escala de ponderación aplicada a cada uno de los ítems del cuestionario, junto con las respectivas opciones de respuesta.

Validez y confiabilidad

Validez

Cada uno de los instrumentos empleados en la recolección de datos garantiza su validez, al permitir la captura de información clave que respalda los resultados de la investigación.

En este marco, Ortiz (2015) señala que la validez de un instrumento se refiere al grado de confianza con el que se mide una variable, cuya característica debe ser evaluada de manera objetiva y basada en hechos. De manera similar, Ñaupas et al. (2018) describen esta validez como la capacidad del instrumento para medir con precisión una variable que requiere un análisis riguroso. El proceso de validación se realiza a través de las siguientes estrategias:

A. Validación mediante prueba piloto: Este método consiste en aplicar la encuesta a un grupo de personas que no pertenece a la población objetivo, con el propósito de realizar una evaluación preliminar del instrumento.

B. Validación del cuestionario mediante el Alfa de Cronbach: Esta técnica se utiliza para evaluar la fiabilidad de la escala, analizando la consistencia interna de los ítems que componen el instrumento.

C. Validación por expertos: En este proceso, investigadores con experiencia en el área son consultados sobre aspectos clave de la investigación, tales como el título, objetivo general, objetivos específicos, operacionalización de variables, dimensiones e indicadores. El objetivo es verificar la coherencia teórica que sustenta el estudio. Esta validación permite a los expertos detectar fortalezas y áreas de mejora en el instrumento, ofreciendo recomendaciones respecto a la

consistencia de los ítems en función de las variables, dimensiones, indicadores, objetivos y su redacción.

D. Recopilación y análisis de las aportaciones de los expertos: El propósito es identificar las convergencias y divergencias en sus evaluaciones de los instrumentos, para perfeccionar su validez.

En consideración a lo anterior, los instrumentos de recolección de datos fueron validados por tres expertos en ingeniería informática, telecomunicaciones y software. Esto aseguró que los cuestionarios se alinearan con los objetivos de la investigación. Además, se utilizaron métodos estadísticos para evaluar la fiabilidad de los instrumentos, verificando su capacidad para alcanzar los objetivos propuestos, así como sus variables, dimensiones e indicadores.

Confiabilidad

El proceso se entiende como la capacidad de un instrumento para generar resultados uniformes, independientemente de cuántas veces se aplique a la misma población de estudio. Cabrera-Tenecela (2023) explica que la confiabilidad hace referencia al valor otorgado a las mediciones realizadas por un instrumento, basado en su exactitud y sin considerar posibles errores. En este marco, la confiabilidad del instrumento fue comprobada mediante la realización de una prueba piloto, aplicada a diez (10) personas externas a la muestra principal, pero que presentaban características similares a las unidades de estudio. Para estimar dicha fiabilidad, se empleó el coeficiente Alfa de Cronbach, el cual también fue utilizado en la validación del cuestionario. Este método permite al investigador evaluar la consistencia interna de un instrumento construido con una escala Likert u otras escalas de opciones múltiples (Castañeda-Mota, 2023). Los datos recolectados fueron introducidos en una hoja de cálculo de Microsoft Excel 2019, que procesó los resultados utilizando el mencionado coeficiente, facilitando así la

verificación de la coherencia interna durante la prueba piloto y su análisis a través de una fórmula matemática (Aguilar-Bernal, 2023). De este modo, la información obtenida fue gestionada con base en la fiabilidad determinada mediante la siguiente fórmula:

$$\alpha = \frac{K}{K-1}\left[1 - \left(\frac{\sum Vi}{Vt}\right)\right]$$

Dónde:

α: Coeficiente Alfa Cronbach

K: Número de ítems

Vi: Varianza de los puntajes

Vt: Varianza de los puntajes totales

Teniendo en cuenta lo anterior, los criterios establecidos para el análisis del coeficiente de Alpha de Cronbach fueron los siguientes:

Tabla 2

Criterios para Determinar la Confiabilidad

Rango	Categoría
De -1.00 a 0.00	No es confiable.
De 0.01 a 0.49	Baja confiabilidad.
De 0.50 a 0.75	Moderada confiabilidad.
De 0.76 a 0.89	Fuerte confiabilidad.
De 0.90 a 1.00	Alta confiabilidad.

Nota. Desglose de los criterios para determinar la confiablidad del cuestionario

Es de resaltar que mediante esta acción se obtuvo la aplicación de la fórmula para la determinar la confiablidad de los siguientes resultados:

α= 0,9979.

Procesamiento de la Información

Técnicas de Procesamiento y Análisis de Datos

Después de haber obtenido la validez y confiabilidad de los instrumentos se llevó a cabo el procesamiento de la información, cuyo cálculo estadístico adecuado para el presente estudio, fue el correspondiente al de la estadística descriptiva. En este marco, para Spinelli (2023), la tabulación es la forma cómo el investigador compila la información y la representa mediante cuadros, gráficos o tablas, la información compilada en los instrumentos de recolección de datos.

Para efecto de esta investigación, la técnica utilizada es la estadística descriptiva en concordancia con el diseño metodológico seleccionado. Esto permite describir la información y/o valores obtenidos para cada variable, analizando sobre la base de la distribución de frecuencias relativas porcentuales.

Fases de la Investigación

Esta investigación tiene en cuenta varias fases, razón por la que se trabaja en la etapa de diagnóstico, evaluación, proposición e identificación.

Fase 1: Diagnóstico

En esta etapa se compilaron los datos en una encuesta diagnóstica cuyos resultados fueron objeto de análisis y representados gráficamente, conforme a los activos de información asociados al IoT en la SDDE, por parte de los actores laborales.

Fase 2: Evaluación

En esta sección se llevó a cabo un análisis documental junto con la aplicación de una encuesta a los actores corporativos, enfocándose en la evaluación del nivel de riesgo que presentan los activos de información vinculados al Internet de las Cosas (IoT). El propósito de esta investigación fue anticipar y mitigar posibles riesgos, en consonancia con los objetivos de seguridad establecidos en la norma ISO 27001.

Fase 3: Proposición del Plan de Acción

Durante este procedimiento, se consideraron cuidadosamente todos los componentes estratégicos y los elementos metodológicos necesarios para el diseño de un plan de acción enfocado en la seguridad de la información en el entorno del Internet de las Cosas (IoT), alineado con los lineamientos de la norma ISO 27001. En este contexto, se desarrollará una propuesta que incluirá los siguientes apartados: denominación, introducción, objetivo, alcance, justificación, actores corporativos involucrados, viabilidad técnica, tecnológica y financiera, así como un cronograma de actividades.

Operacionalización de Variables

Tabla 3

Operacionalización de Variables

Objetivo general: Diseñar un plan de gestión de riesgos de IoT apoyado en la norma ISO/IEC 27001 para proteger la información en la Secretaría Distrital de Desarrollo Económico.

Variable	Definición conceptual	Definición operacional	Indicadores	Ítems
Internet de las Cosas (IoT)	Capacidad de hacer que todo lo que nos rodea, comenzando desde (es decir, máquinas, dispositivos, teléfonos móviles y automóviles), incluso (ciudades y carreteras), se espera que esté conectado a Internet.	Identificación y uso de dispositivos tecnológicos que utiliza el internet como mecanismo de comunicación en un sistema tecnológico.	Heterogeneidad Cambios dinámicos Escala enorme Activos informativos Interconectividad Servicios relacionados con objetos	1 2 3 4 5 6
Protección de la seguridad informática	Es la salvaguarda de la información proveniente de internet, cuyos datos se consignan en dispositivos móviles para prevenir el control de datos por personal no autorizado.	Manejo de medidas de prevención y detección del uso desautorizado y/o inapropiado del sistema informático, por parte de intrusos cuyas intenciones sean vulnerar el suministro de datos empresariales, con la intención de acceder a información de carácter confidencial y lucrarse de manera ilegítima.	Seguridad de hardware Seguridad de software Seguridad de red Integridad Confidencialidad Disponibilidad Autenticación	7 8 9 10 11 12 13

Nota. Definición de las variables y conceptos abstractos que se quieren estudiar

Una vez operacionalizadas las variables del estudio se procedió a implementar una encuesta para el alcance del primer objetivo. Es de señalar que para validar el instrumento se utilizaron como referencia las publicaciones y teorías de Michael Porter, Eric Brynjolfsson, Kevin Ashton y Sanjay Sarma, cuyos estudios sobre tecnología, gestión e impacto en las organizaciones, conceptualización y ejecución del término IoT, además de sus experticias en tecnología IoT, sirvieron de insumos para la formulación de preguntas. A continuación, te presento el cuestionario validado con base en el conocimiento general y alineado con los estudios de los autores antes mencionados:

Tabla 4

Cuestionario Tipo Likert

Preguntas	Opciones de respuesta			
¿Existe un cuadro de mando IoT que genere la suficiente seguridad para analizar, gestionar y añadir datos en directo y, posteriormente, consignarlos en otros dispositivos y sensores?	Siempre	Casi siempre	Algunas veces	Nunca
¿La gestión del ciclo de vida cuenta con la suficiente capacidad de ver, gestionar, operar, activar y dar de baja cualquier activo desde cualquier lugar y en cualquier momento?	Siempre	Casi siempre	Algunas veces	Nunca
¿El control autónomo total de la red posee la flexibilidad para seleccionar y cambiar a múltiples proveedores de conectividad para garantizar una alta disponibilidad para las necesidades de misión crítica?	Siempre	Casi siempre	Algunas veces	Nunca
¿La configuración OTA (Over-The-Air) suele realizarse por vía inalámbrica para la gestión segura y rentable de despliegues nuevos y existentes?	Siempre	Casi siempre	Algunas veces	Nunca
¿Las alertas y cuadros de mando proporcionan a los equipos de asistencia y a los ejecutivos una imagen de la situación y de la información siempre actualizada de todo el funcionamiento del activo asociado a IoT?	Siempre	Casi siempre	Algunas veces	Nunca
¿El cuadro de mandos de IoT y un Plataforma de gestión de la conectividad (CMP) ofrece la prevención adecuada del fraude informático detectándolo en tiempo real?	Siempre	Casi siempre	Algunas veces	Nunca
¿Los 4 tipos de plataformas de gestión de IoT como los dispositivos, conectividad, aplicación y analítica, están en óptimas condiciones para su funcionamiento en la empresa?	Siempre	Casi siempre	Algunas veces	Nunca
¿El personal de la empresa se rige por el Reglamento General de Protección de Datos (GDPR) para proteger la información personal y establecer normas sobre la privacidad de los datos?	Siempre	Casi siempre	Algunas veces	Nunca
¿La gestión del ciclo de vida de IoT admite sus modos de prueba y funciones de control en tiempo real como la activación, suspensión y desactivación de sus activos desplegados y dispositivos conectados?	Siempre	Casi siempre	Algunas veces	Nunca
¿La gestión de activos supervisa y controla cada dispositivo IoT desde una plataforma en línea disponible en la nube?	Siempre	Casi siempre	Algunas veces	Nunca
¿La gestión de activos digitales permite acceder a un CMP desde cualquier lugar y en cualquier momento a través de una conexión a Internet desde un PC, dispositivo móvil o tableta?	Siempre	Casi siempre	Algunas veces	Nunca
¿La gestión de inventarios es ideal para supervisar y controlar los dispositivos IoT a través de un único portal de gestión en línea?	Siempre	Casi siempre	Algunas veces	Nunca

Nota. Herramientas para obtener resultados del diagnóstico, alineados con los objetivos propuestos de la investigación

Resultados

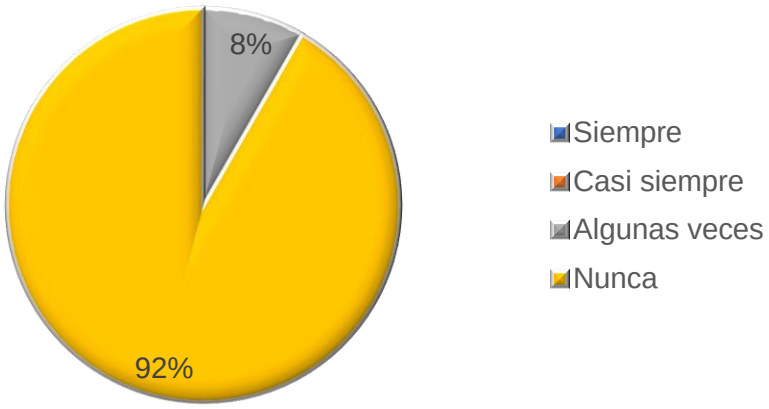
Diagnóstico Situación Actual en la SDDE

La siguiente técnica de recolección de datos fue aplicada a 12 personas que laboran en el escenario objeto de investigación, con el fin de alcanzar la trazabilidad del primer objetivo específico. Las funciones de los actores laborales permitieron saber con objetividad la seguridad de los datos informáticos que se consignan en los dispositivos IoT, razón por la que se describen los hallazgos de dicha encuesta dirigida a los mismos, a partir de una serie de preguntas consignadas en un cuestionario tipo Likert cuyas opciones de respuesta son siempre, casi siempre, algunas veces y nunca:

1. ¿Con qué frecuencia se ejecuta un cuadro de mando IoT para garantizar seguridad en el análisis, gestión y anexo de datos en directo y, posteriormente, consignarlos en otros dispositivos y sensores?

Figura 2

Cuadro de Mando IoT para el Análisis, Gestión y Complemento de Datos



Nota. Análisis gráfico de la existencia de un cuadro de mando IoT

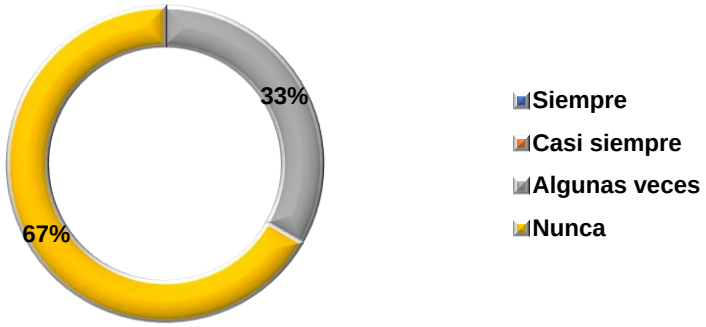
Conforme a la primera pregunta, la figura 2 muestra que 1 de los 12 encuestados consideró que algunas veces se ejecuta un cuadro de mando IoT para generar la suficiente

seguridad en el análisis, gestión y anexo de datos en directo, con el objeto de consignarlos en otros dispositivos y sensores, en contraste con el resto de encuestados que respondieron que nunca se desarrollaba tal acción.

2. ¿La gestión del ciclo de vida cuenta con la suficiente capacidad de ver, gestionar, operar, activar y dar de baja cualquier activo desde cualquier lugar y en cualquier momento?

Figura 3

Gestión Integral del Ciclo de Vida del dispositivo IoT



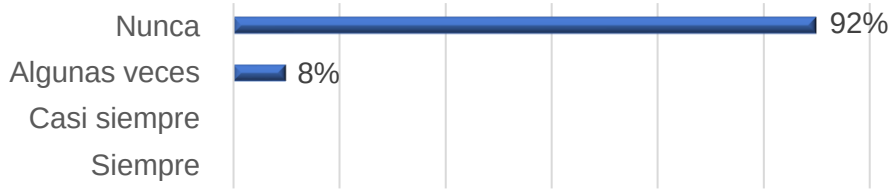
Nota. Resultado gráfico de la gestión de vida útil de los dispositivos IoT

En la figura 3 se muestra de los 12 encuestados, 8 respondieron que la gestión del ciclo de vida nunca ha contado con la suficiente capacidad de ver, gestionar, operar, activar y dar de baja cualquier activo desde cualquier lugar y en cualquier momento, en contraste con 4 encuestados que respondieron que esta actividad era ejecutada algunas veces.

3. ¿El control autónomo total de la red posee la flexibilidad para seleccionar y cambiar a múltiples proveedores de conectividad para garantizar una alta disponibilidad para las necesidades de misión crítica?

Figura 4

Control de la Red para la Selección y Cambio de Proveedores de Conectividad



Nota. Evidencia del control autónomo de la red de los dispositivos IoT

La figura 4 expresa que del 100% de los encuestados el 92% afirmó que nunca el control autónomo total de la red ha sido la flexible para seleccionar y cambiar a múltiples proveedores de conectividad, con el objeto de garantizar una alta disponibilidad para las necesidades de misión crítica, en comparación con el 8% del resto poblacional quien afirmó que algunas veces se llevaba a cabo lo anterior.

4. ¿La configuración OTA (Over-The-Air) suele realizarse por vía inalámbrica para la gestión segura y rentable de despliegues nuevos y existentes?

Figura 5

Vía de Conexión para la Gestión y Configuración OTA (Over-The-Air)

Nota. Resultado de la opción de configuración inalámbrica de los dispositivos IoT

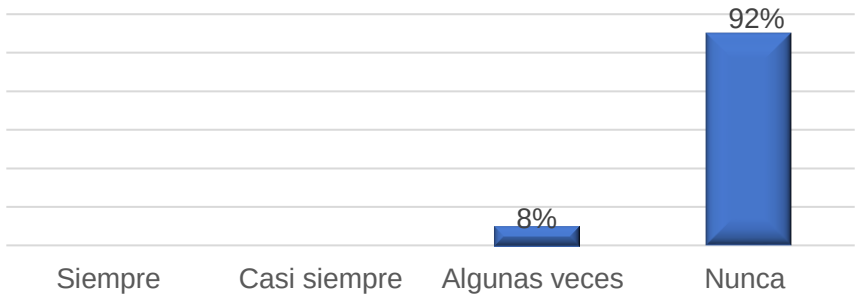
La gráfica 5 muestra que los 12 actores laborales encuestados expresaron que nunca se ha realizado la configuración OTA por vía inalámbrica para la gestión segura de despliegues nuevos

y existentes. Esto pone en desventaja las actualizaciones OTA, pues obstaculiza la efectividad de actualización del software, así como la solución de errores, incorporación, eliminación o cambio de aplicaciones según la interfaz del usuario.

5. ¿Las alertas y cuadros de mando proporcionan a los equipos de asistencia y a los ejecutivos una imagen de la situación y de la información siempre actualizada de todo el funcionamiento del activo asociado a IoT?

Figura 6

Alertas y Cuadros de Mando para una Imagen Actualizada a los Equipos



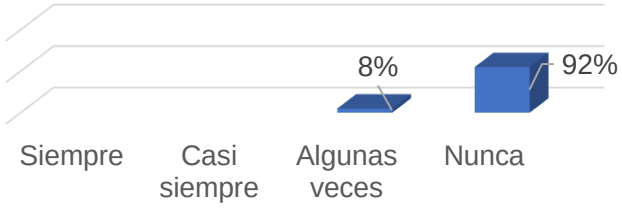
Nota. Análisis gráfico de emisión de alertas de los dispositivos IoT

La figura 6 denota que del 100% de la población encuestada el 92% afirmó que nunca las alertas y cuadros de mando proporcionaban a los equipos de asistencia y a los ejecutivos, una imagen de la situación y de la información actualizada de todo el funcionamiento del activo asociado a IoT, en contraste con el 8% del resto de los encuestados que respondieron que algunas veces se realizaba esta acción.

6. ¿El cuadro de mandos de IoT y una plataforma de gestión de la conectividad (CMP) ofrece la prevención adecuada del fraude informático detectándolo en tiempo real?

Figura 7

Prevención del Fraude Informático para el Cuadro de Mandos de IoT



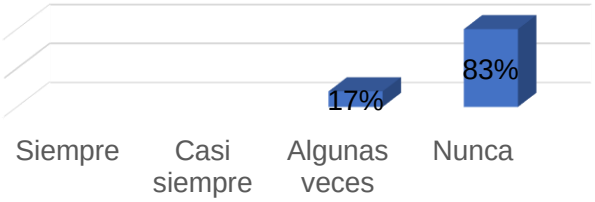
Nota. Evidencia de detección en tiempo real de fraude informático de los dispositivos IoT

La figura 7 demuestra que de los 12 encuestados solo 1 respondió que algunas veces El cuadro de mandos de IoT y una Plataforma de gestión de la conectividad (CMP) ofrecía la prevención adecuada del fraude informático detectándolo en tiempo real, sin embargo, la mayoría afirmó que nunca se ejecutaba tal acción.

7. ¿Los 4 tipos de plataformas de gestión de IoT como los dispositivos, conectividad, aplicación y analítica, están en óptimas condiciones para su funcionamiento en la empresa?

Figura 8

Condiciones de Funcionamiento de la Plataforma para Dispositivos IoT



Nota. Análisis gráfico de emisión de alertas de los dispositivos IoT

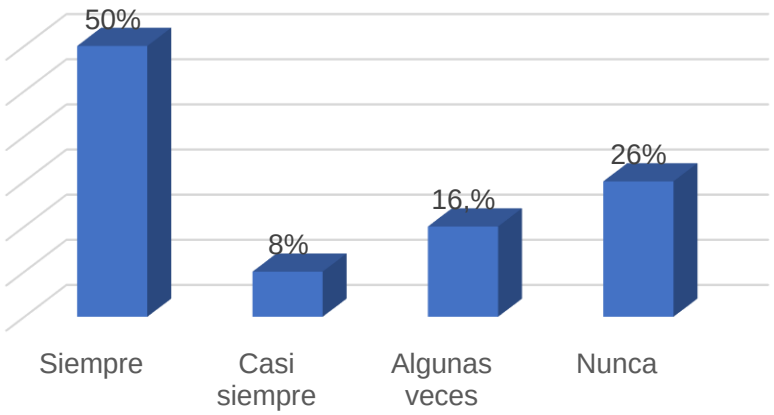
En la figura 8 se muestra que solo 2 de los 12 encuestados respondieron que algunas veces los 4 tipos de plataformas de gestión de IoT como los dispositivos, conectividad,

aplicación y analítica, se encuentran en óptimas condiciones para su funcionamiento, sin embargo, el resto de los encuestados aseveró que nunca se encontraban en buenas condiciones dichas plataformas.

8. ¿El personal de la empresa se rige por el Reglamento General de Protección de Datos (GDPR) para proteger la información personal y establecer normas sobre la privacidad de los datos?

Figura 9

Reglamento General de Protección de Datos para la Información Personal



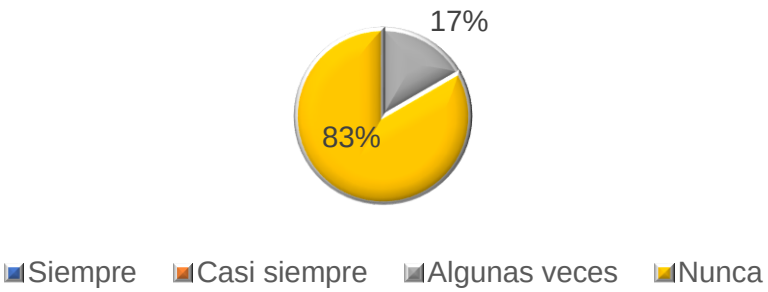
Nota. Muestra del % del uso del Reglamento General de Protección de Datos

En la figura 9 se muestra que de los 12 encuestados, 3 respondieron Nunca, 2 algunas veces, 6 siempre y 1 casi siempre, respecto al cumplimiento del Reglamento General de Protección de Datos (GDPR) para proteger la información personal y establecer normas sobre la privacidad de los datos, cuyos valores porcentuales en las respuestas fueron del 50%, 8%, 16% y 26%.

9. ¿La gestión del ciclo de vida de IoT admite sus modos de prueba y funciones de control en tiempo real como la activación, suspensión y desactivación de sus activos desplegados y dispositivos conectados?

Figura 10

Funciones de Control en Tiempo Real para la Gestión del Ciclo de Vida del IoT



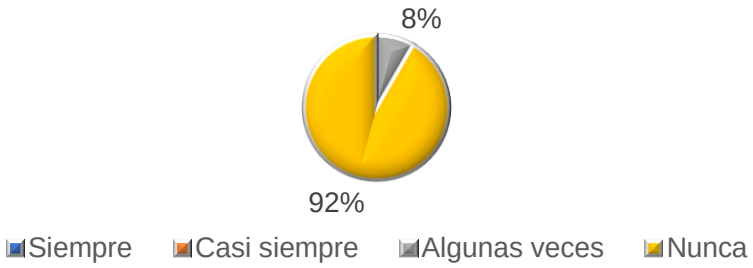
Nota. Análisis gráfico de modos de prueba y funciones de control en tiempo real

La gráfica 10 respecta que de los 12 encuestados, 10 respondieron Nunca y 2 algunas veces conforme a la gestión del ciclo de vida de IoT, sus modos de prueba y funciones de control en tiempo real como la activación, suspensión y desactivación de sus activos desplegados y dispositivos conectados, cuyos valores porcentuales se sitúan en el 83% y 17%.

10. ¿La gestión de activos supervisa y controla cada dispositivo IoT desde una plataforma en línea disponible en la nube?

Figura 11

Gestión de Activos para la Supervisión y Control de Dispositivo IoT en Línea



Nota. Muestra % de uso de plataforma en línea disponible en la nube

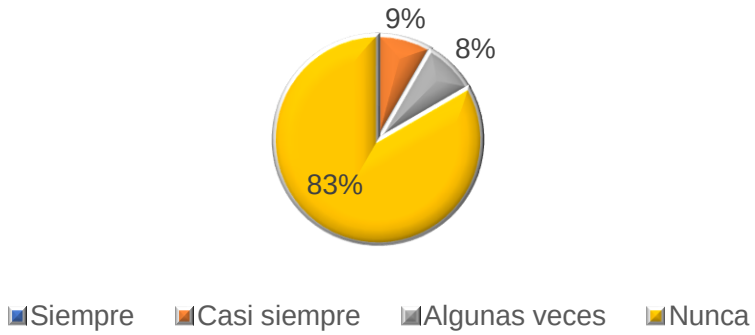
De la figura 11 se deduce que de los 12 encuestados 11 respondieron nunca y solo 1 algunas veces respecto a la frecuencia que la gestión de activos supervisa y controla cada

dispositivo IoT desde una plataforma en línea disponible en la nube, de lo cual se interpreta que del 100% de la población objeto de estudio, la mayoría niega rotundamente esta acción.

11. ¿La gestión de activos digitales permite acceder a un CMP desde cualquier lugar y en cualquier momento a través de una conexión a Internet desde un PC, dispositivo móvil o tableta?

Figura 12

Gestión de Activos Digitales desde un CMP en Cualquier Momento



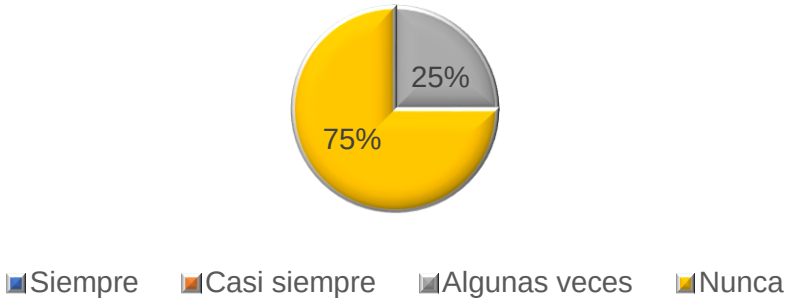
Nota. Muestra % de gestión de los dispositivos IoT desde un CMP

De la gráfica 12 se puede inferir que de acuerdo a la gestión de activos digitales para acceder a un CMP desde cualquier lugar y en cualquier momento mediante una conexión a Internet desde un PC, dispositivo móvil o tableta, del 100% de la población objeto de estudio el 83% consideró que esta acción nunca era ejecutada, en comparación con el 9% restante que afirmó casi siempre y el 8% correspondiente que expresó algunas veces.

12. ¿La gestión de inventarios es ideal para supervisar y controlar los dispositivos IoT a través de un único portal de gestión en línea?

Figura 13

Gestión de Inventarios para la Supervisión y Control de Dispositivos IoT

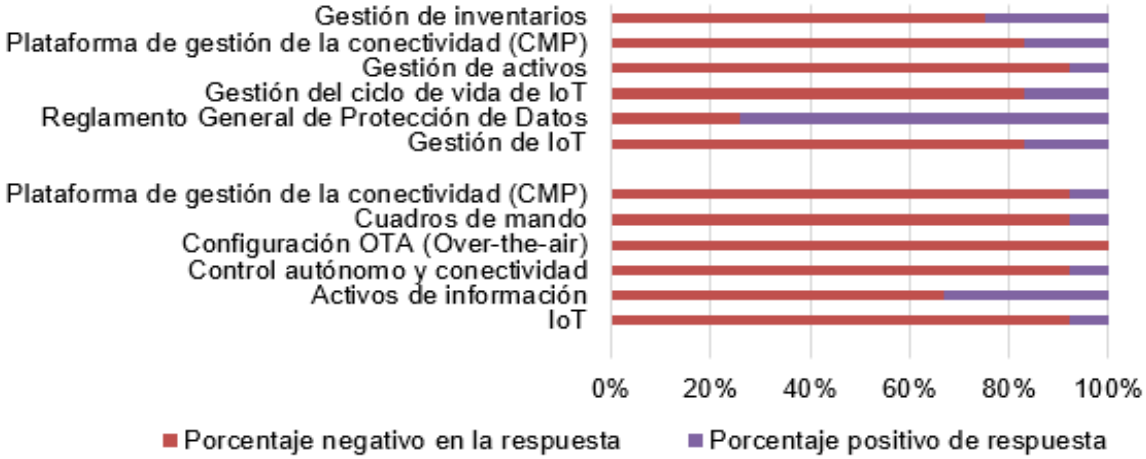


Nota. Análisis gráfico de la gestión de dispositivos IoT desde un portal de gestión en línea

De la gráfica número 13 se pude interpretar que del 100% de la población objeto de estudio, es decir, de los 12 encuestados, 9 cuya equivalencia es del 75%, consideraron, que la gestión de inventarios es ideal para supervisar y controlar los dispositivos IoT a través de un único portal de gestión en línea respondieron, sin embargo, 3 cuyo valor porcentual es del 25%, respondió que dicha acción se llevaba a cabo algunas veces.

Figura 14

Análisis Porcentual Positivo y Negativo de Respuestas del Cuestionario



Nota. Análisis gráfico de las respuestas resultado del cuestionario aplicado.

Identificación Activos de Información Asociados a IoT

Con el fin de abordar el primer objetivo, es pertinente referirse a los lineamientos expuestos en la Norma ISO 27001:2022 y su implementación en el ámbito de la seguridad. El análisis de riesgos representa una de las etapas más críticas que se deben llevar a cabo en la organización, con el propósito de optimizar la protección de la información dentro de la entidad.

Realizar un análisis exhaustivo permite centrar la atención en los riesgos vinculados a los sistemas, procesos y elementos del proyecto de investigación enfocado en los activos de información relacionados con IoT. Para seleccionar los activos de información se tiene en cuenta el impacto potencial en la seguridad de la información de la entidad, esta es una decisión crucial que puede tener un impacto significativo en la efectividad de las medidas de seguridad que se recomienda implementar para mitigar las vulnerabilidades, tanto de hardware como software, ya sea por sistemas con software obsoleto, bases de datos con información sensible, redes expuestas a internet y de activos de información que contienen información confidencial, como son los datos personales tales como huellas digitales que requieren una protección especial.

Entre los activos de información identificados en la consecución del primer objetivo del estudio, se encuentran los siguientes:

- Equipos de comunicaciones (Biométricos y Access Points):

Estos dispositivos almacenan datos que, en caso de ser comprometidos mediante un ataque cibernético, podrían comprometer la seguridad tanto de la información como de los dispositivos electrónicos. Equipados con tecnologías de comunicación 802.11ax y Wi-Fi, actúan como plataformas IoT que proporcionan servicios beneficiosos a los usuarios. Sin embargo, estas mismas características pueden ser aprovechadas por actores malintencionados para explotar vulnerabilidades y comprometer la seguridad.

- Firewall perimetral:

Este dispositivo desempeña una función esencial en la defensa de la organización, limitando el acceso a los sistemas internos, bloqueando la entrada de contenido malicioso en la red privada y previniendo la fuga de información, así como el uso no autorizado de los sistemas corporativos.

Integra hardware y software de última generación, incluyendo algoritmos complejos que permiten tomar decisiones críticas para proteger la entidad frente a ciberataques. Dado que cumple con las características estipuladas en el marco conceptual de este proyecto, se considera un activo de información vinculado al IoT.

- Bases de datos (Gestor Documental):

Este activo de información, una base de datos que facilita la interoperabilidad entre aplicaciones, ha sido seleccionado por su relevancia en la gestión de Peticiones, Quejas, Reclamos, Sugerencias, Denuncias, Solicitudes y Felicitaciones (PQRS) tramitadas por la Secretaría de Desarrollo Económico y otras dependencias de la Alcaldía de Bogotá.

La base de datos cuenta con algoritmos avanzados que automatizan el intercambio de información entre entidades. A través de un servicio web (webservice), detecta automáticamente si debe enviar o recibir datos relacionados con PQRS de origen ciudadano, lo que acelera la gestión de estas solicitudes por parte de la Administración Distrital.

A través del resultado mostrado por las encuestas realizadas se ha permitido indicar el diagnóstico de la situación actual en el que se encuentra la entidad frente a los riesgos a los que se expone por el uso de IoT y con la identificación de los activos de información vinculados con el Internet de las Cosas se permite cumplir con el objetivo de identificar mediante un análisis

diagnóstico los activos de información asociados a IoT en la SDDE, para con ello partir de una base para la evaluación de nivel de riesgos de cada activo.

Evaluación del Nivel de Riesgos de los Activos de Información Asociados a IoT

Una vez identificados los activos de información vinculados al Internet de las Cosas (IoT), ya sea por sus características propias o por manipulaciones humanas, el siguiente paso es reconocer las posibles amenazas o vulnerabilidades que puedan afectarles. Este análisis facilitará la implementación de las sanciones correspondientes al realizar la evaluación del riesgo.

La metodología que se aplicará para la evaluación de riesgos será la sugerida por el Departamento Administrativo de la Función Pública, conforme a lo establecido en su "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas", versión 6 del año 2022. Este documento proporciona los lineamientos esenciales y los criterios clave para la valoración de riesgos relacionados con la seguridad de la información. Según lo estipulado en el segundo paso de la guía, se identifican tres riesgos inherentes a la seguridad de la información, que son:

- Pérdida de confidencialidad
- Pérdida de integridad
- Pérdida de disponibilidad.

Además, se indican los valores que deben ser tenidos en cuenta para determinar el nivel de riegos asociados a los activos de información, relacionando el tipo de actividad (ver tabla 5) y la posibilidad de ocurrencia del riesgo durante un año (ver tabla 6).

Tabla 5

Actividades Relacionadas con la Gestión en Entidades Públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
Tecnología (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia, su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy Alta

Nota. Muestra las actividades relacionadas con la gestión en una entidad pública, bajo estas particularidades se establecen las escalas de probabilidad. Tomado de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (p. 40). por DAFP, (2022).

Tabla 6

Criterios para Definir el Nivel de Probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta de 500 veces al año y máximo 5000 veces por año	80%
	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Nota. Muestra la posibilidad de ocurrencia del riesgo relacionado con las actividades realizadas en una entidad pública. Tomado de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (p. 41). por DAFP, (2022).

Con base en lo anterior, se presenta a continuación la evaluación de riesgos asociados a los activos de información relacionados con el Internet de las Cosas (IoT) en la siguiente tabla:

Tabla 7

Matriz de Riesgos de Seguridad de la Información

Identificación del riesgo									Análisis del riesgo inherente						
ID	**Activo de información**	**Riesgo**	**Amenaza**	**Vulnerabilidad (es)**	**Descripción del Riesgo**	**Impacto**	**Clasificación del Riesgo**	**Frecuencia con la cual se realiza la actividad**	**Probabilidad Inherente**	**%**	**Criterios de impacto**	**Observación de criterio**	**Impacto Inherente**	**%**	**Zona de Riesgo Inherente**
1	Cortafuegos (Firewall)	Pérdida de disponibilidad y confidencialidad	Cibercriminal	Defectos bien conocidos en el software Ausencia de esquemas de reemplazo periódico	La posibilidad de pérdida de disponibilidad y confidencialidad de los servicios de la entidad por cibercriminal, debido a los defectos conocidos en el software y que junto a la ausencia de esquemas de reemplazo periódico que soporta los servicios expuestos a la ciudadanía en general.	Reputacional	Fallas Tecnológicas	8760	**Muy Alta**	100 %	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	**Moderado**	60 %	**Alto**

Identificación del riesgo									Análisis del riesgo inherente						
ID	**Activo de información**	**Riesgo**	**Amenaza**	**Vulnerabilidad (es)**	**Descripción del Riesgo**	**Impacto**	**Clasificación del Riesgo**	**Frecuencia con la cual se realiza la actividad**	**Probabilidad Inherente**	**%**	**Criterios de impacto**	**Observación de criterio**	**Impacto Inherente**	**%**	**Zona de Riesgo Inherente**
2	Bases de datos (Gesdoc)	Perdida de confidencialidad e integridad	Intruso	Punto único de fallas	La posibilidad de pérdida de confidencialidad e integridad en la información de las bases de datos por un intruso, debido a puntos de fallas que permiten interoperabilidad de las bases de datos institucionales con otras entidades distritales.	Reputacional	Fallas Tecnológicas	8760	**Muy Alta**	100 %	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	**Moderado**	60 %	**Alto**
3	Biométricos	Pérdida de confidencialidad	Procesamiento ilegal de datos	Ausencia de protección física de la edificación, puertas y ventanas	La posibilidad de pérdida de confidencialidad de los datos sensibles de los empleados de la entidad, debido a la ausencia presencia de protección física de la edificación, puertas y	Reputacional	Fraude Externo	8760	**Muy Alta**	100 %	El riesgo afecta la imagen de la entidad con algunos usuarios de releva	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro	**Moderado**	60 %	**Alto**

Identificación del riesgo								Análisis del riesgo inherente						
ID	**Activo de información**	**Riesgo**	**Amenaza**	**Vulnerabilidad (es)**	**Descripción del Riesgo**	**Impacto**	**Clasificación del Riesgo**	**Frecuencia con la cual se realiza la actividad**	**Probabilidad Inherente**	**%**	**Criterios de impacto**	**Observación de criterio**	**Impacto Inherente**	**%**	**Zona de Riesgo Inherente**
					ventanas que permita tomar datos de estos biométricos para usar de manera inadecuada.						ncia frente al logro de los objetivos	de los objetivos			
4	Access Points	Pérdida de confidencialidad	Escucha encubierta	Tráfico sensible sin protección	La posibilidad de pérdida de confidencialidad de datos e información sensibles de los usuarios, debido al tráfico sensible sin protección que se transmite por medio de estos dispositivos para su salida a Internet y que puede permitir la captura de estos datos para actividades fraudulentas.	Reputacional	Fallas Tecnológicas	8760	**Muy Alta**	100 %	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	**Moderado**	60 %	**Alto**

Nota. Muestra el panorama de riesgos, amenazas y vulnerabilidades de los activos de información asociados a IoT

A partir del análisis de la probabilidad de ocurrencia y de sus impactos, se determinó la zona de riesgo inherente (ver figura) para cada uno de los activos de información identificados.

Figura 15

Matriz de Calor (Niveles de Severidad del Riesgo)

Probabilidad	Impacto: Leve	Menor	Moderado	Mayor	Catastrófico
Muy Alta			R1, R2, R3 y R4		
Alta					
Media					
Baja					
Muy baja					

Nota. Muestra la ubicación de los riesgos identificados en la matriz de calor

La evaluación de los riesgos de seguridad de la información asociados a cada activo seleccionado indica un nivel de riesgo inherente clasificado como ALTO. Esta valoración se basa en la orientación proporcionada por el Departamento Administrativo de la Función Pública (DAFP), específicamente en el inciso 3.1, titulado "Análisis de riesgos", del Paso 3: "Valoración del riesgo". En concordancia con la tabla de actividades típicas vinculadas a la gestión de entidades públicas, que establece las escalas de probabilidad, se determina que, en el ámbito tecnológico, la probabilidad de materialización del riesgo es considerada Muy Alta.

Los hallazgos encontrados en el análisis de riesgos de los activos de información relacionados con la tecnología IoT en la SDDE, revela que la seguridad de la información se encuentra expuesta a amenazas y vulnerabilidades contempladas en la norma ISO 27001.

Con este resultado presentado se cumple con el objetivo específico de evaluar los riesgos asociados a dichos activos.

Propuesta de Plan de Acción

La Secretaría Distrital de Desarrollo Económico, consciente de los retos actuales, ha reconocido la necesidad de fortalecer su enfoque en la seguridad de la información, con el objetivo de proteger sus recursos digitales y asegurar la continuidad de sus operaciones. En este sentido, la norma ISO 27001 proporciona un marco sólido y reconocido a nivel internacional para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de este estándar no solo asegura el cumplimiento de las mejores prácticas globales, sino que también mejora la capacidad de la Secretaría para enfrentar y mitigar las amenazas cibernéticas.

Para integrar la seguridad de la información vinculada al Internet de las Cosas (IoT) dentro de la cultura organizacional de la Secretaría, resulta esencial desarrollar e implementar un plan de acción integral. Este plan debe alinear las actividades diarias con los principios y requisitos de la norma ISO 27001, abarcando todos los niveles de la organización, desde la alta dirección hasta los empleados y contratistas. Es fundamental que todos comprendan su rol y responsabilidad en la protección de la información. El apoyo y liderazgo de la alta gerencia serán claves para impulsar esta iniciativa, mostrando su compromiso con la seguridad de la información y asignando los recursos necesarios.

La ejecución del plan de acción implicará varias etapas importantes: la identificación y evaluación de los riesgos, la implementación de controles de seguridad adecuados, la capacitación y sensibilización del personal, y el establecimiento de mecanismos de seguimiento y evaluación continuos. También se promoverá una cultura de seguridad entre todos los miembros de la organización, incentivando la responsabilidad colectiva y el compromiso con la protección de la información.

El objetivo de este plan no solo es reducir los riesgos asociados al uso del IoT, sino también fomentar una actitud proactiva hacia la seguridad entre todos los miembros de la organización. De esta forma, la Secretaría fortalecerá su capacidad para enfrentar amenazas cibernéticas, asegurando la confidencialidad, integridad y disponibilidad de sus datos. La implementación de este plan contribuirá a crear un ambiente laboral más seguro y confiable, mejorando la resiliencia operativa y fortaleciendo la confianza de la ciudadanía en los servicios que ofrece la Secretaría Distrital de Desarrollo Económico.

Por lo anterior se concluye que, convertir la seguridad de la información en un elemento clave de la cultura organizacional, fundamentado en la norma ISO 27001, es un paso crucial para que la Secretaría Distrital de Desarrollo Económico pueda maximizar los beneficios del IoT, mientras protege sus datos y sistemas críticos. Esta estrategia no solo garantizará el cumplimiento normativo y la defensa ante amenazas, sino que también consolidará una cultura de seguridad sostenida, posicionando a la Secretaría como una entidad segura, eficiente y confiable en el ámbito digital.

Ciclo PHVA para minimizar los riesgos.

A continuación, se detallan las etapas del ciclo PHVA (Planificar-Hacer-Verificar-Actuar), que se propone como plan de acción para ser aplicado en la entidad con el fin de minimizar los riesgos identificados en los resultados anteriores.

Tabla 8

Propuesta Plan de Acción - Ciclo PHVA

	Actividad	Responsable	Documento
P	Establecer el contexto del proceso	- Comité Institucional de Gestión de Desempeño. - Comité Directivo. - Subdirección de Informática y Sistemas.	Política MSPI de la SDDE
P	Planificar el MPSI	- Comité Institucional de Gestión de Desempeño. - Comité Directivo. - Subdirección de Informática y Sistemas.	Política MSPI de la SDDE
H	Definir y evaluar los controles sugeridos por las buenas prácticas de seguridad TI.	- Subdirección de Informática y Sistemas. - Oficial de Seguridad de la Información	Política MSPI de la SDDE
H	Identificar, actualizar, clasificar y consolidar los Activos de Información	- Líder de proceso - Oficial de Seguridad de la Información	Política MSPI de la SDDE
H	Identificar, analizar y valorar riesgos de cada proceso y sus planes de tratamiento.	- Líder de proceso -Oficial de Seguridad de la Información	Política de Administración de Riesgos de la SDDE Plan de tratamiento de Riesgos de Seguridad de la Información
H	Actualizar y divulgar las políticas de seguridad de la información	Oficial de Seguridad de la Información	Política MSPI de la SDDE
V	Realizar el monitoreo, análisis y evaluación del MSPI	Oficial de Seguridad de la Información	Política MSPI de la SDDE
A	Tomar acciones correctivas, preventivas y de mejora	Oficial de Seguridad de la Información	Política MSPI de la SDDE

Nota. Resumen del plan de acción propuesto, para mitigar los riesgos asociados a los activos de información

Fase de Planear.

Objetivo de la fase: Establecer dentro del MSPI de la entidad el proceso de gestión “Seguridad de la Información” que permita tomar acciones referentes a las tecnologías emergentes.

Para esta fase se proponen las siguientes actividades:

1. Establecer el contexto del proceso.

Crear y caracterizar (ver tabla 9) un proceso que sea exclusivo para la Seguridad de la Información, el cual debe ser revisado por lo menos una vez al año para contemplar las necesidades de la entidad y las expectativas de las partes interesadas.

Tabla 9

Caracterización Propuesta del Nuevo Proceso

Nombre de Proceso	Seguridad de la Información
Objetivo	Planificar, implementar y mantener de manera continua el Modelo de Privacidad y Seguridad de la Información de la SDDE para garantizar, de forma integral, la confidencialidad, integridad y disponibilidad de la información
Alcance	Comienza con la definición de la Política de Seguridad de la Información, como parte del Modelo de Privacidad y Seguridad de la Información, continua con el identificación y análisis de las necesidades para proteger los activos de información y finaliza con la implementación de las acciones de mejora.
Responsable	Subdirección de Informática y Sistemas
Políticas	1. Para lograr el objetivo de manera efectiva, se requiere contar con recursos tecnológicos para garantizar el tratamiento y la custodia. 2.Contar con un Oficial de Seguridad de la Información calificado. 3. El cumplimiento de la Política de Seguridad de la Información es de carácter de obligatorio por parte de todo el personal que labora en la SDDE. 4. El Oficial de Seguridad de la Información será el encargado de ejecutar el Plan de Sensibilización y Capacitación de Seguridad de la Información. 5. En cumplimiento a lo establecido en el MSPI, el Oficial de Seguridad de la Información acompañará a los procesos en la identificación y actualización de los activos de información en la SDDE. 6. Es responsabilidad de todos los procesos de la Secretaria Distrital de Desarrollo Económico la identificación y clasificación de los activos de información. 7.Para reporte de los incidentes de seguridad de la información y su tratamiento se aplicará lo establecido en el MSPI de MinTIC, lo definido por la Alta Consejería Distrital de TIC.

Nota. Descripción proceso propuesto dentro el plan de acción

2. Planificar el Modelo de Privacidad y Seguridad de la Información.

La Secretaria Distrital de Desarrollo Económico debe definir o actualizar políticas, lineamientos, estrategias, procedimientos, roles y responsabilidades para el establecimiento y funcionamiento del Modelo de Privacidad y Seguridad de la Información enfocado en las nuevas tendencias tecnológicas, en este caso, tener en cuenta la singularidad del IoT.

Fase de Hacer.

Objetivo de la fase: Definir y evaluar los controles que mitigarán las vulnerabilidades y amenazas de los activos de información asociados con IoT y generar conciencia en los funcionarios/contratistas sobre la seguridad de la información y sus responsabilidades con el uso de IoT.

Para esta fase se propone las actividades detalladas y descritas en adelante:

1. En aras de disminuir la probabilidad y los impactos de los riesgos encontrados asociados a IoT, la SDDE debe en su proceso de mejora continua constantemente definir y evaluar los controles, acorde a lo sugeridos por las buenas prácticas de seguridad de la información apoyados en la norma ISO 27001.

Para los riesgos encontrados en el desarrollo de este proyecto aplicado de investigación, se propone que la SDDE aplique los siguientes Controles ISO 27001:2022 (ver tabla 10) con los atributos dispuestos, para atacar de manera correcta las amenazas encontradas en los activos de información asociados a IoT.

Dentro del desarrollo del proyecto se realiza el ejercicio de evaluar de los controles propuestos (ver tabla 11) para demostrar que, aplicando controles necesarios a cada riesgo, se puede obtener un desplazamiento del riesgo inherente a una zona moderada que permite a la entidad tener un mejor tratamiento de estos.

El resultado de esta evaluación se fundamenta en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas la versión 4 de 2018*, porque los parámetros señalados en el inciso *3.2.2.3 Análisis y evaluación de los controles* para valoración de los controles continúan vigentes.

Tabla 10

Propuesta de Controles ISO 27001:2022

Identificación del riesgo			Determinar Controles - Atributos de los controles									
								Atributos				
ID	**Activo de información**	**Riesgo**	**No. Control**	**Control ISO 27002:2022**	**Responsable ¿Quién?**	**¿Qué hacer en caso de no cumplir el control o que este se desvíe?**	**Afectación**	**Tipo**	**Implementación**	**Documentación**	**Frecuencia**	**Evidencia**
1	Cortafuegos (Firewall)	Pérdida de disponibilidad y confidencialidad	1	8.8 Gestión de vulnerabilidades técnicas	Contratista de Seguridad de la Información	Validar con el Subdirector de Informática y Sistemas la prioridad de ejecutar las actividades para identificar las vulnerabilidades técnicas	Probabilidad	Preventivo	Manual	Documentado	Aleatoria	Con Registro
			2	8.9 Gestión de la configuración	Profesional de Infraestructura	Solicitar a través del Subdirector de Informática y Sistemas la aplicabilidad de los ajustes técnicos en las	Probabilidad	Preventivo	Automático	Documentado	Aleatoria	Con Registro

Identificación del riesgo			Determinar Controles - Atributos de los controles									
								Atributos				
ID	**Activo de información**	**Riesgo**	**No. Control**	**Control ISO 27002:2022**	**Responsable ¿Quién?**	**¿Qué hacer en caso de no cumplir el control o que este se desvíe?**	**Afectación**	**Tipo**	**Implementación**	**Documentación**	**Frecuencia**	**Evidencia**
						plataformas para su aseguramiento						
2	Bases de datos (Gesdoc)	Perdida de confidencialidad e integridad	3	8.16 Actividades de seguimiento	Profesional de Infraestructura DBA	Gestionar configuración y registro de los eventos de las bases de datos	Probabilidad	Preventivo	Manual	Sin Documentar	Aleatoria	Con Registro

Identificación del riesgo					Determinar Controles - Atributos de los controles							
								Atributos				
ID	**Activo de información**	**Riesgo**	**No. Control**	**Control ISO 27002:2022**	**Responsable ¿Quién?**	**¿Qué hacer en caso de no cumplir el control o que este se desvíe?**	**Afectación**	**Tipo**	**Implementación**	**Documentación**	**Frecuencia**	**Evidencia**
3	Biométricos	Pérdida de confidencialidad	4	7.3 Aseguramiento de oficinas, salas e instalaciones	Profesional de SAF	Validar con la Subdirección Administrativa y Financiera la contratación de la vigilancia privada con circuito cerrado de TV incluido.	Probabilidad	Preventivo	Manual	Documentado	Continua	Con Registro
4	Access Points	Pérdida de confidencialidad	5	8.9 Gestión de la configuración	Profesional de Infraestructura	Gestionar configuración de los equipos Access Points de la SDDE	Probabilidad	Preventivo	Manual	Sin Documentar	Continua	Con Registro

Identificación del riesgo			Determinar Controles - Atributos de los controles									
								Atributos				
ID	**Activo de información**	**Riesgo**	**No. Control**	**Control ISO 27002:2022**	**Responsable ¿Quién?**	**¿Qué hacer en caso de no cumplir el control o que este se desvíe?**	**Afectación**	**Tipo**	**Implementación**	**Documentación**	**Frecuencia**	**Evidencia**
			6	8.20 Seguridad de redes	Profesional de Infraestructura Contratista Seguridad de la Información	Validar con el Subdirector de Informática y Sistemas la prioridad de ejecutar las actividades para identificar las vulnerabilidades técnicas sobre la red LAN	Probabilidad	Preventivo	Automático	Sin Documentar	Continua	Con Registro

Nota. Muestra los controles ISO 27001:2022 propuestos para mitigar las vulnerabilidades de los dispositivos IoT

Tabla 11

Valoración de los Controles ISO 27001:2022 Propuestos y su Impacto en los Riesgos Identificados en los Activos de Información Asociados a IoT

Identificación del riesgo			Determinar Controles - Valoración de los controles									Evaluación del riesgo - Nivel del riesgo residual		
						Atributos								
ID	**Activo de información**	**Riesgo**	**No. Control**	**Control ISO 27002:2022**	**Afectación**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Probabilidad**	**Impacto**	**Zona de**
1	Cortafuegos (Firewall)	Pérdida de disponibilidad y confidencialidad	1	8.8 Gestión de vulnerabilidades técnicas	Probabilidad	Preventivo	Manual	40%	Documentado	Aleatoria	Con Registro	**Media**	**Moderado**	**Moderado**
			2	8.9 Gestión de la configuración	Probabilidad	Preventivo	Automático	50%	Documentado	Aleatoria	Con Registro	**Media**	**Moderado**	**Moderado**

Identificación del riesgo			Determinar Controles - Valoración de los controles								Evaluación del riesgo - Nivel del riesgo residual		
					Atributos								
ID	**Activo de información**	**Riesgo**	**No. Control**	**Control ISO 27002:2022**	**Afectación**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Probabilidad**	**Impacto**	**Zona de**
2	Bases de datos (Gesdoc)	Perdida de confidencialidad e integridad	3	8.16 Actividades de seguimiento	Probabilidad	Preventivo	Manual	40%	Sin Documentar	Aleatoria	Con Registro	**Media**	**Moderado**	**Moderado**
3	Biométricos	Pérdida de confidencialidad	4	7.3 Aseguramiento de oficinas, salas e instalaciones	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	**Media**	**Moderado**	**Moderado**

Identificación del riesgo			Determinar Controles - Valoración de los controles								Evaluación del riesgo - Nivel del riesgo residual		
					Atributos								
ID	**Activo de información**	**Riesgo**	**No. Control**	**Control ISO 27002:2022**	**Afectación**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Probabilidad**	**Impacto**	**Zona de**
4	Access Points	Pérdida de confidencialidad	5	8.9 Gestión de la configuración	Probabilidad	Preventivo	Manual	40%	Sin Documentar	Continua	Con Registro	**Media**	**Moderado**	**Moderado**
			6	8.20 Seguridad de redes	Probabilidad	Preventivo	Automático	50%	Sin Documentar	Continua	Con Registro	**Media**	**Moderado**	**Moderado**

Nota. Muestra la valoración de los controles ISO 27001:2022 propuestos para mitigar las vulnerabilidades de los dispositivos IoT

3. Al menos una vez al año, la SDDE tiene la obligación de llevar a cabo la identificación o actualización de los activos de información. Esta actividad busca garantizar la disponibilidad, integridad y confidencialidad de dichos activos, siguiendo las directrices establecidas por el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

4. La entidad, en colaboración con los líderes de cada uno de sus procesos, deberá realizar anualmente la identificación, análisis y evaluación de los riesgos. A partir de este análisis, se definirán los planes de tratamiento correspondientes, los cuales deberán ser monitoreados en consonancia con los lineamientos estipulados en su Política General del Modelo de Seguridad y Privacidad de la Información.

5. Es responsabilidad de la organización actualizar y difundir las Políticas de Seguridad de la Información cada vez que se introduzcan modificaciones en los documentos que componen el MSPI. Para ello, es necesario establecer un plan de sensibilización y comunicación destinado a que todos los miembros de la entidad se familiaricen con las nuevas políticas.

En el desarrollo de este proyecto aplicado se propone un plan para llevar a cabo la actividad de divulgación en la entidad (ver Anexo 5)

Fase de Verificación.

Objetivo de la fase: Promover se realicen las auditoria periódicas de seguimientos al Modelo de Seguridad y Privacidad de la Información para tener claro qué se debe mejorar para enfrentar los riesgos a los que se expone la entidad.

En esta etapa, se recomienda la siguiente acción:

Monitorear, analizar y evaluar el MSPI.

La Secretaría Distrital de Desarrollo Económico (SDDE), de acuerdo con los lineamientos de su Política General del Modelo de Seguridad y Privacidad de la Información (MSPI), debe implementar un proceso continuo de seguimiento y monitoreo de los riesgos relacionados con la seguridad de la información. El objetivo de este proceso es analizar los resultados de los indicadores de desempeño, con el fin de tomar decisiones informadas que faciliten la transición efectiva hacia la siguiente fase dentro del ciclo de Deming.

Fase de Acción.

Objetivo de la fase: Incentivar a la mejora continua del Modelo de Seguridad y Privacidad de la Información de la entidad que proteja la información de la organización de amenazas y riesgos.

En esta fase, se sugiere la siguiente actividad:

1. Implementar acciones correctivas, preventivas y de mejora.

Como parte del proceso de mejora continua, la SDDE debe documentar detalladamente cada una de las acciones ejecutadas en relación con el MSPI. Este procedimiento debe fundamentarse en los resultados obtenidos durante la fase de verificación, así como en los resultados de la autoevaluación del modelo. De este modo, se podrán adoptar las acciones correctivas, preventivas o de mejora necesarias, garantizando una gestión efectiva y controlada de los riesgos.

Conclusiones

En la era de la digitalización, la incorporación del Internet de las Cosas (IoT) ha transformado radicalmente la manera en que las organizaciones gestionan y optimizan sus procesos. La Secretaría Distrital de Desarrollo Económico (SDDE) no es ajena a esta tendencia, y ha implementado tecnologías IoT con el fin de incrementar tanto la eficiencia como la eficacia de sus operaciones. Este proceso de adopción, sin embargo, también implica la aparición de nuevos desafíos relacionados con la seguridad de la información, los cuales deben ser gestionados de manera eficaz. La norma ISO/IEC 27001 proporciona un marco sólido para la administración de estos riesgos, garantizando la salvaguarda de la confidencialidad, integridad y disponibilidad de la información. El objetivo de este estudio es desarrollar un plan de gestión de riesgos asociado al IoT, basado en la norma ISO/IEC 27001, con el fin de proteger los datos sensibles dentro de la SDDE.

Identificación de Activos de Información Vinculados al IoT

Para formular un plan de gestión de riesgos, el primer paso es reconocer los activos de información vinculados al Internet de las Cosas (IoT) en el contexto de la Secretaria Distrital de Desarrollo Económico (SDDE). Este diagnóstico requiere la realización de un inventario exhaustivo que incluya todos los dispositivos IoT, las redes a las que están conectados, así como los datos que estos dispositivos generan y procesan.

La correcta identificación de estos activos es esencial, ya que permite evaluar los riesgos asociados y definir las estrategias de mitigación más adecuadas. Asimismo, este análisis proporciona una visión integral sobre la interdependencia entre los activos, lo cual es clave para una gestión eficaz de los riesgos.

En el mismo sentido, el diagnóstico de la situación actual permitió conocer que no se encomiendan acciones para garantizar la seguridad en la información que se transmite

mediante los activos de información asociado a IoT, sea para uso interno de la entidad o para comunicarse con organizaciones externas.

Por otra parte, se evidencia poca formación y comunicación formal para el recurso humano sobre los procedimientos, procesos y guías para proteger la información personal y la privacidad de los datos.

Evaluación del Nivel de Riesgos

Una vez que se han identificado los activos, es esencial proceder con una evaluación detallada de los riesgos relacionados. Esta evaluación debe fundamentarse en los principios de seguridad establecidos en la norma ISO/IEC 27001, que prioriza la salvaguarda de la confidencialidad, la integridad y la disponibilidad de la información. El proceso de evaluación de riesgos incluye la identificación de posibles amenazas y vulnerabilidades, junto con el análisis de la probabilidad de que estas se materialicen y el impacto potencial que podrían generar. Este proceso puede utilizar enfoques tanto cualitativos como cuantitativos, y debe contar con la participación de expertos en seguridad y tecnología de la información. La evaluación proporciona una visión clara sobre las áreas críticas que requieren mayor atención y las medidas necesarias para prevenir incidentes de seguridad.

La evaluación de riesgos de los activos de información asociados a IoT, es la piedra angular de este proyecto porque permite precisar la confianza del dispositivo o software usado en el día a día en la entidad, además porque proporciona una visión singular de sus amenazas y vulnerabilidades. En cada uno se han encontrado hallazgos que deben controlarse para mitigar los impactos que puedan generar en la información del organismo distrital.

Propuesta de un Plan de Acción

A partir de los resultados derivados del diagnóstico y la evaluación de riesgos, se diseñará un plan de acción enfocado en fomentar una cultura sólida de seguridad de la información en relación con el IoT dentro de la SDDE. Este plan incluirá la implementación de los controles establecidos en la norma ISO 27001:2022 con el objetivo de minimizar los riesgos y garantizar la protección de todos los activos de información de la Secretaría Distrital de Desarrollo Económico.

Dicho plan deberá ajustarse a los parámetros definidos por la norma ISO/IEC 27001 para asegurar una implementación adecuada. Las estrategias propuestas dentro de este plan pueden incluir:

Desarrollo de Políticas y Procedimientos de Seguridad:

Creación de políticas claras que regulen el uso seguro de los dispositivos IoT.

Procedimientos específicos para la gestión de incidentes de seguridad y la recuperación ante desastres.

Capacitación y Sensibilización del Personal:

Programas de formación para todos los empleados sobre las mejores prácticas en seguridad de la información.

Iniciativas de sensibilización que promuevan la relevancia de la seguridad en el manejo de IoT.

Implementación de Controles de Seguridad:

Uso de tecnologías avanzadas para la detección y prevención de intrusiones.

Controles de acceso y autenticación para salvaguardar los sistemas y datos relacionados con IoT.

Monitoreo y Evaluación Continua:

Establecimiento de mecanismos de vigilancia constante para la detección y respuesta inmediata ante amenazas.

Evaluaciones periódicas de la eficacia de las medidas de seguridad aplicadas.

Implicaciones y Beneficios:

La implementación de un plan de gestión de riesgos de IoT, alineado con la norma ISO/IEC 27001, no solo reforzará la seguridad de la información dentro de la SDDE, sino que también aumentará la confianza ciudadana en los servicios que ofrece. Al promover una cultura organizacional orientada hacia la seguridad garantiza que el personal reconozca la relevancia de proteger la información y adopte las acciones necesarias para ello. Del mismo modo, una gestión eficiente de los riesgos disminuye la probabilidad de eventos que comprometan la seguridad, atenúa el impacto de posibles amenazas y asegura la continuidad operativa.

Por último, la planificación e implementación de un sistema de gestión de riesgos que incluya nuevas tecnologías como IoT, alineado con la norma ISO/IEC 27001, resulta fundamental para resguardar los datos en la Secretaría Distrital de Desarrollo Económico. A través de una identificación exhaustiva de los activos, una evaluación meticulosa de los riesgos y la elaboración de un plan de acción integral, la SDDE podrá consolidar su estrategia de seguridad.

Este enfoque no solo está alineado con las mejores prácticas internacionales, sino que también fomenta una cultura de seguridad que perdurará en el tiempo, contribuyendo a la resiliencia y eficiencia operativa de la organización en un entorno digital cada vez más complejo.

Dado lo anterior, el presente proyecto se convierte en un insumo muy importante para que la Subdirección de Informática y Sistemas complemente las fases del modelo

MSPI en la entidad según las directrices dadas por el MinTIC, para reducir las brechas de seguridad digital.

Además, este proyecto de investigación aplicado sería una base sólida para incentivar a la alta dirección a incluir dentro de los planes institucionales recursos económicos que ayuden a mejorar la vigilancia tecnológica en ciberseguridad considerando el avance constante de las amenazas digitales.

Recomendaciones

En el entorno actual, la incorporación de tecnologías innovadoras, como el Internet de las Cosas (IoT), resulta fundamental para impulsar la transformación digital en las organizaciones, mejorando considerablemente la eficiencia operativa y favoreciendo la toma de decisiones fundamentadas en datos. La SDDE ha implementado dispositivos IoT en sus procesos con el objetivo de optimizar sus operaciones y brindar servicios más eficientes a la población. Sin embargo, estos avances tecnológicos también generan nuevas amenazas y vulnerabilidades que deben ser gestionadas con cautela para salvaguardar la información sensible.

Para abordar estos retos, se ha planteado la creación de un plan de gestión de riesgos centrado en el IoT, tomando como base la norma ISO/IEC 27001. Este marco normativo, reconocido internacionalmente, ofrece pautas claras para la protección de la información. Al seguir estas recomendaciones, la SDDE no solo podrá identificar y reducir los riesgos, sino también fomentar una cultura organizacional orientada a la seguridad de la información. Las acciones clave a implementar son las siguientes:

Fomentar el compromiso de alto direccionamiento y la cooperación activa del personal en la gestión de la seguridad de la información, para que lo involucren en la cultura de la mejora continua en la entidad.

Desarrollar directrices, políticas, procedimientos y planes de seguridad estandarizados, usando normas y metodologías reconocidas para brindar aspectos sólidos que configuren una base de seguridad eficiente para el uso de la tecnología .

Elaborar un inventario detallado de los dispositivos IoT y sus datos asociados, con el fin de mantener una identificación clara del tipo de información que se transfiere por medio de estos elementos.

Clasificar los activos de información según su relevancia y valor para la organización para tener una priorización, para identificar en cada uno de ellos lo posibles impactos que puedan generar cuando se generan ataques o incidentes de seguridad informática.

Documentar los procesos y flujos de información que involucren los activos de información vinculados con el uso de la tecnología IoT.

Evaluar las amenazas y vulnerabilidades específicas que afecten a los dispositivos IoT, porque es importante tener mapeado cada uno de estos elementos y conocer sus debilidades para poder fortalecer su seguridad eficazmente.

Estimar el impacto y la probabilidad de ocurrencia de los riesgos identificados.

Priorizar los riesgos según su criticidad y desarrollar un plan de mitigación adecuado.

Implementar programas de sensibilización y capacitación dirigidos a todos los actores laborales, apoyados con un plan de comunicación donde se muestre los beneficios y las precauciones de seguridad necesarias al usar nuevas tecnologías.

Establecer mecanismos de inspección y valoración continua para constatar la eficacia de las medidas implementadas, es decir, programar auditorias periódicas donde se evalúe y se mejore constantemente la seguridad de la información en la organización.

Finalmente, con la implementación de estas recomendaciones, la SDDE podrá gestionar de manera efectiva los riesgos de seguridad asociados al IoT, garantizando la protección de su información crítica y fortaleciendo su resiliencia operativa en un entorno digital en constante cambio. Este enfoque integral es crucial para mantener la confianza de la comunidad y el aseguramiento de propósitos estratégicos para la organización.

Referencias Bibliográficas

Aguilar, L. J. (2021). Internet de las cosas: Un futuro hiperconectado: 5G, inteligencia artificial, Big Data, Cloud, Blockchain, Ciberseguridad. Alpha Editorial.

Aguilar-Bernal, L. A. (2023). Investigación cualitativa y cuantitativa: complementos brillantes. Paradigmas Socio-Humanísticos, 5(1), 7–11. https://doi.org/10.26752/revistaparadigmassh.v5i1.691

Álava Zambrano, K. B., Basurto Vidal, W. E., & Tóala Vera, R. R. (2022). Vulnerabilidades en los sistemas informáticos owasp top 10: revisión bibliográfica. JOURNAL BUSINESS SCIENCE, 3(2). https://doi.org/10.56124/jbs.v3i2.0001

Álava-Zambrano, K. B., Basurto-Vidal, W. E., & Tóala-Vera, R. R. (2022). Vulnerabilidades en los sistemas informáticos owasp top 10: revisión bibliográfica: Vulnerabilities in computer systems owasp top 10: bibliographic review. Journal Business Science - ISSN: 2737-615X, 3(2), 1–8. https://doi.org/10.56124/jbs.v3i2.0001

Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0. Carnegie Mellon Software Engineering Institute, June, 1–84. http://www.sei.cmu.edu/publications/pubweb.html

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science and Engineering, 40(3), 1153–1166. https://doi.org/10.32604/csse.2022.019938

Alshurideh, M., Alquqa, E., Alzoubi, H., Kurdi, B., & Hamadneh, S. (2023). The effect of information security on e-supply chain in the UAE logistics and distribution

industry. Uncertain Supply Chain Management, 11(1), 145-152. DOI: 10.5267/j.uscm.2022.11.001

Amador-Alarcón, M. P., Torres-Gastelú, C. A., Lagunes-Domínguez, A., Angulo-Armenta, J., Argüello-Rosales, C. A., & Medina-Cruz, H. (2021). Marcos de competencias digitales relacionados con seguridad para docentes. Pädi Boletín Científico de Ciencias Básicas e Ingenierías del ICBI, 9(Especial), 48-52.

Angulo Montenegro, K. L. (2023). Ecosistema de internet de las cosas orientado a la adquisición automática de datos ambientales y de calidad (Doctoral dissertation, PUCESE-Escuela de Ingeniería en Tecnologías de la Información, Pontificia Universidad Católica del Ecuador)

Atif, A., Somroo, N. A., Farooq, U., Asif, M., Akour, I., and Mansoor, W. (2022). "Smartphone Security Hardening: Threats to Organizational Security and Risk Mitigation,". *International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates,* 1-12, doi: 10.1109/ICCR56254.2022.9995769

Balseca-Chávez, F. Colina-Vargas, A. M., & Espinoza-Mina, M. A. (2021). Identificación de amenazas informáticas aplicando arquitecturas de Big Data. INNOVA Research Journal, 6(3.2), 141–167. https://doi.org/10.33890/innova.v6.n3.2.2021.1860

Beltrán Castro, L. H., & Ramirez Zambrano, B. F. (2022). Análisis de vulnerabilidades en aplicaciones WEB de una empresa de Automatización industrial e IOT, para la prevención de ataques Cibernéticos.Aguilar, L. J. (2021). Internet de las cosas: Un futuro hiperconectado: 5G, inteligencia artificial, Big Data, Cloud, Blockchain, Ciberseguridad. Alpha Editorial.

Berrones-Paguay, A. V. (2020). Influencia de las Tecnologías de Información en los procesos contables de las organizaciones. REVISTA DE INVESTIGACIÓN SIGMA, 7(01), 22-28. https://doi.org/10.24133/sigma.v7i01.1845

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. In International Journal of Information Management (Vol. 51). https://doi.org/10.1016/j.ijinfomgt.2019.05.008

Cabrera-Tenecela, P. (2023). Nueva organización de los diseños de investigación. South American Research Journal, 3(1), 37–51. https://doi.org/10.5281/zenodo.8050508

Caicedo, A. J. C., García, A. F. G., Cedeño, J. J. U., & Bravo, J. E. G. (2022). Técnicas e Instrumentos para la Recolección de Datos que Apoyan a la Investigación Científica en Tiempo de Pandemia. Dominio de las Ciencias, 8(1), 58.

Castañeda-Mota, M. (2022). La cientificidad de metodologías cuantitativa, cualitativa y emergentes. Revista Digital de Investigación en Docencia Universitaria, 16(1), e1555. Epub 27 de abril de 2022.https://dx.doi.org/10.19083/ridu.2022.1555

Chacon, J., McKeown, S., & Macfarlane, R. (2020). Towards Identifying Human Actions, Intent, and Severity of APT Attacks Applying Deception Techniques—An Experiment. 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 1-8. https://doi.org/10.1109/CyberSecurity49315.2020.9138859

Cisneros-Caicedo, A. J., Guevara-García, A. F., Urdánigo-Cedeño, J. J., & Garcés-Bravo, J. E. (2022). Técnicas e Instrumentos para la Recolección de Datos que Apoyan a la Investigación Cientí-fica en Tiempo de Pandemia. Dominio De Las Ciencias, 8(1), 1165–1185. https://doi.org/10.23857/dc.v8i1.2546

Contreras-Hernández, L. S., Muñoz Ramírez, C., & Pinzón Moreno, E. I. (2022). Propuesta Integral de gobierno de la información para la Secretaría Jurídica Distrital (Maestría en gestión de la información documental, Universidad de la Salle)

DAFP. (2022). Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238

DNP. (2020). POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL. In Consejo Nacional de Política Económica y Social (p. 51). DNP. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

García, F. Y. H., & Moreta, L. M. L. (2019). Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras. Revista Ibérica de Sistemas e Tecnologias de Informação, (31), 1-17. https://doi.org/10.17013/risti.31.1–17

Geethamanikanta, J., Nikhitha, Y., Ansari, M. F. (2022). rtificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Managemen. *Journal of Positive School Psychology, 6, (*3), 6156–6165. Disponible en: https://journalppw.com/index.php/jpsp/article/view/3522/2300

Gobierno de España. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-

8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Guevara-Vega, E. M. D., Delgado-Deza, J. R., & Mendoza-de-los-Santos, A. C. (2023). Vulnerabilities and threats in information assets: a systematic review. Revista Científica De Sistemas E Informática, 3(1), e461. https://doi.org/10.51252/rcsi.v3i1.461

H., Z., A., H., & M., M. (2015). Internet of Things (IoT): Definitions, Challenges and Recent Research Directions. International Journal of Computer Applications, 128(1), 37–47. https://doi.org/10.5120/ijca2015906430

ITU, U. I. de T. (2016). Descripción General de Internet de los Objetos Y.2060- Y.4000. Y.2060 Y.4000, 20. http://handle.itu.int/11.1002/1000/11559

Jiménez, L. (2020). Impacto de la investigación cuantitativa en la actualidad. Convergence Tech, 4(IV), 59-68.

Journal on Information Security, 2020 (1). https://doi.org/10.1186/s13635-020-00111-0

Juliao, K., Montero, P., & Acevedo, D. (2021). Educación intercultural ante el impacto de las nuevas tecnologías y el Covid 19. Revista de filosofía, 38, 208-224

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. Eurasip

Landaeta-Arcentales, C. E., & Soberon-Hernandez, P. F. (2021). diseño e implementación de un sistema de registro de accesos utilizando iot para mejorar la seguridad física en el datacenter del departamento de informática de la municipalidad distrital de las amazonas-2021. (Tesis de Pregrado, Universidad Científica del Perú).

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and iot cyber risk management. In Future Internet (Vol. 12, Issue 9). DOI: https://doi.org/10.3390/FI12090157

Losada, A., & Marmo, J. (2022). Clasificación de Métodos de investigación en Psicología. PSICOLOGÍA UNEMI, 6(11), 13-31.

Malik, V., & Singh, S. (2020). Internet of Things: Risk Management. Smart Innovation, Systems and Technologies, 141, 419–427. https://doi.org/10.1007/978-981-13-8406-6_40

Marreros, J., Acosta, D., & Mendoza, A. (2024). Mecanismos de seguridad de la información en una organización: una revisión sistemática. Revista Científica Ciencias Ingenieriles, 4(1), 79–90. https://doi.org/10.54943/ricci.v4i1.384

Ming-Lang Tseng, Y. F., Wahyuni-Td, I. S., Lopes de Sousa, A. B., Chiappetta Jabbour, C. J., & Foropon, C. (2023) Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia, *Journal oIndustrial and Production Engineering,* 40:2, 102-116, DOI: 10.1080/21681015.2022.2116495

Moya, J. G. (2023). La importancia de la seguridad informática en la educación digital: retos y soluciones. RECIMUNDO: Revista Científica de la Investigación y el Conocimiento, 7(1), 609-616. Disponible en: http://hdl.handle.net/10609/148513

Muhammad A. H., Ume H., Fiaz M., & Muhammad S. (2021) Adaptive gamification in e-learning based on students. Learning styles, Interactive Learning Environments, 4, 545-565. DOI: 10.1080/10494820.2019.1588745

Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security Risk Assessment in Internet of Things Systems. IT Professional, 19(5), 20–26. https://doi.org/10.1109/MITP.2017.3680959

Ñaupas, H. (2018). Metodología de la Investigación Cuantitativa-Cualitativa y Redacción de la Tesis. Ediciones de la U.

Pin-Hsiang, W., & Marek, M. (2020). Designing Interactive Cross-cultural Mobile-Assisted Language Learning. IGI Global, 1, 452-475. DOI:10.4018/978-1-5225-9279-2.ch021

Raghuvanshi, A., Singh, U. K., Sajja, G. S., Pallathadka, H., Asenso, E., Kamal, M., & Phasinam, K. (2022). Intrusion detection using machine learning for risk mitigation in IoT-enabled smart irrigation in smart farming. *Journal of Food Quality*, 1-8. https://doi.org/10.1155/2022/3955514

Ramos Guzmán, J. E., González, J. C., & Bejarano, M. Á. Implementación de web application firewall basado en servicios Cloud e IoT (Doctoral dissertation, Universidad Santo Tomás).

Rivas, A., González-Briones, A., Hernández, G., Prieto, J., & Chamoso, P. (2021). Artificial neural network analysis of the academic performance of students in virtual learning environments. Neurocomputing, 423, 713-720. https://doi.org/10.1016/j.neucom.2020.02.125

Rodríguez, S. J. (2019). Un recorrido por la técnica de la entrevista en la recolección de datos cuantitativos. Diagramación y Compilación, 117.

Salgado, D., & Awad, G. (2022). Metodología para el análisis estratégico cuantitativo en proyectos a partir del análisis de riesgos. Estudios Gerenciales, 38(165), 424-435. https://doi.org/10.18046/j.estger.2022.165.5198

Sánchez-Bayón, A. (2022). Critica del positivismo formalista en economía y las alternativas heterodoxas para la economía digital. Encuentros multidisciplinares, 24(71), 1-16.

Spinelli, M. (2023). La construcción de datos estadísticos locales: análisis de situación particular de la localidad de Monte Buey (Córdoba). Territorios Productivos, (1). Recuperado a partir de https://territoriosproductivos.unvm.edu.ar/ojs/index.php/territoriosproductivos/article/view/604

Vasquez, J. D. (2023). ISO/IEC 27000. HIGH TECH-ENGINEERING JOURNAL, 3(2), 80-84. https://doi.org/10.46363/high-tech.v3i2.3

Vega Rincón, E. J., García Quintero, R. D., & Carvajal Artuduanga, J. F. (2021). Diseño de un plan de seguridad informática para el sistema de información del colegio gimnasio los pinos.

Velasco, M. D. L. Á. C., Manzano, P. J. G., & Pérez, C. G. (2022). Lo cuantitativo y cualitativo desde un tratamiento estadístico. RICSH Revista Iberoamericana de las Ciencias Sociales y Humanísticas, 11(21), 18-49.

Apéndices

Apéndice A

Encuesta de Diagnóstico

Preguntas	Opciones de respuesta			
¿Existe un cuadro de mando IoT que genere la suficiente seguridad para analizar, gestionar y añadir datos en directo y, posteriormente, consignarlos en otros dispositivos y sensores?	Siempre	Casi siempre	Algunas veces	Nunca
¿La gestión del ciclo de vida cuenta con la suficiente capacidad de ver, gestionar, operar, activar y dar de baja cualquier activo desde cualquier lugar y en cualquier momento?	Siempre	Casi siempre	Algunas veces	Nunca
¿El control autónomo total de la red posee la flexibilidad para seleccionar y cambiar a múltiples proveedores de conectividad para garantizar una alta disponibilidad para las necesidades de misión crítica?	Siempre	Casi siempre	Algunas veces	Nunca
¿La configuración OTA (Over-The-Air) suele realizarse por vía inalámbrica para la gestión segura y rentable de despliegues nuevos y existentes?	Siempre	Casi siempre	Algunas veces	Nunca
¿Las alertas y cuadros de mando proporcionan a los equipos de asistencia y a los ejecutivos una imagen de la situación y de la información siempre actualizada de todo el funcionamiento del activo asociado a IoT?	Siempre	Casi siempre	Algunas veces	Nunca
¿El cuadro de mandos de IoT y un Plataforma de gestión de la conectividad (CMP) ofrece la prevención adecuada del fraude informático detectándolo en tiempo real?	Siempre	Casi siempre	Algunas veces	Nunca

¿Los 4 tipos de plataformas de gestión de IoT como los dispositivos, conectividad, aplicación y analítica, están en óptimas condiciones para su funcionamiento en la empresa?	Siempre	Casi siempre	Algunas veces	Nunca
¿El personal de la empresa se rige por el Reglamento General de Protección de Datos (GDPR) para proteger la información personal y establecer normas sobre la privacidad de los datos?	Siempre	Casi siempre	Algunas veces	Nunca
¿La gestión del ciclo de vida de IoT admite sus modos de prueba y funciones de control en tiempo real como la activación, suspensión y desactivación de sus activos desplegados y dispositivos conectados?	Siempre	Casi siempre	Algunas veces	Nunca
¿La gestión de activos supervisa y controla cada dispositivo IoT desde una plataforma en línea disponible en la nube?	Siempre	Casi siempre	Algunas veces	Nunca
¿La gestión de activos digitales permite acceder a un CMP desde cualquier lugar y en cualquier momento a través de una conexión a Internet desde un PC, dispositivo móvil o tableta?	Siempre	Casi siempre	Algunas veces	Nunca
¿La gestión de inventarios es ideal para supervisar y controlar los dispositivos IoT a través de un único portal de gestión en línea?	Siempre	Casi siempre	Algunas veces	Nunca

Apéndice B

Formato Declaración de Consentimiento Informado para Encuestados

DECLARACIÓN DE CONSENTIMIENTO INFORMADO

Título de la Investigación: Plan de gestión de riesgos asociados a IoT para proteger la información en la Secretaría Distrital De Desarrollo Económico.

Investigador: Joe Alexander Núñez Yaguna.

Este proyecto de investigación se llevará a cabo en la Secretaría Distrital de Desarrollo Económico, ubicado en Bogotá D.C., y permitirá diagnosticar si existen medidas de seguridad para los datos de los activos de información asociados al IoT en la SDDE.

Usted ha sido invitado a ser parte, porque cumple con las características que se enumeran a posteriormente:

1. Es funcionario y/o contratista de la SDDE.
2. Interactúa en la gestión del activo de información.
3. Hace uso de los recursos brindados por los activos de información asociados con IoT.

Factores y riesgos.

Según la Resolución 8430 de 1993 del Ministerio de Salud Colombiano esta investigación es sin riesgo ya que como indica “Son estudios que emplean técnicas y métodos de investigación documental retrospectivos y aquellos en los que no se realiza ninguna intervención o modificación intencionada de las variables biológicas, fisiológicas, sicológicas o sociales de los individuos que participan en el estudio, entre los que se consideran: revisión de historias clínicas, entrevistas, cuestionarios y otros en los que no se le identifique ni se traten aspectos sensitivos de su conducta”.

Aclaraciones.

a. Su participación en la presente investigación será completamente voluntaria.

b. Se le da a conocer que los datos no serán entregados a ningún servicio comercial y que no habrá ninguna retribución por la participación en este estudio.

c. La información obtenida en esta investigación será utilizada solamente para fines académicos e investigativos con una rigurosa confidencialidad.

d. Se le informa que usted puede retirarse en cualquier momento que lo desee sin necesidad de dar explicaciones.

FIRMA DEL CONSENTIMIENTO.

Yo, _____, declaro que fui informado (a) e invitado a participar en esta investigación con un propósito académico y en pleno uso de mis facultades, es mi voluntad participar en esta investigación denominada "Plan de gestión de riesgos asociados a IoT para proteger la información en la Secretaría Distrital De Desarrollo Económico".

Autoriza: _____ **No autoriza**: _____

Fecha: **____/____/____**

_____

Firma

Apéndice C

Carta para Validación de Instrumento por Expertos

Bogotá D.C., Dia/Mes/Año

Señora.
Nombre del experto evaluador.

Asunto: **Validación de instrumento, por criterio de especialista.**

Cordialmente me dirijo a usted, inicialmente para expresarle un cordial saludo e informarle que, como parte del desarrollo de la tesis del Programa Académico de Maestría en Gestión de Tecnología De Información en la Universidad Nacional Abierta y a Distancia, estoy desarrollando el avance de mi tesis titulada "*Plan de gestión de riesgos asociados al IoT para proteger la información en la Secretaría Distrital De Desarrollo Económico*".

En este sentido, fue necesario la elaboración del instrumento y ficha de validación, cuyos resultados deben ser objeto de análisis y, posteriormente interpretados desde las respuestas de los actores institucionales conforme a los activos de información asociados al IoT en la SDDE.

La evaluación de los instrumentos cuantitativos de investigación por parte del Juicio de Expertos es de gran relevancia para lograr la validación de los resultados obtenidos, para tal fin se propone su revisión utilizando cinco criterios básicos para evaluar cada una de las interrogantes, estos son: suficiencia, claridad, coherencia, importancia y pertinencia, a efecto de asegurar el cumplimiento del objetivo propuesto.

Por lo expuesto, con la finalidad de darle rigor científico necesario, se requiere la validación de dichos instrumentos a través de la evaluación de Juicio de Expertos. Es por

ello, que me permito solicitarle su participación como juez, apelando a su trayectoria y reconocimiento como profesional en el área de Seguridad Informática.

Información sobre la Investigación:

Objetivo General:

Diseñar un plan de gestión de riesgos de IoT apoyado en la norma ISO/IEC 27001 para proteger la información en la Secretaría Distrital de Desarrollo Económico.

Objetivos Específicos:

1. Identificar mediante un análisis diagnóstico los activos de información asociados a IoT en la SDDE.

2. Evaluar el nivel de riesgos de activos de la información asociados a IoT para su prevención según los objetivos orientados a la seguridad de la misma que se consignan en la norma ISO 27001.

3. Proponer un plan de acción para que la seguridad de la información en IoT se convierta en cultura organizacional de acuerdo con lo establecido en la norma ISO 27001.

Atentamente,

_____

Joe Alexander Nuñez Yaguna

Anexos:

1. Cuestionario.
2. Formato de Validación del Instrumento.

Apéndice D

Formato de Validación del Instrumento

Criterios de Evaluación del Instrumento.

Para realizar la evaluación de este instrumento de corte cuantitativo, se requiere abordar al menos tres etapas en orden secuenciado, estas son: la validación del contenido, la determinación de la validez y el cálculo de la confiabilidad, esto es:

+ VALIDACIÓN: Juicio de Expertos, a fin de asegurar la fiabilidad del instrumento.

+ VALIDEZ: Realizar el Análisis Factorial Exploratorio (AFE) y más adelante se puede emplear el Análisis Factorial Confirmatorio (AFC), o el Análisis de Varianza Explicada (AVE), Prueba de RHO, etc. según decida el investigador.

+ CONFIABILIDAD: Determinar al menos el Alpha de Cronbach para cada Dimensión y para el Instrumento en general.

De acuerdo con los siguientes indicadores evalúe cada uno de los ítems propuestos según corresponda.

CRITERIO	CALIFICACIÖN	INDICADOR
Suficiencia	1. No cumple con el criterio.	* Los ítems no son suficientes para medir la dimensión.
Los ítems que pertenecen a una misma dimensión y bastan para obtener la medición de ésta.	2. Bajo Nivel.	* Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.
	3. Nivel Moderado.	* Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto Nivel.	* Los ítems son suficientes.
Claridad	1. No cumple con el criterio.	* El ítem no es claro.
El ítem se comprende fácilmente, es decir, su sintaxis y semántica son adecuadas.	2. Bajo Nivel.	* El ítem requiere bastantes modificaciones o una revisión muy grande en el uso de las palabras, su redacción o complemento en la escritura
	3. Nivel Moderado.	* Se requiere una modificación muy específica de algunos de los términos del ítem.

CRITERIO	CALIFICACIÖN	INDICADOR
	4. Alto Nivel.	* El ítem es claro, tiene la semántica y sintaxis adecuada.
Coherencia	1. No cumple con el criterio.	* El ítem no tiene relación lógica con la dimensión.
	2. Bajo Nivel.	* El ítem tiene una relación tangencial con la dimensión.
El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	3. Nivel Moderado.	* El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto Nivel.	* El ítem se encuentra completamente relacionado con la dimensión que está midiendo.
Importancia	1. No cumple con el criterio.	* El ítem puede ser eliminado sin que se vea afectada la comprensión de la dimensión.
El ítem es esencial, significa que si contribuye a entender bien el objeto de estudio.	2. Bajo Nivel.	* El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que éste evalúa.
	3. Nivel Moderado.	* El ítem es relativamente importante.
	4. Alto Nivel.	* El ítem es muy relevante y debe ser incluido.
Pertinencia	1. No cumple con el criterio.	* El ítem puede ser eliminado sin que afecte el análisis o el cumplimiento de propósito del estudio.
El ítem es relevante por su estrecha relación con el propósito establecido.	2. Bajo Nivel.	* El ítem tiene alguna pertinencia, sin embargo, refleja de manera muy vaga su pertinencia con el propósito citado.
	3. Nivel Moderado.	* El ítem es relativamente pertinente en sus implicaciones.
	4. Alto Nivel.	* El ítem es altamente pertinente y debe ser incluido.

Formato de Validación del Instrumento.

Dimensión	Categorías	Preguntas	Suficiencia	Claridad	Coherencia	Importancia	Pertinencia	Observación
Protección de la seguridad informática	Seguridad de la Información	¿Existe un cuadro de mando IoT que genere la suficiente seguridad para analizar, gestionar y añadir datos en directo y, posteriormente, consignarlos en otros dispositivos y sensores?						
Internet de las Cosas (IoT)	Gestión de Infraestructura de TI	¿La gestión del ciclo de vida cuenta con la suficiente capacidad de ver, gestionar, operar, activar y dar de baja cualquier activo desde cualquier lugar y en cualquier momento?						
Internet de las Cosas (IoT)	Gestión de Infraestructura de TI	¿El control autónomo total de la red posee la flexibilidad para seleccionar y cambiar a múltiples proveedores de conectividad para garantizar una alta disponibilidad para las necesidades de misión crítica?						

Dimensión	Categorías	Preguntas	Suficiencia	Claridad	Coherencia	Importancia	Pertinencia	Observación
Internet de las Cosas (IoT)	Gestión de Infraestructura de TI	¿La configuración OTA (Over-The-Air) suele realizarse por vía inalámbrica para la gestión segura y rentable de despliegues nuevos y existentes?						
Protección de la seguridad informática	Seguridad de la Información	¿Las alertas y cuadros de mando proporcionan a los equipos de asistencia y a los ejecutivos una imagen de la situación y de la información siempre actualizada de todo el funcionamiento del activo asociado a IoT?						
Protección de la seguridad informática	Seguridad de la Información	¿El cuadro de mandos de IoT y un Plataforma de gestión de la conectividad (CMP) ofrece la prevención adecuada del fraude informático detectándolo en tiempo real?						
Internet de las Cosas (IoT)	Gestión de Infraestructura de TI	¿Los 4 tipos de plataformas de gestión de IoT como los dispositivos, conectividad, aplicación y analítica, están en óptimas condiciones para su funcionamiento en la empresa?						

Dimensión	Categorías	Preguntas	Suficiencia	Claridad	Coherencia	Importancia	Pertinencia	Observación
Internet de las Cosas (IoT)	Gestión de Infraestructura de TI	¿El personal de la empresa se rige por el Reglamento General de Protección de Datos (GDPR) para proteger la información personal y establecer normas sobre la privacidad de los datos?						
Protección de la seguridad informática	Seguridad de la Información	¿La gestión del ciclo de vida de IoT admite sus modos de prueba y funciones de control en tiempo real como la activación, suspensión y desactivación de sus activos desplegados y dispositivos conectados?						
Internet de las Cosas (IoT)	Gestión de Infraestructura de TI	¿La gestión de activos supervisa y controla cada dispositivo IoT desde una plataforma en línea disponible en la nube?						
Internet de las Cosas (IoT)	Gestión de Infraestructura de TI	¿La gestión de activos digitales permite acceder a un CMP desde cualquier lugar y en cualquier momento a través de una conexión a Internet desde un PC, dispositivo móvil o tableta?						

Dimensión	Categorías	Preguntas	Suficiencia	Claridad	Coherencia	Importancia	Pertinencia	Observación
Internet de las Cosas (IoT)	Gestión de Infraestructura de TI	¿La gestión de inventarios es ideal para supervisar y controlar los dispositivos IoT a través de un único portal de gestión en línea?						

Opinión sobre su aplicabilidad: Aplicable ( ) Aplicable Después de Corregir ( ) No Aplicable ( )

_____

Firma del Juez.

Apéndice E

Propuesta de Sensibilización y Divulgación para que la Seguridad de la Información en IoT se Convierta en Cultura Organizacional

Plan de Sensibilización y Divulgación para que la Seguridad de la Información en IoT se Convierta en Cultura Organizacional.

Introducción

El Decreto 1008 de 2018 establece los lineamientos generales de la Política de Gobierno Digital que deben adoptar las entidades de la administración pública, con el propósito de fomentar la transformación digital y mejorar las capacidades de las TIC. En este contexto, en la última década las TIC se han consolidado como herramientas esenciales para la optimización de procesos y el funcionamiento eficaz de las empresas y entidades públicas. No obstante, el creciente uso de la tecnología trae consigo una serie de amenazas y vulnerabilidades que pueden comprometer la disponibilidad, privacidad e integridad de la información en diversas plataformas, afectando el desempeño normal de las organizaciones. Entre estas amenazas se encuentran los ataques cibernéticos, el malware y las brechas de seguridad, las cuales pueden tener consecuencias nocivas para la operación y reputación de una empresa.

De acuerdo con lo anterior, es fundamental reconocer que el recurso humano puede ser el eslabón más débil en la cadena de seguridad informática. Muchas entidades no integran adecuadamente a su personal en la implementación de medidas de seguridad, lo que insta la necesidad de programas de sensibilización y capacitación sobre la importancia de preservar la disponibilidad, integridad y confidencialidad de la información.

Por todo lo antes mencionado la presente propuesta tiene como objetivo principal, elaborar un plan estratégico para la Gestión de Riesgos de Seguridad y Privacidad de la

Información en la SDDE, que promueva la adopción de una cultura organizacional centrada en la seguridad digital desde la implementación de un plan de acción integral, programas de sensibilización y cualificación que evidencie el compromiso de todo el personal corporativo en la Secretaría de Desarrollo Económico de Bogotá. Todo ello basado en la expedición del Decreto 1008 de 2018, cuya finalidad es mejorar la seguridad de la información identificando las principales amenazas y vulnerabilidades asociadas con el uso de las TIC. Con ello se busca proponer estrategias que fortalezcan la participación del recurso humano en la preservación de la seguridad informática, generando una base sólida para la adopción de prácticas más seguras y eficaces en el manejo de recursos digitales en las entidades públicas.

Objetivos

- Desarrollar un plan de acción integral que incorpore la Gestión de Riesgos de Seguridad y Privacidad de la Información asociados al Internet de las Cosas (IoT) en la SDDE, promoviendo su adopción como una cultura organizacional sostenible y resiliente.
- Diseñar un programa de cualificación dirigido al personal corporativo, destacando la importancia de la gestión de riesgos de seguridad y privacidad de la información a nivel individual e institucional, a fin de generar un impacto positivo en la imagen pública de la Secretaría.
- Fomentar el compromiso de todos los integrantes de la entidad conforme al Sistema de Gestión de Seguridad y Privacidad de la Información, mediante la implementación de políticas claras, procedimientos estandarizados y la promoción de buenas prácticas en el manejo de la información.

- Implementar mecanismos de monitoreo y evaluación continua para medir la efectividad del plan de acción y los programas de capacitación, garantizando la mejora continua en la gestión de riesgos de seguridad y privacidad de la información.

Justificación

En la era digital actual, la seguridad y privacidad de la información son aspectos cruciales para el funcionamiento eficiente y la reputación de cualquier organización, especialmente en el sector público. El Decreto 1008 de 2018 establece un marco normativo para la transformación digital y la mejora de las capacidades de las TIC en las entidades de la administración pública. Sin embargo, la implementación efectiva de estos lineamientos requiere un enfoque integral y la participación activa de todos los actores laborales.

La SDDE se encuentra en un punto crítico donde la adopción de tecnologías avanzadas, como el Internet de las Cosas (IoT), puede generar importantes beneficios en términos de eficiencia y servicio público. En tal sentido, la integración del IoT permite una gestión más eficiente de los recursos, mejora la toma de decisiones basadas en datos en tiempo real y facilita la prestación de servicios más personalizados y efectivos. No obstante, estas tecnologías también introducen nuevas vulnerabilidades y riesgos que deben ser gestionados adecuadamente para proteger la disponibilidad, privacidad e integridad de la información.

La creciente dependencia de las TIC en los procesos operativos de la Secretaría aumenta exponencialmente los puntos de acceso que pueden ser explotados por ciberataques, haciendo imperativo contar con un sólido sistema de gestión de riesgos. Por ello, las consecuencias de no abordar adecuadamente estos riesgos incluyen la interrupción de servicios críticos, la pérdida de datos sensibles, el daño a la reputación de la entidad y posibles implicaciones legales. Además, la naturaleza dinámica de las amenazas

cibernéticas requiere una adaptación continua de las estrategias de seguridad para anticipar y mitigar nuevas formas de ataque.

Esta propuesta responde a la necesidad de establecer un marco estratégico para la Gestión de Riesgos de Seguridad y Privacidad de la Información, promoviendo una cultura organizacional centrada en la seguridad digital. La implementación de un plan de acción integral, junto con programas de sensibilización y capacitación, busca no solo cumplir con los requisitos normativos, sino también garantizar que todos los miembros de la entidad comprendan y se comprometan con la importancia de la seguridad de la información. La capacitación continua y la sensibilización son esenciales para transformar la percepción del personal hacia la seguridad de la información, haciendo que la protección de los datos sea una responsabilidad compartida.

La concienciación y el compromiso del recurso humano son fundamentales, dado que este puede ser el eslabón más débil en la cadena de seguridad. La mayoría de las brechas de seguridad ocurren debido a errores humanos, ya sea por desconocimiento o negligencia. Por ello, se hace imprescindible desarrollar políticas claras y procedimientos estandarizados que sean comprensibles y fáciles de seguir por todos los empleados. Además, se deben establecer mecanismos de monitoreo y evaluación continua para asegurar la mejora continua en la gestión de riesgos. Esto incluye auditorías periódicas, revisiones de políticas e implementación de herramientas tecnológicas avanzadas para la detección y respuesta a incidentes.

En síntesis, esta iniciativa no solo pretende proteger la información y los sistemas de la SDDE, sino también fortalecer su capacidad de respuesta ante incidentes que busquen vulnerar la seguridad informática, mejorando su eficiencia operativa y su imagen pública. Por último, pero no menos importante, la adopción de una cultura de seguridad digital no

solo beneficia a la entidad en términos de cumplimiento normativo y mitigación de riesgos, sino que también contribuye al desarrollo de un entorno de trabajo más seguro y confiable para todos, razón por la que la presente propuesta se constituye en una inversión en términos de sostenibilidad y resiliencia a largo plazo, asegurando el cumplimiento de su misión de manera eficaz y segura en un entorno cada vez más digitalizado.

Alcance

En el contexto actual de transformación digital, la seguridad y privacidad de la información se han consolidado como pilares fundamentales para el funcionamiento eficiente y confiable de las entidades del sector público. La SDDE, comprometida con la implementación del Decreto 1008 de 2018, se enfrenta al desafío de integrar tecnologías avanzadas como el Internet de las Cosas (IoT) mientras asegura la protección de sus datos y sistemas contra amenazas cibernéticas.

La creciente dependencia de las TIC para la optimización de procesos y servicios introduce nuevas vulnerabilidades que requieren una gestión de riesgos robusta y proactiva. Reconociendo la importancia de estos desafíos, la Secretaría ha desarrollado un plan estratégico que busca no solo mitigar riesgos, sino también fomentar una cultura organizacional centrada en la seguridad digital. Este enfoque integral involucra a todo el personal, desde el nivel administrativo hasta los contratistas, señalando la responsabilidad compartida en la protección de la información.

Los alcances de este plan estratégico están diseñados para abordar múltiples dimensiones de la seguridad y privacidad de la información, desde la implementación de un plan de acción integral y programas de capacitación hasta la adopción de políticas estandarizadas y la creación de mecanismos de monitoreo y evaluación continua. Cada uno

de estos componentes es esencial para construir una base sólida que garantice la resiliencia de la Secretaría frente a las amenazas digitales.

A continuación, se detallan los alcances específicos que guiarán la implementación y evaluación de las medidas propuestas, con el objetivo de asegurar la disponibilidad, integridad y confidencialidad de la información en la SDDE. Estos alcances proporcionan un marco estructurado y detallado que permitirá una gestión eficaz de los riesgos asociados al uso de tecnologías avanzadas, fortaleciendo la capacidad de la Secretaría para cumplir con su misión de manera segura y eficiente.

- Implementación del Plan de Acción Integral: Se desarrollará y ejecutará un plan de acción integral para la Gestión de Riesgos de Seguridad y Privacidad de la Información asociados al IoT, adaptado a las necesidades específicas de la SDDE. Este plan incluirá estrategias, políticas y procedimientos destinados a proteger la información y mejorar la resiliencia frente a ciberataques.
- Programas de Sensibilización y Cualificación: Se diseñarán e implementarán programas de sensibilización y capacitación dirigidos a todo el personal administrativo y contratistas de la Secretaría. Estos programas tendrán como objetivo concienciar sobre la importancia de la seguridad de la información, los riesgos asociados y las mejores prácticas para mitigarlos, destacando el impacto en la imagen pública de la entidad.
- Adopción de Políticas y Procedimientos Estandarizados: Se establecerán y formalizarán políticas claras y procedimientos estandarizados dentro del Sistema de Gestión de Seguridad y Privacidad de la Información. Estas políticas y procedimientos serán comunicados y adoptados por todos los miembros de la entidad, asegurando un enfoque coherente y unificado en la protección de la información.

- Mecanismos de Monitoreo y Evaluación: Se implementarán mecanismos de monitoreo y evaluación continua para medir la efectividad del plan de acción y los programas de capacitación. Esto incluirá auditorías periódicas, revisiones de políticas y el uso de herramientas tecnológicas avanzadas para la detección y respuesta ante incidentes de inseguridad.
- Compromiso y Participación del Personal: Se promoverá la participación activa y el compromiso de todos los integrantes de la entidad en la preservación de la seguridad y privacidad de la información. Esto se logrará mediante iniciativas que fomenten una cultura organizacional centrada en la seguridad digital, integrando estos principios en las actividades diarias y en la toma de decisiones estratégicas.
- Evaluación del Impacto: Se realizará una evaluación continua del impacto de las acciones implementadas, tanto en términos de mejora de la seguridad de la información como en la percepción del personal sobre su importancia. Esta evaluación permitirá realizar ajustes necesarios para asegurar la eficacia y sostenibilidad de las medidas adoptada
- Mejora Continua: Se establecerá un proceso de mejora continua que permitirá adaptar y actualizar las estrategias de seguridad y privacidad de la información según las nuevas amenazas y desafíos que surjan en el entorno digital. Este proceso garantizará que la Secretaría permanezca preparada y resiliente frente a futuros riesgos.
- Documentación y Reportes: Se generará una documentación exhaustiva de todas las acciones, políticas, procedimientos y resultados obtenidos, permitiendo un seguimiento detallado y una transparencia en la gestión de la seguridad de la información. Los reportes periódicos facilitarán la comunicación de avances y áreas de mejora tanto a nivel interno como a los organismos de control pertinentes.

Estos alcances proporcionan un marco detallado y estructurado para la implementación y evaluación de las acciones destinadas a mejorar la seguridad y privacidad de la información en la SDDE, asegurando una adopción efectiva y sostenible de una cultura de seguridad digital.

Actores Corporativos Implicados

Para la implementación exitosa del Sistema de Gestión de Seguridad y Privacidad de la Información en la SDDE, es fundamental contar con la participación activa y coordinada de diversos actores corporativos. Cada uno de estos actores desempeña un papel crucial en el desarrollo, implementación y monitoreo de las políticas y procedimientos necesarios para proteger la información y mitigar los riesgos asociados.

La Oficina Asesora de Planeación, la Subdirección de Informática y Sistemas, la Oficina de Control Interno, el departamento de Recursos Humanos, la alta dirección, empleados y contratistas de la Secretaría, trabajan en conjunto para asegurar que los objetivos de seguridad de la información se alcancen de manera efectiva. La colaboración entre estas unidades garantiza una estrategia integral y cohesiva que aborde todas las dimensiones de la seguridad y privacidad de la información. A continuación, se detalla la función específica de cada uno de dichos actores, recalcando su importancia y las responsabilidades que asumen en el marco del Sistema de Gestión de Seguridad y Privacidad de la Información. Esta estructura organizativa busca no solo cumplir con los requisitos normativos, sino también fomentar una cultura organizacional sólida frente a posibles panoramas de riesgo de la seguridad digital.

Oficina Asesora de Planeación: La Oficina Asesora de Planeación, actuando como parte de la segunda línea de defensa y como la dependencia responsable de liderar el desarrollo e implementación del Sistema de Gestión de Seguridad y Privacidad de la

Información, jugará un papel crucial en la adecuación y personalización de la metodología de administración de riesgos propuesta por el Departamento Administrativo de la Función Pública (DAFP) a las necesidades específicas de la SDDE. Esta oficina no solo adaptará la metodología, sino que también proporcionará la asesoría necesaria y las herramientas adecuadas para asegurar la correcta elaboración y ejecución de los procesos. Su responsabilidad incluye garantizar que todos los procedimientos se alineen con los objetivos estratégicos de la Secretaría y cumplan con las normativas vigentes.

Subdirección de Informática y Sistemas: El equipo de la Subdirección de Informática y Sistemas será el encargado de proporcionar el soporte técnico y operativo necesario para el desarrollo e implementación del componente de Administración del Riesgo de Seguridad y Privacidad de la Información. Este equipo recogerá iniciativas, definirá responsabilidades y armonizará los diferentes ejercicios y esfuerzos para la implementación de un proceso de gestión de riesgos más efectivo. Además, se asegurarán de que las soluciones tecnológicas utilizadas sean robustas y estén alineadas con las mejores prácticas internacionales en seguridad de la información. Su función también incluirá la actualización continua de sistemas y protocolos de seguridad para adaptarse a las nuevas amenazas emergentes.

Oficina de Control Interno: La Oficina de Control Interno será fundamental en el seguimiento y la evaluación del Sistema de Gestión de Seguridad y Privacidad de la Información. Este equipo velará por la adecuada elaboración e implementación del mapa de riesgos de cada proceso, asegurando que se promueva su apropiación, entendimiento y evaluación continua por parte de todos los involucrados. La Oficina de Control Interno se encargará de realizar auditorías periódicas, identificar áreas de mejora y asegurar que se implementen las recomendaciones pertinentes para fortalecer la seguridad y privacidad de

la información en toda la Secretaría. También fomentarán una cultura de transparencia y rendición de cuentas, vital para la sostenibilidad del sistema de gestión.

Recursos Humanos: El departamento de Recursos Humanos jugará un papel esencial en la sensibilización y capacitación de todo el personal, incluyendo a los empleados administrativos y contratistas. Serán responsables de diseñar e implementar programas de formación continua que subrayen la importancia de la seguridad de la información y los procedimientos correctos para su manejo. Además, Recursos Humanos trabajará en la integración de políticas de seguridad en todos los niveles organizacionales, promoviendo una cultura de seguridad desde la incorporación de nuevos empleados hasta la formación continua del personal existente.

Alta Dirección: La alta dirección de la SDDE tendrá un rol de liderazgo en la promoción y supervisión de la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información. Serán responsables de garantizar que los recursos necesarios estén disponibles y de apoyar activamente las iniciativas de seguridad de la información. Su compromiso y apoyo visible son cruciales para motivar a todo el personal a seguir las políticas y procedimientos establecidos.

Todos los Empleados y Contratistas: Todos los empleados y contratistas de la SDDE tendrán la responsabilidad de cumplir con las políticas y procedimientos de seguridad de la información. Su participación activa en programas de capacitación y su compromiso con la protección de la información serán esenciales para el éxito del sistema de gestión. La colaboración y el cumplimiento de todos los niveles garantizarán una defensa integral contra amenazas y vulnerabilidades.

Esta estructura organizativa asegura una distribución clara de responsabilidades y un enfoque coordinado en la gestión de riesgos de seguridad y privacidad de la

información, promoviendo una cultura de seguridad integral dentro de la Secretaría Distrital de Desarrollo Económico.

Términos Generales

El Decreto 1008 de 2018 ha sido un catalizador para la transformación digital en las entidades públicas, destacando la necesidad de una gestión robusta de riesgos asociados a las tecnologías de la información y comunicaciones (TIC). En este contexto, conceptos como la seguridad de la información, la privacidad de la información y la gestión de riesgos se vuelven cruciales. Estos términos no solo definen las amenazas y vulnerabilidades que deben gestionarse, sino también las estrategias y medidas necesarias para mitigar estos riesgos y fortalecer la resiliencia organizacional.

La adopción de tecnologías avanzadas como el Internet de las Cosas (IoT) ofrece oportunidades significativas para mejorar la eficiencia y la toma de decisiones basada en datos, pero también introduce nuevas dimensiones de riesgo que deben ser abordadas de manera proactiva. La construcción de una cultura organizacional de seguridad, a través de la sensibilización y capacitación del personal, es vital para garantizar que todos comprendan su rol en la protección de la información.

La Oficina Asesora de Planeación, la Subdirección de Informática y Sistemas, y la Oficina de Control Interno desempeñan roles esenciales en la adecuación, implementación y evaluación de las estrategias de seguridad. A través de un enfoque colaborativo y coordinado, estas dependencias aseguran que las políticas de seguridad y los procedimientos estandarizados se apliquen de manera efectiva en toda la organización.

En este documento, se presentan los términos generales que conforman el núcleo del SGSPI de la Secretaría Distrital de Desarrollo Económico. Estos términos proporcionan un lenguaje común y una comprensión compartida que son esenciales para el éxito de

cualquier iniciativa de seguridad y privacidad de la información. Al familiarizarse con estos conceptos, todos los actores corporativos podrán contribuir de manera más efectiva a la protección de la información y al cumplimiento de las normativas vigentes, asegurando un entorno digital seguro y confiable. En este orden de ideas, dichos términos proporcionan una base terminológica y conceptual que apoya la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI). Estos términos son fundamentales para todos los actores corporativos implicados, desde la alta dirección hasta cada empleado y contratista, asegurando una comprensión uniforme de los principios, políticas y prácticas de seguridad.

Seguridad de la Información: La protección de la información contra una amplia gama de amenazas para garantizar la continuidad del negocio, minimizar el riesgo empresarial y maximizar el retorno de las inversiones y las oportunidades de negocio.

Privacidad de la Información: El derecho de las personas y las organizaciones a proteger sus datos y a decidir cómo se recopila, usa y divulga su información personal y confidencial.

Gestión de Riesgos: El proceso sistemático de identificar, evaluar y controlar las amenazas a los activos de información, incluyendo riesgos tecnológicos, organizacionales y humanos.

Internet de las Cosas (IoT): La interconexión a través de internet de dispositivos informáticos integrados en objetos cotidianos, lo que les permite enviar y recibir datos, y que representa nuevas oportunidades y riesgos para la gestión de la información.

Cultura Organizacional de Seguridad: Un conjunto de valores, creencias y comportamientos compartidos dentro de una organización que priorizan la protección de la

información y la gestión de riesgos como aspectos fundamentales de las operaciones diarias.

Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI): Un marco estructurado de políticas, procedimientos y controles destinados a proteger la información y garantizar la privacidad de los datos, alineado con normativas como el Decreto 1008 de 2018 y las mejores prácticas internacionales.

Plan de Acción Integral: Una estrategia detallada que describe las acciones, responsabilidades y recursos necesarios para implementar eficazmente la gestión de riesgos de seguridad y privacidad de la información en la organización.

Sensibilización y Capacitación: Programas educativos y de formación diseñados para aumentar el conocimiento y la comprensión del personal sobre la importancia de la seguridad y privacidad de la información, así como sobre las mejores prácticas para protegerla.

Mapa de Riesgos: Una representación gráfica y analítica de los riesgos identificados en los procesos de la organización, que permite priorizar y gestionar estos riesgos de manera efectiva.

Auditorías de Seguridad: Evaluaciones sistemáticas y documentadas de los sistemas de información y las prácticas de seguridad de una organización para garantizar el cumplimiento de políticas y normativas, así como para identificar áreas de mejora.

Políticas de Seguridad: Directrices formales que establecen los principios, responsabilidades y prácticas que deben seguirse para proteger la información y los sistemas de una organización.

Procedimientos Estandarizados: Instrucciones detalladas y específicas que describen cómo deben realizarse las tareas y operaciones para cumplir con las políticas de seguridad y gestionar los riesgos de manera efectiva.

Resiliencia: La capacidad de una organización para anticipar, resistir, adaptarse y recuperarse rápidamente de interrupciones o amenazas a la seguridad de la información.

Alta Dirección: Los líderes y ejecutivos de la Secretaría Distrital de Desarrollo Económico, responsables de tomar decisiones estratégicas y proporcionar los recursos y el apoyo necesarios para implementar y mantener el Sistema de Gestión de Seguridad y Privacidad de la Información.

Oficina Asesora de Planeación: La dependencia responsable de liderar el desarrollo e implementación del SGSPI, adecuando la metodología de administración de riesgos a las necesidades de la Secretaría y brindando asesoría y herramientas a los procesos.

Subdirección de Informática y Sistemas: El equipo encargado de brindar apoyo técnico y operativo en la implementación del componente de Administración del Riesgo de Seguridad y Privacidad de la Información, recogiendo iniciativas y armonizando esfuerzos para un proceso más efectivo.

Oficina de Control Interno: El equipo responsable de velar por la adecuada elaboración e implementación del mapa de riesgos, promoviendo su apropiación, entendimiento y evaluación continua en toda la organización.

Recursos Humanos: El departamento encargado de la sensibilización y capacitación del personal, integrando políticas de seguridad en todos los niveles organizacionales y promoviendo una cultura de seguridad.

Empleados y Contratistas: Todos los miembros de la Secretaría Distrital de Desarrollo Económico que deben cumplir con las políticas y procedimientos de seguridad,

participando activamente en la protección de la información y en los programas de capacitación.

Viabilidad del Plan

La viabilidad de este plan proporciona una base sólida para la implementación exitosa del SGSPI, fortaleciendo la capacidad de la Secretaría Distrital de Desarrollo Económico para enfrentar los desafíos de seguridad y privacidad en el entorno digital moderno. En este marco, se describen los tres tipos de viabilidades:

Viabilidad Técnica

La viabilidad técnica de este plan se fundamenta en la existencia de una estructura organizativa robusta y bien definida dentro de la Secretaría Distrital de Desarrollo Económico. La Oficina Asesora de Planeación, la Subdirección de Informática y Sistemas, y la Oficina de Control Interno ya poseen experiencia y capacidades técnicas para liderar y gestionar proyectos complejos de seguridad y privacidad de la información.

Además, el personal de la Secretaría cuenta con un nivel adecuado de competencia y habilidades técnicas para adaptarse a nuevas metodologías y prácticas de gestión de riesgos. La implementación de programas de sensibilización y capacitación asegurará que todo el personal esté adecuadamente preparado para asumir sus responsabilidades en el marco del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

La infraestructura tecnológica actual de la Secretaría es suficiente para soportar las herramientas y sistemas necesarios para la gestión de riesgos de seguridad y privacidad. La integración de tecnologías avanzadas como el Internet de las Cosas (IoT) será manejada por la Subdirección de Informática y Sistemas, que garantizará la compatibilidad y la interoperabilidad con los sistemas existentes.

Viabilidad Tecnológica

La viabilidad tecnológica del proyecto se sustenta en la capacidad de la Secretaría para implementar y mantener soluciones tecnológicas avanzadas que faciliten la gestión de riesgos. Estas soluciones incluyen sistemas de monitoreo continuo, herramientas de detección y respuesta a incidentes de seguridad, y plataformas de capacitación en línea para el personal. La adopción de tecnologías de gestión de riesgos y seguridad de la información permitirá a la Secretaría anticipar, detectar y mitigar amenazas de manera efectiva. La Subdirección de Informática y Sistemas se encargará de evaluar y seleccionar las tecnologías más adecuadas, asegurando que estas estén alineadas con las mejores prácticas internacionales y cumplan con las normativas vigentes. El uso de tecnologías en la nube, inteligencia artificial y análisis de datos mejorará significativamente la capacidad de la Secretaría para gestionar grandes volúmenes de datos y responder rápidamente a incidentes de seguridad. Estas tecnologías también facilitarán la automatización de procesos y la implementación de controles de seguridad avanzados.

Viabilidad Financiera

La viabilidad financiera del proyecto se basa en un análisis detallado de los costos y beneficios asociados con la implementación del SGSPI. Los principales costos incluyen la adquisición de tecnologías y herramientas de gestión de riesgos, el desarrollo e implementación de programas de capacitación, y los recursos necesarios para la adaptación y personalización de metodologías de administración de riesgos. Sin embargo, los beneficios esperados superan significativamente estos costos. La protección de la información y la reducción de riesgos de seguridad y privacidad evitarán pérdidas financieras asociadas con brechas de seguridad, multas por incumplimiento de normativas y daños a la reputación de la Secretaría. Además, la mejora en la eficiencia operativa y la optimización de procesos resultarán en ahorros a largo plazo. La alta dirección de la

Secretaría ha mostrado un fuerte compromiso con la seguridad de la información, lo que garantiza la asignación de los recursos financieros necesarios para el éxito del proyecto. Además, la implementación de políticas y procedimientos estandarizados permitirá una gestión más eficiente de los recursos, optimizando el retorno de la inversión. La Secretaría también puede explorar la posibilidad de obtener financiamiento adicional a través de programas gubernamentales, subvenciones y asociaciones público-privadas que apoyen iniciativas de seguridad de la información y transformación digital. Estos fondos adicionales podrían cubrir una parte significativa de los costos iniciales de implementación.

Finalmente, la viabilidad técnica, tecnológica y financiera de este proyecto es sólida, respaldada por una estructura organizativa competente, una infraestructura tecnológica adecuada y un análisis financiero detallado que demuestra un retorno positivo de la inversión. La implementación del SGSPI no solo mejorará la seguridad y privacidad de la información, sino que también fortalecerá la resiliencia y la capacidad operativa de la Secretaría Distrital de Desarrollo Económico.

Temas de Sensibilización Identificados

A continuación, se proponen los temas de sensibilización para la Secretaría Distrital de Desarrollo Económico, con el fin de iniciar un proceso de culturizar a todo el recurso humano de la entidad:

1. Importancia de la Seguridad de la Información:

- Conciencia sobre la relevancia de proteger la información sensible y los datos personales.
- Impacto de las brechas de seguridad en la reputación y operación de la entidad.

2. Riesgos Asociados al Internet de las Cosas (IoT):

- Identificación de vulnerabilidades específicas del IoT.
- Mejores prácticas para asegurar dispositivos conectados.

3. Políticas y Procedimientos de Seguridad de la Información:

- Conocimiento de las políticas institucionales relacionadas con la seguridad de la información.
- Procedimientos estandarizados para manejar la información de manera segura.

4. Gestión de Incidentes de Seguridad:

- Protocolo de respuesta ante incidentes de seguridad.
- Herramientas y técnicas para la detección y mitigación de amenazas.

5. Privacidad de la Información:

- Principios de privacidad y protección de datos personales.
- Regulaciones y normativas aplicables (ej. Decreto 1008 de 2018).

6. Buenas Prácticas en el Uso de TIC:

- Uso seguro de correos electrónicos, navegación web y redes sociales.
- Prevención de phishing, malware y otros ciberataques.

7. Responsabilidades del Personal en la Seguridad de la Información:

- Roles y responsabilidades individuales en la protección de la información.
- Importancia de la colaboración y el compromiso de todos los empleados.

8. Actualización y Mantenimiento de Sistemas de Seguridad:

- Necesidad de mantener actualizados los sistemas y software de seguridad.
- Procedimientos para la actualización y parcheo de sistemas.

9. Evaluación y Monitoreo Continuo:

- Importancia de la auditoría y evaluación continua de los sistemas de seguridad.
- Métodos de monitoreo y evaluación de la efectividad de las medidas de seguridad.

Medios de Comunicación para Ejecutar el Plan.

1. Capacitaciones Presenciales y Talleres:

- Sesiones interactivas y prácticas para enseñar y reforzar conceptos de seguridad de la información.
- Talleres específicos sobre el uso seguro de IoT y manejo de incidentes de seguridad.

2. Plataformas de Capacitación en Línea:

- Cursos y módulos de e-learning accesibles para todo el personal.
- Evaluaciones en línea para medir la comprensión y retención de conocimientos.

3. Boletines Informativos y Comunicaciones Internas:

- Envío regular de boletines electrónicos con información actualizada sobre seguridad de la información.
- Comunicaciones internas que destaquen políticas, procedimientos y noticias relevantes.

4. Campañas de Concienciación:

- Campañas periódicas con temas específicos de seguridad y privacidad.

- Uso de infografías, videos y materiales visuales atractivos para comunicar mensajes clave.

5. Charlas y Conferencias:

- Invitar a expertos en seguridad de la información para dar charlas y conferencias.
- Sesiones de preguntas y respuestas para abordar preocupaciones específicas del personal.

6. Intranets y Portales Internos:

- Creación de un portal de seguridad de la información con recursos, políticas y guías disponibles.
- Foros y espacios de discusión para compartir experiencias y mejores prácticas.

7. Simulaciones y Ejercicios Prácticos:

- Ejercicios de simulación de ciberataques y gestión de incidentes para practicar la respuesta.
- Evaluaciones periódicas de la preparación del personal ante incidentes de seguridad.

8. Grupos de Trabajo y Comités de Seguridad:

- Establecimiento de grupos de trabajo especializados en diferentes aspectos de la seguridad de la información.
- Reuniones regulares para discutir avances, compartir conocimientos y coordinar esfuerzos.

9. Encuestas y Retroalimentación:

- Realización de encuestas para evaluar la efectividad de las iniciativas de capacitación y sensibilización.
- Recopilación de retroalimentación para mejorar continuamente los programas y estrategias de seguridad.

Implementar estos temas de sensibilización y utilizar diversos medios de comunicación asegurará que todo el personal de la Secretaría Distrital de Desarrollo Económico esté bien informado y comprometido con la protección de la información y la gestión de riesgos, contribuyendo así al éxito del Sistema de Gestión de Seguridad y Privacidad de la Información.

Cronograma de Actividades

CRONOGRAMA					Enero				Febrero				Marzo			
Componente	**Responsables**	**Tema**	**Actividad**	**Veces en el año**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**
Plan de Acción para que la Seguridad de la Información en IoT se Convierta en Cultura Organizacional.	Subdirección de Informática y Sistemas Subdirección Administrativa y Financiera	Política de Tecnología de la Información de la SDDE.	Inducción Corporativa	2												
		Internet de las Cosas.	Boletín Informativo	4												
		Uso de contraseñas, vigencia y complejidad.	Fondo de Escritorio	4												
		Cibercrimen, amenazas e impacto.	Fondo de Escritorio	2												
		Mitigación de Riesgos IoT.	Boletín Informativo	2												
		Peligros de los dispositivos IoT no seguros.	Boletín Informativo	4												
		Consejos de seguridad en dispositivos IoT.	Fondo de Escritorio	5												

		Controles mínimos necesarios de Seguridad de Información.	Boletín Informativo	3													

CRONOGRAMA					**Abril**				**Mayo**				**Junio**			
Componente	**Responsables**	**Tema**	**Actividad**	**Veces en el año**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**
Plan de Acción para que la Seguridad de la Información en IoT se Convierta en Cultura Organizacional.	Subdirección de Informática y Sistemas Subdirección Administrativa y Financiera	Política de Tecnología de la Información de la SDDE.	Inducción Corporativa	2												
		Internet de las Cosas.	Boletín Informativo	4												
		Uso de contraseñas, vigencia y complejidad.	Fondo de Escritorio	4												
		Cibercrimen, amenazas e impacto.	Fondo de Escritorio	2												
		Mitigación de Riesgos IoT.	Boletín Informativo	2												
		Peligros de los dispositivos IoT no seguros.	Boletín Informativo	4												

	Consejos de seguridad en dispositivos IoT.	Fondo de Escritorio	5	
	Controles mínimos necesarios de Seguridad de Información.	Boletín Informativo	3	

CRONOGRAMA					**Julio**				**Agosto**				**Septiembre**			
Componente	**Responsables**	**Tema**	**Actividad**	**Veces en el año**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**
Plan de Acción para que la Seguridad de la Información en IoT se Convierta en Cultura Organizacional.	Subdirección de Informática y Sistemas Subdirección Administrativa y Financiera	Política de Tecnología de la Información de la SDDE.	Inducción Corporativa	2												
		Internet de las Cosas.	Boletín Informativo	4												
		Uso de contraseñas, vigencia y complejidad.	Fondo de Escritorio	4												
		Cibercrimen, amenazas e impacto.	Fondo de Escritorio	2												
		Mitigación de Riesgos IoT.	Boletín Informativo	2												
		Peligros de los dispositivos IoT no seguros.	Boletín Informativo	4												

		Consejos de seguridad en dispositivos IoT.	Fondo de Escritorio	5											
		Controles mínimos necesarios de Seguridad de Información.	Boletín Informativo	3											

CRONOGRAMA					**Octubre**				**Noviembre**				**Diciembre**			
Componente	**Responsables**	**Tema**	**Actividad**	**Veces en el año**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**	**S1**	**S2**	**S3**	**S4**
Plan de Acción para que la Seguridad de la Información en IoT se Convierta en Cultura Organizacional.	Subdirección de Informática y Sistemas Subdirección Administrativa y Financiera	Política de Tecnología de la Información de la SDDE.	Inducción Corporativa	2												
		Internet de las Cosas.	Boletín Informativo	4												
		Uso de contraseñas, vigencia y complejidad.	Fondo de Escritorio	4												
		Cibercrimen, amenazas e impacto.	Fondo de Escritorio	2												
		Mitigación de Riesgos IoT.	Boletín Informativo	2												
		Peligros de los dispositivos IoT no seguros.	Boletín Informativo	4												

	Consejos de seguridad en dispositivos IoT.	Fondo de Escritorio	5	
	Controles mínimos necesarios de Seguridad de Información.	Boletín Informativo	3	