PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR FACULTAD DE INGENIERÍA

Trabajo de Titulación como requisito previo para la obtención del título de Magister en Tecnologías de la Información, mención en Gestión y Administración de Tecnologías

EVALUACIÓN DE LA DISPONIBILIDAD DE SERVICIOS DE CIBERSEGURIDAD DE LA INFORMACIÓN EN USUARIOS FINALES EN M.I MUNICIPALIDAD DE GUAYAQUIL.

Autor: Henry Rubén Arroyo Álvarez

Director: Ing. Damián Nicolalde, M. SC.

Quito, Septiembre del 2024

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Henry Rubén Arroyo Álvarez**, con cédula de ciudadanía No. 0915321582, autor del trabajo de graduación titulado: **"EVALUACIÓN DE LA DISPONIBILIDAD DE SERVICIOS DE CIBERSEGURIDAD DE LA INFORMACIÓN EN USUARIOS FINALES EN M.I MUNICIPALIDAD DE GUAYAQUIL"**, previo a la obtención del título de **Magíster en Tecnologías de Información mención Gestión y Administración de TI**, de la Facultad de Ingeniería:

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Quito, Septiembre del 2024

Atentamente;

Henry Rubén Arroyo Álvarez
Autor del Trabajo de Titulación

APROBACIÓN DEL TUTOR

En mi carácter de Director (a) – Tutor (a) del Trabajo de Posgrado Titulado: **"EVALUACIÓN DE LA DISPONIBILIDAD DE SERVICIOS DE CIBERSEGURIDAD DE LA INFORMACIÓN EN USUARIOS FINALES EN M.I MUNICIPALIDAD DE GUAYAQUIL",** presentado por el maestrante **Henry Rubén Arroyo Álvarez**, con cédula de ciudadanía No. 0915321582, para optar al Grado de Magíster en Tecnologías de Información mención Gestión y Administración de TI, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ingeniería.

En la ciudad de Quito, a los septiembre de 2024.

Atentamente;

Ing. Damián Nicolalde, M. SC.

Tutor del Trabajo de Titulación

TURNITIN: INCLUIR HOJA DEL INFORME CON EL PORCENTAJE

Maestria de Henry Arroyo Corregida 5 sep 2024.docx

INFORME DE ORIGINALIDAD

7%	9%	0%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	miro.com Fuente de Internet	2%
2	pensare.mx Fuente de Internet	2%
3	www.ucatalunya.edu.co Fuente de Internet	2%
4	drones187181223.wordpress.com Fuente de Internet	2%

Excluir citas	Activo	Excluir coincidencias	< 2%
Excluir bibliografía	Activo		

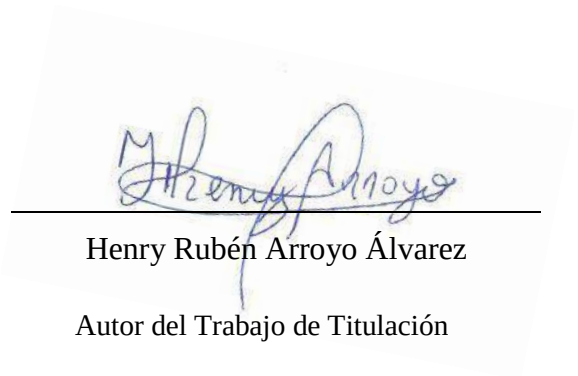
DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, **Henry Rubén Arroyo Álvarez**, con cédula de ciudadanía No 0915321582, declaro que los resultados obtenidos en la investigación **"EVALUACIÓN DE LA DISPONIBILIDAD DE SERVICIOS DE CIBERSEGURIDAD DE LA INFORMACIÓN EN USUARIOS FINALES EN M.I MUNICIPALIDAD DE GUAYAQUIL**", como requisito previo para lo obtención del Grado Académico de Magíster en Tecnologías de Información mención Gestión y Administración de TI son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos, que se desprenden del trabajo de investigación, y luego de la redacción de este documento, son y serán de mi sola y exclusiva responsabilidad legal y académica.

En la ciudad de Quito, a los Septiembre del 2024.

Atentamente;



Henry Rubén Arroyo Álvarez

Autor del Trabajo de Titulación

INDICE DE CONTENIDO

ÍNDICE DE GRAFICAS

ÍNDICE DE TABLAS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN, MENCIÓN EN

GESTIÓN Y ADMINISTRACIÓN DE TECNOLOGÍAS

EVALUACIÓN DE LA DISPONIBILIDAD DE SERVICIOS DE CIBERSEGURIDAD DE LA INFORMACIÓN EN USUARIOS FINALES EN M.I MUNICIPALIDAD DE GUAYAQUIL.

Autor: Henry Rubén Arroyo Álvarez

Director-Tutor: Damián Nicolalde

Fecha: Septiembre de 2024

RESUMEN

El presente proyecto de maestría **"**EVALUACIÓN DE LA DISPONIBILIDAD DE SERVICIOS DE CIBERSEGURIDAD DE LA INFORMACIÓN EN USUARIOS FINALES EN M.I MUNICIPALIDAD DE GUAYAQUIL", se basa en examinar cómo se ejecutan, manipulan, protegen los datos y sistemas informáticos dentro de la entidad pública. En este contexto, se investigan varios aspectos clave como:

El acceso y uso de servicios, protección de datos, políticas y procedimientos, evaluación de Riesgos, Infraestructura y Recursos, donde se revisa como los servicios de ciberseguridad pueden ser accesible para tanto los directores como los usuarios finales, en este caso dando facilidad y la disponibilidad de las herramientas de protección. Además, se evalúa la efectividad de las medidas de seguridad para precautelar la información vital, asegurando que la información este a buen recaudo de accesos no permitidos y posibles ataques cibernéticos.
}
Otro aspecto es ver si existen aplicaciones o políticas y procedimientos que estén alineados con la ciberseguridad, incluyendo a la formación de los usuarios finales sobre el tema, esto incluye identificar riesgos potenciales asociados con los sistemas y servicios.

Y no se deja de lado a la infraestructura tecnológica y los recursos disponibles para la ciberseguridad, evaluando si son los adecuados y si están actualizados para proteger la red de amenazas cibernéticas actuales.

El objetivo general de la evaluación es comprobar si las seguridades informáticas cuentan con un entorno seguro para el manejo y protección de la información para los usuarios finales, minimizando riesgos y asegurando un manejo óptimo de la operatividad de los servicios municipales.

PONTIFICAL CATHOLIC UNIVERSITY OF ECUADOR
FACULTY OF ENGINEERING

MASTER'S DEGREE IN INFORMATION TECHNOLOGIES WITH A MENTION IN IT

MANAGEMENT AND ADMINISTRATION

EVALUATION OF THE AVAILABILITY OF INFORMATION CYBERSECURITY SERVICES FOR END USERS IN MY MUNICIPALITY OF GUAYAQUIL.

Author: Henry Rubén Arroyo Álvarez

Director-Tutor: Damián Nicolalde

Date: September of 2024

ABSTRACT

This master's project "EVALUATION OF THE AVAILABILITY OF INFORMATION CYBERSECURITY SERVICES IN END USERS IN MY MUNICIPALITY OF GUAYAQUIL", is based on examining how data and computer systems are executed, manipulated, and protected within the public entity. In this context, several key aspects are investigated such as:

access and use of services, data protection, policies and procedures, risk assessment, infrastructure and resources, where it is reviewed how cybersecurity services can be accessible to both directors and end users, in this case providing ease and availability of protection tools. Additionally, the effectiveness of security measures to protect vital information is evaluated, ensuring that the information is safe from unauthorized access and possible cyber-attacks.

Another aspect is to see if there are applications or policies and procedures that are aligned with cybersecurity, including training end users on the subject, this includes identifying potential risks associated with systems and services.

And the technological infrastructure and resources available for cybersecurity are not left aside, evaluating whether they are adequate and updated to protect the network from current cyber threats.

The general objective of the evaluation is to verify whether computer security has a secure environment for the management and protection of information for end users, minimizing risks and ensuring optimal management of the operation of municipal services.

.

INTRODUCCIÓN

En la era digital actual, la ciberseguridad es una prioridad fundamental para las entidades tanto públicas como privadas. La M.I. Municipalidad de Guayaquil, como empresa pública de gran relevancia, no es una excepción. La protección de la información y la garantía de la disponibilidad de los servicios de ciberseguridad son esenciales para preservar la integridad, confidencialidad y disponibilidad de los datos que manejan.

El presente proyecto de maestría está enfocado en analizar la disponibilidad de los servicios de ciberseguridad ofreciendo a los usuarios finales de la M.I. Municipalidad de Guayaquil. Esta evaluación busca identificar corroborar si las medidas de seguridad informáticas son efectivas, así como ver las posibles mejoras que podrían ayudar a fortalecer las defensas cibernéticas de la entidad pública.

La importancia radica en el aumento de amenazas y ataques cibernéticos que enfrentan las entidades públicas y privadas. La M.I. Municipalidad de Guayaquil, como empresa que maneja datos e información muy valiosas y servicios críticos para la ciudadanía, debe poseer un sólido esquema de ciberseguridad para proteger sus operaciones y datos. La disponibilidad de estos servicios es primordial para evitar interrupciones que puedan afectar tanto a los empleados como a los procesos administrativos y operativos de la empresa.

Este estudio examinará diversos aspectos relacionados con la ciberseguridad, incluyendo la infraestructura tecnológica, las políticas de seguridad implementadas, el nivel de conciencia y capacitación de los usuarios finales, y la capacidad de respuesta ante incidentes de seguridad. Asimismo, se considerarán las herramientas y recursos disponibles para la protección de la información y la respuesta a posibles incidentes.

Por lo tanto, la evaluación proporciona un completo diagnóstico de la situación de seguridad cibernética actual en la M.I. La municipalidad de Guayaquil y proporcionar recomendaciones basadas en los hallazgos para mejorar la disponibilidad y eficacia de los

servicios de ciberseguridad. Además del estimulante para proteger la información, el análisis mejora la confianza de los usuarios a los servicios digitales proporcionados por la municipalidad.

En conclusión, el presente informe de la evaluación tiene por objeto asegurarse de que M.I. La Municipalidad de Guayaquil está debidamente preparada para abordar los desafíos de la ciberseguridad y asegurarse de que sus servicios digitales son seguros y fiables para todos los usuarios finales.

1. CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1.1.Resumen Ejecutivo

La ciberseguridad es una preocupación creciente para las instituciones públicas, debido a la proliferación de amenazas cibernéticas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. La M.I. Municipalidad de Guayaquil ha reconocido la importancia de proteger sus sistemas, datos contra estos riesgos y ha llevado a cabo una evaluación para determinar la disponibilidad y efectividad de los servicios de ciberseguridad dirigidos a sus usuarios finales.

A medida que la conectividad y las herramientas digitales son más importantes en las operaciones comerciales, se extienden amenazas de ciberseguridad. Esta tesis de maestría tiene como objetivo ayudar a entender mejor las amenazas y la importancia de integrar la ciberseguridad en las operaciones comerciales centrales, además de promover la conciencia de cómo estar protegidos a los usuarios finales. También proporciona información sobre herramientas y enfoques simples y de bajo costo que pueden usar para incrementar su resiliencia ante ataques típicos de seguridad cibernética.

1.2. Justificación

La justificación radica en la importancia crítica de garantizar la seguridad de la información y la protección de los datos confidenciales en una entidad gubernamental de gran envergadura como la Municipalidad de Guayaquil. Para ello, se identificarán algunas razones clave que respaldan esta propuesta:

Protección de datos confidenciales: La Municipalidad de Guayaquil maneja una gran cantidad de datos confidenciales de sus ciudadanos, incluyendo información financiera, de salud y personal. La disponibilidad de servicios de ciberseguridad para los usuarios finales es esencial para proteger estos datos contra posibles amenazas cibernéticas como ataques de malware, phishing o intrusión de hackers.

Otro sería la prestación eficiente de servicios públicos, puesto que la Municipalidad de Guayaquil proporciona una amplia gama de servicios públicos a sus ciudadanos, desde la gestión de residuos hasta la planificación urbana. La interrupción de los sistemas y servicios críticos debido a brechas de seguridad podría afectar negativamente la prestación de estos servicios, causando inconvenientes e insatisfacción entre los ciudadanos.

Además, se deberían cumplir normativas existentes, que son regulaciones y leyes tanto a nivel nacional como internacional, que establecen requisitos específicos en materia de seguridad de la información y protección de datos. La evaluación de la disponibilidad de servicios de ciberseguridad en la Municipalidad de Guayaquil es crucial para asegurar el cumplimiento de estas normativas y evitar posibles sanciones legales.

La confianza de los ciudadanos en la Municipalidad de Guayaquil (Reputación Institucional) puede verse afectada negativamente por incidentes de seguridad cibernética. Una evaluación exhaustiva de la disponibilidad de servicios de ciberseguridad y la implementación de medidas correctivas adecuadas pueden contribuir a preservar la reputación y la credibilidad de la institución.

Y, por último, el panorama de amenazas cibernéticas está en constante evolución, con nuevas técnicas y tácticas emergiendo constantemente. La evaluación de la disponibilidad de servicios de ciberseguridad en la Municipalidad de Guayaquil es fundamental para adaptarse a estos cambios y garantizar la protección continua de los sistemas y datos frente a las últimas amenazas.

En resumen, la investigación propuesta busca abordar una necesidad crítica en la Municipalidad de Guayaquil al evaluar la disponibilidad de servicios de ciberseguridad para usuarios finales, con el objetivo de fortalecer la protección de la información, garantizar la continuidad de los servicios públicos y mantener la confianza de los ciudadanos en la institución.

3.3 Contextualización del tema u objeto: disponibilidad Servicios de ciberseguridad

1.3. Objetivos

1.3.1. Objetivo general:

Elaborar una propuesta para mejorar la disponibilidad de servicios de ciberseguridad de la información en usuarios finales en M.I Municipalidad de Guayaquil.

1.3.2. Objetivos específicos:

Diagnosticar el estado actual de la ciberseguridad de la M.I Municipalidad de Guayaquil.

Identificar las vulnerabilidades que poseen las M.I Municipalidad de Guayaquil con respecto a la disponibilidad de servicios de la ciberseguridad utilizando Ética Hacking.

Proponer soluciones para mitigar las vulnerabilidades identificadas de la disponibilidad de servicios de la ciberseguridad.

Identificar indicadores de gestión que permitan medir la disponibilidad de servicios de la ciberseguridad.

1.4. Limitaciones del estudio

Para realizar la evaluación de disponibilidad de servicios de ciber seguridad en la M.I. Municipalidad de Guayaquil, nos encontramos con varias limitantes que no permiten realizar con normalidad el estudio tratado. A continuación, nombramos las limitantes:

- Movilidad por la ola de delincuencia que azota nuestro país.
- Acceso limitado a la M.I. municipalidad de Guayaquil.
- Permisos por parte de directivos a la hora de conseguir información respecto al estudio.

2. CAPÍTULO II. FUNDAMENTACIÓN TEÓRICA

2.1. Antecedentes de la investigación

El presente proyecto de maestría tomó como referencia proyectos relacionados, lo que implicó revisar diversos antecedentes que, de cierta manera, se relacionan con nuestro proyecto. Dicho estudio nos ha permitido obtener la siguiente información teórica, problemática y metodológica referente a temas como la alta disponibilidad, ciberseguridad, gestión de riesgos y formación de usuarios finales. Para ello, se ha realizado un estudio de los antecedentes tanto nacionales como internacionales, los cuales se muestran a continuación.

"En el artículo ´La concienciación al usuario final como mecanismo efectivo para la gestión de riesgos de seguridad de la información´ (Guatavita Diaz, 2018)." Nos hace referencia a que en el siguiente documento se aborda un tema que es poco tenido en cuenta a la hora de realizar la gestión de riesgos en las organizaciones, se trata de la concienciación al usuario final y como esta puede surtir efectos positivos en la compañía sin necesidad de tener que invertir grandes cantidades de tiempo y dinero en la implementación de controles técnicos. Además, redundando en grandes beneficios tanto para la compañía como para la vida personal de los empleados.

Esta tesis aporta bastante para el proyecto de maestría que se está realizando, puesto que la implementación de ciberseguridad en una institución educativa nos da la pauta que si por motivos cualquiera que sea la institución pública a la que estamos evaluando no posea en totalidad de seguridades de vanguardia, podamos sugerir métodos de ciberseguridades bajo parámetros de normas, gestión de riesgo que aportarían a mitigar las vulnerabilidades que posea.

“El trabajo de tesis ´Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un instituto superior tecnológico público, Lima – 2021´ (Manrique Reyna, 2021).” Nos afirma que la implementación de la metodología de Ciberseguridad, permitirá mejorar aspectos de confidencialidad, integridad y disponibilidad en los sistemas de información, mediante controles, políticas y mecanismos de seguridad que deben ser aplicados basado en la Norma ISO/IEC27032 lo cual va permitir que el instituto de educación superior público pase a un nivel de trasformación digital, ser más eficiente sus servicios digitales, encuentre seguridad en su arquitectura, además de tener más status a nivel nacional educativo ya que los institutos públicos aun no lo realizan, ello brindara mayor prestigio a la institución mostrando la seguridad que posee de manera física como virtual.

Esta tesis aporta bastante para el proyecto de maestría que se está realizando, puesto que la implementación de ciberseguridad en una institución educativa nos da la pauta que si por motivos cualquiera que sea la institución pública a la que estamos evaluando no posea en totalidad de seguridades de vanguardia, podamos sugerir métodos de ciberseguridades bajo parámetros de normas, gestión de riesgo que aportarían a mitigar las vulnerabilidades que posea.

“El trabajo de grado ´Importancia de Estructurar un Gobierno de Seguridad y Ciberseguridad en las Organizaciones´ (Hernández González, 2022).” Hace referencia a lo siguiente: Las organizaciones deben entender que la definición de un gobierno de ciberseguridad les permite mejorar sus procesos organizacionales, definir líneas de defensa y alcances que den valor agregado al aseguramiento de la información. Además, que ayuda a la alta dirección para que sean parte integral del proceso apoyando a permear a toda la organización, no solo pensar en el costo y retorno de la inversión y definir los lineamientos, si no en ser el factor interno que genera el respaldo del gobierno de Ciberseguridad y seguridad

dando la confiabilidad ante sus clientes aplicando buenas prácticas de aseguramiento tecnológico, con el fin de evitar incurrir en errores y sanciones por incumplimiento que puedan afectar su reputación.

Nos hace referencia a cómo podemos involucrarnos en la concepción de un buen departamento de TI para un buen manejo de información con seguridades robustas y a bajo costos.

"La tesis de maestría ´Importancia de la Alta Disponibilidad en la Infraestructura de Tecnologías de la Información´ (Cedeño Zambrano, Muñoz Zambrano, Párraga Ganchozo, & Rengifo Sanclemente, 2022)." Nos dice que el uso acelerado de las tecnologías digitales ha ocasionado un crecimiento de los ataques informáticos, los cuales ocupan la octava posición de los fenómenos con mayor impacto económico a nivel mundial; los cuales afectan seriamente a la disponibilidad de los servicios de Tecnología de la información. La disponibilidad garantiza que todos los equipos y la información que se maneja dentro de un sistema de información sea accesible, cuando se la necesita, por el personal que está autorizado para su uso; El objetivo es asegurar un cierto grado absoluto de continuidad operacional durante un período y medición dado; consiste en una serie de medidas tendientes a garantizar la disponibilidad del servicio.

Esta tesis nos aporta que es indispensable tener una alta disponibilidad en los servicios, puesto que si se presenta alguna novedad esté disponible varias opciones para tener los servicio en alto para así no tener inconvenientes en los procesos que tiene la empresa.

"El trabajo de grado ´La formación a usuarios finales como método de fortalecimiento del sistema de gestión de seguridad de la información´ (Gutiérrez Trujillo, 2018)." Nos plantea una serie de estrategias y metodologías, que permitirán, al área encargada del diseño,

implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) para cualquier empresa, realizar una serie de entrenamientos y transferencia de conocimiento enmarcadas en la formación a los usuarios finales, con el objetivo de dar a conocer y fortalecer el SGSI en la organización.

Este trabajo nos dice que usando un método SGSI se puede formar mejores usuarios finales con los conocimientos de seguridades, esto nos aportaría puesto estamos evaluando que tanta seguridad posee la entidad pública y resultaría una buena sugerencia implementar estos métodos si fuera el caso.

"El trabajo de tesis ´Evaluación de la seguridad de la información con hacking ético en la municipalidad distrital de san juan bautista´ (Rios Rios, 2023)." El presente proyecto va encaminado a revisar qué clase de seguridades posee la Municipalidad de San Juan Bautista y con esa premisa dar soluciones y recomendaciones de cómo resolver los problemas o vulnerabilidades que posea dicha entidad, bajo los parámetros del Hacking Ético se localizara las falencias ´para posterior sugerir un método seguro resguardar sus seguridades y su información que es lo más valioso.

Este proyecto de tesis es un caso similar al que se está planteando, puesto ellos realizan una evaluación a sus seguridades en la Municipalidad de San Juan, donde utilizaron hacking ético para verificar las vulnerabilidades. Este tema nos sirve como una guía para el desarrollo de nuestras premisas.

"La presente maestría ´Estrategia a partir de un análisis de vulnerabilidades para evaluar la seguridad de la información en la Alcaldía Barbosa Antioquia´ (Ramirez Agudelo , 2021)." El presente proyecto pretende crear una estrategia de mejora continua como parte del SGSI en la Alcaldía de Barbosa Antioquia partiendo de un análisis de vulnerabilidades

alineado a las recomendaciones que el Estado por medio de MINTIC establece tomando como marcos de referencia estándares y buenas prácticas de la industria tales como ISO 27000 y la NIST. Integrando herramientas que harán la exploración de las vulnerabilidades en la arquitectura de la red basados en la NIST SP 800-115 como buenas prácticas en los procesos de evaluación de seguridad como apoyo a la estrategia. Finalmente realizar un paso a paso que permita cerrar las vulnerabilidades y realizar las mejoras necesarias para proteger la infraestructura de una organización.

2.2. Fundamentación Teórica y Conceptual

El presente proyecto de maestría tomó como referencia proyectos relacionados, lo que implicó revisar diversos antecedentes que, de cierta manera, se relacionan con nuestro proyecto. Dicho estudio nos ha permitido obtener la siguiente información teórica, problemática y metodológica referente a temas como la alta disponibilidad, ciberseguridad, gestión de riesgos y formación de usuarios finales. Para ello, se ha realizado un estudio de los antecedentes tanto nacionales como internacionales, los cuales se muestran a continuación.

2.2.1. Conceptos Básico

2.2.1.1. Disponibilidad en seguridad informática

La disponibilidad de la información o de los activos de información es un principio fundamental de la seguridad informática que asegura la fiabilidad y el acceso oportuno a los datos y recursos por parte de los individuos o personas autorizadas. Según las mejores prácticas y estándares internacionales de seguridad de la información (serie ISO 27000, NIST, ENISA, ENS), el acceso a la información debe estar basado en el principio de necesidad de conocer, es decir, que solo aquellas personas que necesitan acceder a la información para el desempeño de sus tareas puedan hacerlo cuando lo necesiten.

El objetivo principal de la seguridad informática es proporcionar protección para la disponibilidad, integridad y confidencialidad de la información. Los controles de seguridad y las medidas y mecanismos de seguridad son implementados para proteger estos atributos o dimensiones de la información. Los riesgos, amenazas y vulnerabilidades se miden por su capacidad para comprometerlos.

Grafica N.1 Disponibilidad en seguridad informática

Fuente: https://www.unir.net/ingenieria/revista/disponibilidad-seguridad-informatica/
Elaborado: UNIR

Los dispositivos de red, ordenadores, servidores y demás sistemas de Tecnologías de la Información y las Comunicaciones (TIC) deben proveer la funcionalidad adecuada de manera predecible y eficiente cuando es necesaria. Además, estos deben recuperarse de interrupciones del servicio que prestan de manera segura y rápida para que la productividad o el negocio de las organizaciones no se vea afectada.

Un concepto fundamental a este respecto es el de **alta disponibilidad**, que se basa en el establecimiento de mecanismos para asegurar la tolerancia a fallos de los sistemas y equipamiento, como por ejemplo los clústeres o redundancia, que se basan en tener dos equipos o dos sistemas, funcionando al mismo tiempo activo-activo o balanceo de carga por

si falla uno de ellos, o funcionando uno y el otro de reserva por si falla el principal, maestro-esclavo o primario-secundario. (UNIR, 2021)

2.2.1.1.1. Aspectos principales de la disponibilidad de la Informática

Si bien, a grandes rasgos, ya sabes que es la disponibilidad en seguridades informáticas, este término implica varias cuestiones que merecen la pena mencionar para entenderlo bien:

Accesibilidad

Como hemos visto, el concepto de disponibilidad tiene que ver con la capacidad de garantizar el acceso a usuarios autorizados.

Prevención

También se refiere a la integración de distintos mecanismos que ayuden a prevenir ataques de denegación del servicio. Es decir, impide que los usuarios autorizados no puedan acceder a la información.

Seguridad

Como es lógico, el acceso a la información por parte de personas legitimas debe estas protegido con unos protocolos de seguridad concretos, los cuales variaran en función de la necesidades de tu negocio y son esenciales para frenar la entrada a extraños. (Horcajuela Muñoz , s.f.)

2.2.1.1.2. Garantizar la disponibilidad de la seguridad de la información

Asegurar la disponibilidad de la seguridad de la información es uno de los aspectos más cruciales para mantener una organización protegida y operativa de manera eficiente.

Grafica N.2 Garantizar la disponibilidad de la seguridad de la información

Fuente: https://ipnet.cloud/blog/es/datos/disponibilidad-de-la-seguridad-de-la-informacion-el-concepto/
Elaborado: IPNET.CLOUD

Backup y Recuperación de Desastres: Uno de los primeros pasos para garantizar la disponibilidad es implementar una estrategia de backup eficaz. Realizar copias de seguridad regulares de tus datos críticos es esencial.

Redundancia de Hardware y Redes: La redundancia juega un papel fundamental en el mantenimiento de la disponibilidad. Esto implica duplicar hardware y redes para garantizar que, si un componente falla, otro esté listo para asumir. Esta aproximación minimiza el tiempo de inactividad y mantiene los sistemas funcionando.

Monitoreo y Alertas: El monitoreo constante de los sistemas es esencial para detectar problemas antes de que afecten la disponibilidad. Utiliza herramientas de monitoreo de red y sistemas para seguir el rendimiento, la integridad y la seguridad de tus activos digitales. Configura alertas para ser notificado inmediatamente en caso de problemas.

Seguridad Cibernética: La seguridad cibernética desempeña un papel crítico en garantizar la disponibilidad. La implementación de firewalls, detección de intrusiones, sistemas de prevención de amenazas y prácticas de seguridad sólidas ayuda a proteger tus sistemas contra ataques cibernéticos que pueden comprometer la disponibilidad. (de Sousa, 2023)

Grafica N.3 Controles o medidas de seguridad

Fuente: https://www.unir.net/ingenieria/revista/disponibilidad-seguridad-informatica/
Elaborado: UNIR

2.2.1.2. ¿Qué es la ciberseguridad?

La ciberseguridad es la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones, que se originan tanto desde dentro como desde fuera de una organización.

Gráfico N.4 ¿Qué es la ciberseguridad?

Fuente: https://www.ibm.com/es-es/topics/cybersecurity
Elaborado: IBM

En 2020, el coste medio de una brecha de seguridad en los datos fue de 3,86 millones de dólares a nivel mundial, y 8,64 millones de dólares en Estados Unidos. Estos costes incluyen los gastos de descubrimiento y respuesta a la brecha, el coste del tiempo de inactividad y los ingresos perdidos, así como los daños a la reputación a largo plazo para un negocio y su marca. El objetivo de los ciberdelincuentes es la información de identificación personal (PII) de los clientes, como nombres, direcciones, números de identificación nacional (p. ej., número de la seguridad social en los EE. UU., códigos fiscales en Italia) o datos de tarjetas de crédito, y luego vender estos registros en los mercados digitales clandestinos. La PII comprometida a menudo provoca la pérdida de confianza del cliente, además de acarrear la imposición de multas regulatorias o incluso acciones legales.

La complejidad de un sistema de seguridad, a consecuencia de la aplicación de tecnologías dispares y la falta de experiencia interna, puede incrementar estos costes. Pero las organizaciones con una estrategia de ciberseguridad integral, dirigida por las mejores prácticas y automatizada mediante análisis avanzados, inteligencia artificial (IA) y aprendizaje automático, pueden hacer frente a las ciber amenazas de manera más efectiva y reducir la duración y las consecuencias de las brechas cuando se producen. (IBM, s.f.)

2.2.1.2.1. Dominios de ciberseguridad

La seguridad de la información es una preocupación cada vez más importante para las organizaciones de todos los tamaños y sectores. Para ayudar a garantizar la protección de los datos sensibles, la norma ISO 27001 del año 2022 establece un marco de gestión de la seguridad de la información basado en dominios.

Este marco está compuesto por 14 dominios que deben ser considerados al implementar un sistema de gestión de la seguridad de la información – SGSI (ISMS, por sus siglas en inglés).

A continuación, se listan los 14 dominios de la seguridad de la información que plantea la ISO 27001:

- Política de seguridad de la información
- Planificación
- Apoyo
- Evaluación de riesgos
- Gestión de activos
- Seguridad de la gestión de acceso
- Adquisición, desarrollo e implementación
- Operación de seguridad de la información
- Revisión de seguridad de la información
- Gestión de incidentes de seguridad de la información
- Mantenimiento
- Evaluación y tratamiento de continuidad del negocio
- Cumplimiento legal y normativo
- Mejora continua del ISMS. (Vásquez, 2023)

2.2.1.3. Tipos de amenazas a la ciberseguridad

2.2.1.3.1. Suplantación de identidad (phishing)

La suplantación de identidad (phishing) es la práctica de enviar correos electrónicos fraudulentos que se asemejan a correos electrónicos de fuentes de buena reputación. El objetivo es robar datos sensibles, como números de tarjetas de crédito e información de inicio de sesión. Es el tipo más común de ciberataque. Puede protegerse mediante la educación o una solución tecnológica que filtre los correos electrónicos maliciosos.

Gráfico N.5 Suplantación de identidad (phishing)

Fuente: https://www.globalsign.com/es/blog/que-es-phishing-y-como-evitarlo
Elaborado: GLOBALSIGN

2.2.1.3.2. Ransomware

El ransomware es un tipo de software malicioso. Está diseñado para exigir dinero mediante el bloqueo del acceso a los archivos o el sistema informático hasta que se pague un rescate. El pago del rescate no garantiza que se recuperen los archivos o se restaure el sistema.

Gráfico N.6 Ransomware

Fuente: https://expansion.mx/tecnologia/2022/02/02/evolucion-del-ransomware-historia
Elaborado: EXPANSION

2.2.1.3.3. Malware

El malware es un tipo de software diseñado para obtener acceso no autorizado o causar daños en una computadora

Gráfico N.7 Malware

Fuente: https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it
Elaborado: KASPERSKY

2.2.1.3.4. Ingeniería social

La ingeniería social es una táctica que los adversarios usan para engañarlo a fin de que revele su información confidencial. Pueden solicitarle un pago monetario u obtener acceso a sus datos confidenciales. La ingeniería social puede combinarse con cualquiera de las amenazas listadas anteriormente para predisponerlo a hacer clic en un enlace, descargar malware o confiar en una fuente maliciosa. (CISCO, 2024)

Gráfico N.8 Ingeniería social

Fuente: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering
Elaborado: KASPERSKY

2.2.1.4. Hacking Ético

El hacking ético, también conocido como penetration testing o ethical hacking, es el proceso de utilizar técnicas y herramientas similares a las que usan los hackers maliciosos con el fin de detectar y corregir vulnerabilidades en los sistemas y redes. El objetivo principal del hacking ético es mejorar la ciberseguridad y proteger los sistemas y datos de posibles ataques.

Gráfico N.9 Hacking Ético

Fuente: https://www.pmg-ssi.com/2023/08/que-es-el-hacking-etico/
Elaborado: ESG Innova Group

2.2.1.4.1. Diferencia Hacking Ético y Hacking Malicioso

El hacking ético se diferencia del hacking malicioso en que se realiza con el conocimiento y el consentimiento del propietario del sistema o red, y su finalidad es mejorar la seguridad en lugar de causar daño o robar información. Los hackers éticos también deben cumplir con ciertas normas éticas y legales, mientras que los hackers maliciosos actúan ilegalmente.

Los hackers éticos utilizan una variedad de herramientas y técnicas para detectar y corregir vulnerabilidades en los sistemas y redes. Algunas de las herramientas y técnicas más comunes son:

• Escaneo de puertos: consiste en determinar qué puertos están abiertos en un sistema o red, lo que puede indicar qué servicios están siendo utilizados y si hay alguna vulnerabilidad potencial. Herramientas como Nmap son ampliamente utilizadas para realizar escaneos de puertos.

• Análisis de vulnerabilidades: consiste en escanear el sistema o red en busca de vulnerabilidades conocidas. Estas herramientas, como Nessus o OpenVAS, pueden detectar vulnerabilidades en el software del sistema, como un sistema operativo o una aplicación web.

• Explotación: consiste en probar si las vulnerabilidades detectadas pueden ser explotadas en un ataque real. Metasploit es una herramienta comúnmente utilizada para la explotación.

• Ingeniería social: consiste en manipular a las personas para que revelen información sensible o realicen acciones que comprometan la seguridad. Herramientas como SET (Social Engineering Toolkit) pueden ayudar a crear ataques de ingeniería social.

• Análisis forense: consiste en examinar los rastros dejados por un ataque para determinar su origen, su método y su impacto. Herramientas como Autopsy o FTK (Forensic Toolkit) pueden facilitar el análisis forense. (Cataluña, s.f.)

2.2.1.5. Ley Orgánica de Protección de Datos Personales

El Reglamento establece en su objeto y ámbito, los aspectos necesarios para desarrollar y aplicar el marco legal en favor de la protección, tratamiento y custodia de información protegida constitucionalmente.

Se desarrolla el contenido y procedimiento para la solicitud de derechos protegidos por la ley: acceso, rectificación y actualización, eliminación, oposición, portabilidad.

Se regula lo relativo a la autoridad de protección de datos, estableciendo su forma de funcionamiento y organización del Registro Público a su cargo.

Establece las regulaciones específicas de los actores involucrados en la aplicación y cumplimiento de la ley: responsable del tratamiento, encargado del tratamiento y delegado de protección de datos. (MINTEL, 2021)

Gráfico N.10 Ley Orgánica de Protección de Datos Personales

Fuente: https://moint.ec/ley-organica-de-proteccion-de-datos-personales-en-ecuador/
Elaborado: MOINT

2.2.1.6. NIST (Instituto Nacional de Estándares y Tecnología)

NIST es el acrónimo de Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, en inglés) dependiente del Departamento de Comercio de EE. UU. El Marco de Ciberseguridad del NIST ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este Marco es voluntario. Le brinda a su negocio una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad. (CFC, s.f.)

Gráfico N.11 NIST (Instituto Nacional de Estándares y Tecnología)

Fuente: https://recfaces.com/es/articles/nist-standards-quality-assessment-of-biometric-algorithms
Elaborado: RECFACES

2.2.1.7. Indicadores de Gestión

Son métricas que permiten realizar una evaluación sobre la eficiencia y eficacia del tratamiento de un riesgo dentro de un sistema de gestión, a su vez dan la posibilidad de que se lleve a cabo un seguimiento de los planes de acción que se están ejecutando y que la junta directiva o accionistas puedan llevar un control de este.

Hay que tener en cuenta que en la norma ISO 27001, la cual está dirigida a la seguridad de la información dentro de las compañías, los indicadores juegan un papel crucial dentro de la gestión de riesgos y recomiendan que sean representados en un cuadro, para que su administración sea mucho más fácil, esto permite que se pueda llevar un mejor control y que al momento de generar reportes sobre la gestión de seguridad de la información sea de una manera rápida y concreta.

Cada uno de los indicadores debe contar con un proceso que demuestre si está siendo eficaz y está llegando a su punto de equilibrio dentro del sistema de gestión de seguridad de la información. (Arévalo, 2020)

2.2.1.7.1. ¿Qué son KPI?

Cuando se trata de proteger datos confidenciales, prevenir violaciones de datos y detectar ataques cibernéticos, se debe seguir una lista de verificación para realizar un seguimiento del estado de su seguridad informática. Los indicadores clave de rendimiento (KPI) son una forma eficaz de medir el éxito de cualquier programa y ayudan en la toma de decisiones. Es por eso que te explicaremos sobre las métricas de ciberseguridad.

2.2.1.7.2. ¿Por qué son importantes las métricas de ciberseguridad?

Las métricas de seguridad cibernética son indicadores de seguridad, pero no son un asunto de una sola vez. Las amenazas informáticas evolucionan constantemente, tanto los

procesos como la tecnología necesaria para prevenirlas evolucionan muy rápido. Debes contar con medidas de seguridad para evaluar la eficacia de las protecciones en las que han invertido.

Estas métricas de seguridad son importantes por dos razones:

El análisis de KPI, indicadores clave de riesgo (KRI) y posturas de seguridad proporciona una respuesta rápida de cómo funciona su equipo de seguridad a lo largo del tiempo. Ayudando a comprender mejor lo que está funcionando y lo que está empeorando, mejorando la toma de decisiones sobre proyectos futuros.

Las métricas de seguridad brindan información cuantitativa que puedes usar para mostrar a la gerencia y a los miembros de la junta que se toma en serio la protección y la integridad de la información confidencial y los activos de tecnología de la información.

Informar y brindar contexto sobre las métricas de seguridad cibernética es una parte importante del trabajo de muchos directores en seguridad de la información (CISO) y directores de información (CIO). Es por ello que son impulsados por el creciente interés de informar a los accionistas, reguladores y la junta.

Para muchos miembros de la junta en sectores como los servicios financieros, tienen el deber fiduciario o regulatorio de administrar el riesgo de ciberseguridad y proteger la información de identificación personal (PII).

Esto ha sido impulsado por nuevas regulaciones como la Ley Gramm-Leach-Bliley, la Regulación de Ciberseguridad del NYDFS, PIPEDA y CPS 234. También, se une esto con leyes de protección de datos extraterritoriales como GDPR, CCPA y LGPD, la gestión de la seguridad se convierte en un enfoque clave para cada organización. (Piensasoft, 2022)

Gráfico N.12 Indicadores de Gestión

Fuente: https://www.bizneo.com/blog/kpi/
Elaborado: BIZNEO

2.2.1.7.3. ¿Cómo Medir Algo que Aún no ha Sucedido?

Puede parecer que la seguridad de los datos es algo intangible y difícil de cuantificar y medir, ya que nunca sabemos de antemano a qué tipo de filtración de datos se enfrentará una organización. Los estudios empíricos mencionados en un comienzo (ver, por ejemplo, el informe de seguridad de IBM) comparten un punto de vista diferente.

La mayoría de las filtraciones de datos son causadas por factores conocidos como:

- Credenciales comprometidas (19%)
- Phishing (14%)
- Configuración incorrecta en la nube (19%)

Esto nos da una idea de dónde deben enfocarse los esfuerzos de ciberseguridad.

Si bien no podemos evitar todas las filtraciones de datos, los datos muestran que podemos minimizar su impacto en la organización al:

- Implementar la automatización de seguridad,
- Tener listos un equipo de respuesta y un plan de respuesta,
- Educar a los empleados y
- Probar el entorno empresarial mediante enfoques como las pruebas del equipo rojo. (Savkin, 2021)

2.2.1.7.4. KPI’s útiles en ciberseguridad

Los profesionales experimentados en ciberseguridad usan métricas para administrar los sistemas de seguridad informática, especialmente cuando dan informes a personas naturales o profesionales de otras ramas que no tengan conocimiento de lo que es ciber seguridad.

A continuación, se presentan algunos ejemplos de KPI de ciberseguridad

KPI: Número total de incidentes de seguridad

Medir el número total de incidentes de seguridad durante períodos de tiempo definidos (generalmente 1 mes y 1 año) puede brindarte un parámetro de comparación. Este KPI es fácil de calcular ya que es un conteo bruto de la cantidad de incidentes de seguridad en todas las partes de tu sistema. Cuando veas una mayor actividad, tu nivel de amenaza necesita aumentar.

Gráfico N.13 Número total de incidentes de seguridad

Fuente: https://blogs.manageengine.com/espanol/2024/03/09/metricas-kpi-seguridad-informatica-que-los-ciso-deben-controlar.html
Elaborado: MANAGEENGINE

KPI: Interacciones de los empleados

Con el aumento significativo de SaaS (software como servicio), servicios basados en la nube y BYOD (Trae tu propio dispositivo), las posibles entradas de problemas han aumentado. Tus redes y sistemas son vulnerables no solo a la seguridad de tus sistemas internos, sino también a conexiones y software de terceros que están fuera del control inmediato de tu compañía.

KPI: Tiempo medio de identificación (MTTI) / Tiempo medio de detección (MTTD)

El tiempo medio de identificación (MTTI), también conocido como tiempo medio de detección (MTTD), mide cuánto tiempo se requiere para detectar una violación de seguridad.

KPI: Tiempo medio de contención (MTTC) / Tiempo medio de resolución (MTTR)

El tiempo medio de contención monitorea la cantidad de tiempo que se requiere para contener una violación una vez que ha sido identificada. Este es el conteo de días entre que se identifica que existen problemas de seguridad y el momento en que se implementa la solución.

KPI: Costo por incidente

Los costos van más allá de los aspectos técnicos. Los ingresos perdidos, la reputación de la compañía, los avisos públicos, el tiempo de los empleados y los costos indirectos se acumulan rápidamente.

Gráfico N.14 Costo por incidente

Fuente: https://blog.kawak.net/mejorando_sistemas_de_gestion_iso/tipos-indicadores-gestion-ejemplos
Elaborado: KAWAK

KPI: Disponibilidad / Inactividad

Las disponibilidades de inactividad simplemente se refieren a la frecuencia con la que tu sitio o software funciona (disponibilidad) o no (inactividad).

KPI: Cumplimiento

En muchas industrias, existen normas de cumplimiento que deben seguirse. Generalmente estas son rankings de terceros que son otorgadas a las compañías después de una revisión. La puntuación de seguridad de cada industria puede ser diferente y representarse en una escala de 0-10 o calificación de A-F. (TuDashboard, 2020)

2.2.2. Modelos teóricos

2.2.2.1. ISO/IEC 27001

ISO/IEC 27001 es el estándar más conocido del mundo para **sistemas de gestión de seguridad de la información (SGSI)**. Define los requisitos que debe cumplir un SGSI.

La norma ISO/IEC 27001 proporciona a empresas de cualquier tamaño y de todos los sectores de actividad orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.

La conformidad con ISO/IEC 27001 significa que una organización o empresa ha implementado un sistema para gestionar los riesgos relacionados con la seguridad de los datos que posee o maneja la empresa, y que este sistema respeta todas las mejores prácticas y principios consagrados en esta Norma Internacional.

Gráfico N.15 ISO/IEC 27001

Fuente: https://www.tuvsud.com/en-in/country/bangladesh/solution-offerings/iso-27001-information-security-management-system
Elaborado: TUVSUD

2.2.2.1.1. Importancia ISO/IEC 27001

Con el aumento de los delitos cibernéticos y **la aparición constante de nuevas amenazas**, puede parecer difícil o incluso imposible gestionar los riesgos cibernéticos. ISO/IEC 27001 ayuda a las organizaciones a tomar conciencia de los riesgos e identificar y abordar debilidades de manera proactiva.

ISO/IEC 27001 promueve un enfoque holístico para la seguridad de la información: examinando personas, políticas y tecnología. Un sistema de gestión de seguridad de la información implementado según este estándar es una herramienta para la gestión de riesgos, la ciberresiliencia y la excelencia operativa**.** (ISO, 2022)

2.2.2.2. Reglamento general de protección de datos (RGPD)

El Reglamento es una medida esencial para fortalecer los derechos fundamentales de las personas en la era digital y facilitar la actividad económica, ya que aclara las normas aplicables a las empresas y los organismos públicos en el mercado único digital. Además, la existencia de una norma única pone fin a la fragmentación en distintos sistemas nacionales y a las cargas administrativas innecesarias. (Comision Europea, s.f.)

Gráfico N.16 Reglamento general de protección de datos (RGPD)

Fuente: https://www.mastermarketing-valencia.com/ventas-y-gestion-comercial/blog/reglamento-general-proteccion-datos/
Elaborado: mastermarketing-valencia

2.2.2.3. Modelo CIA

Las tres letras de la "tríada de la CID" significan confidencialidad, integridad y disponibilidad. La tríada de la CID es un modelo común que constituye la base para el desarrollo de sistemas de seguridad. Se utilizan para encontrar vulnerabilidades y métodos para crear soluciones.

La confidencialidad, integridad y disponibilidad de la información es crucial para la operación de un negocio, y la tríada CIA segmenta estas tres ideas en puntos focales separados. Esta diferenciación es útil porque ayuda a guiar a los equipos de seguridad a medida que identifican las diferentes formas en que pueden abordar cada inquietud.

Confidencialidad

La confidencialidad implica los esfuerzos de una organización por garantizar que los datos se mantengan en secreto o privados. Para lograrlo, el acceso a la información debe estar controlado para evitar que se compartan datos sin autorización, ya sea de manera intencional o accidental. Un componente clave para mantener la confidencialidad es asegurarse de que las personas sin la debida autorización no puedan acceder a los activos importantes para su negocio. Por el contrario, un sistema eficaz también garantiza que quienes necesitan tener acceso tengan los privilegios necesarios.

Integridad

La integridad implica asegurarse de que sus datos sean confiables y no hayan sido alterados. La integridad de sus datos se mantiene solo si estos son auténticos, precisos y confiables.

Disponibilidad

Incluso si los datos se mantienen confidenciales y se preserva su integridad, a menudo son inútiles a menos que estén disponibles para las personas de la organización y los clientes a los que sirven. Esto significa que los sistemas, las redes y las aplicaciones deben funcionar como deberían y cuando deberían. Además, las personas con acceso a información específica deben poder consumirla cuando lo necesiten, y acceder a los datos no debe llevar una cantidad excesiva de tiempo. (Fortinet, s.f.)

La importancia de la tríada de la CIA

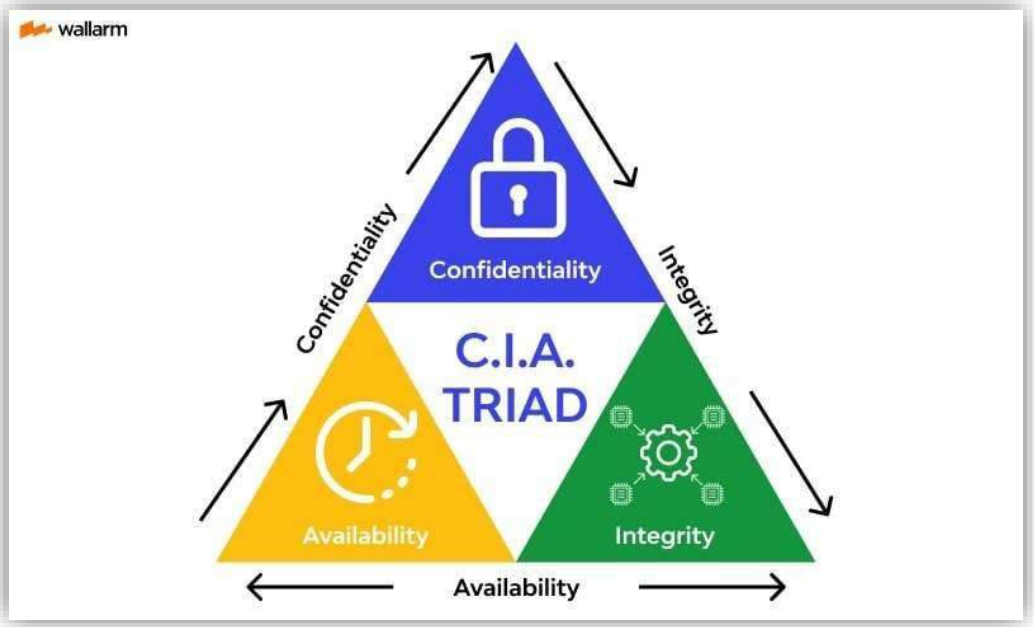
La tríada de la CIA es importante porque establece de manera clara y sencilla los objetivos principales de la seguridad de datos y la ciberseguridad. Si los sistemas de una organización garantizan la confidencialidad, integridad y disponibilidad, entonces las posibles

amenazas cibernéticas a esos sistemas son limitadas. Al hacer que sea fácil pensar y recordar estos objetivos clave, la tríada de la CIA ayuda en el diseño seguro y las revisiones de seguridad.

¿Por qué y cuándo debería usar la Tríada de la CIA?

La tríada de la CIA es una herramienta de uso general para un diseño seguro. Cada sistema debe tener confidencialidad e integridad de datos, y el software y los datos deben estar siempre disponibles para uso legítimo. Esto significa que la tríada de la CIA debe usarse siempre que tome o evalúe decisiones de ciberseguridad. También puede ser útil para realizar post-mortem después de incidentes de seguridad y capacitar a los empleados sobre políticas de seguridad de TI, mejores prácticas de seguridad y amenazas de seguridad comunes. (Software, s.f.)

Gráfico N.17 Modelo CIA



Fuente: https://medium.com/@kenusiva14/cia-triad-in-cyber-security-19e5b5e09913
Elaborado: MEDIUM

2.2.2.4.Modelo de Evaluación de Riesgos

Una evaluación de riesgos es un proceso sistemático utilizado para identificar amenazas potenciales y analizar qué podría suceder si un peligro ocurre. Implica evaluar los posibles resultados de los riesgos identificados, determinar su probabilidad e impacto, y diseñar medidas adecuadas para gestionarlos. Esencialmente, la evaluación de riesgos permite a las empresas priorizar y gestionar los riesgos de una manera proactiva y estratégica.

Cómo funciona una evaluación de riesgos

La evaluación de riesgos es un proceso continuo y multi-etapa que se desarrolla de la siguiente manera:

1. Identificación de riesgos

Se identifican posibles peligros que podrían afectar tu negocio o el producto que estás desarrollando. Estos pueden ser internos, como problemas de personal o fallos técnicos, o externos, como cambios en el mercado o restricciones regulatorias.

2. Análisis

Los riesgos identificados se examinan para comprender su impacto potencial y la probabilidad de su ocurrencia, ayudando a estimar la gravedad de cada riesgo.

3. Evaluación

Los riesgos analizados se ponderan contra los umbrales de tolerancia al riesgo establecidos para determinar el nivel de amenaza que representan.

4. Tratamiento de riesgos

Basándose en su evaluación, los riesgos se abordan con medidas apropiadas, que podrían ser reducción del riesgo, aceptación, evitación o incluso transferencia.

5. Monitorización y revisión

Los escenarios de riesgo cambian con el tiempo, y se necesita un seguimiento y revisión constantes de los riesgos para asegurarse de que las estrategias de gestión de riesgos siguen siendo efectivas.

2.2.2.4.1. Ventajas de realizar una evaluación de riesgos

Los beneficios de llevar a cabo una evaluación de riesgos, tanto en un contexto empresarial como de desarrollo de productos, son múltiples:

Mejora de la toma de decisiones

Con una comprensión más clara de los posibles obstáculos, puedes tomar decisiones estratégicas, lo que te ayuda a innovar sin miedo y dirigir eficazmente.

Optimización de recursos

La evaluación de riesgos te permite priorizar riesgos, lo que te permite asignar tus recursos de una manera más específica y eficiente.

Reducción de pérdidas

Al anticipar posibles problemas, puedes implementar medidas preventivas, reduciendo el potencial de pérdidas financieras y operativas.

Mejora del cumplimiento

Una evaluación de riesgos exhaustiva puede asegurar la adhesión a normas de la industria, leyes y regulaciones.

Aumento de la confianza de los interesados

Demostrar un enfoque proactivo para gestionar el riesgo puede reforzar la confianza de los interesados, lo cual es vital para atraer inversores, satisfacer a los clientes y retener talento. (Miro, s.f.)

Gráfico N.18 Modelo de evaluación de Riesgo

Fuente: https://safetyculture.com/es/temas/analisis-de-riesgos/
Elaborado: Safetyculture

Gráfico N.19 Tabla de Riesgo

Probabilidad		Muy probable	Probable	Improbable	Altamente improbable
Consecuencias	Fatalidad	Alto	Alto	Alto	Medio
	Lesiones importantes	Alto	Alto	Medio	Medio
	Lesiones leves	Alto	Medio	Medio	Bajo
	Lesiones insignificantes	Medio	Medio	Bajo	Bajo

Fuente: https://safetyculture.com/es/temas/analisis-cualitativo/
Elaborado: Safetyculture

2.2.2.5. Tendencias de ciberseguridad

Con respecto a un año de cambios y nuevas tendencias en el campo de ciberseguridad, las amenazas cibernéticas están en incremento y sofisticación, se han creado varios modelos de ciberseguridad como prioridad operativa para asegurar las entidades tanto públicas como

privadas. A continuación, se presenta un listado de modelos de ciberseguridad que están a la vanguardia.

Tabla N.1 Modelos de Ciberseguridad

Tendencias de Modelos de Ciberseguridad	
Inteligencia Artificial y Aprendizaje Automático	La IA y el aprendizaje automático están desempeñando un papel crucial en la detección y respuesta a amenazas cibernéticas. **Estos sistemas pueden analizar grandes volúmenes de datos en tiempo real para identificar patrones sospechosos y predecir posibles ataques**.
Seguridad Zero Trust	Este modelo se basa en el principio de "nunca confiar, siempre verificar". Cada acceso a la red debe ser autenticado y autorizado, independientemente de su origen.
Seguridad de IoT (Internet de las Cosas)	Con el aumento de dispositivos conectados, la seguridad de IoT se ha vuelto esencial. Esto incluye la implementación de medidas de seguridad robustas para proteger estos dispositivos y las redes a las que están conectados.
Ciberseguridad en la Nube	A medida que más empresas migran a la nube, la seguridad en este entorno se ha vuelto una prioridad. Esto incluye el uso de cifrado, autenticación multifactor y otras medidas para proteger los datos en la nube.
Ataques Multi-vector	Los atacantes están combinando múltiples técnicas y vectores de ataque en una sola campaña, lo que hace que los ataques sean más difíciles de detectar y contener.
Seguridad Móvil	Con el aumento del trabajo remoto, la seguridad de los dispositivos móviles se ha vuelto crítica. Esto incluye la protección contra malware móvil y la implementación de políticas de seguridad para dispositivos personales.
Blockchain y Ciberseguridad	La tecnología blockchain se está utilizando para mejorar la seguridad de las transacciones y la integridad de los datos.
IA y Machine Learning	La inteligencia artificial y el ML desempeñarán un papel fundamental en la batalla por la ciberseguridad. Sus capacidades avanzadas de análisis de datos ya se están utilizando para identificar y predecir amenazas, lo que mejora los sistemas de detección temprana y se puede responder mejor a nuevos peligros.
Computación cuántica	Sus capacidades van a mejorar los métodos de cifrado, desarrollar algoritmos más sofisticados para detectar ciber amenazas y gestionar de manera eficiente operaciones de datos a gran escala. Sin embargo, también va a suponer grandes retos debido a su capacidad para romper métodos de cifrado tradicionales, lo que podría dejar vulnerables a muchos sistemas de seguridad actuales.
Securización del trabajo en remoto	Los trabajadores en remoto pueden ser más vulnerables a los ciberataques, pues suelen tener redes y dispositivos menos protegidos. Por ello, las empresas deben invertir en formación del equipo.

Seguridad cloud con pentesting	Los test de penetración son ciberataques simulados que atacan al sistema informático de una compañía para comprobar si existen vulnerabilidades explotables. Esta ayuda a aumentar el cortafuego de aplicaciones (WAF), así como ajustar las políticas de seguridad y parchear las vulnerabilidades.
Firewall de malla híbrida	Los rojos corporativos se están volviendo cada vez más distribuidos y heterogéneos. Con una combinación de ubicaciones remotas, basadas en la nube y locales, puede resultar difícil implementar y administrar soluciones de firewall que brinden protección y cumplimiento de seguridad consistentes en todo el entorno de red de una organización. Sin embargo, ofrecer esta seguridad consistente también es fundamental para proteger a la organización contra ataques avanzados.
CNAPP	La aparición de entornos de nube ha tenido un impacto dramático en el desarrollo y la seguridad de las aplicaciones. Los entornos de nube permiten ciclos de desarrollo DevOps rápidos y pueden eliminar la necesidad de que los desarrolladores mantengan y protejan los entornos donde reside su aplicación. Además, el crecimiento de la nube ha fomentado el uso de contenedores para garantizar que la aplicación pueda moverse libremente entre entornos locales y diversos entornos de nube.
Gestión de la exposición a amenazas	La gestión de exposición a amenazas (TEM) es un enfoque centrado en el riesgo para la planificación estratégica de la seguridad. Los equipos de seguridad identifican las amenazas potenciales para la organización y evalúan el riesgo que cada una representa para la empresa. Con base en esta información, la organización puede desarrollar, priorizar e implementar estrategias de mitigación para diversos riesgos.

Fuente: https://www.checkpoint.com/es/cyber-hub/cyber-security/top-7-cyber-security-trends-in-2024/
Elaborado: Henry Rubén Arroyo Álvarez

2.2.3. Aplicaciones practicas

2.2.3.1. Seguridad para el usuario final

La seguridad para el usuario final, o seguridad de los endpoints, hace referencia a la protección de los dispositivos con los que trabajan los usuarios y los que los usuarios poseen. Debido a la gran cantidad de ciberataques que comienzan con un correo electrónico de suplantación de identidad (phishing), la seguridad para el usuario final es esencial.

Entre los tipos más frecuentes de protección para el usuario final se incluyen los siguientes:

- Actualización de dispositivos
- Uso de software antivirus actualizado
- Filtro de DNS para bloquear sitios web maliciosos

- Protección del firmware para evitar intrusiones en la capa de firmware
- Bloqueo de pantalla con contraseña
- Administración y detección de dispositivos remotas

Las organizaciones que no aplican la seguridad para el usuario final podrían ser víctimas de una filtración a través de un dispositivo desprotegido de un empleado que se infecte con malware y, a continuación, propague esa infección por toda la red de la empresa. (AO Kaspersky, 2024)

2.2.3.2. Otras recomendaciones para la empresa

Como decíamos al principio de este artículo, la ciberseguridad es cosa de todos: de empleados y de la empresa. Por eso, hemos reunido algunos consejos y servicios de ciberseguridad a tener en cuenta en el área IT de las organizaciones:

Formación y concienciación en ciberseguridad para empleados, pues estos son el mejor firewall humano y participan en todos los procesos del tratamiento de la información (recopilación, procesamiento, almacenamiento y recuperación).

Gestión segura de identidades, accesos y contraseñas con el fin de asegurar que la persona adecuada acceda al recurso necesario en el momento y el lugar idóneos.

Realización de auditorías de ciberseguridad para detectar amenazas y corregir vulnerabilidades, así como comprobar el grado de exposición a posibles riesgos y aplicar mejoras. (Cibernos Comunicación, s.f.)

2.2.3.3. Estrategias de ciberseguridad para proteger a tu empresa

Los riesgos a la ciberseguridad pueden surgir tanto desde adentro como desde fuera de la organización, por ello, las estrategias están enfocadas en el manejo de herramientas y la capacitación del personal de toda la empresa.

Profundizaremos en cada estrategia y en las acciones que puedes implementar para reducir riesgos.

Realizar una evaluación de riesgos de ciberseguridad

Las evaluaciones de riesgos de ciberseguridad se basan en los siguientes pasos:

- Identificación de activos
- Análisis de amenazas
- Evaluación de riesgos
- Recomendaciones

Capacitar en ciberseguridad al personal

Cuando ejecutas una adecuada capacitación puedes ayudar a las personas a:

- Identificar las amenazas de ciberseguridad y saber cómo responder a ellas.
- Usar las herramientas y los recursos de ciberseguridad de forma eficaz.
- Adoptar prácticas seguras en su trabajo y en su vida personal.

¿En qué debe centrarse la formación en ciberseguridad? Este es un ejemplo de temas que puedes tratar:

- Concientizar sobre las amenazas
- Prácticas de seguridad
- Reacción a incidentes

Crear políticas de seguridad

¿Qué políticas podrías implementar? Estos son algunos ejemplos:

- Requerir que las contraseñas sean seguras y se cambien con frecuencia.
- Tener prohibido abrir archivos adjuntos de remitentes desconocidos.
- Requerir que los datos confidenciales se encripten y se eliminen de forma segura.
- Definir los pasos a seguir en caso de un ataque de ciberseguridad.

Implementar controles de seguridad

Implementar controles de seguridad te ayudará a prevenir, detectar y responder a estos incidentes. Toma en cuenta que existen 3 tipos de controles que puedes implementar:

- Controles de prevención
- Controles de detección
- Controles de respuesta

Realizar encriptación de datos

Puedes utilizar la encriptación de datos en diferentes escenarios, como:

- Almacenamiento de datos
- Transmisión de datos
- Uso de dispositivos móviles

Diseñar un plan de respuesta a incidentes

El PRI debe incluir los siguientes elementos:

- Definición de incidentes
- Equipo de respuesta a incidentes
- Procedimientos de respuesta
- Comunicación

Usar la inteligencia artificial para detectar ataques más rápido

La inteligencia artificial (IA) no solo sirve para crear los ataques sino para detenerlos. Existen soluciones con esta tecnología que ayudan a identificar datos ocultos, anomalías en accesos y detectar amenazas más rápidamente. (Platzi, s.f.)

2.2.3.4. Una buena estrategia de ciberseguridad

Estas son algunas recomendaciones que debe incluir una buena estrategia de seguridad informática:

2.2.3.4.1. Gestión de activos

Uno de los aspectos más complicados pero suma importancia.

- Es necesario realizar un inventario completo y clasificado de las computadoras, celulares corporativos, tabletas, servidores, software, monitores, proyectores y más.
- Clasificar la información considerando las tres propiedades de la seguridad informática; confidencialidad, integridad y disponibilidad.
- Una vez clasificada se aplican las medidas para su protección.
- Gestionar los soportes, con esto se evita que se revele, modifique o elimine de forma no autorizada la información almacenada.
- Diseñar y mantener una base de datos de gestión de configuración que contenga los elementos para proporcionar un servicio y la relación entre ellos.

2.2.3.4.2. Seguridad de las operaciones

Todas las actividades encaminadas a asegurar el correcto funcionamiento de los equipos donde se procesa la información, deben considerar lo siguiente:

- Establecer y documentar los procedimientos y responsabilidades que se realizan en la organización.
- Garantizar la instalación de los sistemas y aplicaciones que se realizan conforme a los requisitos de seguridad de la organización.
- Monitorear y analizar la capacidad de los servidores y dispositivos.
- Gestionar y controlar los sistemas de antivirus de la empresa.
- Implantar un sistema de copias de seguridad.

2.2.3.4.3. Gestión de los incidentes y recuperación ante desastres

Es importante establecer un plan para estar preparados ante cualquier eventualidad. Se deben establecer responsabilidades y procedimientos.

- Definir la gestión de incidencias de seguridad.
- Establecer un plan de recuperación ante desastres.

Control de acceso a sistemas y aplicaciones

Como medida de prevención al acceso no autorizado a los sistemas y aplicaciones, se deben establecer políticas de control de acceso físico y lógico.

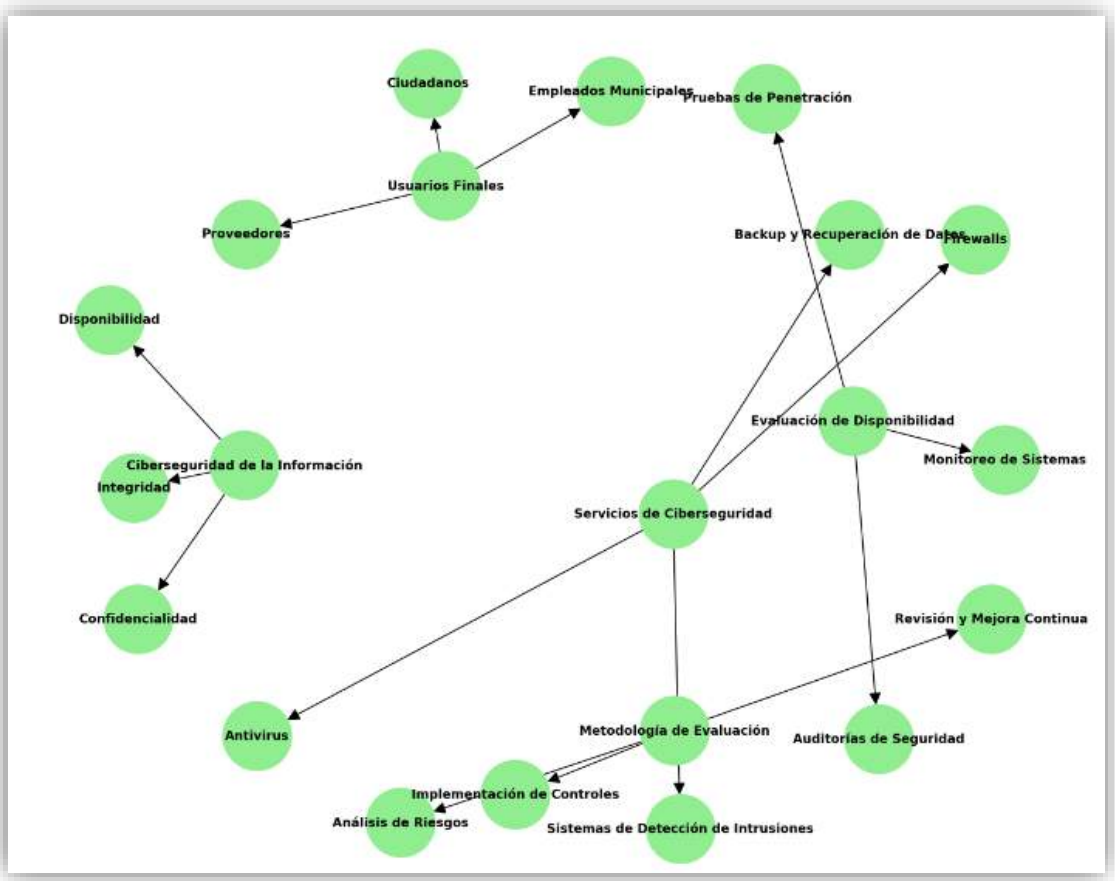
- Controlar el acceso a aplicaciones críticas y zonas restringidas
- Administrar los accesos lógicos, gestionar credenciales, permisos, atributos y medidas de autenticación.
- Gestionar usuarios y dividir funciones.
- Aplicación segura de las contraseñas. (infosecurity, s.f.)

3. CAPÍTULO III. METODOLOGÍA

En este capítulo se hace referencia a la metodología que se utilizó en este trabajo de investigación, con el motivo de recabar información esencial y dar respuesta a los objetivos planteados en la propuesta de maestría. Fue necesario utilizar los procedimientos de orden metodológico necesarios para ejecutar las normas de la investigación.

A continuación, veremos el Grafico N.20 donde se muestra gráficamente como se entrelazan todas las partes de la evaluación, tanto en sus partes de Disponibilidad, los servicios de ciberseguridad y como la metodología nos permitirá para resolver las incógnitas que se tienen en esta problemática.

Gráfico N.20 Diagrama Conceptual sobre la Metodología de Evaluación de la Disponibilidad de Servicios de Ciberseguridad



Fuente: Datos de Maestría
Elaborado: Henry Rubén Arroyo Álvarez

Según (Ortega, s.f.) nos dice: “La metodología de la investigación es el método que utilizarás para resolver un problema de investigación mediante la recopilación de datos utilizando diversas técnicas, proporcionando una interpretación de los datos recopilados y sacando conclusiones sobre los datos de la investigación. En esencia, la metodología de la investigación es el proyecto de una investigación o estudio”.

Con el objetivo de obtener los beneficios óptimos relacionados con la problemática planteada, la modalidad de investigación será combinada esto quiere decir que nuestra modalidad se utilizaran varios instrumentos de investigación, que lleven o encaminen a la obtención de información requerida para responder a las preguntas de los objetivos planteados. Para efecto de esta investigación se verificará el tipo y diseño de investigación, la población, muestra, validación de datos del tema tratado. Esto nos permitirá identificar los principales recursos, riesgos, vulnerabilidades y posibles soluciones que ayudarán a mitigar las falencias que posea dicha entidad pública.

La metodología de investigación para la evaluación de la disponibilidad de servicios de ciberseguridad en la M.I. Municipalidad de Guayaquil se estructuró en varias fases clave. A continuación, se detalla cada una de estas fases, describiendo los métodos y técnicas utilizados para recopilar y analizar la información.

3.1. Diseño de la investigación

Según (Jain, 2023) nos explica que: “Un diseño de investigación se define como el plan o estructura general que guía el proceso de realización de la investigación. Se trata de un componente esencial del proceso de investigación y sirve de modelo para determinar cómo se llevará a cabo un estudio, incluidos los métodos y técnicas que se utilizarán para recopilar y analizar los datos. Un estudio de investigación bien diseñado es esencial para garantizar que se cumplen los objetivos de la investigación y que los resultados son válidos y fiables”.

Tomando en cuenta que el objetivo principal de la M.I. Municipalidad de Guayaquil es la evaluación de la disponibilidad de servicios de ciberseguridad en usuarios finales, es importante realizar una exhaustiva investigación que permita recopilar información valiosa tanto teórica como empírica. Esta información debe proporcionar respuestas a las inquietudes

que se presenten a lo largo del proyecto y posibles soluciones a la problemática identificada. Por ello, se debe utilizar varias investigaciones las cuales poseen los instrumentos necesarios como entrevista, encuestas, recopilación de información de varias maneras, etc., que permita estudiar los objetivos de la problemática y, a partir de esas investigaciones, se puedan aportar soluciones técnicas y tecnológicas para mejorar la situación. En otras palabras, se efectuará un estudio donde las principales variables del objeto de estudio serán evaluadas tal como las proporcionan los elementos investigados.

Gráfico N.21 Diseño de Investigación

Fuente: https://ideascale.com/es/blogs/que-es-el-diseno-de-la-investigacion/
Elaborado: Henry Rubén Arroyo Álvarez

3.2. Tipo de investigación

En esta parte se describe los componentes metodológicos utilizados para alcanzar las respuestas de los objetivos de la investigación. Para esto, se utilizó un enfoque mixto que combino técnicas cuantitativas y cualitativas con un alcance bastante amplio al momento de recolectar la información optima que permita responder a las incógnitas planteadas.

> Las investigaciones mixtas se refieren a un enfoque de investigación que integra tanto métodos cuantitativos como cualitativos en un mismo estudio. En lugar de utilizar únicamente uno de estos enfoques, se combinan y se utilizan de manera complementaria para abordar preguntas de investigación más complejas y obtener una comprensión más completa del fenómeno estudiado.
>
> En las investigaciones mixtas, los métodos cuantitativos se centran en la recopilación y análisis de datos numéricos, empleando técnicas estadísticas y matemáticas para analizar patrones, establecer relaciones y generalizar resultados a una población más amplia.
>
> Por otro lado, los métodos cualitativos se enfocan en la recopilación y análisis de datos no numéricos, como entrevistas, observaciones y análisis de texto, con el objetivo de explorar significados, contextos y experiencias subjetivas. (Vilchez, 2024)

Por eso para este proyecto donde estamos utilizando el enfoque mixto, utilizaremos investigaciones como explorativa, descriptiva y de campo, de las cuales se utilizó instrumentos de cada una de ellas. A continuación, ampliaremos más de cada una de ellas.

3.2.1. Investigación Exploratoria

La investigación exploratoria no pretende dar explicaciones respecto del objeto de estudio, sino recopilar información, identificar antecedentes generales, ubicar aspectos

relevantes, como tendencias y relaciones potenciales entre variables que habrán de examinarse a profundidad en futuras investigaciones. (ULA, 2017)

En este caso, la fase exploratoria nos permitirá conocer más sobre la problemática y una posible solución, como se propone en el proyecto de maestría. Para esto, se utilizarán fuentes secundarias, ya que con esa información se podrá contrastar y buscar similitud con el tema en cuestión, relacionándolo con la disponibilidad de servicios de ciberseguridad en los usuarios finales, que es el tema central de esta propuesta. Es importante indicar que las fuentes tomadas en cuenta serán de sustento empírico-bibliográfico, como revistas y libros científicos, páginas web públicas y privadas, enciclopedias web, tesis y maestrías.

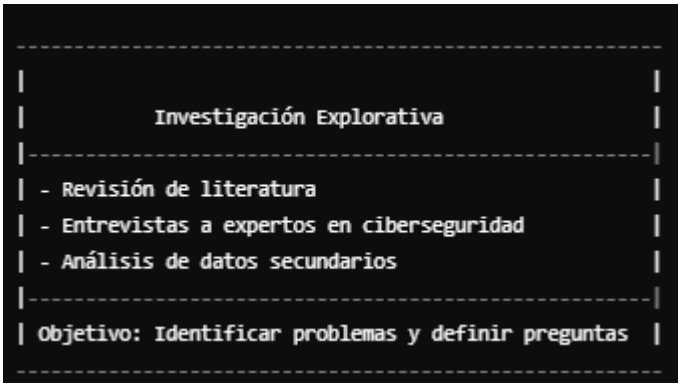
Por eso nos planteamos los siguientes puntos:

Objetivo: Identificar y definir problemas o preguntas de investigación.

Métodos: Revisión de literatura, entrevistas a expertos, análisis de datos secundarios.

Aplicación en el estudio: Explorar la percepción general y las necesidades de ciberseguridad de los usuarios finales.

Gráfico N.22 Investigación Explorativa



Fuente: https://ideascale.com/es/blogs/que-es-el-diseno-de-la-investigacion/
Elaborado: Henry Rubén Arroyo Álvarez

3.2.2. Investigación descriptiva

La investigación descriptiva ofrece a los investigadores una forma de presentar los fenómenos tal y como ocurren de forma natural. Enraizada en una naturaleza abierta y no

experimental, este tipo de investigación se centra en retratar los detalles de fenómenos o contextos específicos, ayudando a los lectores a obtener una comprensión más clara de los temas de interés. (Stewart, s.f.)

La fase descriptiva permitirá medir en puntos porcentuales cómo se encuentran actualmente las seguridades, además de detectar las necesidades actuales de la red en el ámbito de ciberseguridad. Asimismo, se identificarán los principales problemas que se presentan al utilizar los servicios o aplicativos. Lo mencionado anteriormente se realizará mediante encuestas y entrevistas, ambas utilizadas con el método de investigación empírica.

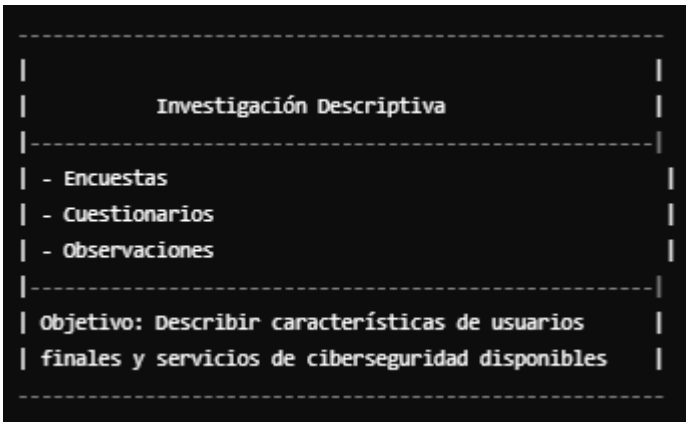
Por eso nos planteamos los siguientes puntos para la investigación descriptiva:

Objetivo: Describir las características de la población o fenómeno en estudio.

Métodos: Encuestas, cuestionarios, observaciones.

Aplicación en el estudio: Recoger datos específicos sobre la disponibilidad y uso de servicios de ciberseguridad entre los usuarios finales.

Gráfico N.23 Investigación Descriptiva



Fuente: https://ideascale.com/es/blogs/que-es-el-diseno-de-la-investigacion/
Elaborado: Henry Rubén Arroyo Álvarez

3.2.3. Investigación de campo

Investigación de campo, estudio de campo o trabajo de campo, es el proceso que permite obtener datos de la realidad y estudiarlos tal y como se presentan, sin manipular las

variables. Por esta razón, su característica esencial es que se lleva a cabo fuera del laboratorio, en el lugar de ocurrencia del fenómeno. (Rhoton, 2023)

La fase de campo permite recabar información real y relevante con respecto al problema. Utilizando la investigación de campo, se podrán realizar visitas técnicas a las diferentes áreas donde interactúan los usuarios finales de la red de la M.I. Municipalidad de Guayaquil para verificar qué tipo de seguridades poseen tanto en hardware como en software.

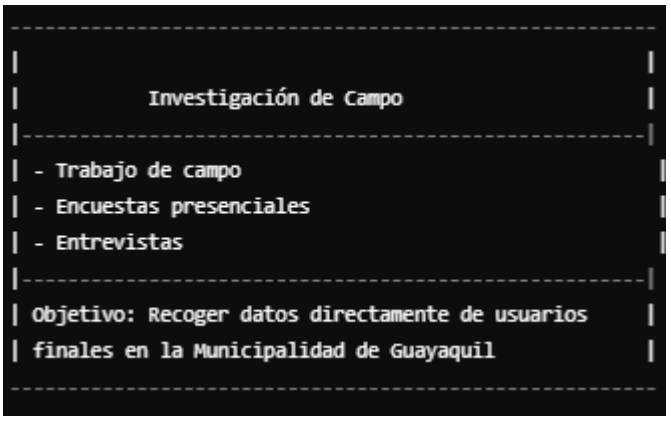
Para eso seguiremos los siguientes pasos:

Objetivo: Recoger datos directamente de la realidad.

Métodos: Trabajo de campo, encuestas presenciales, entrevistas.

Aplicación en el estudio: Recoger datos directamente de los usuarios finales en la Municipalidad de Guayaquil.

Gráfico N.24 Investigación de Campo



Fuente: https://ideascale.com/es/blogs/que-es-el-diseno-de-la-investigacion/
Elaborado: Henry Rubén Arroyo Álvarez

3.3.Métodos, técnicas e instrumentos para la recolección de datos

Para realizar la evaluación de servicios de ciberseguridad de la Información en usuarios finales en M.I. Municipalidad de Guayaquil, se utilizaron una combinación de métodos, técnicas e instrumentos de recolección de datos.

3.3.1. Métodos de recolección de datos

3.3.1.1. Métodos cualitativos

Entrevista: Permitió obtener información detallada sobre las experiencias y conocimientos al respecto de los servicios de ciberseguridad.

Observación: Revisión el entorno de los usuarios para observar la interactuación con los servicios de ciberseguridad

3.3.1.2. Modo cuantitativo

Encuesta: se utilizó esta herramienta popular para la recolección de datos para diseñar una encuesta para medir satisfacción y percepción de los usuarios sobre los servicios de ciberseguridad.

Análisis de registros: se utilizó para revisión y análisis de datos existentes, como registros de incidentes de seguridad, para identificar tendencias y patrones, como indicadores de gestión y matriz de riesgo.

3.3.2. Técnicas de Recolección de Datos

3.3.2.1. Técnicas Cualitativas:

Entrevistas: Se realizó un cuestionario de preguntas abiertas y cerradas para obtener información detallada y especifica de que tanto saben sobre ciberseguridad.

3.3.2.2. Técnicas Cuantitativas:

Cuestionarios: Se realizó un cuestionario con preguntas cerradas que permitieron obtener datos cuantificables y fáciles de analizar.

Experimentos controlados: Se realizaron pruebas específicas (Ethical Hacking) para evaluar la efectividad de diferentes medidas de ciberseguridad.

3.3.3. Instrumentos de Recolección de Datos

Software de encuestas en línea: Para la recolección de información se utilizó la herramienta Google Forms para crear y distribuir encuestas.

Software de pruebas: Para las pruebas de hacking se utilizó la herramienta KALI LINUX para la realizar el laboratorio de Seguridades.

La implementación de la investigación mixta, utilizando estos métodos, técnicas e instrumentos de recolección de datos, se permitió obtener una visión completa y detallada de la disponibilidad de los servicios de ciberseguridad en la M.I. Municipalidad de Guayaquil.

3.4. Población y muestra

La población considerada será los empleados del departamento de TI y usuarios finales que prestan servicio a los departamentos internos de la información de la M.I. Municipalidad de Guayaquil, ya que ellos son los encargados de manipular la información final en sus distintos puestos.

La evaluación se realizó con dos unidades de estudio, el primero como unidad principal, que fueron las personas encargadas del departamento de TI de la M.I. Municipalidad de Guayaquil, a las cuales se le realizo una entrevista de cómo esta configurados y que herramientas posee la entidad para contrarrestar el Cyber ataque y por otro lado se le realizo un cuestionario al personal (usuarios finales) para conocer su conocimientos o nociones de que es ciberseguridad y si hay alguna implementación en sus unidades de trabajo.

4. CAPÍTULO IV. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL AL EVALUAR LA DISPONIBILIDAD DE SERVICIOS DE CIBERSEGURIDAD DE LA M.I. MUNICIPALIDAD DE GUAYAQUIL

En este capítulo se realizó un análisis detallado de la disponibilidad de servicios de seguridades en la M.I. Municipalidad de Guayaquil. El objetivo primordial es diagnosticar las seguridades de la red e identificar los posibles problemas que pueden tener a la hora de ser hackeados o que personas ajenas a la entidad pública ingresen sin autorización a la red.

Además, los resultados de la encuesta realizada a los profesionales del departamento de TI y a los usuarios finales nos aportara algunos o muchos indicios de cómo se encuentra la entidad con respecto a la ciberseguridad.

4.1. Resultados de la encuesta aplicada

Las encuestas realizadas a los empleados de la M. I. Municipalidad de Guayaquil, se preguntó a 50 empleados en el tema de estudio, entre los que se encontraba expertos en redes, profesionales en sistemas, ingenieros eléctricos y usuarios finales. El propósito de este cuestionario fue evaluar que tanto saben de ciberseguridad y sus normas o policías, para así evaluar que tan disponible se encuentra los servicios de ciberseguridad si se presenta alguna vulneración en la red y sistemas de la entidad pública.

P1. **¿Cuál es su edad?**

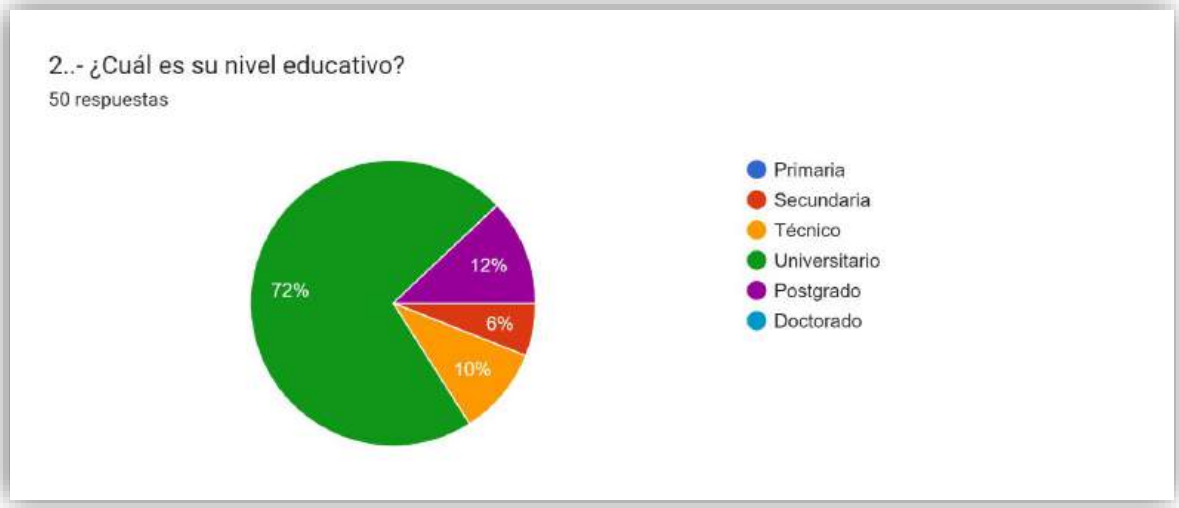
Gráfico N.25 Edad de los Encuestados

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

El 46% de los encuestados oscilan en edad de 46 a 60 años, el 32% están entre los 18 a 30 años, el 16% están entre los 31 a 45 años y el 6% más de 60 años, los que quiere decir que la mayoría de personal promedian en una edad mayor.

P2. ¿Cuál es su nivel educativo?

Gráfico N.26 Nivel Educativo

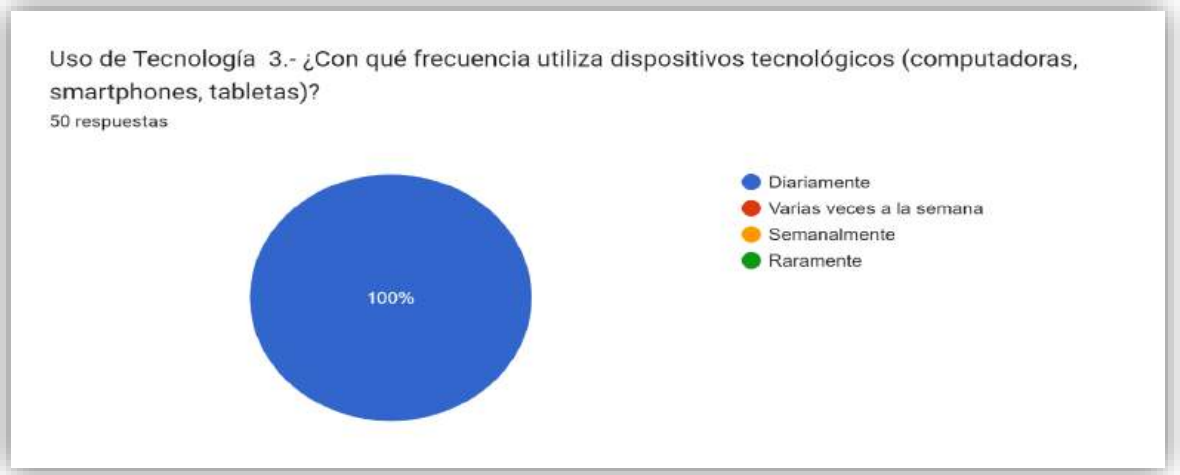


Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Los resultados obtenidos, exponen el 72% de los encuestados son titulados (Universidad), el 12% posee un postgrado, el 10% son técnicos y el 6% solo estudio la secundaria.

P3. ¿Con qué frecuencia utiliza dispositivos tecnológicos (computadoras, smartphones, tabletas)?

Gráfico N.27 Frecuencia de utilización de Dispositivos Tecnológicos

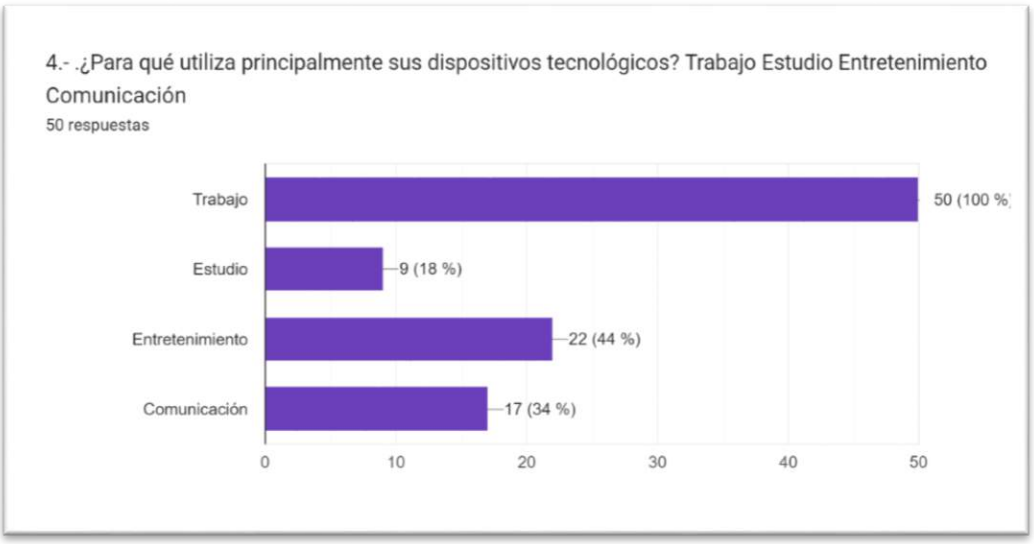


Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Con respecto a la utilización de dispositivos, el 100% de los encuestados respondieron que utilizan dispositivos tecnológicos diariamente.

P4. ¿Para qué utiliza principalmente sus dispositivos tecnológicos?

Gráfico N.28 Utilización de Dispositivos Tecnológicos

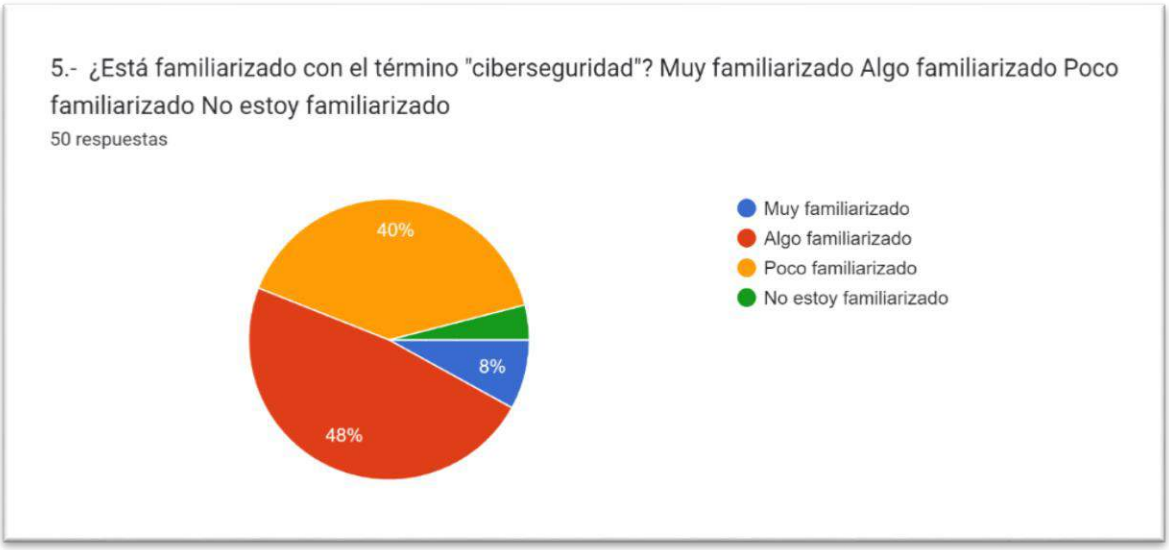


Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Con respecto a la pregunta en que utilizan los dispositivos tecnológicos, el 44% la utiliza para trabajar y entretenimiento, el 34% para trabajar y comunicación y el 9% para trabajar y estudiar, pero todos concordaron que las utilizan para trabajar.

P5. ¿Está familiarizado con el término "ciberseguridad"

Gráfico N.29 Conocimiento de Ciberseguridad



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Con respecto a la pregunta, el 48% de los encuestados respondieron en algo conocer, el 40% están poco familiarizado, el 8% están muy familiarizado y el 4% no están familiarizado con lo que es ciberseguridad.

P6. ¿Ha recibido alguna vez formación en ciberseguridad?

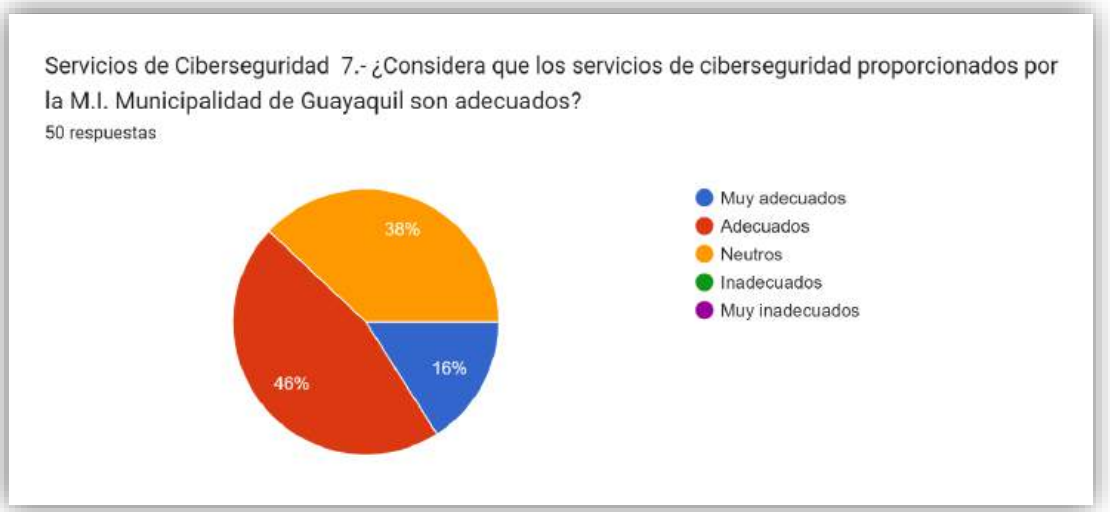
Gráfico N.30 Formación en Ciberseguridad

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Respecto a la pregunta, un 70% de los encuestados responden que no tienen formación en ciberseguridad, pero están interesados en conocer del tema, un 22% respondieron conocer, pero informalmente (autodidacta), el 6% si conocen del tema por talleres y certificaciones, y el 2% no está interesado en el tema.

P7. **¿Considera que los servicios de ciberseguridad proporcionados por la M.I. Municipalidad de Guayaquil son adecuados?**

Gráfico N.31 Servicios de Ciberseguridad Adecuados



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

La respuesta a la pregunta, el 46% consideran que son los adecuados, el 38% son neutros a la pregunta y el 16% respondieron que los servicios de ciberseguridad son muy adecuados.

P8. **¿Qué servicios de ciberseguridad considera más importantes que sean implementados o mejorados por la M.I. Municipalidad de Guayaquil?**

Gráfico N.32 Mejoras en Servicios de Ciberseguridad

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

La respuesta a la pregunta, el 50% responde nunca haber tenido algún incidente de seguridad informática, el 32% no está seguro si habrá tenido algún incidente, el 12% responde que, si ha tenido, pero hace más de un año y el 6% que si pero en el último año.

P10. Si respondió "Sí" a la pregunta anterior, ¿reportó el incidente a la M.I. Municipalidad de Guayaquil?

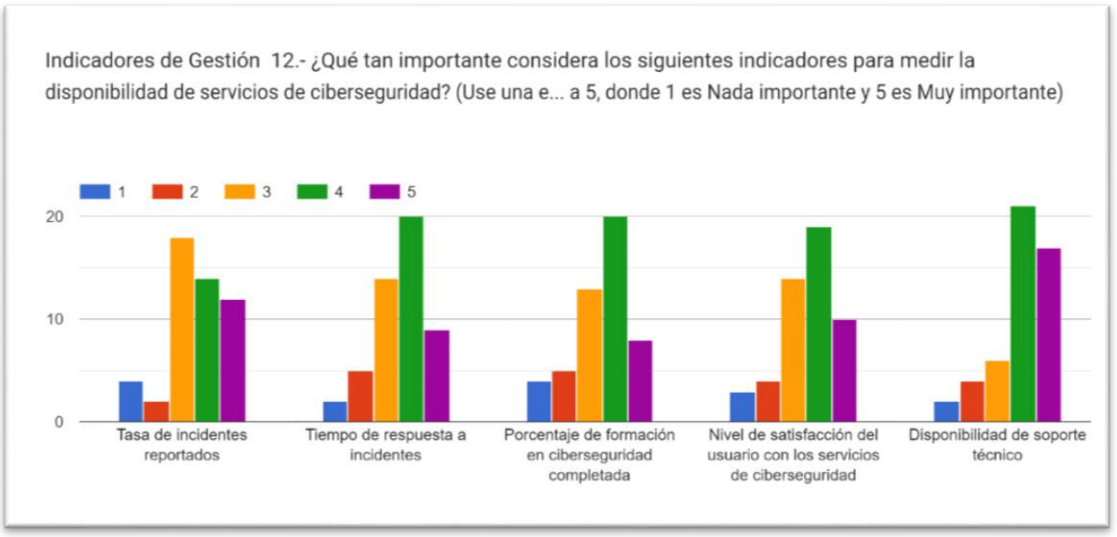
Gráfico N.33 Reporte de Incidencias en Servicios de Ciberseguridad

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Con respecto a la pregunta, el 48% de los encuestados están satisfecho con respecto a la respuesta que da la M.I. Municipalidad de Guayaquil ante los incidentes sobre ciberseguridad, el 38% en neutra ante la pregunta y el 14% responde estar muy satisfecha ante la respuesta.

P12. ¿Qué tan importante considera los siguientes indicadores para medir la disponibilidad de servicios de ciberseguridad?

Gráfico N.34 Indicadores de Gestión

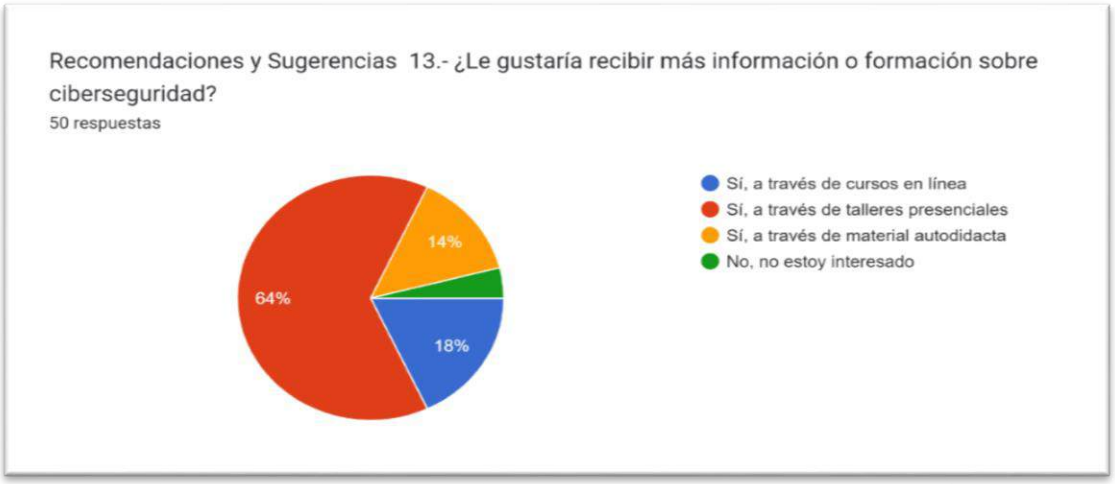


Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Con respecto a la pregunta de indicador de gestión con respecto a medir la disponibilidad de servicio de ciberseguridad notamos que: en el primer ítem es respondieron que es muy importante, en el segundo ítem también es muy importante, en el tercer ítem también es muy importante, en el cuarto ítem es muy importante y el quinto también es muy importante.

P13. ¿Le gustaría recibir más información o formación sobre ciberseguridad?

Gráfico N.35 Recomendaciones y Sugerencias



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Con respecto a la pregunta, el 64% de los encuestados si desea recibir información a través de talleres presenciales, el 18% si desea pero por medio de cursos en línea, el 14% a través de material autodidáctico y el 4% no le interesa nada sobre el tema.

P14. ¿Qué tan dispuesto estaría a participar en programas de formación en ciberseguridad ofrecidos por la M.I. Municipalidad de Guayaquil?

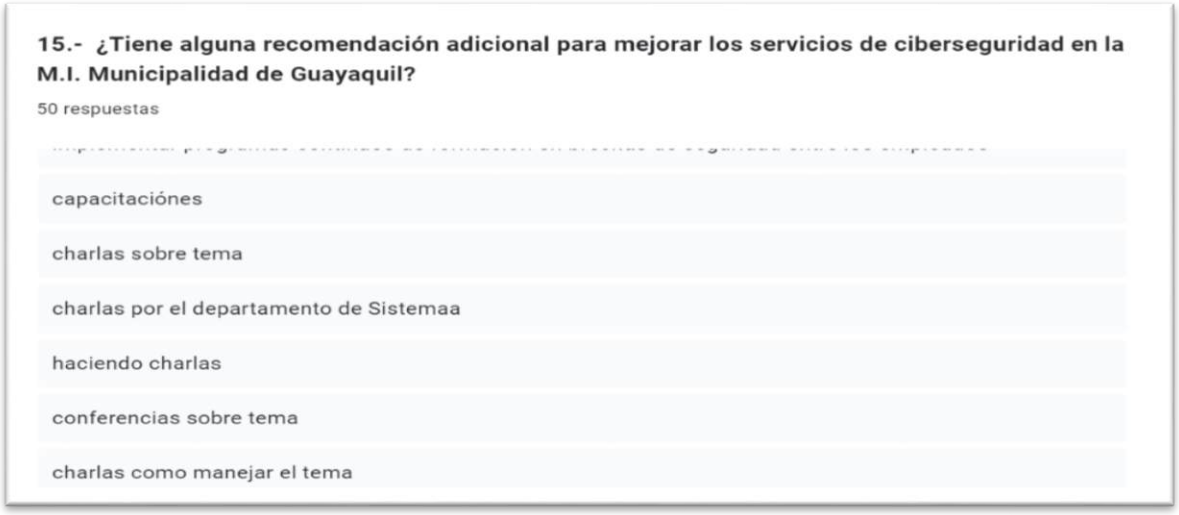
Gráfico N.36 Disponibilidad de Formación en Ciberseguridad

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Con respecto a la pregunta, el 52% están dispuesto a participar en programas de formación, el 24% están muy dispuesto a participar, el 22% están indecisos a la propuesta y el 2% están poco dispuesto a participar en programas de formación de ciber seguridad.

P15. **¿Tiene alguna recomendación adicional para mejorar los servicios de ciberseguridad en la M.I. Municipalidad de Guayaquil?**

Gráfico N.37 Recomendaciones Adicionales



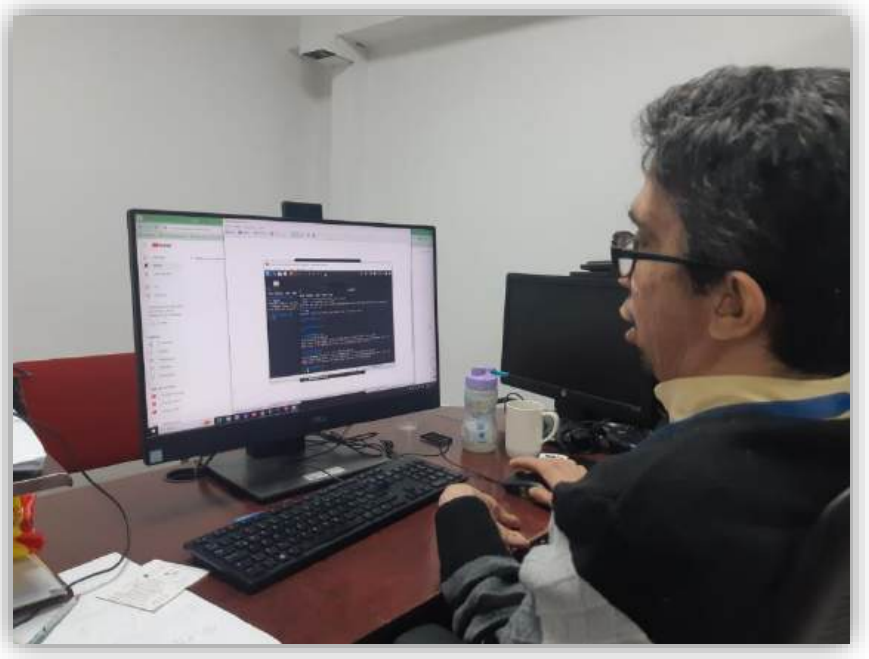
Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Con respecto a la pregunta, las respuestas fueron muy variadas pero lo que sí están muy interesados sobre el tema de ciberseguridad ya que la mayoría desean charlas, cursos, talleres y además que actualicen las herramientas de ciberseguridad.

4.2. Resultados al evaluar la disponibilidad de servicios de ciberseguridad de la M.I. Municipalidad de Guayaquil

Lo primordial fue comprobar y evaluar el estado actual de la información, para esto se realizó una visita al departamento de TI y bajo la supervisión del delegado que encomendó la entidad pública, se realizó un chequeo de que seguridades poseían.

Gráfico N.38 Visita de Campo al Departamento de TI



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

En primera instancia se revisó la infraestructura del departamento de TI, en el cual poseía un Data Center que poseía elementos actuales como por ejemplo en el caso del hardware poseían Servidores, Rack, Switch, Modem, computadoras, laptops y Firewall de última generación, en el caso del software poseen Sistema Operativo, aplicaciones, programas y seguridades actualizados que permitían un buen desempeño en las labores que desarrolla la entidad pública.

Gráfico N.39 Infraestructura del Departamento de TI

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

También se revisó la infraestructura de seguridad informática actual, en la cual se revisó que poseían firewall, sistemas o aplicativos de detección y prevención de intrusos, antivirus y antimalware los cuales estaban debidamente configurados y actualizados.

Gráfico N.38 infraestructura de seguridad informática

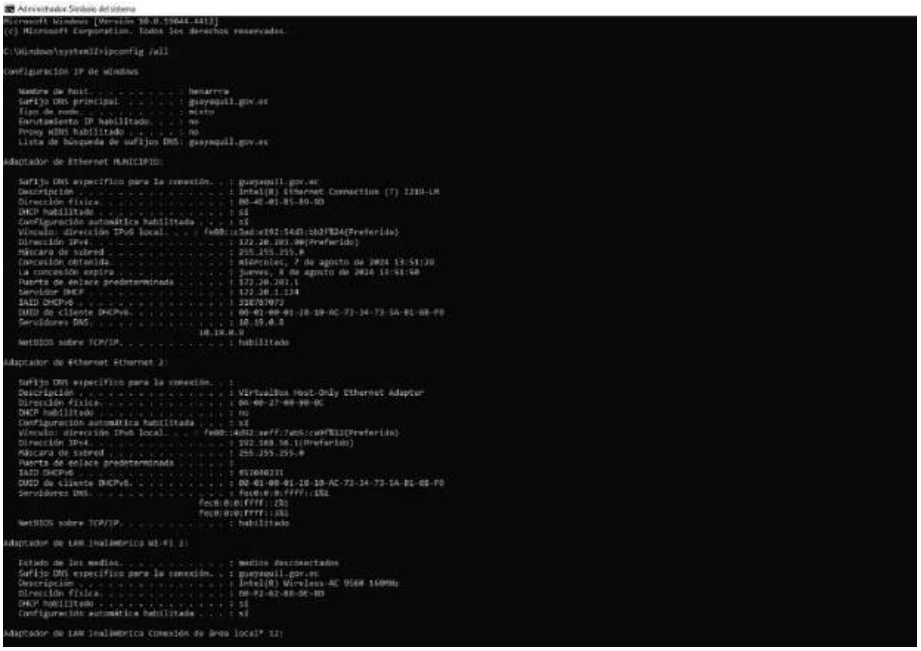
Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Para el caso de los administradores del TI y empleados en el área de usuarios finales, se comprobó que poseían políticas básicas en el caso de uso de información y ciberseguridad, pero solo el área administrativa tenía conocimiento de que conlleva tener seguridades y lo que implica cuidar su información para no ser vulnerado por hacker o personas ajenas.

Puesto que realizado la encuesta se pudo comprobar que efectivamente la mayoría de los usuarios finales no tenían conocimiento de la existencia de políticas y seguridades informáticas que aportarían una seguridad a la información que maneja la M. I. Municipalidad de Guayaquil.

Con esto se verifico en qué estado se encontraba las seguridades informáticas, las cuales nos serviría para posterior realizar el laboratorio informático de ciber seguridad, ya que con los datos recolectados de la visita seria el punto de partida para hacer los ataques a la red y sistema, con el fin de comprobar hasta qué punto nos permiten ingresar a su sistema y red. Además, se recolectas información proporcionada por la Municipalidad de Guayaquil, para realizar los indicadores de gestión y así dar respuesta a como se encuentra las seguridades a la hora de suceder algún percance o ataque a la infraestructura y sus sistemas.

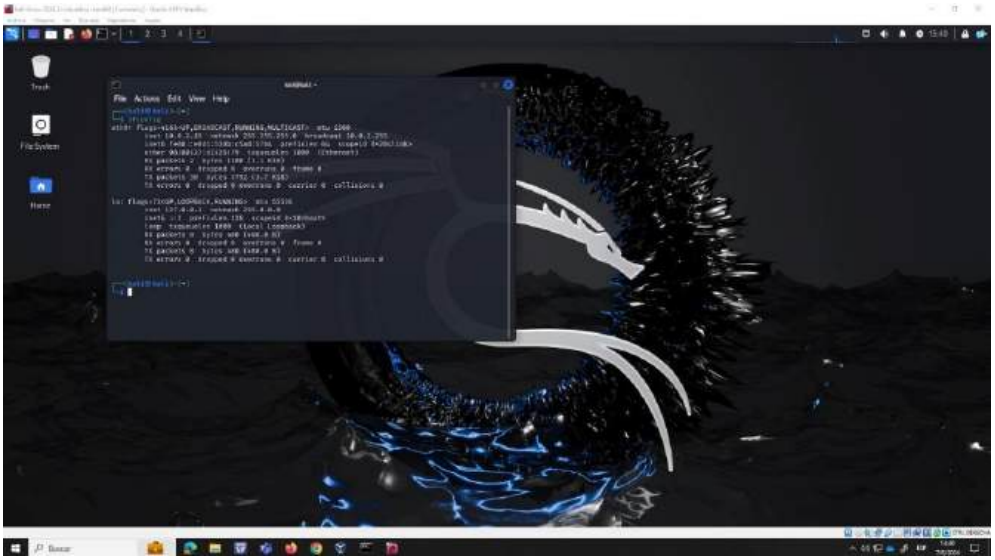
Gráfico N.39 Configuración de IP y Sistema Operativo



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Para evaluar la disponibilidad de los servicios de ciberseguridad de la entidad pública, implementamos una herramienta como es KALI LINUX que nos ayudara a realizar un ETHICAL HACKING para poder verificar si existen anomalías o falencias que nos permitirá hacer las respectivas sugerencias y recomendaciones.

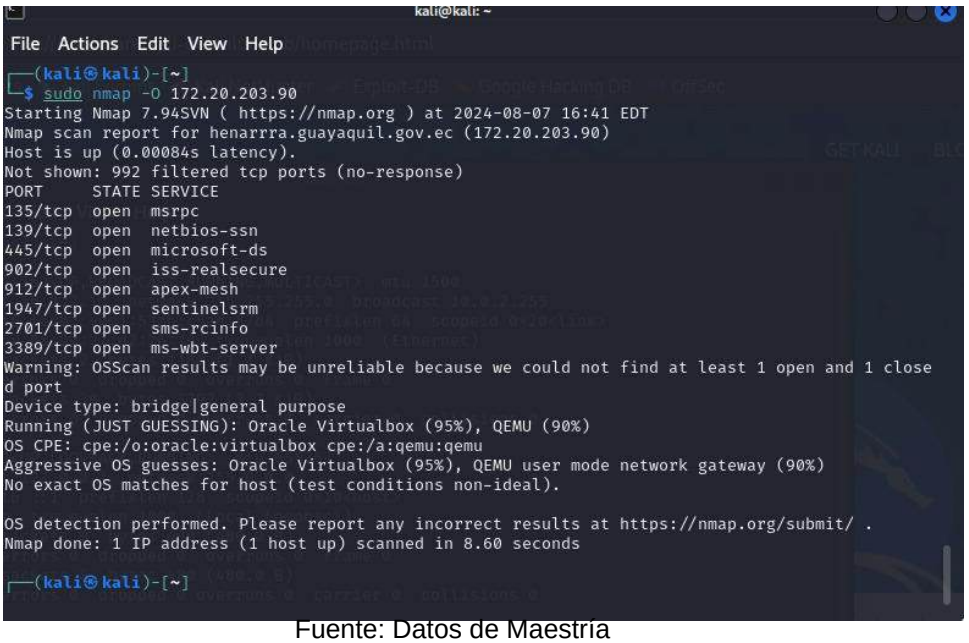
Gráfico N.40 KALI LINUX



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

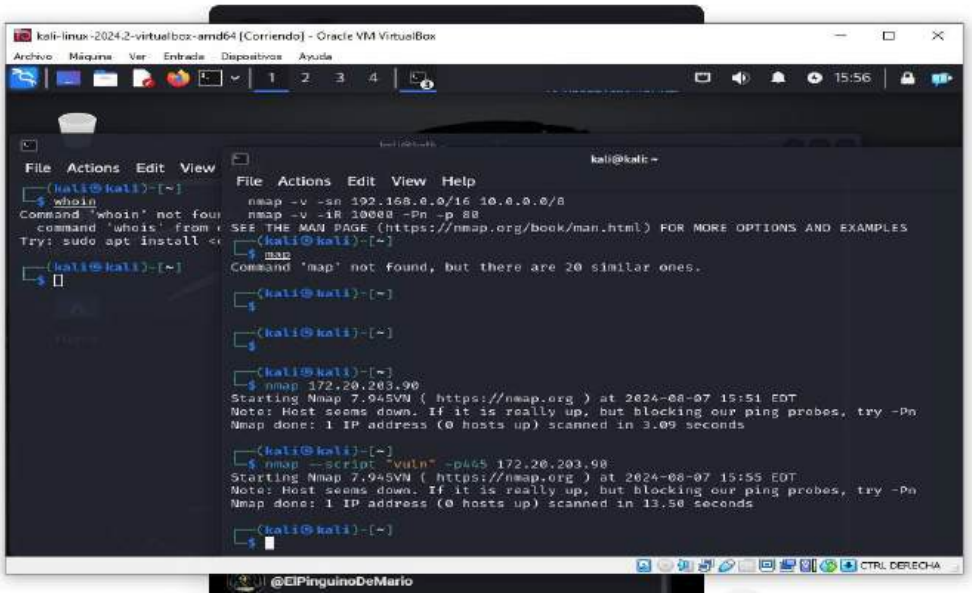
Para empezar el laboratorio de seguridades con ETHICAL HACKING utilizamos herramientas de verificación de puertos como es NMAP, el cual nos permitió revisar cuales puertos se encuentran abiertos, cerrado o en stand y, esta herramienta nos permitió verificar que sistema operativo utiliza la M.I. Municipalidad de Guayaquil.

Gráfico N.41 Utilización de NMAP



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Gráfico N.42 Escaneo de SO y Vulnerabilidades con NMAP

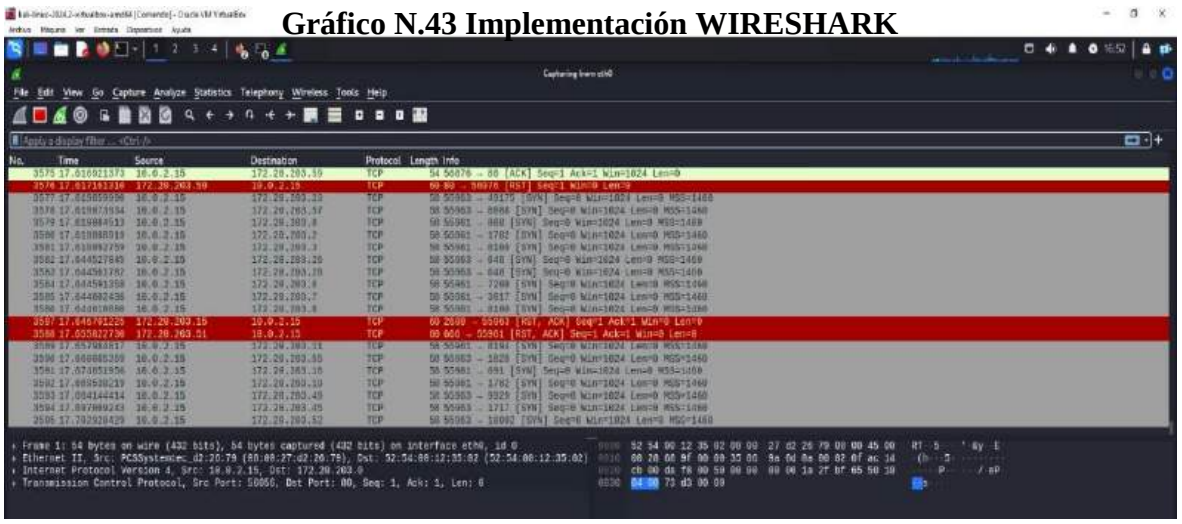


Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

En este caso como vemos en la Grafica N.22 y 23, el escaneo tanto de puertos y de datos de la red y sistema, dio como resultado que las seguridades solo permita el inicio del escaneo puesto que al continuar las seguridades que posee la red, nos denegaba el ingreso a las opciones de las cuales se quería verificar.

Otra herramienta utilizada fue WIRESHARK, la que sirve para analizar el tráfico de paquetes de toda la red, en un principio se reflejaba la captura de toda la información que pasa a través de la conexión.

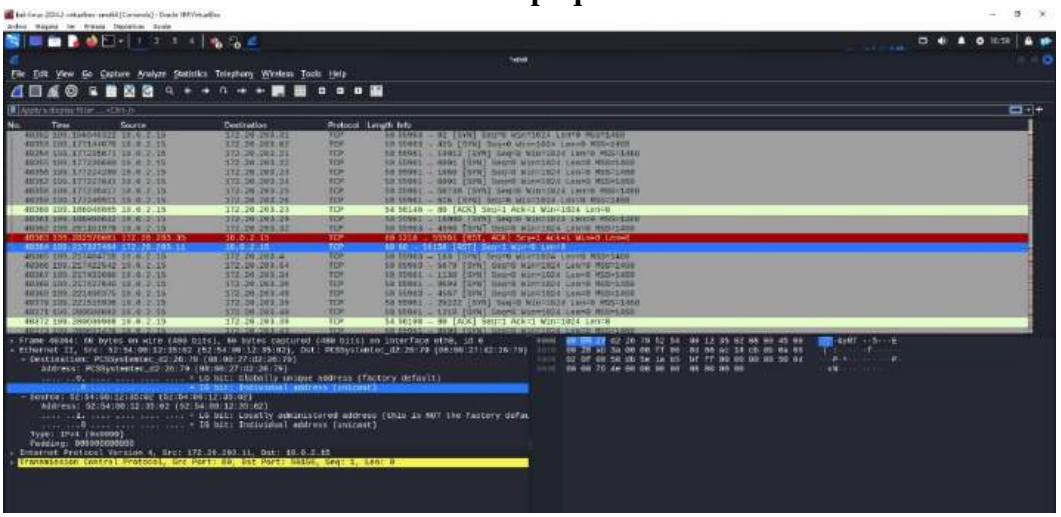
Gráfico N.43 Implementación WIRESHARK



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Como se puede apreciar en la Grafica N.43, el tráfico se nota fluido, pero se ve que al enviar paquetes desde el computador emisor del cual se realiza con el computador receptor la trama de información llega, pero al devolverlo no se realizaba, en este caso no había comunicación (franjas en rojo). Esto demostró que las seguridades no permitían la comunicación y el traspaso de información entre el usuario (hacker) que deseaba irrumpir al sistema y red de la entidad pública y la máquina que estaba siendo atacada. No obstante tiende a que esa comunicación pueda ser intersecada por un ataque de ataque Man in té Middle (MitM) que recolectaría alguna información que le sería beneficiosa para sus ataques posterior.

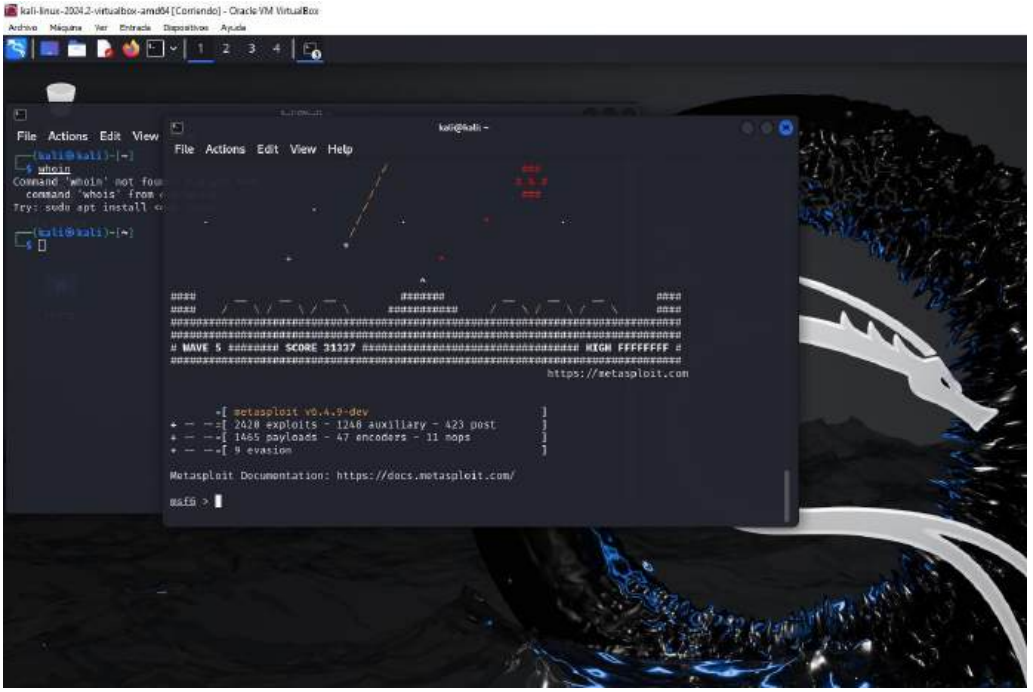
Gráfico N.44 Trafico de paquetes con WIRESHARK



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

También se utilizó la herramienta METASPLOIT para realizar pruebas de penetración, el cual se realizó ataques a la red y al sistema, donde se puede ver que al inicio de la herramienta se pudo empezar con el ataque.

Gráfico N.45 Utilización de METASPLOIT

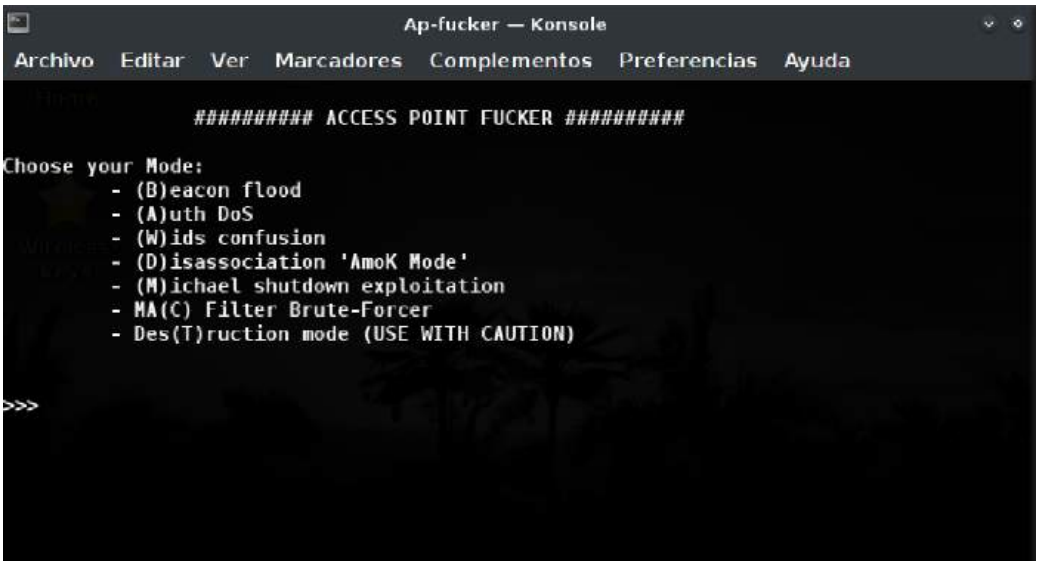


Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Para esta prueba con METASPLOIT, se verifico con las otras herramientas si se encontraba alguna vulneración con respecto a puertos abiertos o alguna caída de sus seguridades, en tal caso se realizó la respectiva prueba de penetración a sus seguridades, a las cuales en primera instancia se inició la vulneración pero al instante nos impidieron, puestos que se levantaron las seguridades y se restringió el acceso a la red como al sistema.

Además se realizaron pruebas de penetración a contraseñas, denegaciones de servicios, explotación de diccionario, fuerza bruta, cifrado WPA Y WPA2, etc. las cuales dieron que las contraseñas son robustas y cifradas para lo cual es muy complejo el poder obtener las claves. Para este proceso se utilizaron herramientas como: AP-FUTCHER, AIRGEDDON, JOHN THE RIPPER.

Gráfico N.46 Utilización de AP-FUCKER

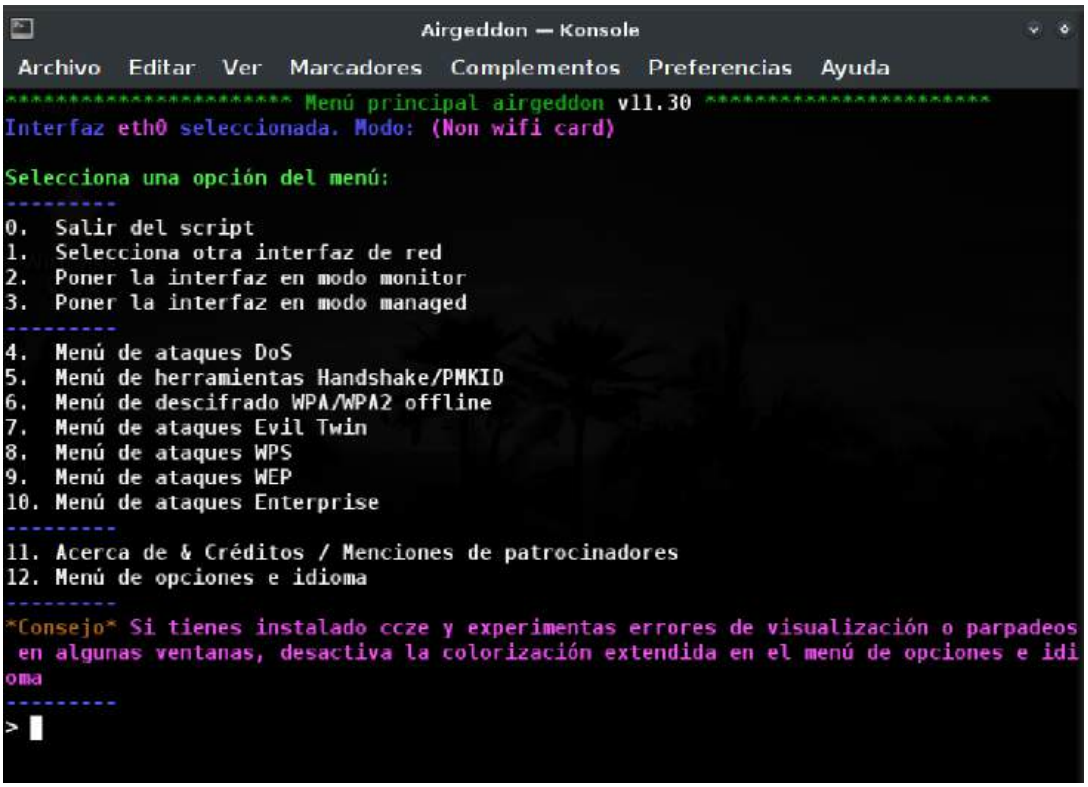


Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Gráfico N.47 AIRGEDDON

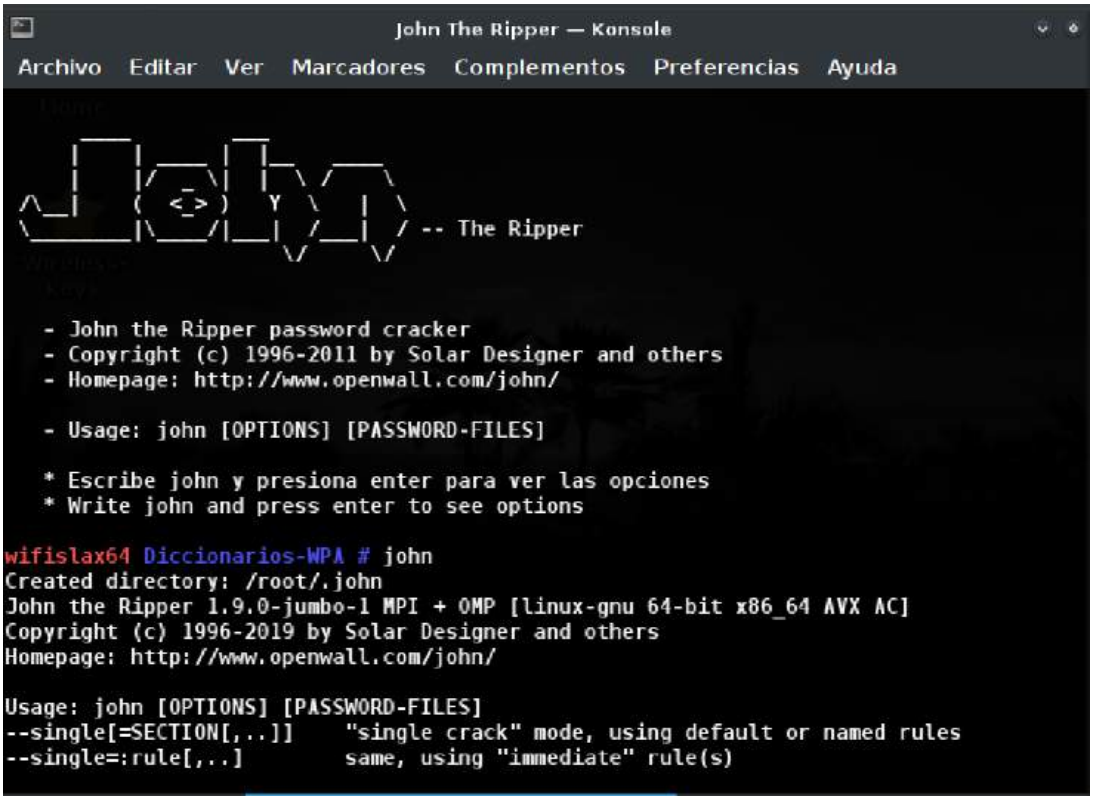
Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Gráfico N.48 Utilización de METASPLOIT



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Gráfico N.49 Utilización de JOHN THE RIPPER



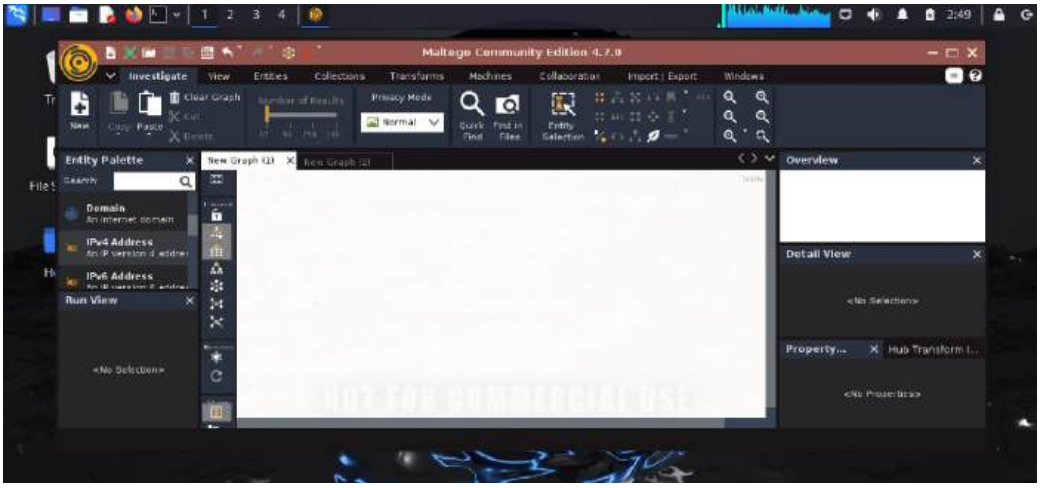
Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Otra opción que se uso fue realizar una Ingeniería Social, en la cual utilizamos herramientas como MALTEGO, WIFIPISHING. Esto con la finalidad de ver el comportamiento de los usuarios finales al momento de realizar una conversación y delimitar que tanto saben de las políticas que poseen para dar información para posterior realizar alguna incursión con estas herramientas antes mencionadas.

Gráfico N.50 Utilización de WIFIPISHER

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Gráfico N.51 Utilización de MALTEGO



Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

En este caso se realizaron duplicación de redes, phishing, robo de contraseñas, email maliciosos, mensajes de WhatsApp y otros ataque que como se esperaba la gran mayoría por falta de información o capacitación desconocían que protocolos o mecanismos se debían seguir para no caer en las trampas que los hacker usaban, logrando recabar información como direccionamientos ip, contraseñas privadas y empresariales, virus ingresados a la red, etc. a la hora de navegar, activar alguna ventana de la web o recibir algún correo sea al teléfono o computador, que utilicen no verifican la procedencia de dichos email, poniendo en riesgo seguridad informática de la entidad pública.

4.3. Indicadores de Gestión para Medir la Disponibilidad de Servicios de Ciberseguridad en la M.I. Municipalidad de Guayaquil

Para medir la disponibilidad de los servicios de ciberseguridad, es primordial realizar indicadores de gestión claros y efectivos. Estos indicadores serán de gran ayuda para evaluar el rendimiento, detectar vulnerabilidades y garantizar que los servicios de ciberseguridad se mantengan operativos y eficaces.

Para realizar los cálculos de los Indicadores de Gestión se tomaron datos proporcionados por el encargado del departamento de TI.

Disponibilidad del Servicio de Seguridad (Uptime)

Para este servicio los datos dados son:

Se estuvo operativo 720 horas en un mes de 730 horas

$$Disponibilidad\ de\ Servicios = \frac{\text{Tiempo Total Operativo}}{\text{Tiempo Total Programado}} X\ 100 =$$

$$Disponibilidad\ de\ Servicios = \frac{720}{730} X\ 100 = 98{,}6\%$$

Objetivo: Mantener una disponibilidad del servicio de al menos el 99.9%.

Tiempo Medio de Respuesta a Incidentes (MTTR - Mean Time to Respond)

Para este servicio los datos dados son:

Se respondieron 10 incidentes en un total de 250 minutos, el MTTR es:

$$\text{MTTR (Respuesta)} = \frac{\text{Tiempo Total de Respuesta}}{\text{Numero Total de Incidentes}} =$$

$$\text{MTTR (Respuesta)} = \frac{250}{10} X\ 100 = 25\ minutos$$

Objetivo: Reducir el MTTR a menos de 30 minutos.

Tiempo Medio de Resolución (MTTR - Mean Time to Repair)

Se resolvieron 5 incidentes en un total de 10 horas, el MTTR es:

$$\text{MTTR (Resolucion)} = \frac{\text{Tiempo Total de Resolucion}}{\text{Total de Incidentes}} =$$

$$\text{MTTR (Resolucion)} = \frac{10}{5} = 2\ horas$$

Objetivo: Mantener el MTTR dentro de 2 horas.

Número de Incidentes Críticos Resueltos Dentro del SLA

Se resolvieron 38 de 40 incidentes críticos dentro del SLA, el porcentaje es:

$$\text{ICR Dentro del SLA}(\%) = \frac{\text{Nu´mero de Incidentes Resueltos Dentro del SLA}}{\text{Nu´mero Total de Incidentes Criticos}} X\ 100 =$$

$$\text{Incidentes Crıticos Resueltos Dentro del SLA}(\%) = \frac{38}{40} X\ 100 = 95\%$$

Objetivo: Resolver al menos el 95% de los incidentes críticos dentro del SLA.

Tasa de Falsos Positivos en Alertas de Seguridad

Se generaron 200 alertas y 20 resultaron ser falsos positivos, la tasa es:

$$\text{Tasa de Falsos Positivos}(\%) = \frac{\text{Numero de Falsos Positivos}}{\text{Numero Total de Alertas}} X\ 100 =$$

$$\text{Tasa de Falsos Positivos}(\%) = \frac{20}{200} X\ 100 = 10\%$$

Objetivo: Mantener la tasa de falsos positivos por debajo del 10%.

Frecuencia de Actualización de Parches y Definiciones de Seguridad

Se realizaron 5 actualizaciones en un trimestre

$$\text{Frecuencia de Actualizacion} = \text{Numero de Actualizaciones Realizadas en el Perıodo}$$

La frecuencia de actualización es una actualización cada 3 semanas.

Objetivo: Realizar actualizaciones mensuales o según las recomendaciones de los proveedores.

Porcentaje de Cumplimiento con Políticas de Seguridad

$$\text{Cumplimiento de Politicas}(\%) = \frac{\text{Numero de Sistemas/Usuarios Cumplidos}}{\text{Numero Total de Sistemas/Usuarios Revisados}} X\ 100 =$$

$$\text{Cumplimiento de Politicas}(\%) = \frac{90}{100} X\ 100 = 90\%$$

Objetivo: Lograr un cumplimiento superior al 90%.

Disponibilidad de Sistemas de Respaldo y Recuperación

$$\text{Disponibilidad de Respaldo}(\%) = \frac{\text{Tiempo Total Disponible de Respaldo}}{\text{Tiempo Total de Respaldo Programado}} X\ 100 =$$

$$\text{Disponibilidad de Respaldo}(\%) = \frac{720}{730} X\ 100 = 98{,}6\%$$

Objetivo: Mantener una disponibilidad de respaldo superior al 99%.

4.4. Desarrollo del tema

Una vez realizado el diagnostico actual de la ciber seguridad de la M.I. Municipalidad de Guayaquil, donde encontramos unas seguridades bastantes robustas, en la cual poseen un firewall de última tecnología y protocolos de red que son bastantes óptimos para poder mitigar las vulnerabilidades, no obstante se verifico que la debilidad de las seguridades informáticas de la entidad pública son los usuarios finales, puesto que por motivo de desconocimiento en el ámbito de ciberseguridad y la no capacitación para poder mitigar esa vulnerabilidad, acarrea a que sea la entrada de personas ajenas o hacker que quieran usurpar la red y apoderarse de la información valiosa que posee la Municipalidad de Guayaquil.

En el caso de la normativa o políticas que se emplea, la entidad pública usa políticas y gestiones enmarcadas en el modelo NIST, en la que se enmarca metodologías de implementación, normas bajo que rango se implementa, etc., esta información podremos realizar una comparación con el modelo ISO 27001 que se está empleando en este proyecto, lo cual se verá reflejado en la siguiente tabla comparativa.

Tabla N.2 Tabla Comparativa de Modelo de Gestión Actual e ISO 27001

Indicador	Modelo de la Entidad (NIST)	ISO 27001
Recursos y métodos para la implementación	Suministra documentación para desarrollar metodologías de implementación	Provee metodologías de implementación
Está orientado a procesos	Si	Si
Ejecuta la seguridad que está basada en gestión de riesgos	El propósito principal de la norma es la seguridad	El propósito principal de la norma es la seguridad

Se puede aplicar a diferentes empresas	Está orientada a empresas de los Estados Unidos	Se emplea en cualquier tipo de empresa y de cualquier tamaño
Objetivos claramente definidos	Requiere de información previa para definir los objetivos	Requiere de información previa para definir los objetivos
Estructura de gestión claramente definida	No	No
Cobertura de los controles	Se enfoca en la seguridad de los equipos de cómputo.	Tiene controles de seguridad para cada proceso de implementación
Utiliza certificados	Sólo en Estados Unidos	Si
Número de requisitos	Tienen diversos catálogos de controles y cinco funciones.	El Anexo A de ISO 27001 cuenta con 93 controles
Etapa operativa y nivel técnico	Es más técnico y adecuado para las etapas iniciales de un programa de riesgos de ciberseguridad o cuando se intenta mitigar un incidente.	ISO 27001 se inclina hacia la gestión basada en riesgos y la madurez operativa
Costos Esperados	Es voluntario, lo que permite a las organizaciones implementar el estándar a su propio ritmo y recursos.	ISO 27001 implica una serie de auditorías y certificaciones que conllevan un mayor gasto

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Como podemos ver las normativas de seguridad tanto actual como la que se está implementando son diferentes en varios aspectos dando a conocer las fortalezas de cada una de ellas, dependiendo para que ámbitos o proceso se desee implementar, en este caso la ISO 27001 va más enmarcada globalmente a las seguridades informáticas y la actual solo se utiliza para ciertos sectores o procesos en las que se utiliza.

Además la norma ISO 27001, posee un estándar internacional y requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) y cualidades como la confidencialidad, integridad, disponibilidad, evaluación de riesgos, mejoras continuas y cumplimientos legales, estas cualidades hacen que la normativa sea una buena opción para ciberseguridad y esencial para cualquier organización.

Tabla N.3 Tabla de Indicadores de Brechas

Identificador de Brechas	
Capacitación y Desarrollo	Del personal que se encuentra manipulando los diferentes departamentos, solo se capacita en ciberseguridad al departamento de TI.
Actualización de Procesos de ciberseguridad	Las actualizaciones de los procesos de ciberseguridad se realizan esporádicamente en en la red.
Implementación de Nuevas Tecnologías	No implementan tecnologías de vanguardia, con el inconveniente de ser vulnerados por nuevos ataques.
Monitoreo y Evaluación	El monitoreo y evaluación de la ciberseguridad se la realiza esporádicamente.

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

En este caso encontramos brechas significativas que se podrían cambiar con la implementación de la ISO 27001, esto aportaría a que las seguridades en la entidad pública soporte vulnerabilidades nuevas y aumenten las seguridades de la M.I. Municipalidad de Guayaquil.

Para contrarrestar las brechas antes mencionadas se podría tomarían acciones para mitigar esas brechas o espacios que no son tomados en cuenta por la actual norma que se está empleando.

Tabla N.4 Plan de Acción para Cerrar brechas

Plan de Acción para Cerrar Brechas	
Capacitación y Desarrollo:	Capacitar a todo el personal tanto del departamento de TI y usuarios finales en el área de ciberseguridad.
Actualización de Procesos de ciberseguridad	Verificación y actualización de los procesos internos para mejorar la seguridad informática interna.

Implementación de Nuevas Tecnologías	Utilizar o implementar tecnologías de ciberseguridad que faciliten el cumplimiento de los estándares de la ISO 27001.
Monitoreo y Evaluación	Realizar un sistema de monitoreo continuo para asegurar que las implementaciones se mantengan y se ajusten según lo necesario.

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Por eso sería beneficioso la implementación de normas ISO 27001 en términos de seguridad y cumplimiento, aunque algunas entidades son reacias a utilizarlas por sus costos iniciales, la utilización de recursos y tiempo, el cambio cultural y mantenimiento continuo, no se compararía con los beneficios a largo plazo que esta norma le serviría a la entidad pública.

Otra opción sería combinar ambas normativas tanto la que se maneja actualmente en la entidad pública y la que se presenta en este proyecto, aunque poseen distintos enfoque y orígenes, pueden ser el complemento una a la otra sin problemas. La entidad pública posee su programa de ciberseguridad que tiene beneficios, pero al incluir a la certificación ISO 27001 los procesos serán más sólidos a medida que estén las dos juntas.

En la siguiente etapa, se prosiguió con el Ethical Hacking en las cuales se pudo comprobar que las seguridades del sistema y red son bastantes buenos, pero se encontró un pequeño problema en el ámbito de los usuarios finales, donde se realizó una Ingeniería Social y se comprobó que no son cautos a la hora de dar información y además tienden a sufrir de ataques de phishing, ataques a sus contraseña, también suplantación de ip, sufrir de ataques de hombre de medio, todo esto por desconocimiento de ellos en el ámbito de la ciber seguridad.

Además esto se da a notar en la encuesta que se le realizo a los directores y usuarios finales, donde se vio que la gran mayoría de los encuestados desconocen o no tienen conocimientos de que es ciberseguridad y no saber de políticas informáticas que le ayuden a verificar ya sea si un email, un WhatsApp, un mensaje de texto estén infectados por algún virus o malware que le ayude al ciber atacante a realizar su intrusión al sistema o red, pudiendo dañarlo o robar información primordial de la entidad pública.

Tabla N.5 Vulneraciones detectadas Ethical Hacking y Encuesta

Vulnerabilidades detectadas	
Ataques	**Vulnerabilidad**
Hombre del Medio	Recolección sin autorización de trafico de información entre dos dispositivos.
Email Malicioso	Email infectados donde engañan a los usuarios para que compartan credenciales.
Phishing	Robo de credenciales
Suplantación de Ip (Spoofing de IP)	Duplicado de Ip de un dispositivo para hacerse pasar por otro dentro de un sistema o red.
DDOS	Inyección de múltiples solicitudes y detención del funcionamiento de sitios web o aplicativos.
Troyanos de mensajería instantánea	Robo de nombres de usuario y contraseña de programas de mensajería como WhatsApp, Facebook Messenger, Skype y muchos otros.
Escaneo de Puertos	Sirve o se utiliza para descubrir puertas abiertas o puntos débiles en una red.

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Como podemos observar en la tabla N.3 las vulnerabilidades que se pudieron detectar al realizar el laboratorio de ciberseguridad y las respuestas del cuestionario realizado, podemos darnos cuenta que efectivamente, aunque tenga una seguridad informática de alta calidad, no está exenta de que se le pueda realizar ataques que puedan tener una eficacia para los ciberdelincuentes y vulneren sus seguridades.

Tabla N.6 Impacto de vulnerabilidades en el sistema de ciberseguridad

Impacto de vulnerabilidades en el sistema de ciberseguridad	
Vulnerabilidades	**Impacto**
Hombre del Medio	Por falta de seguridades tiende a que personal no autorizado tenga acceso al tráfico de información entre usuarios.
Email Malicioso	Los empleados pueden ser engañados con email maliciosos que permitirían el ingreso no autorizado.
Phishing	Los empleados pueden ser engañados para revelar sus credenciales, permitiendo el acceso no autorizado a sistemas internos.
Suplantación de Ip (Spoofing de IP)	Ingreso no autorizado de personas, que suplantan ip para hacerse pasar por personal autorizado.

DDOS	Envió de solicitudes masivas a sitios web o aplicativos, con el objeto de hacer caer la red y poder ingresar.
Troyanos de mensajería instantánea	Robo de nombres de usuario y contraseña de programas de mensajería como WhatsApp, Facebook Messenger, Skype y muchos otros.
Escaneo de Puertos	Sirve o se utiliza para descubrir puertas abiertas o puntos débiles en una red.

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

La necesidad de ir de la mano con las tecnologías, actualizaciones y nuevos métodos de ciberseguridad es lo que representaría una mayor eficacia, para contrarrestar las vulnerabilidades que día a día los hackers van realizando. Es por eso que sería necesario laboratorios de seguridades informáticas con el objetivo de ver como se encuentra las seguridades informáticas y confirmar si las seguridades que poseen están a la altura o si es necesario un cambio de metodología, políticas e infraestructura para la seguridad de su información.

Para contrarrestar estas vulnerabilidades se creó una tabla en la cual vemos medidas correctivas para mitigar estos ataques.

Tabla N.7 Medidas correctivas para mitigar vulnerabilidades

Medidas correctivas para mitigar vulnerabilidades			
Vulnerabilidad	**Medida correctiva**	**Responsable**	**Cronograma**
Hombre del Medio	Empleo de claves públicas de cifrado, cifrado de la información, uso de certificados y firmas digitales.	Departamento de TI	Inicio: 1 de septiembre de 2024 Finalización: 15 de septiembre de 2024
Email Malicioso	Realizar un escaneo con un antivirus y antispyware actualizados	Departamento de TI	Inicio: 16 de septiembre de 2024 Finalización: 30 de septiembre de 2024
Phishing	Utilización de software de seguridad, manteniendo actualizados los programas antivirus, antimalware y anti phishing, y la verificación de fuentes, la autenticidad de sitios web y los correos electrónicos.	Departamento de TI	Inicio: 1 de octubre de 2024 Finalización: 30 de octubre de 2024
	Utilización de software de seguridad, manteniendo	Departamento de TI	Inicio: 1 de octubre de 2024

Spoofing de IP	actualizados los programas antivirus, antimalware y anti phishing, y la verificación de fuentes, la autenticidad de sitios web y los correos electrónicos.		Finalización: 30 de octubre de 2024
DDOS	Sistema de detección y prevención de intrusiones (IDS/IPS) utilizar un dispositivo o software con funcionalidad mixta (antivirus, cortafuegos y otras)	Departamento de TI	Inicio: 1 de noviembre de 2024 Finalización: 15 de noviembre de 2024
Troyano de mensajería	Utilización de software de seguridad, manteniendo actualizados los programas antivirus, antimalware y anti phishing, y la verificación de fuentes, la autenticidad de sitios web y los correos electrónicos.	Departamento de TI	Inicio: 1 de octubre de 2024 Finalización: 30 de octubre de 2024
Escaneo de Puertos	Utilizar software de seguridad sólido, herramientas de escaneo de puertos y alertas de seguridad que monitoreen los puertos y eviten que actores maliciosos lleguen a su red.	Departamento de TI	Inicio: 1 de octubre de 2024 Finalización: 30 de octubre de 2024

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Estas correcciones ayudaran a que sus sistemas de ciberseguridad se mantengan al día y actualizados contra estos ataques, pero se deben capacitar al personal (usuarios finales), con el fin de que las vulnerabilidades no se repitan.

Por otro lado, los indicadores de gestión aportan en gran parte como se maneja en los tiempos de reacción las seguridades informáticas de la M.I. Municipalidad de Guayaquil, puesto que bajo los estándares de la ISO 27001 ayudan a asegurar que la entidad pública cumple con los estándares y regulaciones de seguridad informática. Esto se ve reflejado en los resultados que a continuación se presenta en esta tabla.

Tabla N.8 Indicadores de Gestión de la M.I. Municipalidad de Guayaquil

	INDICADORES	VALORES	OBJETIVO	DETALLE
Disponibilidad del Servicio de Seguridad	Tiempo de Actividad (Uptime)	98,6	99.9%	Ha tenido un tiempo de actividad de 98,6% en el último trimestre
	Tiempo Medio Entre Fallos (MTBF)	1	10	El SDI ha tenido un el MTBF 450 horas, con un promedio de 1 fallo por cada 450 horas
Tiempo de Respuesta y Resolución	Tiempo Medio de Respuesta a Incidentes (MTTR - Mean Time to Respond)	25 minutos	Menos de 30 minutos	El tiempo de promedio para responder alertas de seguridad es de 25 minutos.
	Tiempo Medio de Resolución (MTTR – Mean Time to resolution)	2 horas	Menos de 1 día	El tiempo promedio para resolver incidentes de seguridad es de 2 horas, desde identificado el problema hasta su restauración del servicio.
Efectividad de la Detección y Prevención	Número de Incidentes Críticos Resueltos Dentro del SLA	95%	95%	En el último mes, se detectaron 40 incidentes de seguridad, de los cuales 38 fueron resueltos, dando un porcentaje de 95%.
	Tasa de Falsos Positivos en Alertas de Seguridad	10%	Por debajo del 10%	De 500 alertas generadas por el sistema, 50 fueron falsas alarmas, lo cual da una tasa de falsos positivo de 10%.
	Tasa de Falsos Negativos	2,6%	Por debajo del 10%	De los 38 incidentes confirmados, 10 no fueron detectados por el sistema de seguridad, resultando en una tasa de falsos negativos del 2.6%.
Cumplimiento de Políticas y Normativas	Número de Incumplimientos de políticas de seguridad	3	Por debajo de los 5	Se han registrado 3 incumplimientos importantes de las políticas de ciberseguridad en el último trimestre, relacionados con accesos no autorizados a datos sensibles.
	Porcentaje de Cumplimiento con Políticas de Seguridad	90%	Superior al 90%	Se realizaron 2 auditorías de seguridad en el último semestre, con resultados que indicaron un cumplimiento del 95% de las políticas de seguridad establecidas.
Satisfacción del usuario	Encuesta de satisfacción	85%	X	Porcentaje de satisfacción por parte de encuestados por la disponibilidad y tiempo de respuesta del soporte de ciberseguridad.
Capacitación y concientización	Número de horas de capacitacion	120 horas	X	Se han invertido 120 horas de capacitación en ciberseguridad solo para el personal administrativo y técnicos.
	Evaluación de concientización	30%	100%	El 30% de los empleados pasaron la evaluación de ciberseguridad con una puntuación de 80%.

Costos y Presupuestos	Costo por incidentes	1500	X	El costo promedio por gestión y resolución de un incidente de seguridad.
	Cumplimiento del Presupuesto	98%	X	El gasto de ciberseguridad asignado, lo que da buen alineamiento en los recursos disponibles.
Actualización y Mantenimiento	Frecuencia de Actualización	Cada 30 dias	X	Cada mes se actualizan con cobertura del 100%en parches críticos.
	Numero de Parcheos Pendientes	5 parches pendiente	X	Números de parches de seguridad pendientes.
	Disponibilidad de Sistemas de Respaldo y Recuperación	98,6%	Superior al 99%	El método de respaldo y recuperación del sistema de seguridad está en optima condición.

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Los resultados de los indicadores de gestión en ciberseguridad bajo la normativa ISO 27001, nos permiten medir y evaluar la efectividad de las políticas y controles que se emplean es este proyecto, las principales son detectar y cuantificar las amenazas y vulnerabilidades bajo los parámetros de tiempo de actividad, de fallos, respuesta, etc.

Al observar los indicadores se puede apreciar que la disponibilidad de servicios de seguridad está activos la mayor parte del tiempo salvo interrupciones esporádicas y los tiempos de respuesta y de resolución están activos pero un poco demorados. En el caso de detección y prevención para la verificación de falsos positivos y falsos negativos la soluciones para incidentes críticos son muy elevados y tienden a resolver problemas la mayor parte.

Otro aspecto es el cumplimiento de políticas y normativas se manejan en un alto porcentaje pero poseen incumplimiento que podrían acarrear a vulnerabilidades que pueden afectar a la entidad y al realizar encuestas de disponibilidad y respuestas de los servicios de ciberseguridad el porcentaje de aceptación es el 83% pero solo el área administrativa fue la encuestada, sería necesario involucrar más al resto del personal como es el caso de los usuarios finales para que estén al tanto de las seguridades informáticas y más con exactitud del mundo llamado ciberseguridad, en este caso ser capacitados en este ámbito.

Los costos que influyen por incidencias que se han su citado en la entidad pública, promueven a que sea más costoso, ya que el valor por incidencia es alto pero se ajusta al presupuesto. Por último la actualización, mantenimiento y respaldo se lleva a cabo según lo previsto en el modelo que se está utilizando, se actualizan cada mes, se respalda y recupera información que haya sido involucrada en algún inconveniente de entorno de ciberseguridad, pero al momento suelen demorar en el parche de algunos aplicativos o del sistema.

Para concluir se desarrolló un plan de monitoreo detallado para mejorar continuamente la ciberseguridad en la M.I. Municipalidad de Guayaquil.

Tabla N.9 Plan de Monitoreo detallado de ciberseguridad

Plan de Monitoreo detallado de ciberseguridad	
Número de Incidentes de Seguridad	**Frecuencia**: Mensual
	Herramientas: Sistemas de gestión de incidentes (InvGate Service Desk)
	Responsables: Departamento de TI
Tiempo de Respuesta a Incidentes	**Frecuencia**: Mensual
	Herramientas: Sistemas de gestión de incidentes, registros de tiempo (InvGate Service Desk)
	Responsables: Personal de Respuesta a Incidentes de TI
Tasa de Cumplimiento:	**Frecuencia**: Trimestral
	Herramientas: Auditorías internas, herramientas de cumplimiento.
	Responsables: Equipo de Cumplimiento
Número de Vulnerabilidades Detectadas:	**Frecuencia**: Mensual
	Herramientas: Escáneres de vulnerabilidades, pruebas de penetración(KALI LINUX)
	Responsables: Departamento de TI
Tasa de Capacitación:	**Frecuencia**: Trimestral
	Herramientas: Sistemas de gestión de aprendizaje (LMS)
	Responsables: Recursos Humanos, Equipo de Seguridad

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Una vez obtenido los datos a través del monitoreo serán analizados para identificar áreas de mejora, tendencia y oportunidades para fortalecer las seguridades informáticas.

Tabla N.10 Uso de Datos para Mejora Continua

Uso de Datos para Mejora Continua	
Análisis de Tendencias	Revisar los datos históricos para identificar patrones y tendencias en los incidentes de seguridad y vulnerabilidades.
Evaluación de Eficacia	Evaluar la eficacia de las medidas de seguridad implementadas y ajustar las estrategias según sea necesario.

Retroalimentación y Mejora	Utilizar los resultados del análisis para proporcionar retroalimentación a los equipos y ajustar los planes de acción.
Actualización de Políticas	Revisar y actualizar las políticas y procedimientos de seguridad basados en los hallazgos del monitoreo.
Capacitación Continua	Desarrollar programas de capacitación basados en las áreas de debilidad identificadas a través del monitoreo.

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

En conclusión, según estos datos recopilados en estos indicadores, podemos decir que la seguridad informática de la M.I. Municipalidad de Guayaquil está en óptimas condiciones, pero se podría mejorar con nuevos métodos con sus políticas y normativas para así tener un mejor margen de respuestas al momento de tener alguna incidencia de ciberseguridad.

4.5. Matriz de Riesgo con normativa ISO/IEC 27001 para la Municipalidad de Guayaquil

A continuación se realizó una matriz de riesgo utilizando la normativa ISO/IEC 27001, la cual permite proteger la confidencialidad, integridad y disponibilidad de la información, además nos ayudara a tomar conciencia de los riesgos e identificar y abordar debilidades que posea la empresa en seguridades informáticas de manera proactiva.

Tabla N.11 Matriz de Riesgo

		MATRIZ DE RIESGOS				
		CONSECUENCIA				
		Mínima	Menor	Moderada	Mayor	Máxima
PROBABILIDAD		1	2	4	8	16
Muy Alta	5	5	10	20	40	80
Alta	4	4	8	16	32	64
Media	3	3	6	12	24	48
Baja	2	2	4	8	16	32
Muy Baja	1	1	2	4	8	16

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Tabla N.12 Nivel de Riesgo

NIVEL DEL RIESGO	COLOR
Riesgo Aceptable	
Riesgo Tolerable	
Riesgo Alto	
Riesgo Extremo	

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Para esta matriz de eventos están incluidos los eventos que se encontraron al momento de realizar el diagnostico a las ciberseguridades de la M.I. Municipalidad de Guayaquil (Ethical Hacking y Encuesta), además de posibles eventos que también pueden hacer que fallen el sistema y red, esto haría que al suceder estos inconvenientes las seguridades informáticas fallen y serian blanco fácil de que generen vulnerabilidades en su sistema.

Tabla N.13 Matriz de Eventos Municipalidad de Guayaquil

EVENTO	PROBABILIDAD	CONSECUENCIA	NIVEL DE RIESGO
Fallo de hardware	Media	Mayor	24
Caída de servicio	Media	Menor	6
Uso inadecuada de las instalaciones	Media	Moderada	12
Ataque de virus	Alta	Moderada	16
Fuga de información sensible	Alta	Moderada	16
Falta de disponibilidad de aplicaciones	Alta	Mayor	32
Descontrol del personal	Media	Moderada	12
Perdida de información	Alta	Mayor	32
Errores de Software	Alta	Menor	8
Ejecución de aplicaciones	Media	Mayor	24
Inoperancia del personal	Media	Moderada	12

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

Para concluir se creó la Matriz de Riesgo de la M.I. Municipalidad de Guayaquil donde podrán observar a detalle las acciones que pueden suceder al momento de verificar si la disponibilidad de servicios de ciberseguridad esta óptima.

Tabla N.14 Matriz de Riesgo de M.I. Municipalidad de Guayaquil

RI/OP	DESCRIPCION	PROBABILIDAD	RELEVANCIA	CAPACIDAD	PRIORIDAD	ACCIONES
1	Fallo de hardware	Media	Alta	Media	1	Realizar mantenimiento preventivo y plan de recuperación
2	Caída de servicio	Media	Media	Baja	1	Plan de respaldo o redundancia
3	Uso inadecuada de las instalaciones	medio	Baja	Baja	3	Readecuación de instalaciones
4	Ataque de virus	Alta	Alta	Alta	1	Utilizar servicios de protección de ciberseguridad
5	Fuga de información	Alta	Media	Media	2	Implementación de políticas estricta de Manejo de Información
6	Falta de disponibilidad de aplicaciones	Alta	Media	Baja	2	Respaldo de aplicativos o espejo
7	Descontrol del personal	Media	Baja	Baja	3	Políticas de Administración del personal
8	Perdida de información	Alta	Media	Media	1	Implementación de Backup física o en la nube
9	Errores de Software	Media	Media	Baja	2	Mantenimiento y actualización de Software
10	Ejecución de Aplicaciones	Media	Alto	Media	2	Mantenimiento de Aplicaciones
11	Inoperancia del personal	Media	Alto	Media	3	Capacitación al personal

Fuente: Datos de Maestría
Elaboración: Henry Rubén Arroyo Álvarez

5. CAPÍTULO V. RESULTADOS CONCLUSIONES Y RECOMENDACIONES

5.1.Conclusiones

El diagnostico que se realizó en la M.I. Municipalidad de Guayaquil, nos revelo que la infraestructura y sistemas de seguridad de la entidad pública se encuentra en optimo estado, pero propenso a que sufra alguna anomalía en sus seguridades informáticas.

La evaluación ha identificado algunas vulnerabilidades en los sistemas de ciberseguridad, que podrían ser explotadas por atacantes para acceder a información valiosa y de vital importancia para la M. I. Municipalidad de Guayaquil.

Se ha observado que la disponibilidad de los servicios de ciberseguridad tiende a ser susceptible a que el funcionamiento sea irregular y por ende sufra de ciberataques. Cualquier interrupción de los servicios de ciberseguridad pueden afectar significativamente la operatividad de la entidad pública y la confianza de los usuarios finales.

Existe la necesidad urgente de capacitar y concienciar al personal en temas de ciberseguridad. Muchos incidentes (vulneraciones) de ciberseguridad pueden ser prevenidos con la formación adecuada.

La infraestructura y sistemas actual se podría mejorar para soportar las demandas crecientes y garantizar la disponibilidad continua de los servicios de ciberseguridad.

Los indicadores de gestión nos demuestran que la disponibilidad de los servicios de ciberseguridad se encuentra estables y con buena respuesta a la hora de sufrir algún inconveniente pero tienden a que puedan sufrir algún problema que pueda interrumpir el desarrollo de las actividades de la entidad pública.

5.2. Recomendaciones

Implementación de medidas de seguridad avanzadas como actualización de firewalls, sistemas de detección de intrusos y cifrado de datos para proteger la información sensible.

Desarrollar, implantar y mantener un plan de continuidad del negocio que incluya estrategias para la recuperación rápida de servicios de ciberseguridad en caso de ataques cibernéticos.

Realizar y establecer programas de capacitación continua para el personal con respecto a la ciberseguridad, enfocándose en la identificación de amenazar y respuestas a incidentes cibernéticos que puedan generarse.

Realizar e implementar periódicamente evaluaciones de ciberseguridad para identificar nuevas posibles vulneraciones y asegurar que las medidas de seguridad estén actualizadas.

Buscar la colaboración de expertos en ciberseguridad para realizar auditorías y recibir asesoramiento sobre las mejores prácticas y tecnologías de vanguardia.

En temas generales podría certificarse con la ISO 27001, pero por su alto costo sería recomendable combina ambas normativas, la actual que maneja la entidad pública basada NIST y la ISO 27001 la que se está usando en este proyecto, ya que podría ayudar a mejorar sus seguridades e implementar políticas y normativas que mitiguen en lo posible los nuevos ataques que en la actualidad se ven generados.

Bibliografía

AO Kaspersky, L. (2024). *AO Kaspersky Lab*. Obtenido de AO Kaspersky Lab: https://latam.kaspersky.com/resource-center/preemptive-safety/cybersecurity-training?srsltid=AfmBOop8iAyxax0gI55b-4UyQKJtfepdNAHWp_vRI95kCy7qdiPT8n48

Arévalo, M. C. (15 de 10 de 2020). *piranirisk.com*. Obtenido de piranirisk.com: https://www.piranirisk.com/es/blog/indicadores-de-seguridad-de-informacion

Auditool. (25 de 04 de 2024). *auditool.org*. Obtenido de auditool.org: https://www.auditool.org/blog/auditoria-de-ti/principios-basicos-de-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad-cia

Cataluña, U. d. (s.f.). *Ciberseguridad y hacking ético: conceptos, herramientas y casos de éxito.* Obtenido de https://www.ucatalunya.edu.co/blog/ciberseguridad-y-hacking-etico-conceptos-herramientas-y-casos-de-exito

Cedeño Zambrano, J. R., Muñoz Zambrano, C. C., Párraga Ganchozo, A. G., & Rengifo Sanclemente, T. R. (2022). *Importancia de la Alta Disponibilidad en la Infraestructura de Tecnologías de la Información.* Obtenido de https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/sigloxxi/XI/CIDEIT/S3/CIDEIT-S3-007.pdf

CFC. (s.f.). *Marco de ciberseguridad del NIST.* Obtenido de https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist#:~:text=El%20Marco%20de%20Ciberseguridad%20del,proteger%20sus%20redes%20y%20datos.

Cibernos Comunicación. (s.f.). *grupocibernos.com*. Obtenido de grupocibernos.com: https://www.grupocibernos.com/blog/ciberseguridad-buenas-practicas-empleados

CISCO. (2024). *Cisco Systems, Inc.* Obtenido de Cisco Systems, Inc.: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~how-cybersecurity-works

Comision Europea. (s.f.). *La protección de datos en la UE*. Obtenido de https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es

de Sousa, B. (20 de 12 de 2023). *IPNET*. Obtenido de IPNET: https://ipnet.cloud/blog/es/datos/disponibilidad-de-la-seguridad-de-la-informacion-el-concepto/

Fortinet. (s.f.). *Fortinet*. Obtenido de Fortinet: https://www-fortinet-com.translate.goog/resources/cyberglossary/cia-

triad?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=rq#:~:text=The%20three%20letters%20in%20%22CIA,the%20development%20of%20security%20systems.

Guatavita Diaz, D. A. (2018). *La concienciación al usuario final como mecanismo efectivo para la gestión de riesgos de seguridad de la información.* Obtenido de https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8615/La%20concienciacion%20al%20usuario%20final%20como%20mecanismo%20efectivo%20para%20la%20gestion%20de%20riesgos%20de%20seguridad%20de%20la%20informacion.pdf?sequence=1&isAllowed=y

Gutiérrez Trujillo, P. C. (2018). *La formación a usuarios finales como método de fortalecimiento del sistema de gestión de seguridad de la información.* Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2747/00004327.pdf?sequence=1

Hernández González, H. S. (2022). *Importancia de Estructurar un Gobierno de Seguridad y Ciberseguridad en las Organizaciones.* Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/12278

Horcajuela Muñoz , P. (s.f.). *salesystems.es*. Obtenido de salesystems.es: https://salesystems.es/que-es-disponibilidad-seguridad-informatica/

IBM. (s.f.). *IBM WEB*. Obtenido de IBMWEB: https://www.ibm.com/es-es/topics/cybersecurity

infosecurity. (s.f.). *infosecuritymexico*. Obtenido de infosecuritymexico: https://www.infosecuritymexico.com/es/ciberseguridad.html

ISO. (2022). *ISO/CEI 27001:2022.* Obtenido de https://www.iso.org/standard/27001

Jain, N. (2023). *ideascale*. Obtenido de ideascale: https://ideascale.com/es/blogs/que-es-el-diseno-de-la-investigacion/

Manrique Reyna, V. H. (2021). *Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un instituto superior tecnológico público, Lima - 2021*. Lima. Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/84954/Manrique_RVH-SD.pdf?sequence=1&isAllowed=y

MINTEL. (2021). *Reglamento a Ley Orgánica de Protección de Datos Personales.* Obtenido de https://www.telecomunicaciones.gob.ec/ley-y-reglamento-de-la-ley-de-proteccion-de-datos-personales/

Miro. (s.f.). *Miro*. Obtenido de Miro: https://miro.com/es/planificacion-estrategica/que-es-evaluacion-riesgos/

Ortega, C. (s.f.). *QuestionPro*. Obtenido de QuestionPro: https://www.questionpro.com/blog/es/metodologia-de-la-investigacion/#Que_es_la_metodologia_de_la_investigacion

Piensasoft. (2022). *Piensasoft*. Obtenido de Piensasoft: https://pensare.mx/seguridad-informatica/metricas-de-ciberseguridad-e-indicadores-clave-de-rendimiento-kpi/

Platzi. (s.f.). *Platzi*. Obtenido de Platzi: https://platzi.com/blog/emp-estrategias-ciberseguridad/

Ramirez Agudelo , J. F. (2021). *Estrategia a partir de un análisis de vulnerabilidades para evaluar la seguridad de la información en la alcaldía barbosa antioquia.* Antioquia. Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/8216/Estrategia%20a%20partir%20de%20un%20análisis%20de%20vulnerabilidades%20para%20evaluar%20la%20seguridad.pdf?sequence=1&isAllowed=y

Rhoton, S. (17 de 11 de 2023). *Significados.com*. Obtenido de Significados.com: https://www.significados.com/investigacion-de-campo/

Rios Rios, E. R. (2023). *Evaluación de la seguridad de la información con hacking ético en la municipalidad distrital de san juan bautista.* Peru. Obtenido de http://repositorio.ucp.edu.pe/bitstream/handle/UCP/2725/EDGARD%20RUBENS%20RIOS%20RIOS%20–%20TESIS%20–%20INFORMATICA%20Y%20DE%20SISTEMAS.pdf?sequence=1&isAllowed=y

Savkin, A. (24 de 3 de 2021). *BSC Designer*. Obtenido de BSC Designer: https://bscdesigner.com/es/estrategia-de-ciberseguridad.htm

Software, C. P. (s.f.). *Check Point Software Technologies Ltd*. Obtenido de Check Point Software Technologies Ltd: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-it-security/what-is-the-cia-triad/#:~:text=El%20t%C3%A9rmino%20%E2%80%9Ctr%C3%ADada%20CIA%E2%80%9D%20se,datos%20y%20muchos%20sistemas%20seguros.

Stewart, L. (s.f.). *ATLAS.TI*. Obtenido de ATLAS.TI: https://atlasti.com/es/research-hub/investigacion-descriptiva

TuDashboard. (7 de 2 de 2020). *tudashboard.com*. Obtenido de tudashboard.com: https://tudashboard.com/que-es-tudashboard/

ULA, O. (2017). *Universidad Latinoamericana*. Obtenido de Universidad Latinoamericana: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://practicasprofesionales.ula.edu.

mx/documentos/ULAONLINE/Maestria/MAN/HRM558/Publicaci%C3%B3n/Semana_3/Estudiante/HRM558_S3_E_Inv_explo.pdf

UNIR. (2021). *Disponibilidad en seguridad informática: ¿en qué consiste este término?* Universidad Internacional de La Rioja. Obtenido de https://www.unir.net/ingenieria/revista/disponibilidad-seguridad-informatica/

Vásquez, G. (7 de 2 de 2023). *codigoonclick.com*. Obtenido de codigoonclick.com: https://codigoonclick.com/conoce-los-dominios-de-la-seguridad-de-la-informacion/

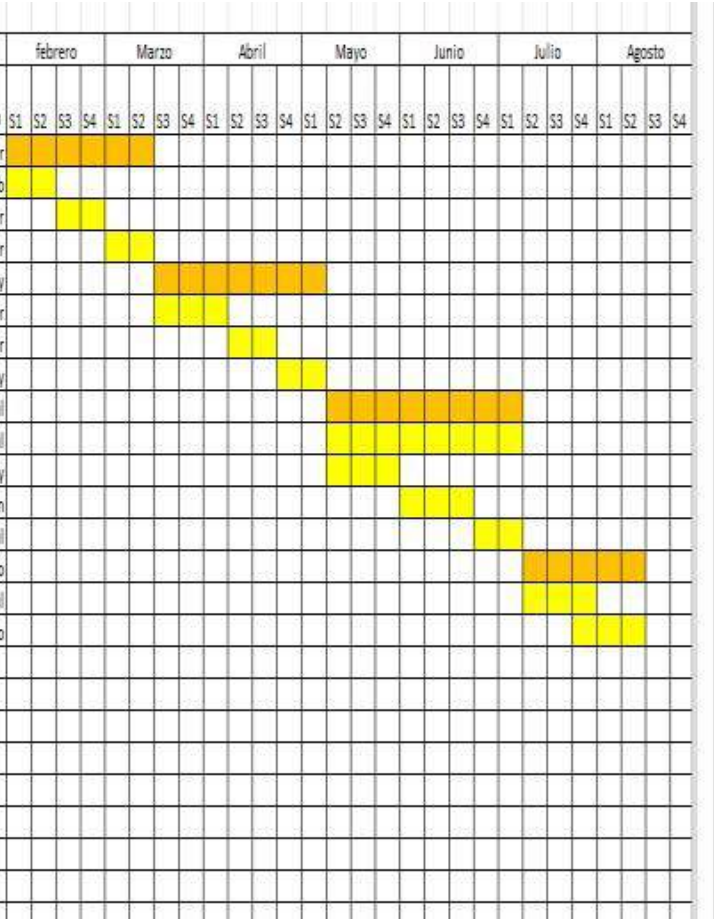
Vilchez, A. M. (8 de 2 de 2024). *Medium*. Obtenido de Medium: https://medium.com/@ajmv2000/investigaciones-mixtas-los-desaf%C3%ADos-de-combinar-lo-cuantitativo-y-lo-cualitativo-en-la-38b775a839cd

ANEXOS

Cronograma de Trabajo de Maestría

CRONOGRAMA DE ACTIVIDAD

No.	Tareas	Recursos	Resposables	Entregables	Coresponsable	Duración (Dias)	Fecha de inicio	Fecha de Finalización
1	Introducción					28	14-feb	22-mar
1,1	Justificación	Internet, Computador	Henrry Arroyo	Documento con la justificación escrita		8	14-feb	23-feb
1,2	Planteamiento del problema	Internet, Computador	Henrry Arroyo	Documento con el plantemianto del problema		10	26-feb	8-mar
1,3	Hito de retroalimentación	Internet, Computador	Henrry Arroyo	Documentos con la introducción		10	11-mar	22-mar
2	Revisión de la literatura					30	25-mar	3-may
2,1	Antecedentes	Internet, Computador	Henrry Arroyo	Documento con los antecedentes escritos		10	25-mar	5-abr
2,2	Fundamentos teóricos	Internet, Computador	Henrry Arroyo	Documento con los fundamentos teóricos escritos		10	8-abr	19-abr
2,3	Hito de retroalimentación	Internet, Computador	Henrry Arroyo	Documento con la Revisión de la literatura		10	22-abr	3-may
3	Metodología					45	6-may	5-jul
3,1	Diagnostico de la situación actual					45	6-may	5-jul
3.1.1	Revision del estado actual de seguri	Computador portatil, Et	Henrry Arroyo	Archivo con los datos actuales de seguridad		20	6-may	31-may
3.1.2	Identificacion de Vulnerabilidades	Computador portatil, Et	Henrry Arroyo	Documento con los resultados obtenidos en la revision		15	3-jun	21-jun
3.1.3	gestion de Seguridades informatica	Computador portatil	Henrry Arroyo	Documento con los resultados obtenidos de la gestion Informatica		10	24-jun	5-jul
4	Soluciones y Recomendaciones	Computador portatil	Henrry Arroyo			30	8-jul	16-ago
4.1	Posibles Soluciones de Vulnerabilid	computador portatil, Int	Henrry Arroyo	Documentos con las posibles soluciones a la segu	José Pérez	15	8-jul	27-jul
4.2	Recomendaciones para mutigar vul	computador portatil, Int	Henrry Arroyo	Documento con las recomendaciones para mitigar	las vulnerabilidades er	15	29-jul	16-ago



Encuesta a usuarios finales de la M.I. Municipalidad de Guayaquil

CUESTENARIO USUARIOS FINAL

Este cuestenario es en base a un estudio sobre la Evaluación de la Disponibilidad de Servicios de Ciberseguridad de la Información en usuarios finales en M.I Municipalidad de Guayaquil

Datos Demográficos *

1.- ¿Cuál es su edad?

- ○ Menos de 18 años
- ○ 18-30 años
- ○ 31-45 años
- ○ 46-60 años
- ○ Más de 60 años

2..- ¿Cuál es su nivel educativo? *

- ○ Primaria
- ○ Secundaria
- ○ Técnico
- ○ Universitario
- ○ Postgrado
- ○ Doctorado

Uso de Tecnología *

3.- ¿Con qué frecuencia utiliza dispositivos tecnológicos (computadoras, smartphones, tabletas)?

- ○ Diariamente
- ○ Varias veces a la semana
- ○ Semanalmente
- ○ Raramente

4.- .¿Para qué utiliza principalmente sus dispositivos tecnológicos? Trabajo Estudio Entretenimiento Comunicación *

- [ ] Trabajo
- [ ] Estudio
- [ ] Entretenimiento
- [ ] Comunicación

5.- ¿Está familiarizado con el término "ciberseguridad"? Muy familiarizado Algo familiarizado Poco familiarizado No estoy familiarizado *

- ( ) Muy familiarizado
- ( ) Algo familiarizado
- ( ) Poco familiarizado
- ( ) No estoy familiarizado

6.- ¿Ha recibido alguna vez formación en ciberseguridad? *

- ( ) Sí, formal (cursos, certificaciones)
- ( ) Sí, informal (autodidacta, talleres)
- ( ) No, pero estoy interesado
- ( ) No, y no estoy interesado

*

Servicios de Ciberseguridad

7.- ¿Considera que los servicios de ciberseguridad proporcionados por la M.I. Municipalidad de Guayaquil son adecuados?

- ( ) Muy adecuados
- ( ) Adecuados
- ( ) Neutros
- ( ) Inadecuados
- ( ) Muy inadecuados

8.- ¿Qué servicios de ciberseguridad considera más importantes que sean implementados o mejorados por la M.I. Municipalidad de Guayaquil? *

- ◯ Protección contra malware
- ◯ Formación en ciberseguridad
- ◯ Auditorías de seguridad
- ◯ Soporte técnico 24/7
- ◯ Monitoreo de amenazas

*

Experiencia Personal

9.- ¿Ha sufrido algún incidente de ciberseguridad (por ejemplo, virus, phishing, robo de identidad)?

- ◯ Sí, en el último año
- ◯ Sí, hace más de un año
- ◯ No, nunca
- ◯ No estoy seguro

10.- Si respondió "Sí" a la pregunta anterior, ¿reportó el incidente a la M.I. Municipalidad de Guayaquil? *

- ◯ Sí, y recibí asistencia
- ◯ Sí, pero no recibí asistencia
- ◯ No, no sabía que podía reportarlo
- ◯ No, decidí no reportarlo

11.- ¿Qué tan satisfecho está con la respuesta de la M.I. Municipalidad de Guayaquil ante incidentes de ciberseguridad? *

- ◯ Muy satisfecho
- ◯ Satisfecho
- ◯ Neutro
- ◯ Insatisfecho
- ◯ Muy insatisfecho

*

Indicadores de Gestión

12.- ¿Qué tan importante considera los siguientes indicadores para medir la disponibilidad de servicios de ciberseguridad? (Use una escala de 1 a 5, donde 1 es Nada importante y 5 es Muy importante)

	1	2	3	4	5
Tasa de incide...	○	○	○	○	○
Tiempo de res...	○	○	○	○	○
Porcentaje de f...	○	○	○	○	○
Nivel de satisfa...	○	○	○	○	○
Disponibilidad ...	○	○	○	○	○

*

Recomendaciones y Sugerencias

13.- ¿Le gustaría recibir más información o formación sobre ciberseguridad?

- ○ Sí, a través de cursos en línea
- ○ Sí, a través de talleres presenciales
- ○ Sí, a través de material autodidacta
- ○ No, no estoy interesado

14.- ¿Qué tan dispuesto estaría a participar en programas de formación en ciberseguridad ofrecidos por la M.I. Municipalidad de Guayaquil? *

- ○ Muy dispuesto
- ○ Dispuesto
- ○ Neutro
- ○ Poco dispuesto
- ○ Nada dispuesto

15.- ¿Tiene alguna recomendación adicional para mejorar los servicios de ciberseguridad en la M.I. Municipalidad de Guayaquil? *

Texto de respuesta larga