OFICINA DE POSGRADOS

Tema:

MODELO DE MEJORA DEL ESTADO DE LA CIBERSEGURIDAD EN LA GOBERNACIÓN DE TUNGURAHUA

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación, Innovación y Desarrollo

Protección de datos y comunicaciones

Autor:

ING. HÉCTOR VLADIMIR ROBAYO VILLARROEL

Director:

ING. PAUL FERNANDO BERNAL BARZALLO, Msc.

Ambato - Ecuador

Enero 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

MODELO DE MEJORA DEL ESTADO DE LA CIBERSEGURIDAD EN LA GOBERNACIÓN DE TUNGURAHUA

Línea de Investigación:

Protección de datos y comunicaciones

Autor:

HÉCTOR VLADIMIR ROBAYO VILLARROEL

Paúl Fernando Bernal Barzallo, Ing. MSc. f._____
CALIFICADOR

Diego Fernando Ávila Pesantez, Ing. MSc. f._____
CALIFICADOR

Firmado electrónicamente por:
DIEGO FERNANDO AVILA PESANTEZ

Liliana del Rocío Mena Hernández, Ing. MSc. f._____
CALIFICADOR

Juan Carlos Acosta, Padre, MSc. f. _____
DIRECTOR UNIDAD ACADEMICA

Hugo Rogelio Altamirano Villarroel, Dr. f._____
SECRETARIO GENERAL PUCESA

Ambato – Ecuador

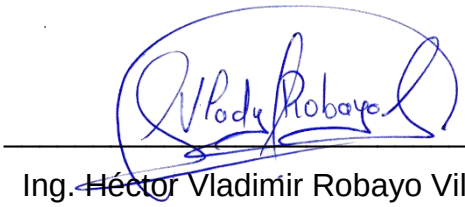
Enero 2022

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo, Héctor Vladimir Robayo Villarroel, con cc: 1803054616, autor del trabajo de graduación intitulado “MODELO DE MEJORA DEL ESTADO DE LA CIBERSEGURIDAD EN LA GOBERNACIÓN DE TUNGURAHUA”, previa la obtención del título profesional de MAGISTER EN CIBERSEGURIDAD, en la oficina de Posgrados.

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 Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad

Ambato, enero 2022



Ing. Héctor Vladimir Robayo Villarroel

cc: 1803054616

AGRADECIMIENTO

Deseo agradecer, en primer lugar, a Dios Todopoderoso que me dan desde el primer aliento hasta el pensamiento para realizar cada actividad, gracias por ser el gestor de mi vida y mis triunfos, gracias por hacerme un hombre bienaventurado y dichoso, gracias por todo lo que soy y por todo lo que tengo.

Un señalado agradecimiento a mi tutor Mg. Paul Fernando Bernal Barzallo, quien con sus conocimientos y apoyo me supo guiar en cada etapa de este proyecto para alcanzar los resultados que buscaba.

A las autoridades y funcionarios de la Gobernación de Tungurahua, gracias por darme la apertura en la Gobernación y proporcionarme todos los recursos, apoyo y herramientas que fueron necesarios para llevar a cabo el proceso de investigación.

Deseo expresar un agradecimiento especial a toda mi familia, por brindarme su completo apoyo, por ser la luz en cada paso de este sendero. Gracias por ser la principal inspiración para cumplir este gran sueño, por confiar y creer en mis expectativas, por los consejos, valores y principios que me han inculcado.
Muchas gracias a todos.

DEDICATORIA

El presente proyecto de investigación y desarrollo está dedicado a:

Principalmente a Dios, por haberme dado la vida y permitirme haber llegado hasta la culminación de esta etapa tan importante de mi formación profesional. A mis familiares, por ser el principal pilar y por demostrarme siempre su cariño y apoyo incondicional.

A todos los docentes quienes con su amplia experiencia supieron impartir sus conocimientos y me orientaron al correcto desenvolvimiento académico, personal y profesional y a través de ellos a la Pontificia Universidad Católica del Ecuador sede Ambato Universidad, autoridades, personal administrativo y docentes.

Muchas gracias a todos.

RESUMEN

En el presente Trabajo Final de Maestría titulado Modelo de mejora del estado de la Ciberseguridad en la Gobernación de Tungurahua, surge de la necesidad de mejorar el estado de la ciberseguridad en la institución gubernamental, Gobernación de la Provincia de Tungurahua, en los últimos años ha tenido inconvenientes relacionados con este ámbito, ante la indisponibilidad de documentación, políticas y procesos, se han producido escenarios que son peligrosos o de interés para los ciberdelincuentes. Con este antecedente, se desarrolló una revisión bibliográfica sobre los diferentes modelos existentes, mediante la identificación de las mejores características de cada modelo, se elaboró un modelo propio que es implementado en la Gobernación de Tungurahua, el cual, está desarrollado en tres fases; la fase de diagnóstico se realizó mediante el uso de herramientas tecnologías que permiten la identificación de vulnerabilidades que se presentan en los recursos humanos, tecnológicos, networking y de comunicación que dispone la institución, mediante la segunda fase de implementación se realizó la corrección de las vulnerabilidades, y en la fase final de control mediante el uso de herramientas tecnologías verificar el estado de la ciberseguridad institucional. El producto final se presenta a través del análisis resultante del modelo aplicado, que evidencie la disminución de las vulnerabilidades de potenciales riesgos y amenazas encontradas en el diagnóstico inicial y que mantenga un control constante de la ciberseguridad de la entidad; y que cumpla así con el objetivo general propuesto.

Palabras Clave: Modelo, Ciberseguridad, Gobernación de Tungurahua, vulnerabilidades

ABSTRACT

The Master's Final Project entitled Model of improvement of the state of Cybersecurity in the Government of Tungurahua arises from the need to improve the status of cybersecurity in the government institution, Government of the Province of Tungurahua, since in the last years it has had problems in this area, due to the unavailability of documentation, policies and processes, there have been scenarios that may be dangerous or of interest to cybercriminals. With this antecedent, a bibliographic review was developed on the different existing models, by identifying the best characteristics of each model, an own model was elaborated that will be implemented in the Government of Tungurahua which is developed in three phases; the diagnosis phase was carried out through the use of technological tools that allow the identification of vulnerabilities that occur in the human, technological, networking and communication resources available in the institution, through the second phase of implementation, the vulnerabilities were corrected , and in the final phase of control through the use of technological tools to verify the state of the institutional cybersecurity. The final product will be presented through the analysis resulting from the applied model, providing evidence of the reduction of the vulnerabilities of potential risks and threats found in the initial diagnosis and maintaining constant control of the institution's cybersecurity; thus fulfilling the proposed general objective.

Key Words: model, cybersecurity, Tungurahua Government, vulnerabilities

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

“El entendimiento no puede intuir nada, y los sentidos no pueden pensar nada. Sólo de su unión puede originarse conocimiento”. Emmanuel Kant

El uso de diferentes tecnologías de la información y de comunicaciones han impuesto un importante avance en la revolución del mundo, tanto que hasta forma parte de la vida cotidiana de los seres humanos, desde el ámbito laboral, económico, salud, hasta actividades que satisfacen el ocio. Sin embargo, dicha evolución no solo ha traído notables ventajas para la sociedad, sino que la ha convertido en un blanco fácil para los ciberdelincuentes, puesto que toda la información, se encuentra de manera digital o virtualizada y en su gran mayoría no cuenta con la seguridad adecuada.

El ciberataque, se considera al conjunto de acciones ofensivas realizadas por ciberdelincuentes en contra de dispositivos tecnológicos, redes informáticas, base de datos, entre otros, con el objeto de tomar el control, desestabilizar o dañar un sistema, empresa o individuo, el interés del ataque de estos delincuentes, se centra en víctimas cuyas seguridades tecnológicas estén obsoletas, nulas, con vulnerabilidades expuestas y en ciertos casos su objetivo puntual está basado en un persona u organización específica, objetivo del ataque. Las organizaciones, tanto públicas como privadas han sido víctimas de varios ciberataques (ataques informáticos) y de las consecuencias que estos ocasionan, no obstante, uno de los objetivos más cotizados son las instituciones gubernamentales debido a la importancia de su información.

La presente investigación está enfocada en estudios asociados a las metodologías y estrategias de mejoramiento de la ciberseguridad de una organización, sea pública o privada, se toma en cuenta los que mayor concordancia tienen con esta investigación, se citan:

Existe un trabajo de tesis doctoral en donde presenta una propuesta de modelo de organización” (Villalba Fernández, 2015) , que detalla la evolución de los incidentes de la ciberseguridad en España, las estrategias nacionales de seguridad, las

iniciativas internacionales en el ámbito del planeamiento de la ciberseguridad, el planeamiento de ciberseguridad en España y la propuesta de un modelo de organización de la ciberseguridad en el mismo país, en este sentido, resulta oportuno manifestar que en el trabajo desarrollado por (Inoguchi Rojas & Macha Moreno, 2017), busca el mejoramiento de los niveles de ciberseguridad de pequeñas y medianas empresas con la propuesta de gestión y prevención de seguridad informática, de manera idéntica es observable, en la tesis (Mogollón Flores, 2017), la cual, muestra el desarrollo de las amenazas cibernéticas tanto internacionales como nacionales, así como la estrategia de Ciberseguridad que maneja Ecuador y sus diferentes respuestas ante ciberataques.

En los planteamientos anteriormente mencionados ponen mayor atención en el desarrollo de varias metodologías que permitan identificar, controlar y mejorar el nivel de ciberseguridad de equipos y redes computaciones, aplicaciones y recursos informáticos (páginas *web*, bases de datos, controles, entre otros) de las organizaciones.

En este contexto, la Gobernación de la Provincia de Tungurahua, al ser una institución pública, que posee información confidencial de interés gubernamental, se convierte en un objetivo atractivo para el ataque de delincuentes informáticos, quienes, al contar con equipos y conocimiento especializado, incrementan las posibilidades de que las ciber amenazas multipliquen y como consecuencia potencial de este ataque, lograr perjudicar a la institución o funcionario y, también, afectar el normal desenvolvimiento de las actividades diarias de los funcionarios públicos. En este mismo sentido, la institución antes mencionada al no disponer de toda la protección en ciberseguridad, además, de no existir ningún estudio o investigación relacionada con el tema, se ve expuesta a la problemática descrita, por lo que, se plantea la siguiente interrogante, ¿Cómo mejorar el estado de la ciberseguridad en la Gobernación de Tungurahua?

Con el propósito de evidenciar que la aplicación del modelo de ciberseguridad, mejora las condiciones en la Gobernación de Tungurahua, se tiene como objetivo principal desarrollar un modelo de mejora del estado de ciberseguridad aplicado en

la entidad. En concordancia con esta idea, para cumplir con el mencionado propósito, se plantea desarrollar las siguientes actividades:

- Diagnosticar el estado de la situación actual de la ciberseguridad de la institución, mediante el levantamiento y evaluación de información obtenida de la infraestructura *networking*, componentes de red y comunicaciones, servidores, aplicaciones *web*, estaciones de trabajo y factor humano
- Implementar medidas y correcciones necesarias que mejoren el estado de la ciberseguridad institucional, mediante la planificación y aplicación de herramientas y métodos que contribuyan a esta actividad
- Controlar la gestión de los componentes de la infraestructura de red, comunicaciones, servidores, aplicaciones *web*, estaciones de trabajo y factor humano de la Institución, mediante acciones y procedimientos que verifiquen el estado del nivel de ciberseguridad de la entidad

Para el presente trabajo, se utilizan los siguientes tipos de investigación:

Según el enfoque: Investigación Cuantitativa: La investigación cuantitativa “Usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías” (Hernández, Fernández & Baptista 2006)

Según el Nivel: Investigación Cuantitativa – De*script*iva: La investigación de*script*iva “Busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice. Describe tendencias de un grupo o población”. (Hernández, Fernández & Baptista 2006)

Se toma en cuenta el objetivo de la investigación, es necesario conocer la información con exactitud y para ello es necesario realizar encuestas, en las que, se analiza las debilidades de cada uno de los activos de la entidad gubernamental.

En el desarrollo de esta investigación, se utiliza la metodología:

Cuantitativo No Experimental: “Se realiza sin manipular deliberadamente variables, es decir, no se hace variar en forma intencional las variables independientes, para observar su efecto sobre otras variables; sino que, se observan los fenómenos” (Hernández, Fernández & Baptista 2006)

A partir de los resultados obtenidos sobre el nivel de ciberseguridad en la Gobernación de Tungurahua, se desarrolla un modelo de mejora que cumpla con los requerimientos de la entidad. Se justifica esta investigación por su alto nivel de importancia debido a su contribución como un aporte fundamental para mejorar la ciberseguridad en la Gobernación de Tungurahua, esto se lleva a cabo mediante el desarrollo de una metodología adecuada a las necesidades y requerimientos de la entidad gubernamental. Cabe recalcar que la implementación de dicho modelo mejora la ciberseguridad en los componentes de infraestructura de red, comunicaciones, servidores, aplicaciones *web*, estaciones de trabajo y factor humano. Finalmente, es necesario dar a conocer que el presente proyecto es factible y realizable, se tiene al alcance todos los recursos disponibles (económicos, logísticos, humanos, etc.) para su elaboración y de una fuente verificable, como son los funcionarios, infraestructura y equipamiento de la Gobernación de Tungurahua.

Con la aplicación del modelo resultante de la presente investigación, se evidencia la importancia del mejoramiento de los niveles del estado de ciberseguridad en la institución, lo que, convierte en un aporte científico aplicable a cualquier organización.

PLANTEAMIENTO DEL PROBLEMA

La Gobernación de la Provincia de Tungurahua, al ser una entidad pública, que posee información confidencial de interés gubernamental, se convierte en una de las ventanas de oportunidad más atractivas para el ataque de varios ciberdelincuentes, quienes, al contar con equipos y utilizar en la mayoría de las ocasiones, infraestructura de la misma institución incrementan las posibilidades de multiplicar las ciber amenazas y cumplan con sus planes de fraude, robo, chantaje, falsificación, lanzar ataques a terceros o cualquier otro de índole delictivo (Centeno, 2015), de esta manera llegar a afectar el normal desenvolvimiento de las actividades diarias que realizan los funcionarios públicos o perjudicar a la Institución o a una personal en de manera particular (García, 2019).

La Gobernación de Tungurahua no dispone de medidas de diagnóstico, implementación y protección en ciberseguridad, por lo que está expuesta a la problemática descrita, además, no existe ningún estudio o investigación relacionado al mencionado tema, pero, habría estudios de otras gobernaciones. En síntesis, el problema, se enuncia de la siguiente manera: ¿Cómo mejorar el estado de la ciberseguridad en la Gobernación de Tungurahua?

IDEA A DEFENDER

La aplicación del modelo de ciberseguridad, mejora las condiciones en la Gobernación de Tungurahua.

OBJETIVOS

OBJETIVO GENERAL

a) Desarrollar un modelo de mejora del estado de la ciberseguridad en la Gobernación de Tungurahua.

OBJETIVOS ESPECÍFICOS

a) Identificar desde una perspectiva teórica los modelos existentes de ciberseguridad.
b) Sintetizar las mejoras prácticas de las metodologías existentes para el desarrollo de un modelo de ciberseguridad.
c) Elaborar el modelo de ciberseguridad para la mejora del estado de Gobernación de Tungurahua.
d) Validar el modelo de ciberseguridad aplicado en la Gobernación de Tungurahua

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

A continuación, se presentan diferentes tipos de investigaciones desarrolladas en el ámbito internacional, nacional y local, las mismas que están relacionadas con el problema y la deficiente protección de información en entidades gubernamentales específicamente referidas en la Gobernación de la provincia de Tungurahua Ecuador.

1.1 FUNDAMENTACIÓN TEÓRICA SOBRE CIBERSEGURIDAD.

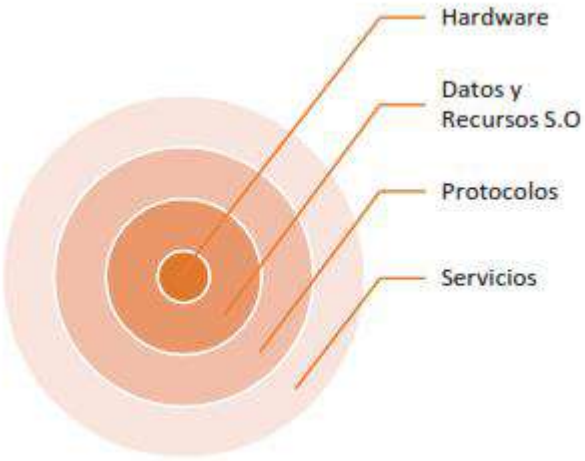
1.1.1 La ciberseguridad en el contexto internacional

En la actualidad las tecnologías de la información han llegado a ocupar importante en la sociedad esto ha conllevado a que, se convierta en un sector estratégico que contribuye al aumento de la productividad, innovación, desarrollo económico y social en sectores económicos críticos como la banca, servicios financieros, aviación, transporte y varias instituciones públicas gubernamentales.

La Agencia de Seguridad de la Información (ANSSI) describe la ciberseguridad como un “estado deseable para que un sistema de información permita resistir a los eventos del ciberespacio, cuyo objetivo es asegurar la confidencialidad, integridad y disponibilidad de la información”, para ISACA 2, define la ciberseguridad como “la protección de los activos de información al abordar las amenazas a la información procesada, almacenada y transportada por los sistemas de información trabajados en Internet”. En general, “el término de ciberseguridad, se refiere a todos los factores destinados a proteger a la empresa y sus empleados contra ataques intencionales, infracciones, incidentes y sus impactos” (ISACA, 2014). Otro concepto sobre la ciberseguridad establece que: consiste en procesos o pasos para garantizar que los recursos del sistema de información (material informático o programas) o equipo de cómputo, de una organización sean utilizados de la manera correcta, es decir, al decidir que el acceso a la información sen encuentre almacenada ahí, así como su posible modificación, sólo sea a través de las personas debidamente acreditadas y dentro de los límites de su autorización (Costas, 2011).

En la figura 1, se observa los niveles de protección de la información.

Figura 1: Nivel de protección



Fuente: (Pinzón, 2018)

En concordancia a lo mencionado anteriormente, la ciberseguridad, se genera a partir de una combinación de métodos, reglas y habilidades que permiten mejorar la gestión de riesgos de la información lo que permite así mejorar la integridad, confidencialidad, disponibilidad de la misma; para comprender mejor la seguridad cibernética y la protección que esta brinda a los activos cibernéticos es necesario conocer conceptos claves que permiten obtener políticas de seguridad como lo son: Confidencialidad, Disponibilidad, integridad y trazabilidad.

Se toma en cuenta los niveles de protección que para lograr una protección eficaz de la información, se considera primero todo el hardware o parte física, también, conocida como infraestructura, con su seguridad para la conexión con el software; en el siguiente nivel, se encuentran los datos junto a los recursos de los sistemas operativos, los mismos que permiten las configuraciones propias de seguridad; el nivel de protocolos de comunicación constituyen las normativas para la transmisión de datos entre dispositivos, seguidamente, se tiene los servicios y su protección para todas las posibles aplicaciones del hardware, en el nivel superior está el usuario y sobre este, se cita la seguridad de la información que esta enfocada en el resguardo organizacional, por lo que, es de vital importancia que en la implementación de metodologías o estrategias permitan salvaguardar dicha información.

Las definiciones de estos conceptos están presentes en la norma ISO 27001 (27001:2013, 2013).

1) La confidencialidad es una característica aplicada a la información. Proteger y preservar la confidencialidad de la información significa asegurar que no esté disponible o revelada a entidades no autorizadas. En este contexto, las entidades incluyen tanto a personas como a procesos.
2) Integridad: dentro del estrecho contexto de la seguridad de la información, el término integridad significa proteger la precisión y la integridad de la información.
3) La autenticidad es una propiedad o característica de una entidad.
4) Una entidad es auténtica si es lo que dice ser.

Para definir los pilares fundamentales para una estrategia de ciberseguridad eficaz, se ha realizado el estudio de un conjunto de estrategias implementadas en países como:

1. Francia

La eficacia de la estrategia de ciberseguridad de Francia se basa en los elementos de su recomendación para los sectores público y privado. Sin embargo, se ajusta entre el interés del gobierno y los objetivos de las empresas industriales; Entonces, cómo esta estrategia extermina estas fuerzas contradictorias: Estados, industriales, expertos que intentaron satisfacer sus necesidades más que traer una solución al problema de la ciberseguridad.

Finalmente, las ambiciones de Francia sobre el desarrollo de soluciones de seguridad son más que el poder del mercado industrial. Esta industria todavía sufre de debilidad de capital, fragilidad de la industria digital y la ausencia de profesionales nacionales en este campo, lo que representa un límite crítico para la implementación de esta estrategia.

2. Bélgica

El objetivo de la guía de ciberseguridad belga es ayudar a las empresas a aplicar su visión y el proceso de las organizaciones para proteger su información. Se trata de un manual de alto rendimiento que introduce la base de seguridad aplicada en el sector privado, pero no en las administraciones y la ciudadanía, por ser el principal punto débil de este modelo.

3. Unión Europea

Las Uniones Europeas en su estrategia de ciberseguridad afirman la importancia de dar responsabilidades a todas las partes interesadas y preserva la necesidad de proteger la privacidad en los procesos de seguridad con un marco de protección adecuado.

Finalmente, los objetivos más importantes de la estrategia europea es crear el vínculo de cooperación entre los estados miembros de la unión, de hecho, todos los miembros son responsables de respetar las normas comunes, pero eso no siempre es cierto; por tanto, uno de los principales factores críticos de la estrategia de la UE es proporcionar equilibrio y coherencia entre las estrategias nacionales y comunes. La ausencia de algunas definiciones da lugar a otra pregunta, si los estados están representados como partes interesadas de esta estrategia o es una UE en su conjunto sin prestar atención a los estados miembros que especifica.

La estrategia europea insiste en el intercambio de información con las autoridades públicas, pero ¿cómo el sector privado confía en los demás? ¿Cuáles son los límites de comunicar diferentes incidentes nacionales, no solo a sus autoridades sino, también, a una comisión que incluya a todos los estados miembros, especialmente en un entorno competitivo?

4. Estados Unidos.

La estrategia estadounidense define claramente la visión sobre el sector privado: en primer lugar, esta estrategia insistió en el intercambio de datos clasificados sobre amenazas cibernéticas entre defensa, agencias de inteligencia y empresas.

Sin embargo, las empresas reciben incentivos para seguir los estándares de seguridad. Finalmente, no hay ningún requisito para que las empresas divulguen públicamente las infracciones a menos que, se trate de información de identificación. La estrategia de EE. UU. describe su relación con la privacidad en puntos de remolque: la información compartida es limitada a las amenazas cibernéticas y no contendría contenido de correos electrónicos privados, por ejemplo, las empresas del sector privado no están obligadas a divulgar información sobre sus clientes, su estrategia de ciberseguridad con fecha del 12 de febrero de 2013 adopta dos proyectos que son rechazados por el Congreso de los Estados Unidos, además, el decreto no separa la medición de los legisladores, finalmente, la estrategia estadounidense sirve como modelo para otras regiones y naciones en la formulación de sus estrategias nacionales de ciberseguridad.

5. Reino Unido

Para asegurar los vastos beneficios económicos y sociales del ciberespacio, el Reino Unido transforma su propia estrategia de ciberseguridad, tiene en cuenta un enfoque confiable para proteger y promover el Reino Unido en un mundo digital. En esta sección, se establece su estrategia de ciberseguridad, donde la visión es descubrir los beneficios económicos y sociales del uso de un ciberespacio seguro.

Sin embargo, "para obtener un enorme valor económico y social de un ciberespacio vibrante, resistente y seguro, donde las acciones, guiadas por los valores fundamentales de libertad, equidad, transparencia y el estado de derecho, mejoran la prosperidad, la seguridad nacional y una sociedad fuerte".

1.1.2 Ciberseguridad en el Ecuador y Latinoamérica

La situación y el problema actual que Ecuador presenta respecto a ciberseguridad indica que el ente encargado de los protocolos se seguridad de la información es el Ministerio de Telecomunicaciones y de la Sociedad de la Información, que como tal, se encarga de normativas, leyes, proyectos y estrategias (Ministerio de Telecomunicaciones, 2020).

En el estudio realizado por la empresa (ISDEFE S.A., s.f.) establece un concepto nuevo de seguridad y defensa de acuerdo a el desarrollo de las TIC's, así mismo involucra a todos los sectores tanto públicos como privados como actores en la protección de la seguridad del territorio de las infraestructuras críticas y de los ciudadanos.

Los países de Latinoamérica según este nuevo escenario geopolítico tecnológico han iniciado la incorporación de una cultura de seguridad que sensibilice el cumplimiento de normas que fomenten la seguridad de la información, se observa, por ejemplo, que Colombia junto con Brasil son las naciones más completas en el área de Ciberseguridad. Según el informe Ciberseguridad 2016 del Observatorio de la Ciberseguridad en América Latina, se establece el porcentaje de acceso al internet y recoge la siguiente información, respecto al desarrollo de las políticas y estrategias en el ámbito de la ciberdefensa (Tates & Recalde, 2019). En la tabla 1, se observa una comparativa de la información respecto al desarrollo de políticas para la ciberseguridad.

Tabla 1: Comparativa de políticas de Ciberseguridad

ECUADOR 43 %	COLOMBIA 53 %	BRASIL 58 %	CHILE 72 %	ARGENTINA 65 %
NO ha desarrollado una **ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA**, Ecuador ha hecho avances en los últimos años para fortalecer su capacidad para abordar las amenazas informáticas	El Consejo Nacional de Política Económica y Social del Gobierno de Colombia estableció **LA POLÍTICA NACIONAL DE SEGURIDAD CIBERNÉTICA CONPES** 3701 bajo el auspicio del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de Defensa, el Departamento Nacional de Planeación y otras instituciones nacionales clave	En 2010 el Departamento de Seguridad de la Información y Comunicaciones publicó la Guía de Referencia para la Protección de Infraestructuras Críticas de Información y el Libro Verde de Seguridad Cibernética en Brasil. **ESTRATEGIA NACIONAL DE SEGURIDAD DE LAS COMUNICACIONES DE INFORMACIÓN Y SEGURIDAD CIBERNÉTICA DE LA ADMINISTRACIÓN PÚBLICA FEDERAL.**	El Ministerio del Interior y Seguridad Pública, el Secretario General de la Presidencia y la Subsecretaría de Telecomunicaciones son los principales organismos nacionales que establecen **LA POLÍTICA DE SEGURIDAD CIBERNÉTICA A NIVEL GUBERNAMENTAL.**	Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) y en coordinación con diversos organismos, instituciones académicas y el sector privado, el Gobierno de Argentina ha desarrollado un proyecto de **ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA** Argentina se distingue por haber formado el primer CSIRT nacional en 1994, que desde 2011 ha funcionado bajo el ICIC. ICIC-CERT
El Centro de Operaciones Tecnológicas Estratégicas y Contrainteligencia de la Secretaría de Inteligencia se encarga de los aspectos técnicos de la seguridad cibernética del país y un CSIRT nacional, el EcuCERT, entró en funcionamiento en noviembre de 2013	Las fuerzas del orden y el Poder Judicial tienen la capacidad de investigar y manejar casos de delincuencia cibernética	Las Fuerzas Armadas brasileñas también discuten las preocupaciones sobre defensa cibernética en su Libro Blanco de Defensa Nacional 2012. Recientemente crearon un Comando de Defensa Cibernética formal y una Escuela Nacional de Defensa Cibernética, además del Centro para la Defensa Cibernética del Ejército (CD-Ciber)	Las ramas de las Fuerzas Armadas de Chile comparten responsabilidades de defensa cibernética e información pero no tienen una estructura central de mando y control.	2015 la Presidencia de la República de Argentina emitió el Decreto nº 1067/2015 que reestructuró el control gubernamental de la ICN, y estableció una Oficina Nacional bajo la dirección de la **Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad** bajo la Jefatura del Gabinete de Ministros y Secretaría del Gabinete

Fuente: (Ministerio de Telecomunicaciones, 2020)

El Gobierno ecuatoriano, ha realizado un esfuerzo por reducir estos problemas, por estas razones el país tomó varias decisiones del tipo político-coyuntural. Por ejemplo, se conformó un Centro de Operaciones Estratégico Tecnológico, que tenía como finalidad realizar un monitoreo de ataques informáticos en los equipos de seguridad de algunas instituciones del sector público. De igual manera, se ejecutaron proyectos como: la implementación del Ecucert para el tratamiento de los incidentes Informáticos. Algunas instituciones incorporaron en sus planes estratégicos institucionales objetivos para incrementar la ciberseguridad como: la secretaria nacional de Inteligencia (Tates & Recalde, 2019).

1.2 FUNDAMENTACIÓN TEÓRICA SOBRE CIBERATAQUES.

Un ciber ataque, se entiende como la situación de daño cuyo riesgo de producirse es significativo, dado que deliberadamente o no, produce afectación contra la seguridad e integridad de la información (Erreyes, 2017), según López (2013) define que un daño a un sistema informático es el perjuicio que presenta si este deja de funcionar o falla, el mismo que, se cuantifica en base a términos de: coste económico, tiempo de recuperación, esfuerzo requerido para que el sistema regrese a su normalidad, este daño es provocado o presentarse de manera fortuita.

Los ataques informáticos a estructuras críticas, sistemas Informáticos tienen graves afectaciones en la sociedad, así como en la economía del mismo, esto ha permitido observar a la ciberseguridad como uno de los retos más importantes a medida que las sociedades dependen más de las TIC's (Leiva, 2015), de igual manera, los crímenes informáticos están originados y orientados hacia los países y las economías, por ejemplo, de América Latina que están en aumento, se ha convertido en el cuarto mayor mercado en el mundo y la mitad de su población utiliza internet (AETecno, 2016), de acuerdo con los indicadores de que Latinoamérica es uno de los blancos de ciberataques no todos los gobiernos han tomado a la ciberseguridad como un aspecto prioritario en la seguridad nacional, en la actualidad en Ecuador, se aprecia que delitos cibernéticos son mucho más frecuentes y sofisticados, están enfocados en el robo de información personal, estafas económicas, espionaje industrial y político, se han generado ataques a estructuras gubernamentales críticas tanto por parte de grupos organizados como por individuos, tal es así que, a diario las personas, están propensos a afrontar cualquier tipo de ciberataque provocado o de manera accidental; el hardware y los sistemas no son la excepción, también, son víctimas de situaciones anómalas que interrumpen su normal funcionamiento.

1.2.1 Vulnerabilidades.

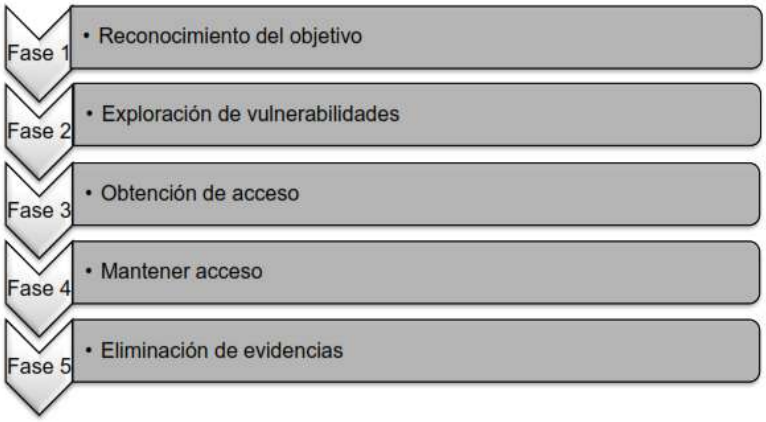
Según López (2013), se define a la vulnerabilidad como las deficiencias que el sistema presenta y que provoca un fallo, para Netcloud (2017) los orígenes de las vulnerabilidades son muy diferentes, estos son debido a los fallos en el diseño del

sistema, carencia de procedimientos o simples errores de configuración; por otro lado, la comunidad de investigadores de seguridad ha reconocido que el comportamiento humano tiene un papel crucial en muchos fallos de seguridad (Altamirano & Bayona, 2017).

Las vulnerabilidades han aumentado en un 9% en el último año, esto principalmente debido a que la mayoría de las empresas exigen ciclos de lanzamiento de aplicaciones de manera mucho más rápida. De acuerdo a un informe en donde, se analizó a 45.000 sitios *web*, de igual manera a redes de escaneos realizados sobre 5.700 objetos de análisis a partir de abril de 2015 hasta marzo de 2016, los resultados permiten observar que el 55% de los sitios *web* tienen una o más vulnerabilidades con una gravedad alta, este tipo de comportamiento, se ha deteriorado significativamente en sólo un año, lo que provoca un crecimiento del 9% con respecto al informe presentado en el año 2015, además, se notó que el 84% de las aplicaciones de Internet tienen vulnerabilidades de mediana gravedad, mientras que el 16% de los activos de la red perimetral, también, fueron susceptibles al menos en una vulnerabilidad de gravedad media (Naudi, 2016).

Al entender los diferentes procesos y etapas que involucran un ciberataque permite tener una perspectiva de aprendizaje en base a la forma de actuar de los atacantes, lo que refleja en no menospreciar su forma de pensar. Desde el punto de vista del profesional encargado de la seguridad de la información, es necesario utilizar estas habilidades de entender y distinguir la forma en que los hackers llevan a cabo un ataque cibernético (Philco, 2017). En la figura 2, se aprecia las etapas de manera general de un ciberataque.

Figura 2: Etapas de Ciberataques



Fuente: (López & Kirk, 2017)

Una vez identificadas las etapas de un ataque, estas son clasificadas según su autoría, tal como se observa en la tabla 2

Tabla 2: Clasificación de las autorías de Ciberataques

Autores	Objetivos		
	Gobierno	Sector privado	Ciudadanos
Ataques patrocinados por estados	Espionaje, ataques contra infraestructuras críticas, APT	Espionaje, ataques contra infraestructuras críticas, APT	-
Ataques patrocinados por el sector privado	Espionaje	Espionaje	-
Terroristas, extremismo político e ideológico	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	-
Hacktivistas	Robo y publicación de información clasificada o sensible, ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	Robo y publicación de información clasificada o sensible, ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	Robo y publicación de datos personales
Crimen organizado	Espionaje	Robo de identidad digital y fraude	Robo de identidad digital y fraude
Ataques de perfil bajo	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	Ataques contra las redes, sistemas o servicios de terceros, ataques contra servicios de internet, infección con malware	
Ataques de personal con accesos privilegiados	Espionaje, ataques contra infraestructuras críticas, ataques	Espionaje, ataques contra infraestructuras críticas, ataques	-

Fuente: (Ciberseguridad, 2016)

En (López & Kirk, 2017), se observa una clasificación de los ciberataques según el impacto en sus víctimas, como se detalla, a continuación:

1) **Spear-phishing**

Es un tipo de estafa informática, enfocada en ataques mediante el uso de correo electrónico y que tiene como objetivo adquirir un acceso no autorizado, a datos de alta confidencialidad e importancia. Estos ataques, se ejecutan de manera general y sus víctimas son del sector público o privado (Philco, 2017), los correos usados están elaborados para parecerse a correos oficiales que son enviados por las instituciones bancarias, gubernamentales o algunas marcas reconocidas (Philco, 2017), esto conlleva al destinatario a una página o sitio *web* falso, en donde, se ingresaría datos privados, los mismos que son: números de tarjeta de débito, cuenta bancaria, tarjeta de crédito, entre otros, la finalidad que tiene este tipo de ciberataque consiste en sustraer información personal, datos financieros (Philco, 2017).

Este tipo de estafa informática, es desarrollada principalmente por hackers que son o no patrocinados por alguna entidad gubernamental. Todo esto es realizado con el objetivo de utilizar o revender los datos confidenciales obtenidos a los gobiernos o empresas de carácter privado (Philco, 2017), estos grupos de hackers utilizan diferentes herramientas de diseño *web*, así como de ingeniería social con el fin de personalizar y presentar de tan convincente forma las páginas *web* (Kaspersky, 2017).

2) **Watering-hole**

Este tipo de ataques cibernéticos depende de la observación, analiza las páginas *web* que la futura víctima usa de manera frecuente, estos son infectados con *malware* o virus informático, para a su vez infecten al equipo informático de la víctima, el objetivo es recolectar diferente tipo de información, utilizan una vulnerabilidad o fallos de seguridad denominadas de día cero, se denomina así porque no se publica o anuncia antes de ser activa una vulnerabilidad (Philco, 2017); con esto los hackers evitan la posibilidad de toparse con tecnologías que les impida perpetuar su ciberataque (Symantec Corporation, 2016).

3) Man in the middle

Es un ataque cibernético intermediario (Hombre en la mitad), que provoca una violación a la ciberseguridad, se produce si la información es almacenada sin autorización y luego pasa a ser retransmitida para engañar al receptor en operaciones no autorizadas tales como falsa identificación o una transacción duplicada (Philco, 2017), para ejecutar este tipo de ciberataque solamente es requerido que el hacker encuentre entre las dos entidades que intentan establecer una comunicación; un mecanismo de defensa para este ciberataque es utilizar un sistema de cifrado fuerte entre el servidor y el cliente (Kaspersky Lab, 2017).

4) Masquerade

Este ciberataque, se caracteriza por utilizar credenciales falsas, como una identidad a nivel de red, para así obtener acceso a un equipo dentro de una red, se realizan si adquiere y utiliza credenciales de usuarios y contraseñas con un keylogger (Philco, 2017), generalmente mediante inicios de sesión no autorizados, ya sea por descuido del personal o a su vez si encuentra alguna vulnerabilidad en el proceso de autenticación. Un método estándar para contrarrestar este tipo de ciberataque es desarrollar algoritmos o reglas de seguridad que detectan de manera eficaz y eficientemente las acciones sospechosas en los equipos (López & Kirk, 2017).

5) Modificación

Este ataque ocurre si alguna persona o software realiza modificaciones que no están autorizadas al código fuente de algún software, además, la información transmitida a través de un medio, es atacada de formas diferentes (Philco, 2017).

6) Negación de servicios

Tipo de ataque cibernético que tiene como consecuencia que un recurso o servicio ofrecido por un sistema o dispositivo de red sea inaccesible para los usuarios legítimos (Philco, 2017), generalmente, se dividen en dos clases; las denegaciones de servicio por la emisión de solicitudes falsas para que no responda a las solicitudes reales, y las denegaciones de servicio por explotación de vulnerabilidades de seguridad (Philco, 2017).

7) Ingeniería Social

Este tipo de ataques utiliza el engaño a personas, para que revelen información de tipo confidencial al hacker, este tipo de información son, por ejemplo, contraseñas de acceso a un servidor de una organización (Philco, 2017), se diferencia de otro tipo de ciberataques porque no se aprovecha de vulnerabilidades de un equipo o sistema informático para la obtención de la información (López & Kirk, 2017).

8) Trashing

Considerado un ataque que busca información dentro de la basura informática, como la papelera de reciclaje, por lo general, esto representa una amenaza importante para usuarios que no destruyen información crítica o confidencial al eliminarla (Philco, 2017).

1.2.2 Servicios de Ciberseguridad.

Estos servicios permiten tener protección sobre la información en un infraestructura o entidad pública o privada, entre los más importantes, se tiene:

a) Información reservada

La confidencialidad o reserva de la información o datos, es un servicio de ciberseguridad que impide que cualquier persona, entidad o proceso no autorizado distinto del receptor leer, copiar, descubrir o modificar el contenido de los mensajes (Philco, 2017), esta característica, se vuelve de vital importancia para el acceso a la lectura de información no autorizada del tipo confidencial que transita dentro de una red resulta desastrosa.

b) Integridad del mensaje

Esta característica está basada en la capacidad de garantizar que la información enviada no ha sido modificada o manipulada sin autorización, para esto, se compara el mensaje, el cual, sería exactamente igual a la que se envió. Un claro ejemplo, es un trámite bancario online, en donde, se garantiza que ningún intruso capture y modifique los datos en tránsito (Philco, 2017).

c) Verificación

En esta característica, se verifica la identidad digital del emisor de un mensaje en una comunicación. Este servicio busca garantizar al receptor la identidad del emisor del mensaje, así como de manera viceversa.

d) Control de acceso

Este servicio de ciberseguridad está orientado para la autorización o la negación del acceso, esto logra que el sistema este en la condición de decidir entre permitir o denegar el acceso a una entidad, así esta previamente se haya autenticado, para lograr esto, se basa en políticas o reglas de seguridad de acceso implementadas previamente (Philco, 2017).

1.2.3 Penas legales por ataques cibernéticos

La infracción de políticas de ciberseguridad establecidas, dictamina que el infractor sea sancionado por el Código Orgánico Integral Penal del Ecuador (Ministerio de Justicia, 2014), en el que contempla en su sección tercera, una gran cantidad de artículos que están relacionados con los delitos realizados en contra de la seguridad de los activos de los sistemas de información y comunicación, los mismos son descritos, a continuación:

Artículo 231.-Transferencia electrónica de activo patrimonial:

“El individuo o grupo de personas que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programas o sistemas informáticos, telemático, mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años”. “Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona (Ministerio de Justicia, 2014)”.

Artículo 232.- Ataque a la integridad de sistemas informáticos:
"La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad (Ministerio de Justicia, 2014)".

Artículo 233.- Delitos contra la información pública reservada legalmente:
"La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años". "Cuando se trate de información reservada, cuya revelación compromete gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad (Ministerio de Justicia, 2014)".

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones:

"La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal *web*, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (Ministerio de Justicia, 2014)".

1.3 ESTANDARES, MODELOS Y NORMATIVAS DE CIBERSEGURIDAD.

A continuación, se realiza breve análisis de las diferentes modelos o metodologías de análisis de amenazas que se aplican actualmente en la Ciberseguridad.

1.3.1 IRAM 2

Es una normativa o metodología que permite la evaluación de riesgos desarrollada por la organización ISF, la misma que es uno de los líderes en investigación y creación de buenas prácticas de seguridad. Fue desarrollada a partir de diversas consultas a un gran grupo de expertos en ciberseguridad, este modelo posee seis fases de aplicación, las cuales, se realiza actividades claves que permiten cumplir con objetivos, además, que permiten identificar factores críticos de riesgo.

Identificación del alcance

Es la primera actividad a desarrollarse en el modelo IRAM 2, se realiza el análisis de los procesos de negocio y características de la tecnología que se dispone, para obtener un perfil de evaluación de riesgos a nivel de procesos de negocio, así como de servicios tecnológicos (Martínez, 2018).

Evaluación del impacto en el negocio

En este paso se realiza la identificación de la información que tiene una vital importancia para la organización, se define su tiempo de utilidad, además, se calcula el posible impacto de la pérdida o degradación de alguno de los atributos

de la ciberseguridad, hay que tomar en cuenta dos posibles casos; el realista y el peor de los casos (Martínez, 2018).

Perfilado de amenazas

Se realiza una clasificación y reconocimiento de posibles amenazas que comprometan de alguna manera a la información manejada en la organización, para lograr este paso, se toma en cuenta diversos atributos de las amenazas ya antes detalladas en esta investigación.

Evaluación de vulnerabilidades

En esta etapa, se estudian las debilidades identificadas para que los eventos reconocidos en el paso anterior tengan éxito. Los auditores determinan la eficiencia de los controles, así como sus fortalezas.

Evaluación del riesgo

Se determina la probabilidad de éxito que llega a tener una amenaza en un determinado escenario en la organización.

Tratamiento del riesgo

En este paso final, al implementar este modelo, se determinan los posibles enfoques y soluciones para tratar o eliminar los riesgos identificados, se elabora un plan de tratamiento del riesgo.

1.3.2 NIST

El Instituto nacional de Estándares y Tecnología (NIST), es una agencia federal que fue fundada en el año 1901 con la finalidad de la administración de tecnología del departamento de Comercio de los Estados Unidos, esta organización ha elaborado diferentes publicaciones científicas enfocadas a la seguridad de la información, de las cuales, se obtuvo la metodología NIST que provee de una base para el desarrollo de la gestión de la ciberseguridad (Martínez, 2018). Esta metodología comprende varias etapas ejecutadas de manera secuencial, lo que logra que sea un proceso totalmente iterativo

- Etapa 1: Preparación para la evaluación
- Etapa 2: Llevar a cabo la evaluación
- Etapa 3: Comunicar los resultados
- Etapa 4: Mantenimiento de la evaluación

En cada etapa, se realizan varias actividades que tienen como propósito una seguridad de la información optima, esas tareas, se definen como la identificación de las fuentes de amenaza, ocurrencias de amenaza, estudio de vulnerabilidades, condiciones de predisposición, probabilidad de ocurrencia, impacto, determinación del riesgo, informe de respuesta del riesgo, informe de evaluación del riesgo, sumario de tareas (Teodoro, 2015).

1.3.3 MAGERIT

Es una normativa o estándar para análisis de riesgos de la información para la Administración Pública Española, se basa en un análisis sobre posibles riesgos a los activos de la información que se organiza en función de su importancia, los activos de mayor importancia son servicios que se prestan al ciudadano en función de, por ejemplo, aplicaciones de software, servidores, elementos de comunicación, personal de desarrollo, sistemas, entre otros. Esta normativa se realiza en dos fases, en la primera, se realiza un análisis de los activos según las dependencias, esto permite determinar amenazas de dichos activos; en la segunda etapa, se realiza las salvaguardas existentes que permite medir el riesgo actual.

La normativa MAGERIT, se utiliza como una herramienta fundamental, que tiene una licencia gratuita para organismos públicos y de pago para empresas que deseen implementarla.

1.3.4 ISO 31000

Se trata de una norma desarrollada por la International *Organization for Standardization*, tiene como propósito proporcionar los principios y directrices para gestionar los riesgos, además, permite implementar un sistema de gestión a nivel estratégico y operativo, esta normativa o modelo ha sido desarrollada para que sea aplicada a cualquier empresa ya sea pública o privada. La ISO 31000 proporciona

directrices que permiten tener una cultura organizacional, la cual, se aplica a diferentes tipos de riesgos para una empresa o institución, se basa en tres grandes pilares, los que se detallan, a continuación:

Principios

Permite una gestión efectiva sobre el riesgo mediante los siguientes aspectos:

- La gestión del riesgo crea valor, y lo protege
- Es una parte integral de todos los procesos de la institución
- Forma parte del proceso interno de toma de decisiones
- Es estructurado, sistemático y transparente
- Considera factores humanos y culturales de los individuos

Marco

Para garantizar una correcta y efectiva gestión, se establece un marco al interior de la institución con base a cubrir todas las áreas y niveles, sin ningún tipo de excepción. El marco no reemplaza ningún sistema de gestión, al contrario, permite asistir a la organización ya establecida mediante los siguientes aspectos:

- Establecer un marco para la gestión del riesgo, en donde se:
  - Entiende el contexto de la organización
  - Establece una política para la gestión de riesgos
  - Identifica responsabilidades
  - Integra los diferentes departamentos de la empresa
- Identifica mecanismos de comunicación
- Monitoriza y revisar el marco establecido
- Establece una mejora continua

Procesos

Los procesos son acciones que se realizan para lograr ser parte integral de la cultura y las prácticas de la institución, para esto, se considera las siguientes áreas:

- Consultar y comunicar todas las partes afectadas
- Establecer el contexto en donde se lleva a cabo la gestión del riesgo
- Definir un criterio de riesgo
- Revisión continua

1.3.5 ISO 27000

Esta normativa o modelo a partir del año 2013 es conocida como la ISO 27001; permite a las diferentes organizaciones poseer un sistema que la gestione la seguridad de la información, se compone de 11 ítems, es de manera obligatoria el cumplimiento desde el ítem 4 al 10, además, contiene un anexo A con 14 dominios que permiten abarcar la mayoría de los aspectos de la seguridad de la información en una organización o institución:

- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Seguridad relativa a los recursos humanos
- Gestión de activos
- Control de acceso y Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relación con proveedores
- Gestión de incidentes de la seguridad de la información
- Aspectos de seguridad de la información para la gestión continua
- Cumplimiento

1.3.6 Octave Allegro

Esta normativa denominada *Operationally Critical Threat, Asset*, and *Vulnerability Evaluation*, fue desarrollado en el año 2007, que permite una evaluación del entorno de riesgo operacional de una organización, con el objetivo de obtener resultados sólidos sin necesidad de contar con un conocimiento intensivo de la evaluación de riesgos, se centra en los activos de información, que se enfocan en cómo se usan, la forma de almacenamiento, transporte y proceso, se analiza cómo están expuestos consecuente a las amenazas, vulnerabilidades y disrupciones. Consta de ocho pasos, los cuales, están agrupados en cuatro fases: Establecer impulsores, Perfilar Activos, Identificar Amenazas, Identificar y Mitigar Riesgos, de manera tradicional esta metodología está orientada al análisis cualitativo de riesgos, esto conlleva a limitaciones en la priorización de riesgos, así como el tratamiento de los mismos.

1.3.7 Modelo Bell-LaPadula

Es un modelo multinivel que permite fortalecer el control de acceso en aplicaciones del tipo militar y del gobierno (CISSP, 2018). Por lo general para estas aplicaciones, se generan niveles de seguridad, por ejemplo, no cualquiera tendría acceso a la información clasificada, catalogada como *top secret*. Este modelo se enfoca en la confidencialidad, que permite definir dos reglas para el control de acceso mandatorio y una regla para el control de acceso discrecional; las cuales, poseen las siguientes propiedades:

- **Seguridad simple:** un usuario con un nivel de seguridad bajo no accede a un objeto de nivel de seguridad mayor.
- **Seguridad estrella:** un usuario con un nivel de seguridad dado, no escribe o modifica algún objeto de un nivel de seguridad mayor.
- **Seguridad discrecional:** mediante el uso de una matriz de acceso, permite el control de acceso.

1.3.8 Modelo de BIBA

Este modelo permite describir un conjunto de reglas para el control de acceso, las mismas que están diseñadas para garantizar la integridad de la información, se

diseña mediante niveles ordenados de seguridad, de tal manera que los usuarios no accedan a información en un rango superior o inferior al de ellos (CISSP, 2018). Este modelo es similar al de Bell-LaPadula, sin embargo, este modelo no permite realizar modificaciones hacia arriba o abajo, también, permite una mejora en la integridad de la información, está basado en tres objetivos:

- Prevenir la modificación de la información por entidades no autorizadas
- Prevenir la modificación de información no autorizada por cualquier entidad
- Mantener la consistencia interna y externa.

1.3.9 Modelo Clark & Wilson

Este modelo maneja la integridad de la información como su objetivo principal, mediante el uso de políticas de integridad que permiten definir reglas de aseguramiento y reglas de certificación. Está diseñado para entornos comerciales, posee tres características de mayor relevancia: confidencialidad, integridad y disponibilidad. Las políticas de seguridad que se establecen permiten enfocarse en dos controles primordiales: “transacciones correctas” y “separación de obligaciones”.

1.3.10 Ciclo PHVA

Es un modelo de gestión que fue presentada en los años 50, está basado en cuatro etapas, las mismas que se detallan, a continuación:

- **Planificar:** en esta etapa, se realiza una proyección sobre los objetivos a alcanzar, se realiza una verificación de los procesos que permiten alcanzar resultados de acuerdo a las políticas de la entidad. De igual manera, se determinan los parámetros de medición para el control y seguimiento de procesos.

- **Hacer:** se realiza una serie de implementación de cambios o correcciones planificados, con el objetivo de mejorar la eficacia y eliminar errores.

- **Verificar:** mediante un plan de mejoras, se realiza el ajuste a las correcciones planteadas, de igual manera, se fija un lapso para conocer la efectividad.

- **Actuar:** si se finaliza la verificación, de ser el caso, se realiza los ajustes necesarios para asegurar el cumplimiento de los objetivos establecidos.

2 CAPÍTULO II. DISEÑO METODOLÓGICO

Este apartado comprende la metodología y técnicas de investigación utilizadas para el modelo de mejora del estado de la ciberseguridad en la Gobernación de Tungurahua, ubicada en el cantón Ambato; para determinar la importancia, grado de aceptación y nivel de impacto por parte usuarios y personal administrativo. El estudio ayudó a obtener información detallada y confiable, para proseguir con el presente proyecto, y a través de ello ejecutar un adecuado plan de implementación para obtener óptimos beneficios

2.1 METODOLOGÍA DE LA INVESTIGACIÓN

Los métodos utilizados durante el desarrollo de esta investigación fueron: el de*script*ivo, documental y analítico, dado que, se realizó un estudio de los tipos, formas y consecuencias de los ciberataques, información que coadyuba a comprenderlos de una manera clara y concisa, de esta manera, permite el desarrollo del modelo para mejorar la ciberseguridad de la Gobernación de Tungurahua, que acredite o desacredite la hipótesis planteada en la presente investigación.

A continuación, se enlista los pasos implementados para el desarrollo de los métodos expuestos anteriormente:

1) Buscar bibliografía relacionado a los conceptos, estándares, modelos o normativas establecidas.
2) Seleccionar estándares y modelos mediante una comparativa
3) Definir una plantilla de comparación y similitudes
4) Elegir un modelo de referencia que permita la mejora de ciberseguridad

Además, se establecieron criterios necesarios para la selección de conceptos, modelos y estándares para la Ciberseguridad, se toma en cuenta tres criterios para el estudio comparativo de modelos y estándares de ciberseguridad:

a) Los modelos, estándares y normativas, se orientan a la seguridad o mejora en un sentido amplio o directamente con la ciberseguridad.

b) De todos los modelos, estándares y normativas disponibles, se selecciona aquellos que tengan mayor relación con la ciberseguridad de información.
c) Seleccionar a aquellos en los que la información esté disponible y accesible.

2.1.1 Enfoque de la investigación

Según Ramírez Atehortúa y Zwerg Villegas (2012) el modelo cualitativo, se enfoca a la compresión de un fenómeno de estudio de la realidad en distintas percepciones, que fomenta en el proceso inductivo de la investigación, y el método cuantitativo, se refiere al análisis de los resultados obtenidos que me indican el resumen de un conjunto de datos, con este antecedente, y en virtud el enfoque del presente proyecto, esta investigación concibe utilizar la metodología cualitativa, permite observar los elementos de la problemática propuesta, de esta manera, planificar el diseño de la investigación mediante el uso de diferentes estrategias, con la finalidad de obtener información precisa, así como su respectivo análisis de resultados. El cuestionario informatizado es una herramienta electrónica específica para la recolección de información, el interés por estudiar, desarrollar y diseñar buenos cuestionarios para su administración informatizada está plenamente justificado en el campo de las encuestas.

Entre las herramientas que se utiliza, se determina técnicas tradicionales como observación, cuestionarios de tipo *checklist* y encuestas, que emitan información de interés y que den a conocer información relevante sobre la institución, de manera especial, en la infraestructura *networking*, componentes de red y comunicaciones, servidores, aplicaciones *web*, estaciones de trabajo y factor humano.

2.1.2 Encuesta en pantalla única

En una encuesta de pantalla única, las preguntas se presentan sin la necesidad de saltos de página. Lo que permite que toda la encuesta sea visible y accesible en una sola pantalla, lo que conlleva al beneficio de responder al cuestionario de una sola vez. Sin embargo, al finalizar todas las preguntas, los encuestados presionan en el botón “Finalizar” para declarar que han terminado de responder al cuestionario de investigación, se nota un ejemplo en la figura 3.

Figura 3: Encuesta pantalla única

Fuente: (Question Pro, 2018)

Para esta investigación, se realizó el enfoque como población de estudio a funcionarios y autoridades de la Gobernación de Tungurahua como los principales beneficiarios, quienes son los encargados del manejo de la diferente información de la institución, como población secundaria, se consideró y a los usuarios que hacen uso de los diferentes servicios de la institución.

El muestreo aleatorio/probabilístico es el único tipo de muestreo que cuenta con una teoría matemática que permite estimar los errores que conlleva generalizar los resultados a la población y, por lo tanto, permite generalizar a dicha población los resultados obtenidos en la muestra dentro de unos márgenes de error que se estiman y tienen en cuenta en la interpretación ya análisis (Martín, 2011).

2.2 METODOLOGÍA DE DESARROLLO

2.2.1 Comparativa de estándares, modelos o normativas.

Para lograr una comparativa optima, se utilizó el método de estudio MSSS (Similitud entre Modelos y Estándares) (Gasca G., 2010), el cual, permite conocer de manera más detallada el conjunto de estándares, modelos y normativas, que están orientadas al análisis de riesgos para la información. Para realizar la comparativa, se divido en dos grupos: comparativa de estándares, normativas y comparativa

entre los modelos ya implementados. Para la comparativa de estándares y normativas, se tomó en cuenta las fases que se emplean en cada uno de los estándares, modelos o normativas detallados en el capítulo 1. Posterior a realizar el análisis comparativo que se presenta la tabla 3, en donde se concluye que todos los estándares, modelos o normativas poseen una misma filosofía, es decir, comparten patrones comunes en sus diferentes fases, las mismas que se detallan, a continuación:

- **Fase 1:** se realiza la identificación del contexto, ámbito o conceptos de lo que se va a partir.
- **Fase 2:** se realiza un análisis del impacto de manera temprana, es decir, antes que la aplicación de las otras fases, este análisis solo se ve implementado en el modelo IRAM2, mientras que los demás realizan el mismo análisis de manera posterior.
- **Fase 3:** se realiza una identificación de las vulnerabilidades o riesgos, de manera dinámica para un entorno relacionado con la ciberseguridad.
- **Fase 4:** estimar y analizar los riesgos potenciales, se considera el factor cambiante en el tiempo.
- **Fase 5:** determinar y realizar una evaluación de los riesgos potenciales, mediante un cálculo que permita realizar una automatización de la toma de decisiones, la misma que es realizada por un responsable.
- **Fase 6:** se realiza tratamientos, recomendaciones para los riesgos considerados críticos, en esta fase al igual que en la anterior es necesario la intervención de un ser humano a pesar que se automatiza riesgos ya conocidos o tratados anteriormente.

Cada una de los estándares y normativas posee una secuencia y tiempo para realizar cada una de sus fases, de tal manera que independientemente de la seleccionada, existe algún tipo de coincidencia con entres sus fases.

Tabla 3: Tabla comparativa de modelos

FASES	ESTANDARES - MODELOS - NORMAS					
	IRAM2	NIST	MAGERIT	ISO31000	ISO27001	OCTAVE ALLEGRO
FASE 1	Identificar el alcance y analizar el contexto de la institución	Caracterizar el sistema en su contexto	Determinar el contexto de la institución	Establecer el marco de un contexto organizacional	Organizar las políticas de seguridad como alcance	Establecer criterios para medir e identificar los activos de la información
FASE 2	Analizar e impacto mediante un escenario realista y del pero caso	Evaluación de impactos, amenazas y riesgos				
FASE 3	Realizar un perfil de amenazas. Participan auditores	Identifica amenazas potenciales	Identifica riesgos potenciales	Identifica riesgos potenciales	Identifica amenazas y riesgos potenciales	Identifica amenazas y riesgos potenciales
FASE 4	Realizar un análisis de vulnerabilidades. Participan auditores	Identificar vulnerabilidades mediante un análisis de controles y probabilidades	Análisis de riesgos potenciales	Análisis de riesgos potenciales	Análisis de riesgos y amenazas potenciales	Análisis de riesgos y amenazas potenciales
FASE 5	Evaluación de riesgos tomando en cuenta factores complejos	Determinar los riesgos potenciales	Evaluar los riesgos potenciales	Evaluar los riesgos potenciales	Evaluar la implementación de los controles	
FASE 6	Tratamiento recomendable de los riesgos	Recomendaciones documentales	Elaborar un plan de tratamiento de riesgos y evaluación continua	Elaborar un plan de tratamiento de riesgos y evaluación continua	Elaborar un plan de tratamiento de riesgos y evaluación continua	Elaborar procedimientos para la mitigación de riesgos

Fuente: (elaboración propia)

Para realizar un análisis comparativo de los modelos anteriormente descritos, se considera las características principales obtenidas mediante la revisión bibliográfica, el resultado de este proceso ha permitido definir que:

- **El modelo Bell-LaPadula, BIBA, Clark & Wilson:** permiten el desarrollo de niveles de seguridad, enfocados en la confidencialidad mediante el uso de reglas de seguridad.

- **El modelo PHVA:** es diferente a los anteriores, establece cuatro pasos la manejar la seguridad de la información en una institución.

2.2.2 Encuesta sobre amenazas y medidas.

Las amenazas cibernéticas a menudo son asociadas con grandes organizaciones e instituciones financieras, lo que definitivamente es una mala interpretación del entorno existente (Tirumala, Valluri, & Babu, 2019).

Es posible personas que posee ciertas habilidades de piratería informática no inviertan tiempo y esfuerzo en piratear bases de datos seguras de grandes organizaciones, en la actualidad, el sector social es uno de los entornos más utilizados para robar información individual y datos privados. Para investigar más a fondo, es necesario comprender las principales preocupaciones de varios sectores de la población, de modo que, se crea un nivel apropiado de asociación entre las preocupaciones y el marco de mejora de la ciberseguridad.

2.3 MODELO DE MEJORA

El modelo de mejora del estado de la ciberseguridad que se implementa en la Gobernación de Tungurahua, está basado en la normativa ISO 27001 y en el modelo PHVA. Su aplicación está destinada para instituciones cuyas actividades, se enfoquen en el uso estratégico de las tecnologías de la información, debido a que es un modelo orientado a salvaguardar la confidencialidad, integridad, disponibilidad, seguridad y privacidad de la información. El modelo establecido busca que su correcta aplicación contribuya al mejoramiento de la ciberseguridad institucional, su objetivo, se encuentra dirigido de manera precisa en componentes de la infraestructura de red, comunicaciones, servidores, aplicaciones *web*, estaciones de trabajo y factor humano, mediante el apoyo de diversas herramientas y procesos que alcancen una mayor eficiencia y transparencia en su ejecución. Este proceso, se desarrolla con la implementación de tres fases tal como se observa en la figura 4. y son detallados, a continuación:

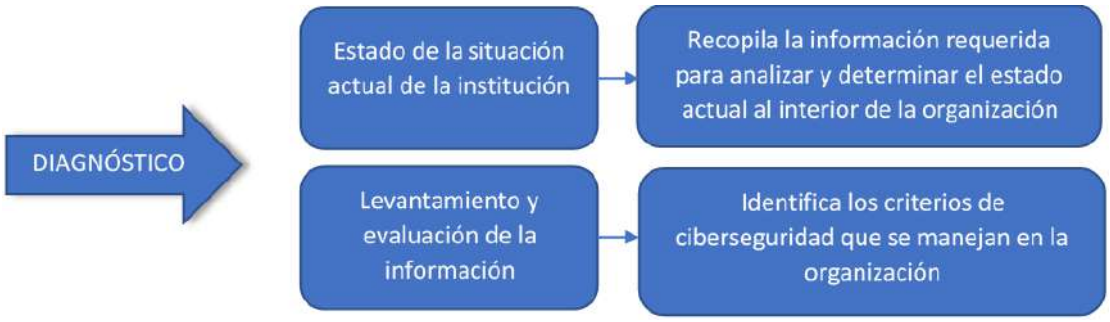
Figura 4: Modelo de mejora

Fuente: (elaboración propia)

2.3.1 Diagnóstico

Esta fase está orientada a obtener detalladamente toda la información de la institución, conocer y comprender los objetivos del servicio público que ésta persigue, visión, misión, estructura orgánica y funcional; inventariar y evaluar los activos informáticos, tecnológicos utilizados en los procesos de generación, ingreso, almacenamiento y envío de información, dicho de otra manera, lo que pretende en esta etapa, es adquirir datos necesarios que permitan analizar, identificar y evaluar posibles vulnerabilidades, así como riesgos potenciales que afecten el nivel de ciberseguridad institucional. El levantamiento de estos datos se lo realiza en dos etapas, como se observa en la figura 5.

Figura 5: Metas de la fase de diagnóstico



Fuente: (elaboración propia)

2.3.1.1 Estado actual de la Institución

En esta etapa, se recopila toda la información requerida para analizar y determinar el estado actual de la ciberseguridad de la institución, enfocada en la misión, visión, organigrama de la entidad, recursos humanos, tecnológicos, networking y de comunicación que dispone la institución, descubrir todos los medios o dispositivos informáticos conectados, recopilar sus características, función y naturaleza dentro de la red. Durante esta actividad, se realiza la identificación de los activos que estén relacionados al manejo de la información y que sean de mayor importancia para la institución.

La Gobernación de Tungurahua es una entidad pública cuya máxima autoridad es el gobernador o gobernadora, quien es el representante del presidente de la República del Ecuador en la provincia, encargada de coordinar y controlar las

políticas del gobierno nacional y dirigir las actividades de funcionarios y representantes de la Función Ejecutiva en cada provincia. El edificio principa,l se encuentra ubicado en las calles Castillo 4-44 y Sucre, en la ciudad de Ambato, dispone de oficinas a nivel cantonal con Jefaturas Políticas y Comisarías Nacionales y a nivel parroquial con Tenencias Políticas, un total de 62 dependencias a nivel provincial.

- **Misión:**

"Direccionar y orientar la política del Gobierno Nacional en la provincia, los planes y proyectos promovidos por el Ministerio del Interior a nivel provincial, a través de una gestión eficiente, eficaz, efectiva, transparente y pública, para el fortalecimiento de la gobernabilidad y la seguridad interna para el buen vivir (Gobernación Tungurahua, 2018)".

- **Visión:**

"La Gobernación de Tungurahua es reconocida por la sociedad como la entidad que, con estricto respeto a la constitución y la participación ciudadana, genera las condiciones fundamentales para el desarrollo provincial, al garantizar la seguridad interna y la gobernabilidad del estado; brinda servicios a la colectividad regidos por los principios de eficiencia eficacia, calidad, jerarquía, desconcentración, descentralización, participación, planificación, transparencia y evaluación (Gobernación Tungurahua, 2018)".

- **Valores:**

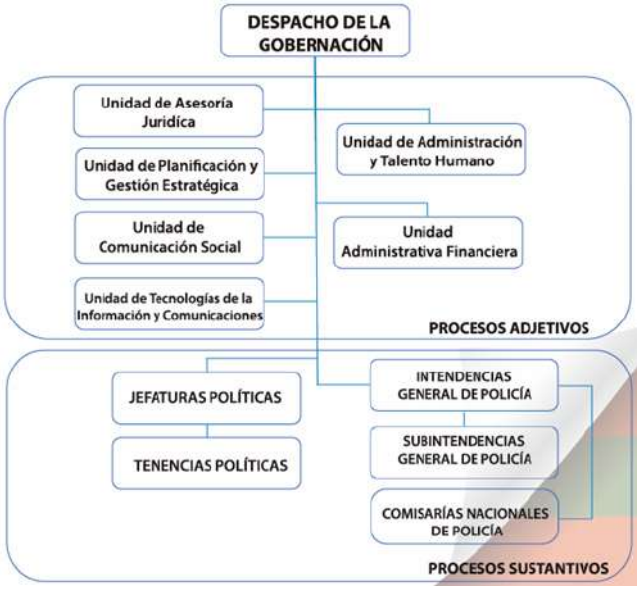
"La Gobernación de Tungurahua cuenta con Normas y Reglas de Valores Éticos para las funcionarias, funcionarios, servidoras, servidores, obreras y obreros públicos que laboran en la Institución, dentro de los cuales, constan los siguientes: probidad, destreza, justicia, templanza, idoneidad, responsabilidad, aptitud, capacitación, actitud, imparcialidad, respeto, información, discreción, declaración patrimonial jurada, obediencia, independencia de criterio, equidad, igualdad de trato, ejercicio adecuado del cargo, uso adecuado de los bienes del estado, colaboración, uso de información reservada, obligación de denunciar, dignidad y

decoro, honor, tolerancia, equilibrio, preservación y cuidado del entorno ecológico, imagen institucional (Gobernación Tungurahua, 2018)".

- **Organigrama:**

La figura 6 permite observar la distribución la Gobernación de Tungurahua.

Figura 6: Organigrama de la Gobernación de Tungurahua



Fuente: (elaboración propia)

- **La estructura de la institución**

La estructura de la institución está compuesta por el Despacho del Gobernador, según los procesos a realizar, se tiene: Procesos Sustantivos y Procesos Adjetivos. Los procesos sustantivos están desarrollados por las diferentes jefaturas y tenencias políticas establecidas en cada uno de las parroquias y cantones de la provincia de Tungurahua. Los procesos Adjetivos son desarrollados por los departamentos o unidades de gestión, cada uno con sus competencias y actividades respectivas, como a continuación, se detallan:

Unidad Jurídica: Es el órgano técnico de consulta y asesoría legal, que para el cumplimiento de sus atribuciones.

Unidad de Planificación y Gestión Estratégica: Se encarga de Coordinar, dirigir, controlar y evaluar la implementación de los procesos estratégicos institucionales a través de la gestión de planificación, seguimiento e inversión, administración por procesos, calidad de los servicios y tecnologías de la información, a fin de contribuir a la mejora continua, eficiencia y eficacia de los productos y servicios de la institución.

Unidad de Comunicación Social: Ejecuta estrategias de comunicación pública y fortalecimiento de la imagen institucional, y mantiene contacto con los medios de comunicación para la realización de ruedas de prensa y comunicados oficiales.

Unidad de Administración y Talento Humano: Es la encargada de Planificar, Organizar, dirigir y controlar el sistema integrado de desarrollo del talento humano, que aplica las normas expedidas por el Ministerio de Relaciones laborales.

Unidad Administrativa Financiera: Es la encargada de administrar, planificar, organizar, dirigir, coordinar y controlar eficientemente los recursos humanos, financieros y bienes materiales de la Secretaría de Territorio hábitat y vivienda para el cumplimiento de las actividades, proyectos y servicios programados.

Unidad de Tecnologías de la Información y Comunicación: Conforma el conjunto de recursos necesarios para manipular y/o gestionar la información: los computadores, los programas informáticos y las redes necesarias para convertirla, almacenarla, administrarla, transmitirla y encontrarla. De igual manera es el responsable de garantizar la dotación de infraestructura tecnológica, redes informáticas, telecomunicaciones y mantenimiento de los recursos requeridos para las operatividad y disponibilidad de todos los servicios que ofrece la institución, de los que se destaca el uso de sistemas informáticos ejecutados mediante internet y que son herramientas principales para el cumplimiento de las labores de los empleados de cada dependencia. Los funcionarios que laboran a nivel provincial en las diferentes unidades que forman parte de la Gobernación de Tungurahua, se detallan en la tabla 4.

Tabla 4: Distributivo de funcionarios

COBERTURA	DEPENDENCIA		Cantidad Funcionarios
	Nombre	Cant.	
Planta Central	Administrativo	1	6
	Archivo	1	1
	Comunicación	1	2
	Despacho	1	3
	Financiero	1	3
	Intendencia Policía	1	3
	Jurídico	1	2
	Planificación	1	1
	Seguridad	1	2
	Talento Humano	1	2
	TICS	1	1
Cantonal	Comisarías de Policía	9	18
	Jefaturas Políticas	9	18
Parroquial	Tenencias Políticas	43	86
TOTAL		**72**	**148**

Fuente: (elaboración propia)

Infraestructura tecnológica y de comunicaciones

La infraestructura tecnológica y de comunicaciones del edificio principal de la Gobernación de Tungurahua está distribuida en tres plantas, dentro de los cuales, están ubicados y distribuidos las oficinas de los distintos departamentos o unidades de gestión, dedicas a los procesos adjetivos y sustantivos de la institución, esta edificación tanto interna como externamente está dotada de conexiones tecnologías, redes y comunicación, servicio de internet, equipos de cómputo (uno por funcionario), teléfonos IP e impresoras (uno por dependencia), cuenta un circuito cerrado de televisión (CCTV). En el ámbito provincial en lo referente a las Comisarías de Policía, Jefaturas Políticas y Tenencias Políticas, cada oficina cuenta con una conexión individual de internet, dos computadores (uno por funcionario), una impresora (una por dependencia), dispone de un aplicativo o sitio

web y servicio correo electrónico institucional alojado en un servidor de propiedad gubernamental, como se detalla en la tabla 5, los detalles de las especificaciones técnicas de mencionados equipos reposan en los archivos de inventario de la Institución.

Los funcionarios para el desarrollo de sus actividades diarias, utilizan aplicaciones estatales como es el caso de eSIGEF y SPRYN del Ministerio de Finanzas, SIITH del Ministerio de Trabajo y software para el Manejo y Control de los Bienes y Existencias del Sector Público.

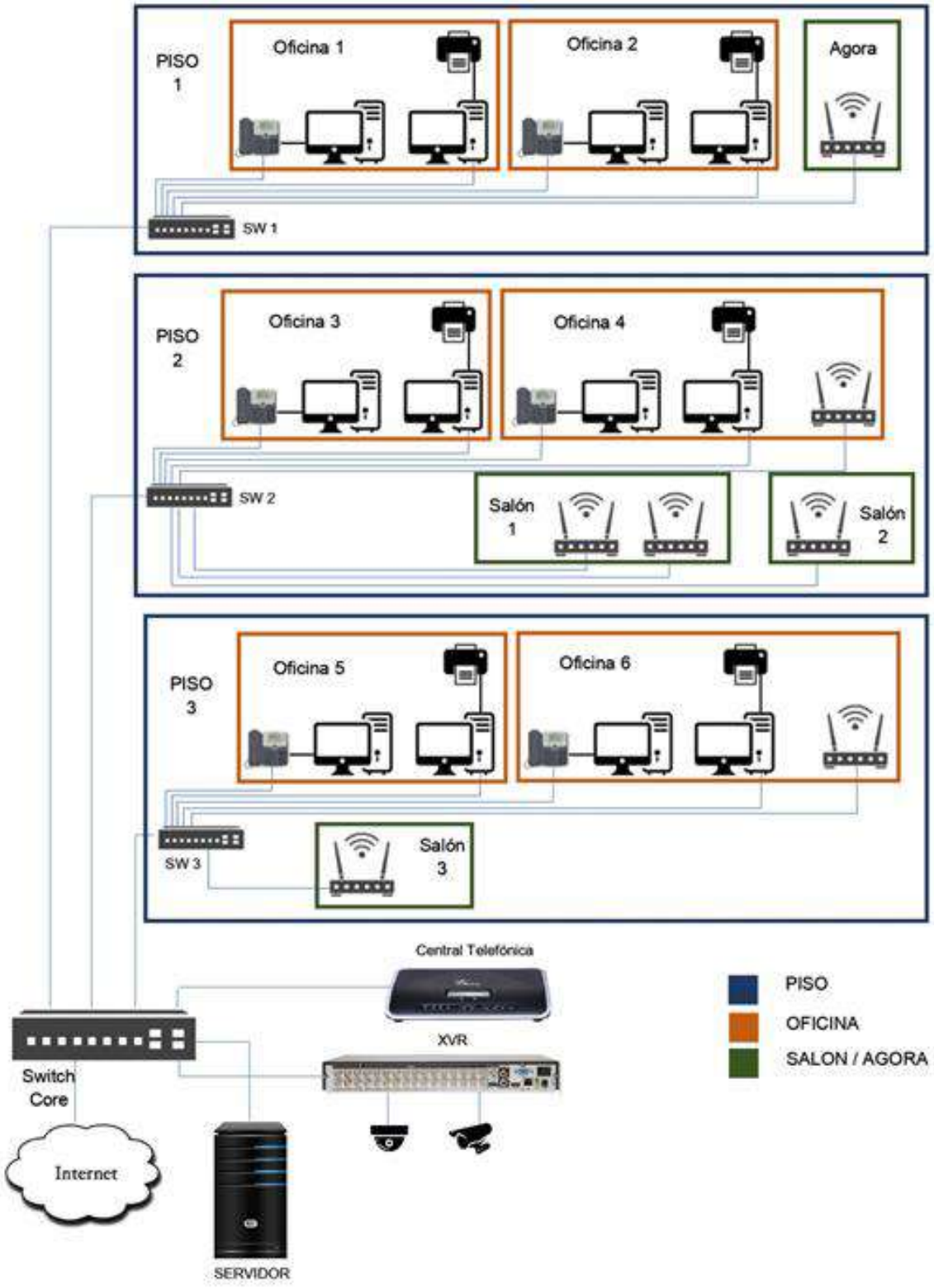
Tabla 5: Equipos informáticos, red, telefonía Ip, CCTV, servidores

EQUIPO	**MARCA**	**MODELO**	**CARACTERÍSTICAS**
SWITCH	D-Link	DGS-1210-24	24 puertos
Cableado	Nexxt	UTP Cat. 5	
Access Point	TP-Link		
Patch Panel	Nexxt	19 "	24 puertos, conectores RJ45 Cat. 5
XVR	Dahua	XVR4116HSX	16 canales
Cámara CCTV	Dahua	COOPER B1A21	2 mp
Computadora	Hp	COMPAQ 6005	AMD Athlon X2 B24 - HDD 500 - RAM 1
Impresora	Epson	L210	Sistema de Tinta
Central Telefónica	Grandstream	UCM-6102	
Teléfono IP	Grandstream	GXP280	
Servidor	HP		

Fuente: (elaboración propia)

Un resumen de lo anteriormente mencionado, se observa en la figura 7, el mapa *networking* y telefonía institucional.

Figura 7: Mapa de proceso



Fuente: (elaboración propia)

2.3.1.2 Levantamiento y evaluación de la información

En esta etapa, se identifican los criterios de ciberseguridad que se manejan en la institución, se aplica procedimientos que permitan revisar, evaluar y comprobar si sus recursos humanos, tecnológicos y de comunicaciones, se encuentran en condiciones seguras para su operatividad. Este procedimiento inicia con la evaluación de resultados, basados en la información obtenida en la fase de diagnóstico, que permitan determinar componentes objetivo (en adelante: objetivo) tanto de la infraestructura *networking*, componentes de red y comunicaciones, servidores, aplicaciones *web*, estaciones de trabajo y factor humano que se consideren críticos para la ciberseguridad y que infieran con un papel importante dentro de la institución.

Con el objetivo determinado, el proceso continúa con el reconocimiento, detección y análisis especifico de sus vulnerabilidades, mediante el empleo de varios tipos de instrumentos, como son:

- Encuestas: dirigidas a autoridades y funcionarios, que permiten obtener resultados sobre su nivel de conocimiento en ciberseguridad y el manejo de la seguridad de la información.
- *Checklist*: enfocado a recopilar datos requeridos sobre el estado actual de la infraestructura física, tecnológica, red y comunicaciones institucional;
- Herramientas de escaneo de vulnerabilidades para la infraestructura *networking* y servicios que brinda la institución.

Para el desarrollo de esta etapa, se utilizaron las siguientes herramientas:

- **Encuesta**

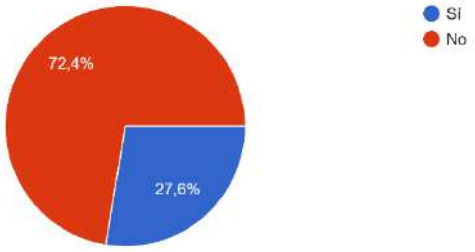
Las preguntas de las encuestas están enfocadas al y conocimiento general sobre ciberseguridad aplicado en la Gobernación de Tungurahua. En este instrumento, se considera como objetivo a 3 autoridades principales que laboran dentro del edificio central de la institución que son: Gobernador, Jefe Político del cantón Ambato y Comisario Nacional de Policía del cantón Ambato y a 87 funcionarios de la Gobernación de Tungurahua, se toma en cuenta al personal administrativo de

planta central, autoridades y asistentes de cantones y parroquias, es menester recalcar que existen asistentes que están encargados de realizar sus funciones en varias dependencias, por lo que se reducen el número de encuestas.

Encuesta a funcionarios

1) ¿Usted es capaz de identificar los efectos producidos por virus/*malware* informático?

Figura 8: Tabulación pregunta 1 funcionarios.



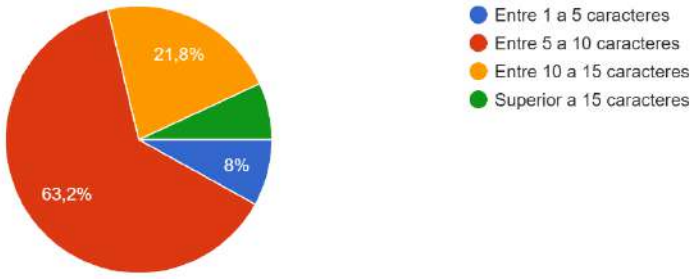
Fuente: elaboración propia

Interpretación:

Se observa que un 72,4% no identifica los efectos que produce un virus informático por lo que, se deduce que sus computadores llegan a contagiarse con virus informático que puede provocar una falla en la seguridad informática.

2) ¿Las contraseñas que usted usa tienen una longitud normalmente de?

Figura 9: Tabulación pregunta 2 funcionarios



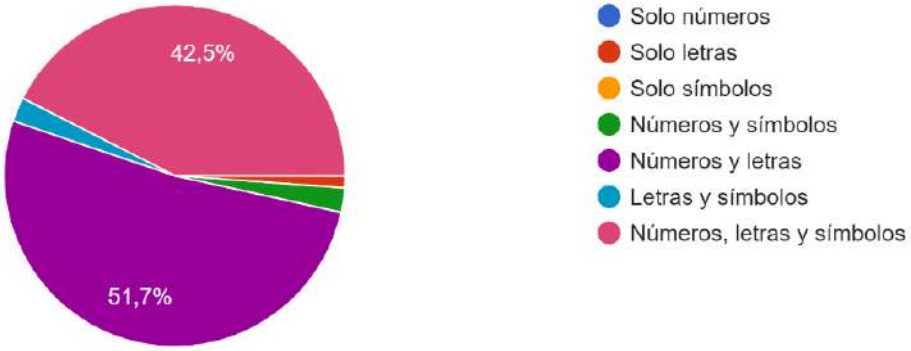
Fuente: elaboración propia

Interpretación:

Según las respuestas obtenidas, se aprecia que el 63,2% lo que simboliza más de la mitad de los funcionarios poseen contraseñas que poseen de 5 a 10 caracteres, lo que simboliza una longitud de contraseña estándar.

3) ¿Las contraseñas que usted implementa por lo general están compuestas de?

Figura 10: Tabulación pregunta 3 funcionarios



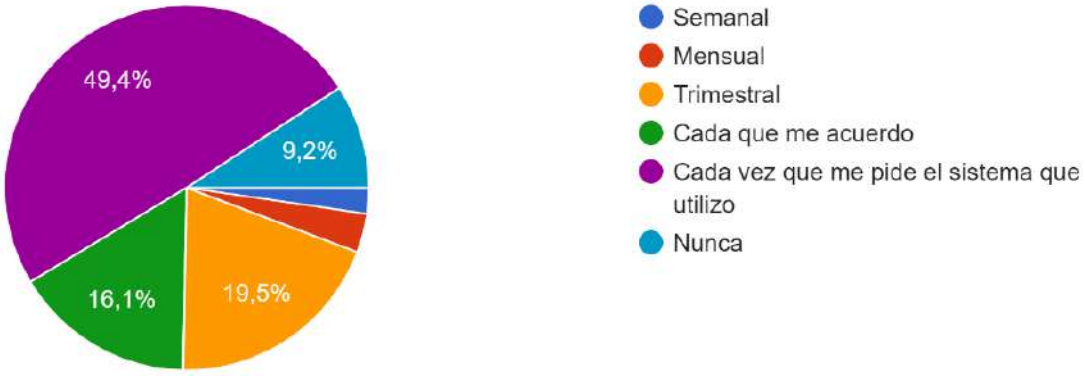
Fuente: elaboración propia

Interpretación:

Se observa que el 51,7% de funcionarios utilizan únicamente números y letras en sus contraseñas, considerado como un nivel de seguridad muy baja.

4) ¿Con que frecuencia cambia sus contraseñas?

Figura 11: Tabulación pregunta 4 funcionarios



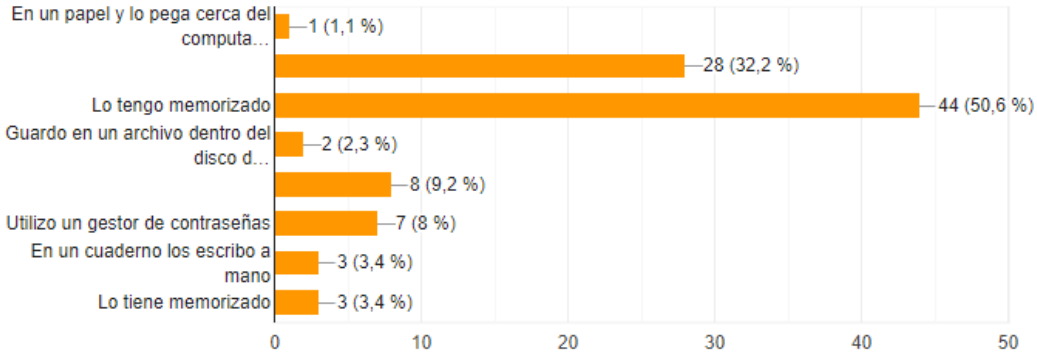
Fuente: elaboración propia

Interpretación:

Según la respuesta obtenidas el 49,4% que simboliza casi la mitad de funcionarios, actualiza su contraseña solo si el propio sistema lo considera necesario, lo que involucra una alerta de seguridad.

5) ¿Dónde almacena las contraseñas que utiliza?

Figura 12: Tabulación pregunta 5 funcionarios



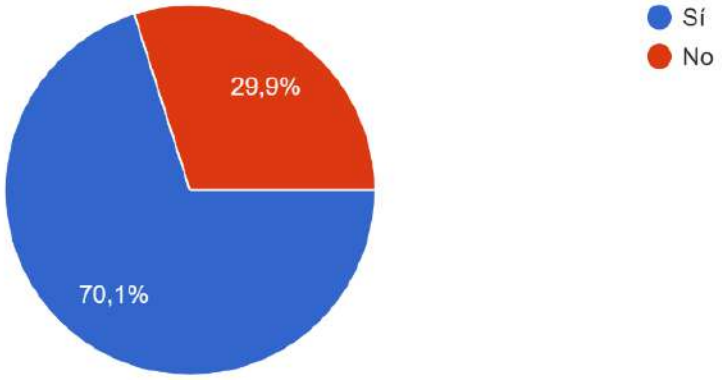
Fuente: elaboración propia

Interpretación:

En esta pregunta el funcionario seleccionaría más de una opción, por lo que el resultado, se clasificó de acuerdo a las combinaciones recibidas, la mitad de los funcionarios no almacenan sus contraseñas en ningún medio físico, mientras que el 32,2% de los funcionarios almacenan en un cuaderno sus contraseñas.

6) ¿Cree usted que las redes wifi públicas y/o gratuitas son peligrosas?

Figura 13: Tabulación pregunta 6 funcionarios



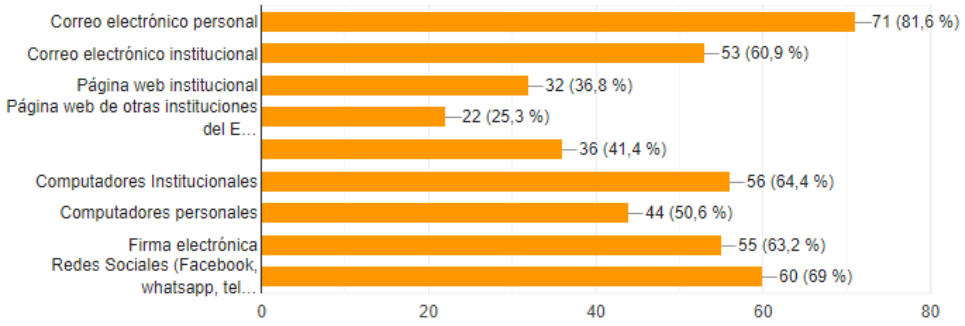
Fuente: elaboración propia

Interpretación:

Se observa que el 70,1% de los funcionarios considera que el uso de redes públicas es un potencial peligroso para el manejo de la información.

7) ¿Del siguiente listado selecciones que tecnologías utiliza para desarrollar las labores institucionales?

Figura 14: Tabulación pregunta 7 funcionarios



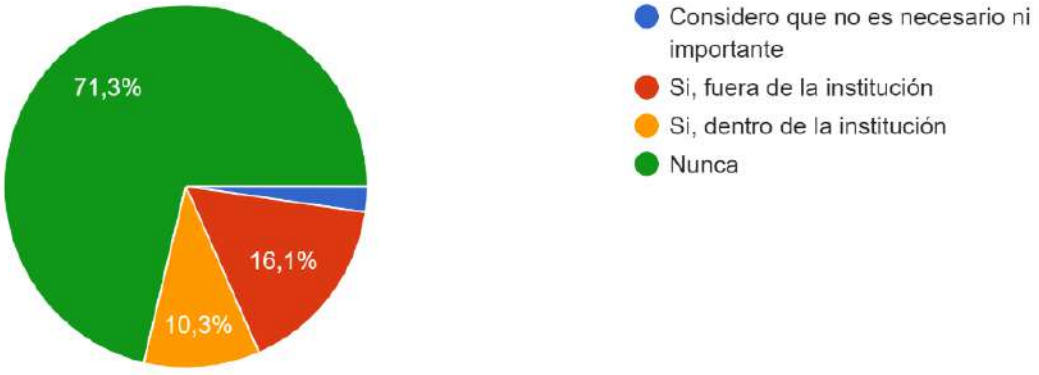
Fuente: elaboración propia

Interpretación:

En esta pregunta los funcionarios tenían la opción de seleccionar más de una opción, se obtiene como resultados que la tecnología que más usan para desarrollar sus labores institucionales es el correo electrónico, de igual manera el uso de redes sociales tiene una importancia significativa para los funcionarios.

8) ¿Ha recibido capacitación en temas relacionados a ciberseguridad?

Figura 15: Tabulación pregunta 8 funcionarios



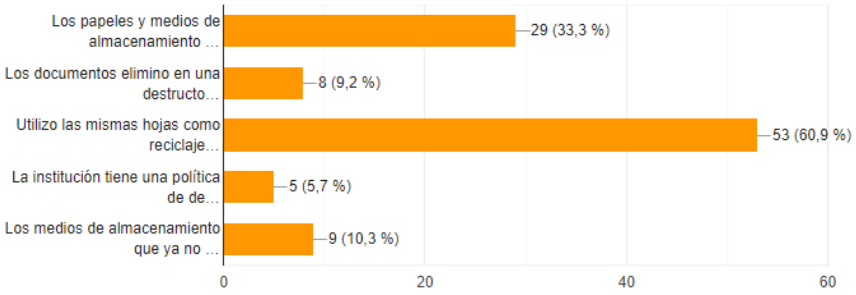
Fuente: elaboración propia

Interpretación:

Se observa que el 71,3% que representa a 62 funcionarios nunca ha recibido capacitación sobre la ciberseguridad, y en un 26,4% si está capacitado.

9) ¿Qué método utiliza para desechar la información o medios de almacenamientos (*flash memory*, cd) que no va a utilizar?

Figura 16: Tabulación pregunta 9 funcionarios



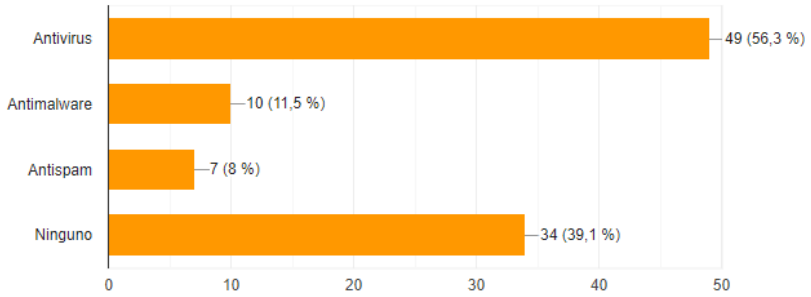
Fuente: elaboración propia

Interpretación:

Según la respuesta obtenida la mayoría de los funcionarios utilizan las hojas utilizadas como papel de reciclaje, además que, se concluye que luego de cumplir con esta acción, se arroja a la basura, así como los medios de almacenamientos externos.

10) ¿Conoce sobre algún sistema de protección contra ciberataques para computador o dispositivo móvil?

Figura 17: Tabulación pregunta 10 funcionarios



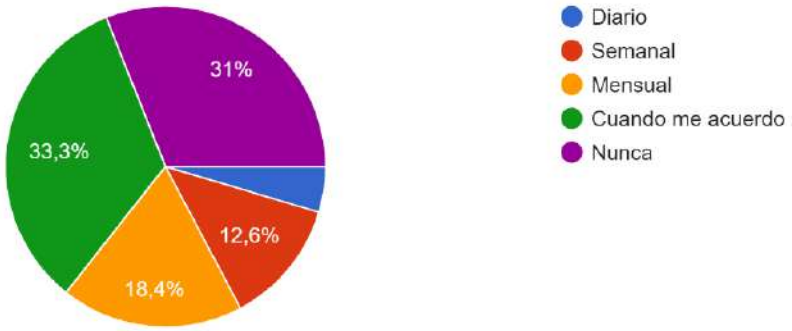
Fuente: elaboración propia

Interpretación:

Se concluye mediante las respuestas que la mayoría de los funcionarios solo maneja el antivirus como medio de protección para sus equipos de trabajo.

11) ¿Con qué frecuencia realiza copias de seguridad de su información y correo electrónico personal?

Figura 18: Tabulación pregunta 11 funcionarios



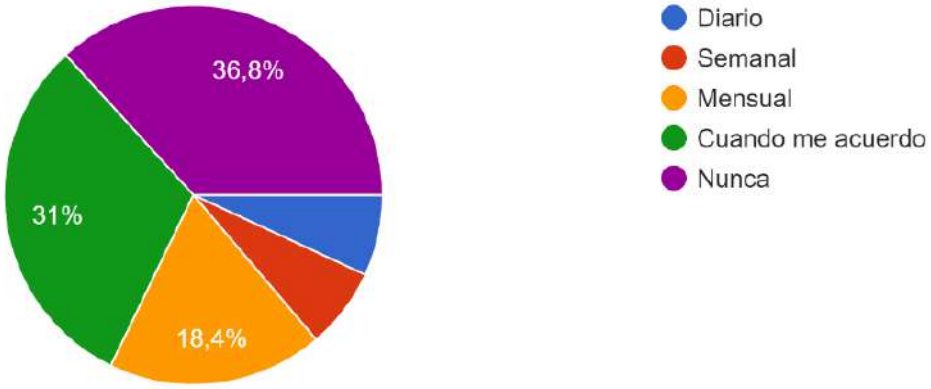
Fuente: elaboración propia

Interpretación:

Según la respuesta obtenida la información obtenida es respaldada por el 33,3% que son 29 funcionarios solo cuando se acuerdan de hacerlo, por lo que información de vital importancia para la institución se perdería.

12) ¿Con qué frecuencia realiza copias de seguridad de su información y correo electrónico institucional?

Figura 19: Tabulación pregunta 12 funcionarios



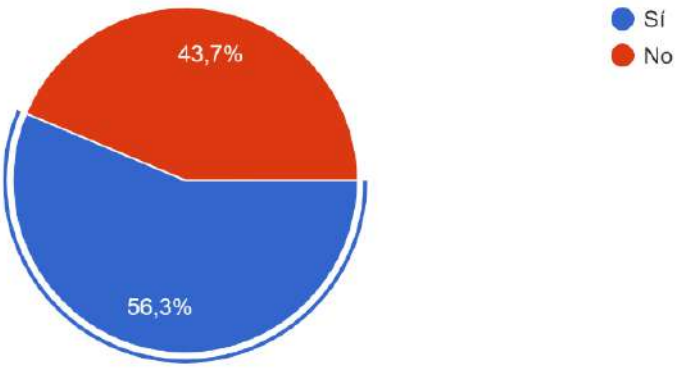
Fuente: elaboración propia

Interpretación:

Según la respuesta obtenida la información obtenida es respaldada por el 33,3% que son 29 funcionarios cuando se acuerdan de hacerlo, por lo que información personal se perdería.

13) ¿Conoce los principales peligros asociados con el uso del internet y tecnologías de la información?

Figura 20: Tabulación pregunta 13 funcionarios



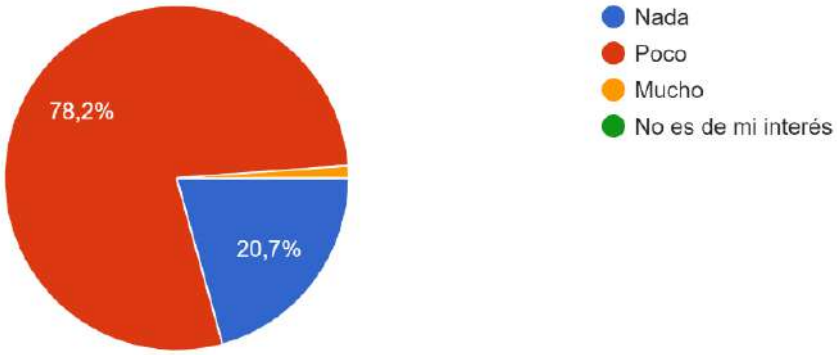
Fuente: elaboración propia

Interpretación:

Según las respuestas obtenidas más de la mitad de funcionarios desconoce los peligros que conlleva el uso del internet, asociadas a las tecnologías de información.

14) ¿Cuál es el grado de conocimiento que usted posee sobre ciberseguridad?

Figura 21: Tabulación pregunta 14 funcionarios



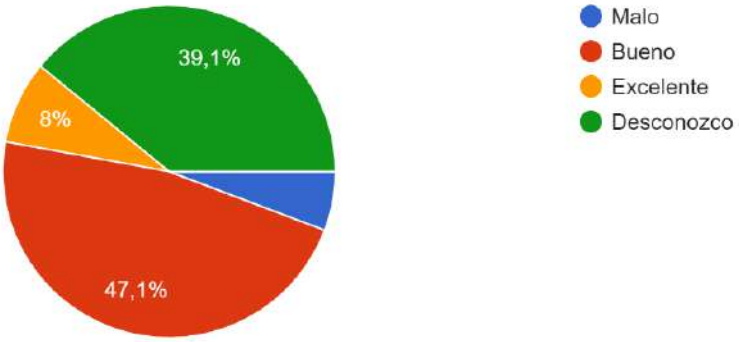
Fuente: elaboración propia

Interpretación:

Se concluye que la mayoría de los funcionarios que laboran en la Gobernación de Tungurahua no poseen conocimientos sobre Ciberseguridad.

15) ¿Según su criterio, el nivel de ciberseguridad en la institución es?

Figura 22: Tabulación pregunta 15 funcionarios



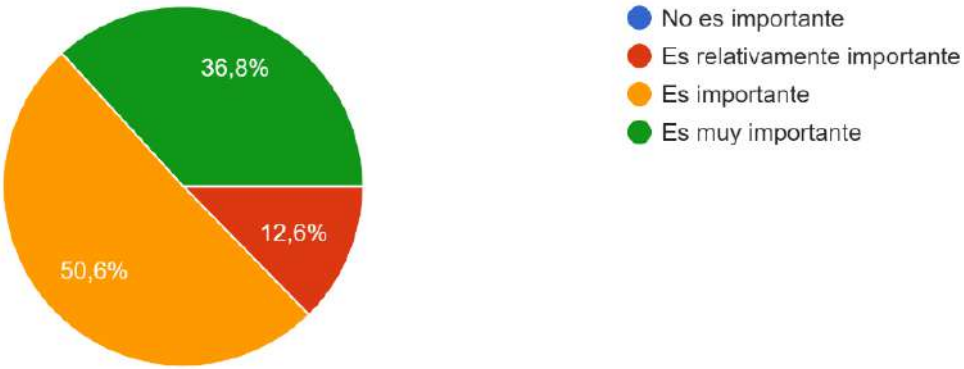
Fuente: elaboración propia

Interpretación:

Según las respuestas obtenidas, se concluye que solo 41 funcionarios consideran que el nivel de seguridad de la información que posee la Gobernación de Tungurahua es considera buena, mientras que 39 funcionarios consideran que la seguridad es deficiente.

16) ¿Cree que concientizar sobre la ciberseguridad es una medida básica para laborar en un ciberespacio más seguro?

Figura 23: Tabulación pregunta 16 funcionarios



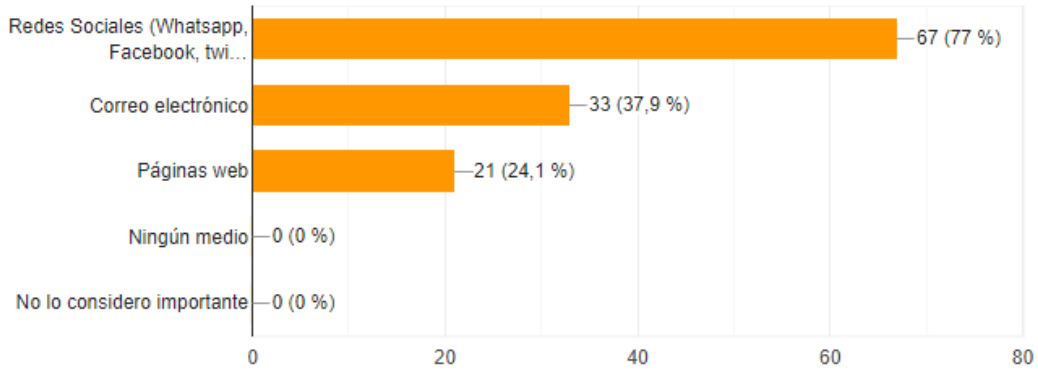
Fuente: elaboración propia

Interpretación:

Las respuestas indican que 87,4% que representa a 76 funcionarios consideran que una medida básica para mejorar la seguridad es concientizar sobre la ciberseguridad al personal que labora en la Gobernación de Tungurahua.

17) ¿A través de qué medio cree que se debería realizar campañas de concienciación sobre temas de ciberseguridad?

Figura 24: Tabulación pregunta 17 funcionarios



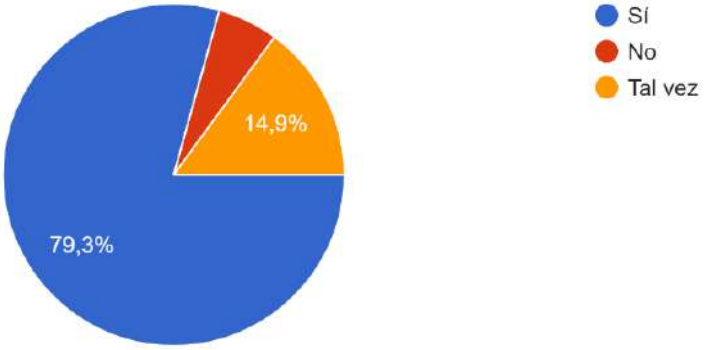
Fuente: elaboración propia

Interpretación:

Se concluye que gracias a las respuestas obtenidas que la mayoría de funcionarios (77%) preferiría usar las redes sociales como WhatsApp, Facebook, etc. Para capacitarse sobre temas de ciberseguridad.

18) ¿Le interesaría leer en su correo electrónico o redes sociales boletines o noticias que traten sobre temas de ciberseguridad?

Figura 25: Tabulación pregunta 18 funcionarios



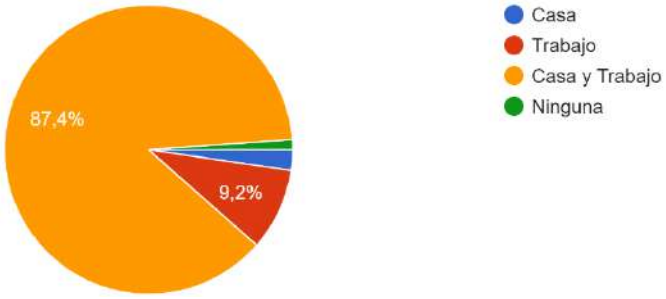
Fuente: elaboración propia

Interpretación:

Se concluye que la mayoría de funcionarios desea recibir noticias relacionadas con la ciberseguridad en la Gobernación de Tungurahua, por medio de correos electrónicos o mediante el uso de redes sociales.

19) ¿Cree usted que es necesario implementar medidas de ciberseguridad en?

Figura 26: Tabulación pregunta 19 funcionarios



Fuente: elaboración propia

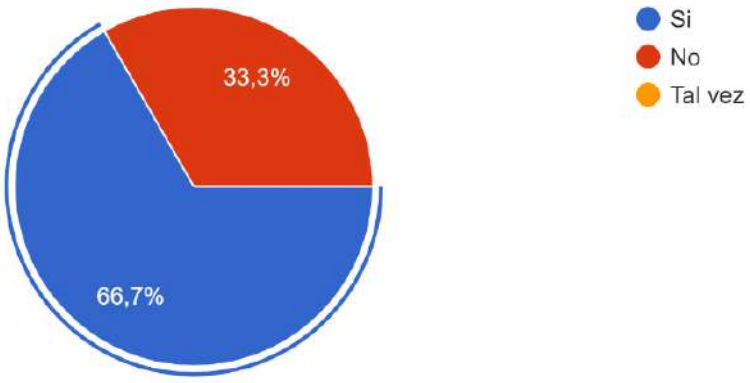
Interpretación:

Según las respuestas 76 funcionarios que representan al 87,4% creen necesaria la implementación de medidas de ciberseguridad tanto en su trabajo como en su hogar.

- **Encuestas de Autoridades.**

1) ¿Conoce usted si la institución cuenta con personal especializado en seguridad informática o un equipo de respuesta a incidentes de seguridad informática (CSIRT- Computer Security Incident & Response Team)?

Figura 27: Tabulación pregunta 1 Autoridades



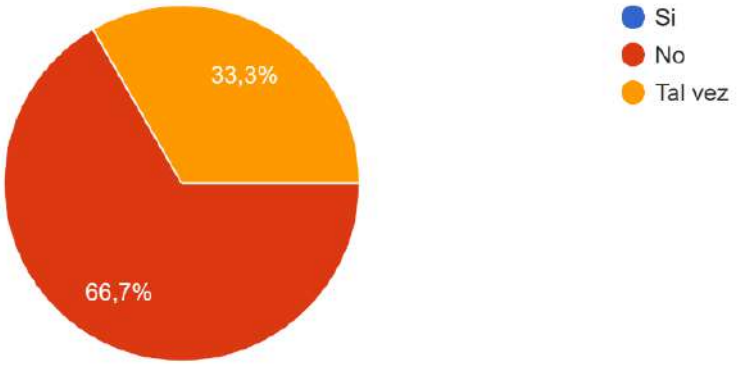
Fuente: elaboración propia

Interpretación:

Según las respuestas obtenidas dos de tres Autoridades tienen conocimiento sobre la existencia de personal y equipo de seguridad informática en la Gobernación de Tungurahua.

2) ¿Conoce usted si la Institución posee con una metodología para el análisis de vulnerabilidades y/o gestión de riesgo de ciberseguridad?

Figura 28: Tabulación pregunta 2 Autoridades



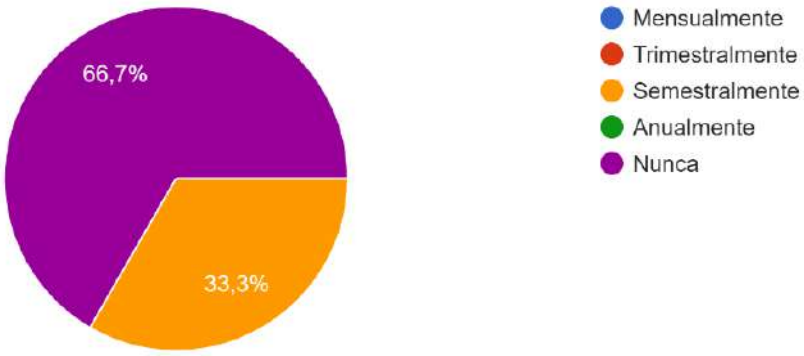
Fuente: elaboración propia

Interpretación:

Se concluye que las autoridades no conocen sobre la existencia de metodologías para la gestión de riesgos sobre la ciberseguridad en la Gobernación de Tungurahua.

3) ¿Con que periodo la institución realiza capacitaciones a los funcionarios sobre temas de ciberseguridad?

Figura 29: Tabulación pregunta 3 Autoridades



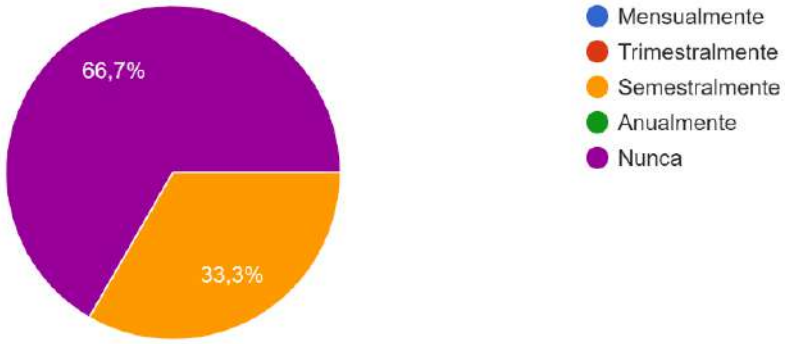
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por las autoridades, la Gobernación de Tungurahua no proporciona capacitaciones a sus trabajadores sobre temas de ciberseguridad.

4) ¿Con que frecuencia, se realizan auditorías externas o internas, aplicadas a la gestión de incidentes de seguridad informática o evaluaciones de riesgo de ciberseguridad?

Figura 30: Tabulación pregunta 4 Autoridades



Fuente: elaboración propia

Interpretación:

Se concluye que la Gobernación de Tungurahua no han realizado auditorias que permitan conocer el nivel de ciberseguridad existente.

5) ¿Existen servidores (equipo informático) dentro de la Institución?

Figura 31: Tabulación pregunta 5 Autoridades

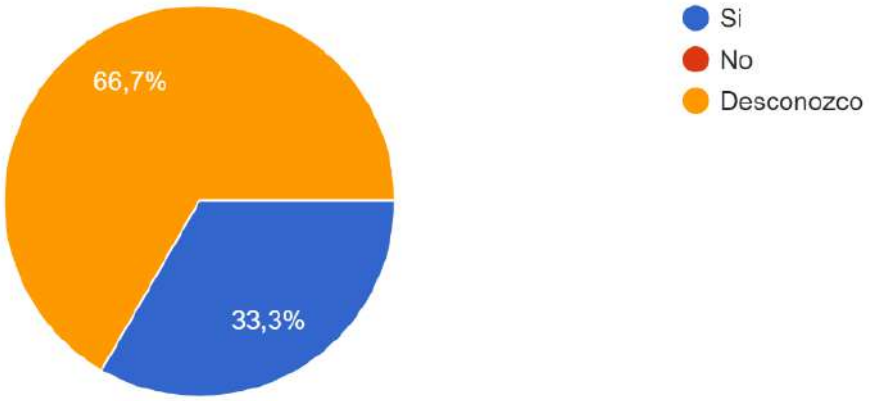
Fuente: elaboración propia

Interpretación:

Se concluye que las autoridades conocen la existencia de Servidores para el uso de labores al interior de la Gobernación de Tungurahua.

6) ¿Existen servidores (equipo informático) fuera de la Institución?

Figura 32: Tabulación pregunta 6 Autoridades



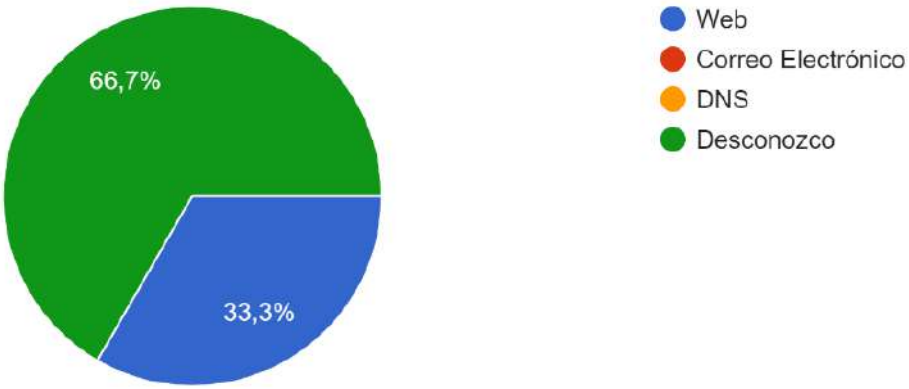
Fuente: elaboración propia

Interpretación:

Según las respuestas obtenidas la mayoría de Autoridades desconocen sobre el uso de servidores externos para el desarrollo de actividades competentes de la Gobernación de Tungurahua.

7) ¿Qué servidores existen dentro de la Institución?

Figura 33: Tabulación pregunta 7 Autoridades



Fuente: elaboración propia

Interpretación:

Mediante las respuestas recopiladas, se pude concluir que las autoridades conocen sobre el uso de servidores en la Gobernación de Tungurahua, sin embargo, desconocen su uso de manera específica.

8) ¿En qué lugar se encuentran los servidores (equipos informáticos) y equipos de comunicación de su Institución?

Figura 34: Tabulación pregunta 8 Autoridades

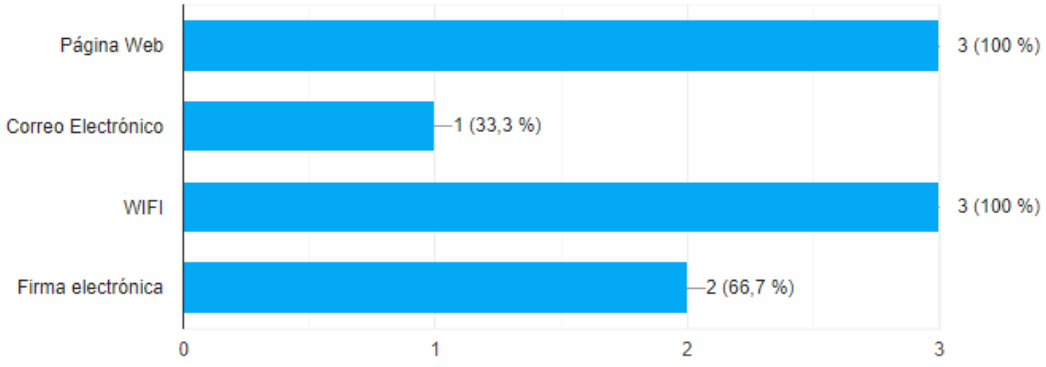
Fuente: elaboración propia

Interpretación:

Se concluye gracias a las respuestas obtenidas que las autoridades no conocen la ubicación exacta de los servidores al interior de la institución.

9) ¿Del siguiente listado, señale qué servicios tecnológicos dispone la institución?

Figura 35: Tabulación pregunta 9 Autoridades



Fuente: elaboración propia

Interpretación:

Según las respuestas obtenidas, se concluye que las autoridades únicamente conocen los servicios de Página *Web* y Wifi como los más usados en la Gobernación de Tungurahua.

10) ¿Del siguiente listado, señale qué servicios tecnológicos externos utiliza para sus labores en la institución?

Figura 36: Tabulación pregunta 10 Autoridades

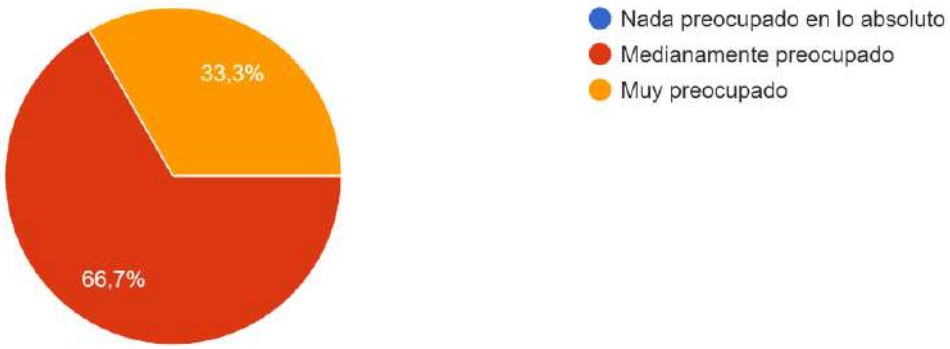
Fuente: elaboración propia

Interpretación:

Las Autoridades según sus respuestas utilizan mayoritariamente Quipux y WhatsApp para realizar sus actividades cuando no se encuentran en la institución.

11) ¿Cuál es su nivel de preocupación sobre los ciberataques a instituciones públicas?

Figura 37: Tabulación pregunta 11 Autoridades



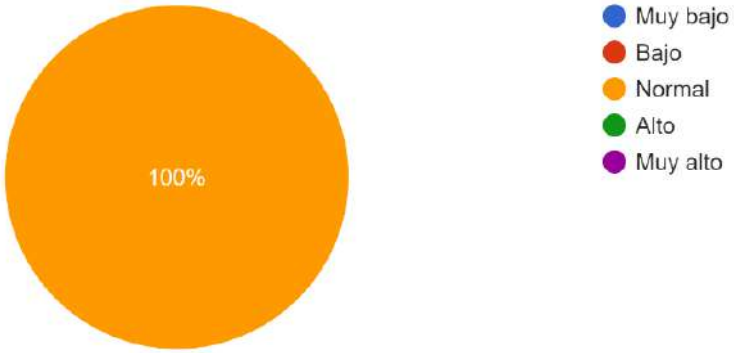
Fuente: elaboración propia

Interpretación:

Las respuestas obtenidas permiten concluir que a las autoridades de la Gobernación de Tungurahua no poseen una preocupación elevada sobre la posibilidad de ciberataques a instituciones públicas.

12) ¿Cuál cree usted que es el nivel de seguridad que actualmente dispone la gobernación de Tungurahua?

Figura 38: Tabulación pregunta 12 Autoridades



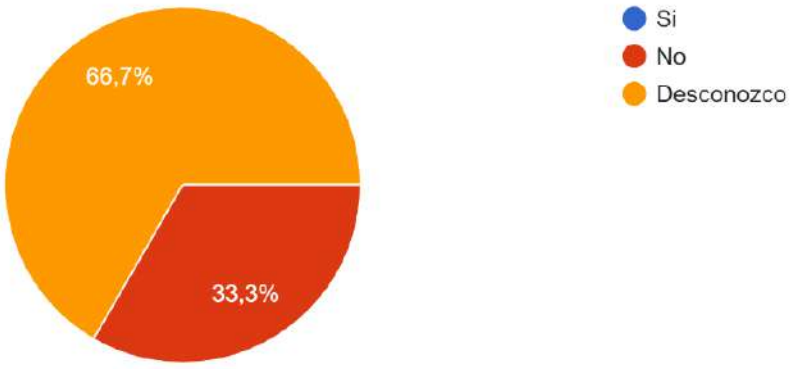
Fuente: elaboración propia

Interpretación:

Se concluye que el nivel de ciberseguridad que las Autoridades consideran presente en la Gobernación es normal.

13) ¿Conoce usted si la Institución cuenta con planes de contingencia, políticas de seguridad, reglamentos u otros documentos que regulen el uso de correo electrónico, gestión de contraseñas, uso del wifi, prevención de riesgos informáticos, entre otros?

Figura 39: Tabulación pregunta 13 Autoridades



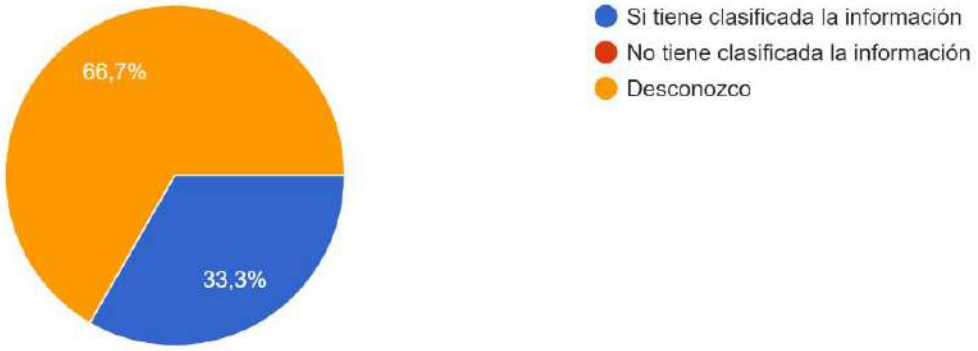
Fuente: elaboración propia

Interpretación:

Es preocupante ver que la mayoría de las Autoridades desconoce sobre la existencia de políticas de seguridad de la información o reglamentos que regulen el uso del correo electrónico.

14) ¿Conoce usted si la Institución tiene una correcta clasificación de la información producida, recibida y almacenada (Confidencial, pública, etc.)?

Figura 40: Tabulación pregunta 14 Autoridades



Fuente: elaboración propia

Interpretación:

Las diferentes respuestas obtenidas por las autoridades causan una seria preocupación, se desconocen técnicas de clasificación de la información producida.

- ***Checklist***

Esta herramienta esta creada y adaptada en base a los recursos tecnológicos y de comunicaciones con los que cuenta la institución pública, el listado está formado por una combinación de ítems basados en varios requisitos para el cumplimiento de normas y estándares como son: ISO 27001, IEEE 80211, ANSI/TIA/EIA-568-569-606, los mismos que proporcionan información que permite identificar vulnerabilidades en la administración e instalaciones de espacios de telecomunicaciones, cuartos de equipos, dispositivos informáticos, condiciones de seguridad física, implementación de controles, entre otros; tal como se observa en el Anexo 1.

- **Herramientas de escaneo de vulnerabilidades**

Permiten evaluar vulnerabilidades mediante la valoración de los controles de seguridad tanto internos como externos de los equipos, aplicaciones y sistemas objetivo, con la finalidad de proporcionar una amplia visión sobre las fallas existentes, lo que conlleva a identificar amenazas que impliquen un serio peligro para los activos de la institución.

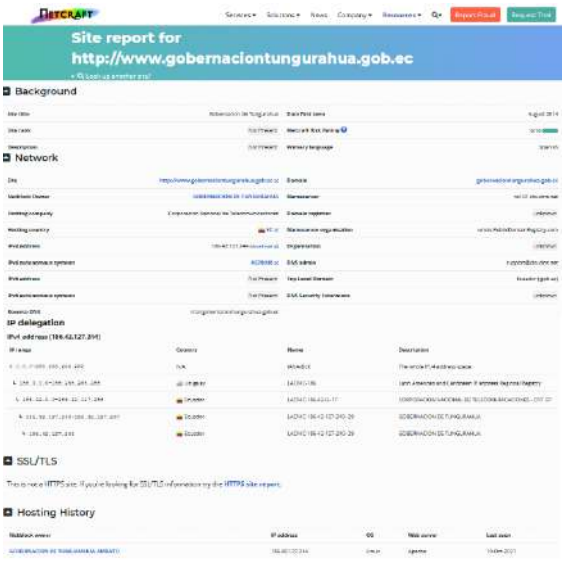
Entre las diversas herramientas *open source* y de pago existentes, para el desarrollo de este trabajo, se considera a Kali Linux y aplicaciones *web* como las opciones más viables para el desarrollo de esta etapa, están orientadas a tareas de auditoría e investigación en seguridad, descubrimiento de información, forense de equipos informáticos, pruebas de penetración, entre otros.

El empleo de las herramientas que tiene Kali Linux como *whatweb, whois, nmap, nessus, wireshark* y aplicaciones *web* como *netcraf, wappalyzer, sucuri, wpsec* y *hacker target*, permiten recolectar la mayor cantidad de datos relevantes de los objetivos de evaluación, como son direcciones IP, servidores, escaneo de puertos, versión del sistema operativo; con los datos obtenidos, se procede a diagnosticar, identificar y analizar las vulnerabilidades encontradas. Los resultados obtenidos en esta fase se detallan, a continuación:

Netcraft – Wappalyzer:

Con el uso de estas herramientas, se obtiene información respecto a la lista de subdominios, gestor de contenidos, servidor *web*, lenguaje de programación, seguridades con certificados SSL / TLS, base de datos y demás tecnologías asociadas al sitio *web* institucional, como se muestra en la figura 41.

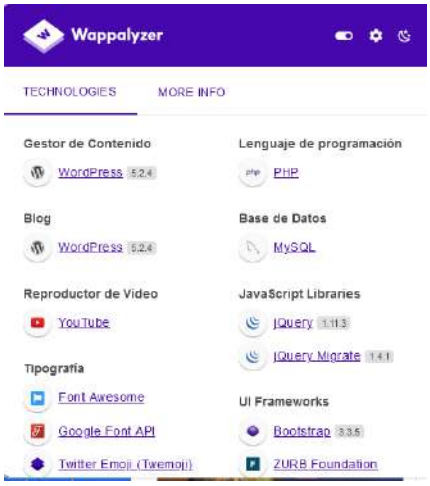
Figura 41: Información del sitio *web* reportado por Netcraf



Fuente: elaboración propia

Este *plugin Wappalyzer* de navegadores de internet permite obtener información del sitio *web* en el que se navega, en el caso con la dirección url de la institución https://www.gobernaciontungurahua.gob.ec, presenta la información representada en la figura 42.

Figura 42: Información del sitio *web* reportado por Wappalyzer

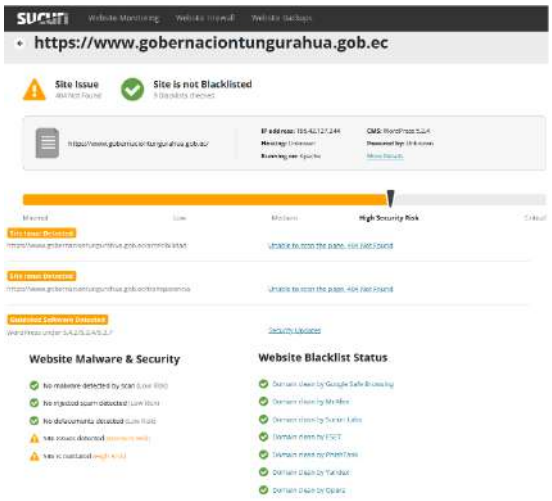


Fuente: elaboración propia

Sucuri:

Esta herramienta escanea el sitio *web* sin importar su plataforma de creación WordPress, Joomla, Drupal, etc., y permite identificar *malware*, estado de lista negra, SPAM inyectado y desconfiguraciones, como se observa en la imagen 43.

Figura 43: Información, vulnerabilidades y problemas encontrados del sitio *web* reportado por Sucuri



Fuente: elaboración propia

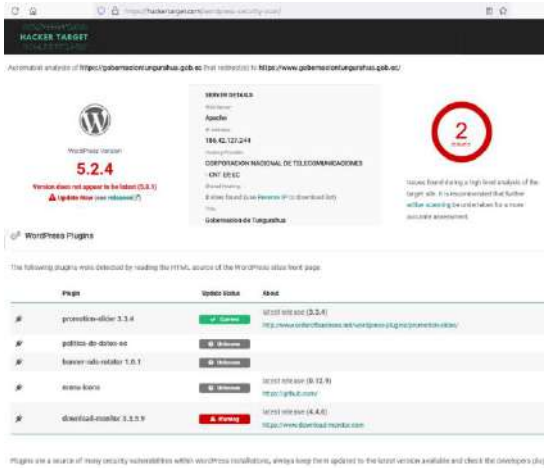
Wpsec - Hackertarget - Ssllabs - What*web*

Los resultados de la aplicación de las herramientas anteriores determinan, que el sitio *web* institucional es realizado en WordPress, por consecuencia, se utiliza estas aplicaciones *web*, mediante las cuales, se identifica los componentes, complementos y *plugin*, compara sus versiones con las actuales y se obtiene la siguiente información de este proceso, se presenta las vulnerabilidades encontradas, como se observa en la imagen 44-48.

Figura 44: Información y vulnerabilidades encontradas del sitio *web* reportado por Wpsec

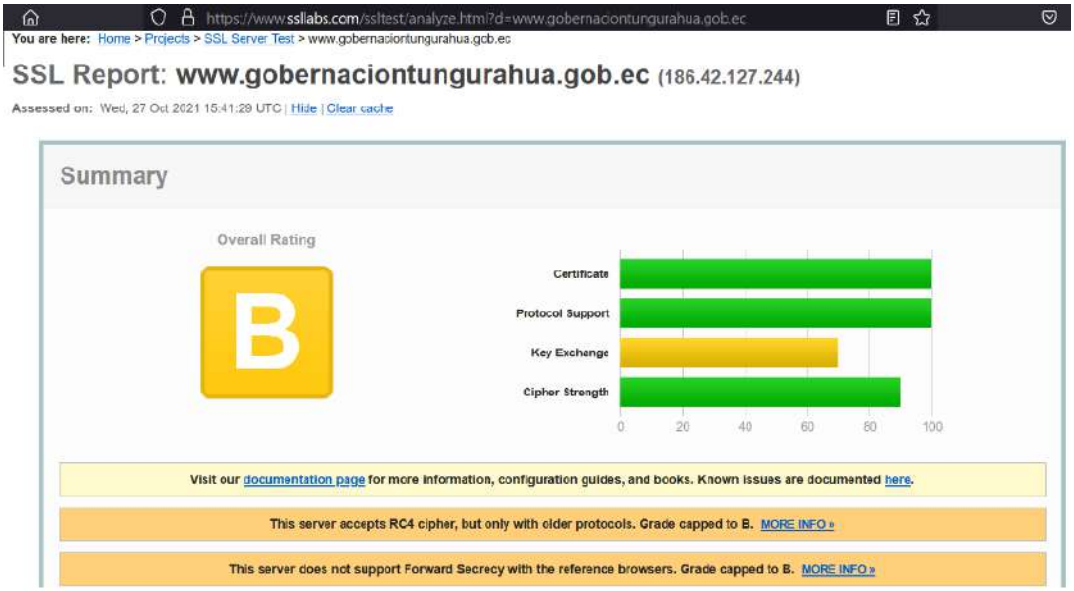
Fuente: elaboración propia

Figura 45: Información y vulnerabilidades encontradas del sitio *web* reportado por *Hackertarget*



Fuente: elaboración propia

Figura 46: Reporte del sitio *web*, con la herramienta Ssllabs (Qualys)



Fuente: elaboración propia

Figura 47: Protocolos del sitio *web*, reportado por Ssllabs (Qualys)

Fuente: elaboración propia

Figura 48: Información y vulnerabilidades encontradas en el sitio *web*, reportado por el comando *Whatweb* de Kali Linux

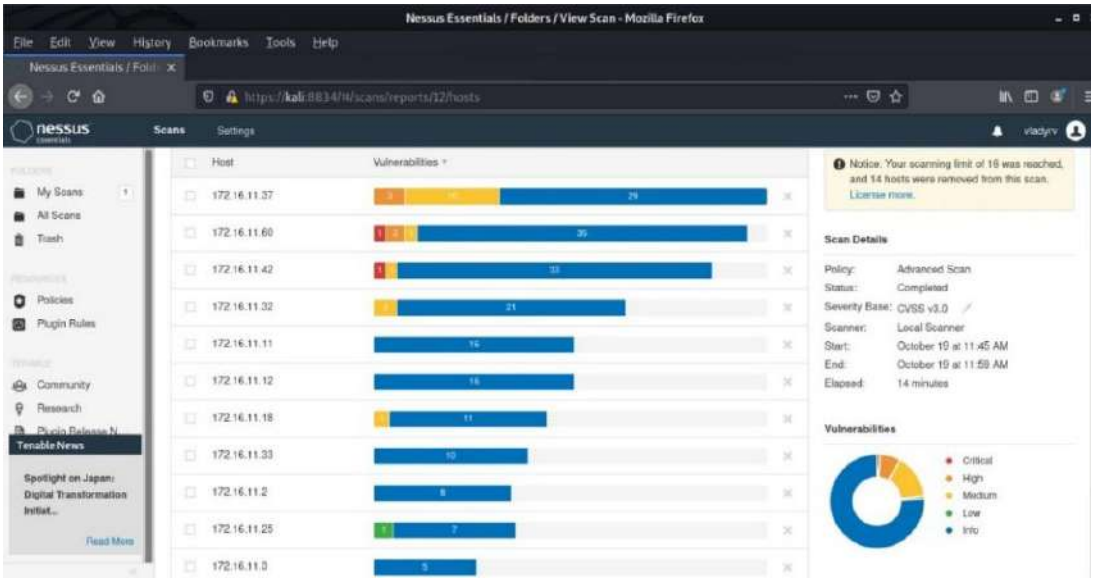
Fuente: elaboración propia

Nessus

La instalación de esta herramienta en Kali Linux, proporciona información que permite evaluar e identificar vulnerabilidades, compatibilidades, *malware* y configuración sobre los activos informáticos y comunicación, dispositivos de red, sistemas operativos, servidores y aplicativos *webs* de la institución. La información obtenida se muestra, a continuación.

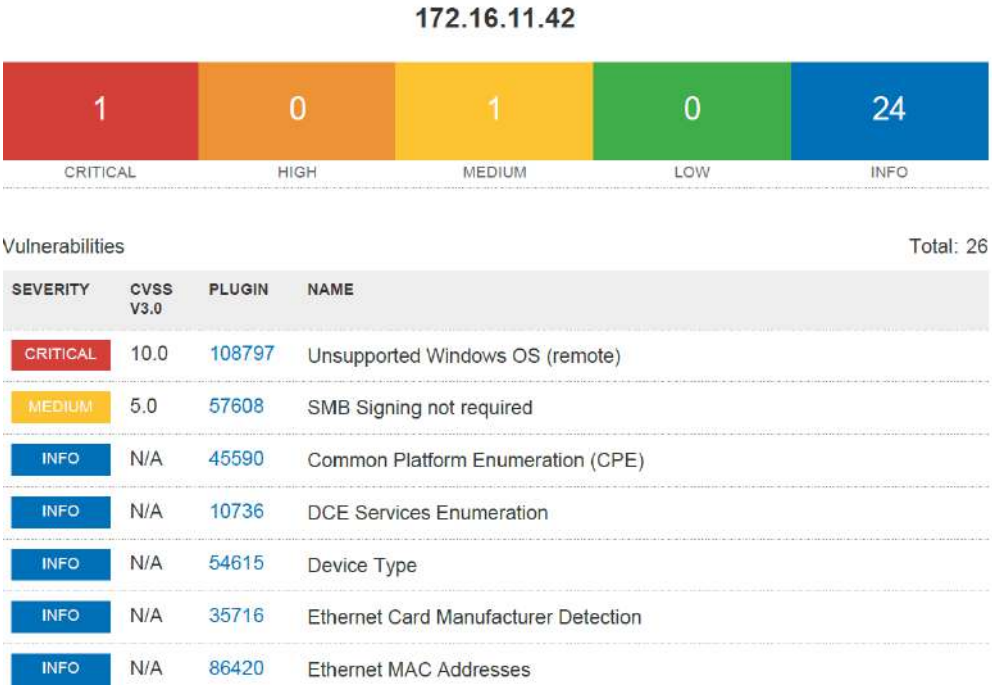
Escaneo de la red

Figura 49: Escaneo de equipos de la red con información de vulnerabilidades reportada por Nessus



Fuente: elaboración propia

Figura 50: Vulnerabilidades en computadores reportada por Nessus vulnerabilidades dispositivo de red



172.16.11.42

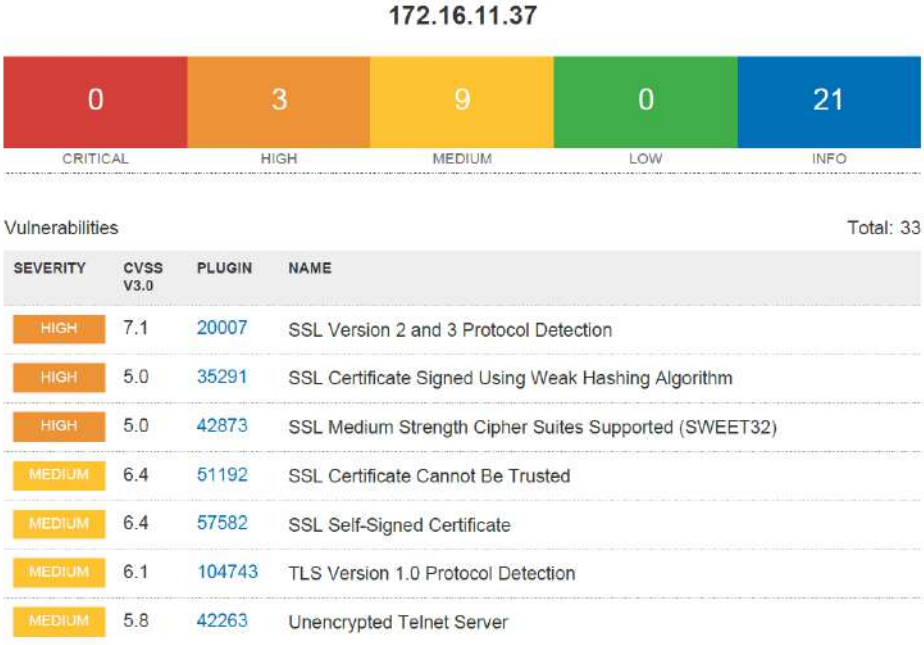
1	0	1	0	24
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 26

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses

Fuente: elaboración propia

Figura 51: Vulnerabilidades encontradas en equipo de comunicación Access Point reportada por Nessus



172.16.11.37

0	3	9	0	21
CRITICAL	HIGH	MEDIUM	LOW	INFO

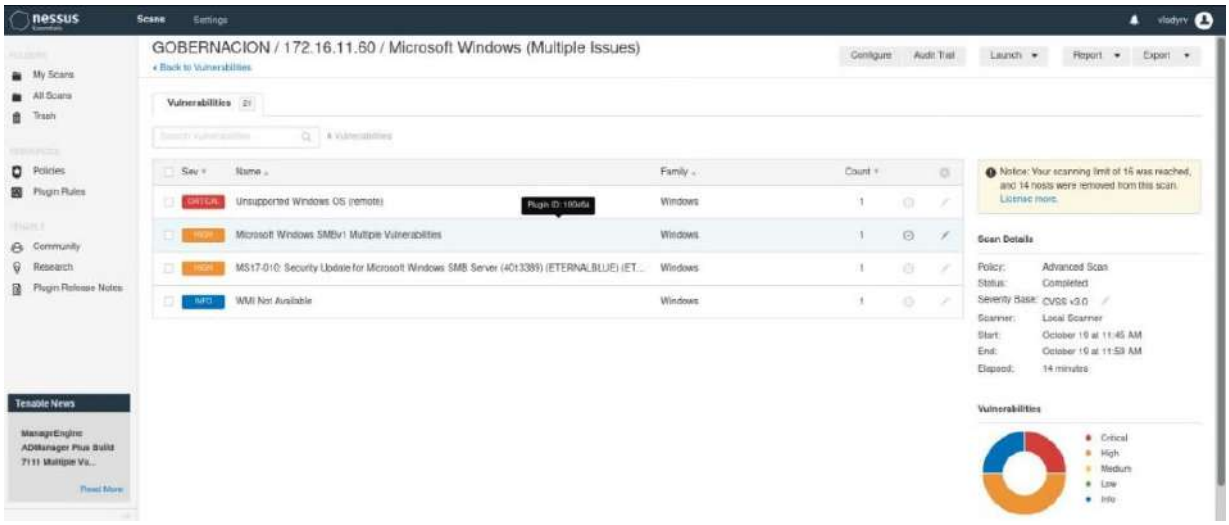
Vulnerabilities — Total: 33

SEVERITY	CVSS V3.0	PLUGIN	NAME
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
HIGH	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	42263	Unencrypted Telnet Server

Fuente: elaboración propia

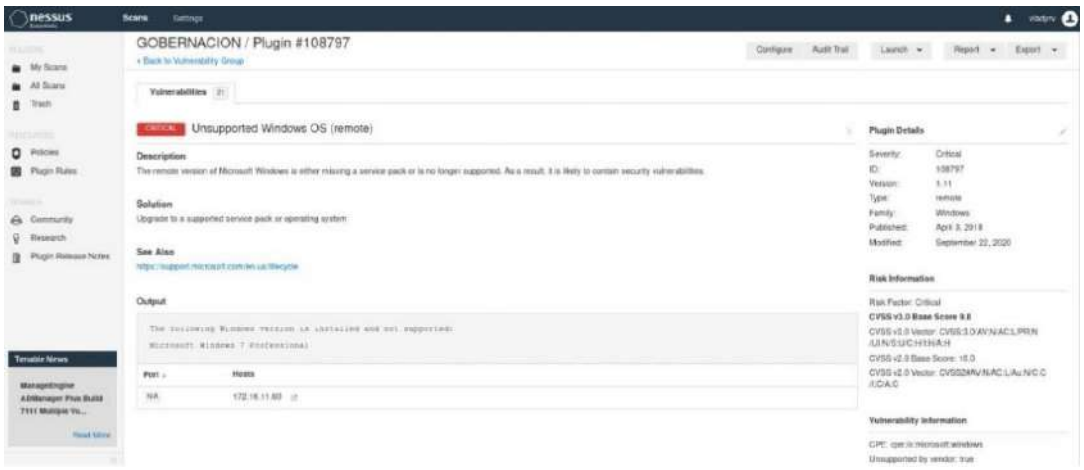
Vulnerabilidades computador

Figura 52: Vulnerabilidades encontradas en un computador reportada por Nessus



Fuente: elaboración propia

Figura 53: Evidencia de vulnerabilidad critica en computador reportada por Nessus



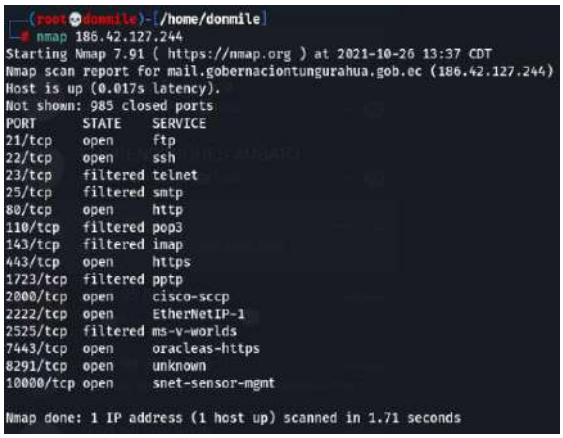
Fuente: elaboración propia

NMAP

Con la aplicación de esta herramienta *open source,* se logra escanear el objetivo, conocer sus puertos, detectar remotamente los sistemas operativos o aplicaciones en ejecución, tipo de *Firewall* y filtros de paquetes que utilizan. Se aplican varios comandos y *script*s propios de la herramienta, con la información resultante, se descubren e identifican vulnerabilidades presentes tanto en la red como en equipos y aplicaciones.

Se realiza un barrido de puertos para descubrir la cantidad de puertos y servicios que funcionan en el servidor *web* como lo muestra en la figura 54.

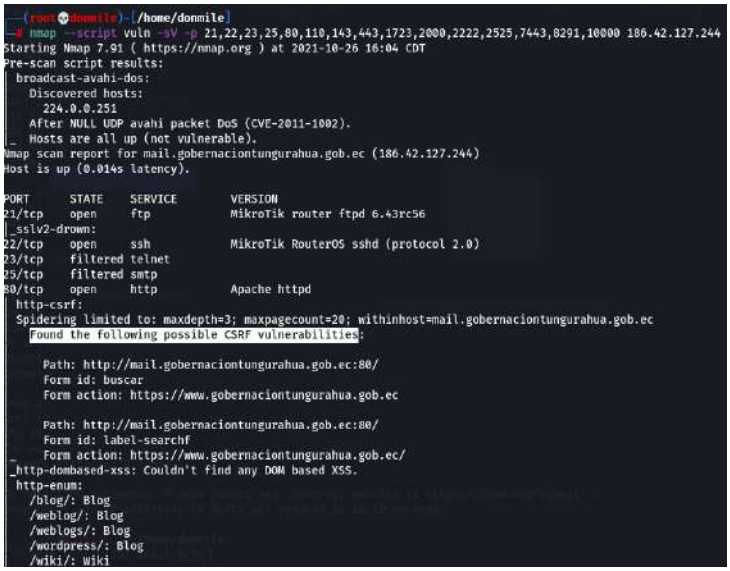
Figura 54: Puertos en funcionamiento del servidor *web*



Fuente: elaboración propia

El *script* vuln de Nmap, permite realizar un análisis de vulnerabilidades del servidor y mostrar los puertos filtrados, como se observa en la Figura 55.

Figura 55: Vulnerabilidades del servidor *web* y de correo



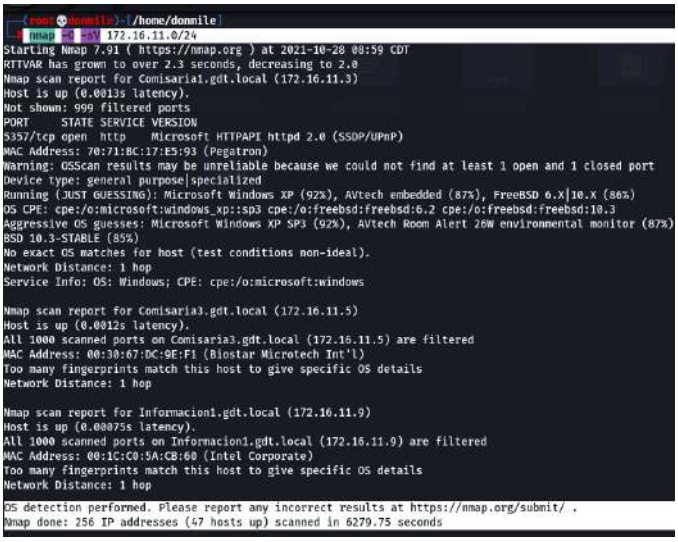
Fuente: elaboración propia

Figura 56: Vulnerabilidades del servidor *web* y en uno de sus puertos

Fuente: elaboración propia

Con la aplicación de esta herramienta, se descubren en total 47 equipos conectados a la red institucional, detallados con el sistema operativo, puertos abiertos y versiones, impresoras, computadoras, teléfonos Ip, dispositivos de CCTV y de comunicaciones.

Figura 57: Descubrimiento de 47 equipos de la red institucional



Fuente: elaboración propia

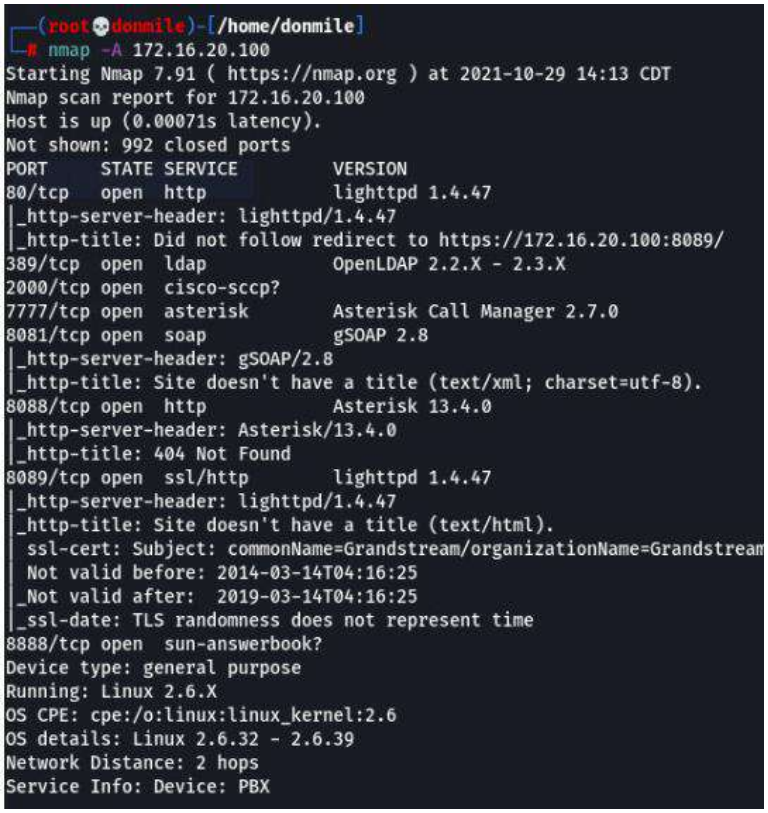
Figura 58: Descubrimiento dispositivos del sistema de video vigilancia

```
Nmap scan report for DVR1.gdt.local (172.16.11.11)
Host is up (0.0052s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
80/tcp  open  http
554/tcp open  rtsp    Lorex IP camera rtspd
1 service unrecognized despite returning data. If you know the service/version
e :
SF-Port80-TCP:V=7.91%I=7%D=10/28%Time=617AAEAA%P=x86_64-pc-linux-gnu%r(Get
SF:Request,10F8,"HTTP/1\.1\x20200\x20OK\r\nCONNECTION:\x20close\r\nDate:\x
SF:20Thu,\x2028\x20Oct\x202021\x2009:10:23\x20GMT\r\nLast-Modified:\x20Tue
SF:,\x2007\x20Mar\x202017\x2012:30:18\x20GMT\r\nEtag:\x20\"1488889818:370c
SF:\"\r\nCONTENT-LENGTH:\x2014092\r\nP3P:\x20CP=CAO\x20PSA\x20OUR\r\nCONTE
SF:NT-TYPE:\x20text/html\r\n\r\n<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//D
SF:TD\x20XHTML\x201\.0\x20Strict//EN\"\x20\"http://www\.w3\.org/TR/xhtml1/
SF:DTD/xhtml1-strict\.dtd\">\x20<html>\x20<head>\x20<title>WEB\x20SERVICE<
```

Fuente: elaboración propia

Con la ejecución del comando namp -A, se visualiza las características y los puertos abiertos de la central telefónica.

Figura 59: Descubrimiento central telefónica



```
┌──(root💀donmile)-[/home/donmile]
└─# nmap -A 172.16.20.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-29 14:13 CDT
Nmap scan report for 172.16.20.100
Host is up (0.00071s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE         VERSION
80/tcp   open  http            lighttpd 1.4.47
|_http-server-header: lighttpd/1.4.47
|_http-title: Did not follow redirect to https://172.16.20.100:8089/
389/tcp  open  ldap            OpenLDAP 2.2.X - 2.3.X
2000/tcp open  cisco-sccp?
7777/tcp open  asterisk        Asterisk Call Manager 2.7.0
8081/tcp open  soap            gSOAP 2.8
|_http-server-header: gSOAP/2.8
|_http-title: Site doesn't have a title (text/xml; charset=utf-8).
8088/tcp open  http            Asterisk 13.4.0
|_http-server-header: Asterisk/13.4.0
|_http-title: 404 Not Found
8089/tcp open  ssl/http        lighttpd 1.4.47
|_http-server-header: lighttpd/1.4.47
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Grandstream/organizationName=Grandstream
| Not valid before: 2014-03-14T04:16:25
|_Not valid after:  2019-03-14T04:16:25
|_ssl-date: TLS randomness does not represent time
8888/tcp open  sun-answerbook?
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.39
Network Distance: 2 hops
Service Info: Device: PBX
```

Fuente: elaboración propia

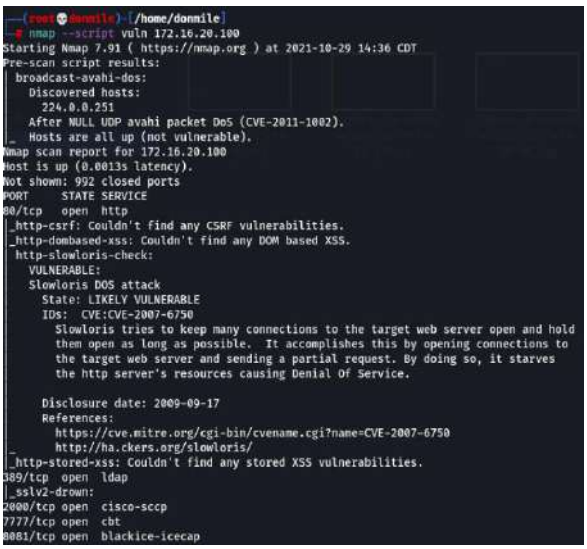
El comando svmap permite identificar los dispositivos SIP conectados a la central telefónica

Figura 60: Identificación dispositivos SIP con svmap

Fuente: elaboración propia

Con la aplicación del comando nmap –*script* vuln, se observa las vulnerabilidades que presentan los puertos de la central telefónica como se observa en la figura 61.

Figura 61: Vulnerabilidades en los puertos de la central telefónica (parte 1)



Fuente: elaboración propia

Figura 62: Vulnerabilidades en los puertos de la central telefónica (parte 2)

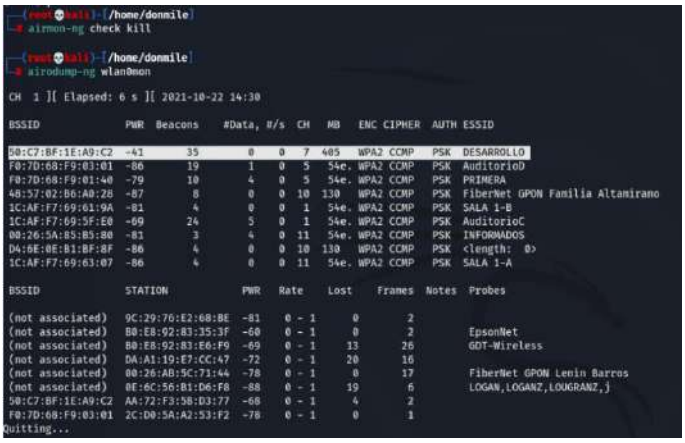
Fuente: elaboración propia

Los puertos 80 y 8089 presentan vulnerabilidades (CVE-2007-6750 y CVE-2015-4000) del protocolo TLS y falla en transmitir correctamente una opción de conjunto de cifrado DHE_EXPORT respectivamente.

***Aircrack*-ng:**

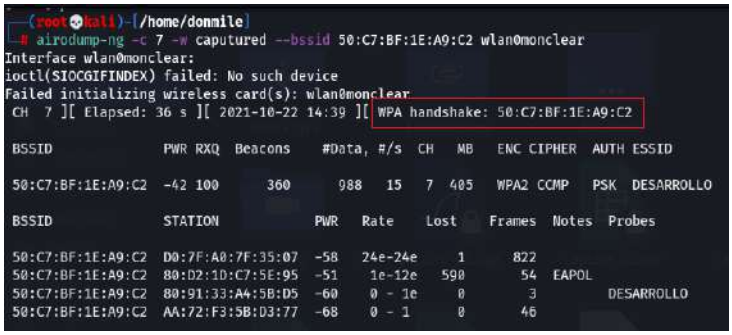
Mediante el uso de esta suite de herramientas de Kali Linux, cuya utilidad es la de auditar y monitorizar en tiempo real redes inalámbricas Wi-Fi, se ejecuta los comandos necesarios con la finalidad de determinar el nivel de seguridad respecto a la robustez de las contraseñas utilizadas en los dispositivos de comunicación inalámbrica distribuidos en todo el edificio de la institución. En las imágenes detalladas, a continuación, se describe cada uno de los pasos realizados para descifrar la contraseña de acceso a una de las redes wifi de la institución y determinar si existen vulnerabilidades en la seguridad wifi.

Figura 63: Inicio de proceso de detección de redes



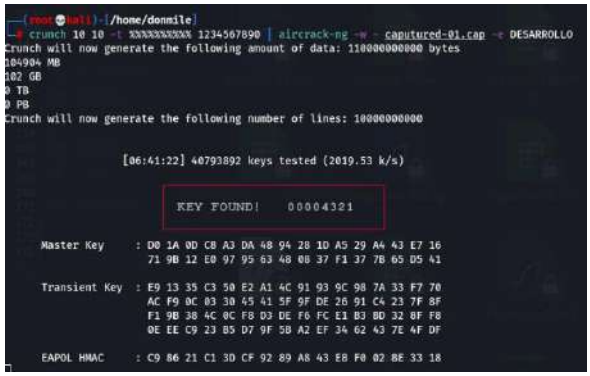
Fuente: elaboración propia

Figura 64: Proceso de validación de nuevo ingreso de un usuario al dispositivo



Fuente: elaboración propia.

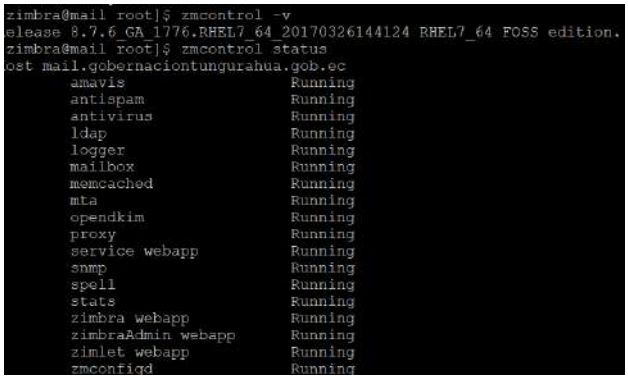
Figura 65: Evidencia de contraseña encontrada



Fuente: elaboración propia.

Con la ejecución del comando zmcontrol -v, se visualiza la versión instalada del servicio de correo electrónico Zimbra y el comando zmcontrol status permite observar los servicios ejecutados.

Figura 66: Detección de correo zimbra

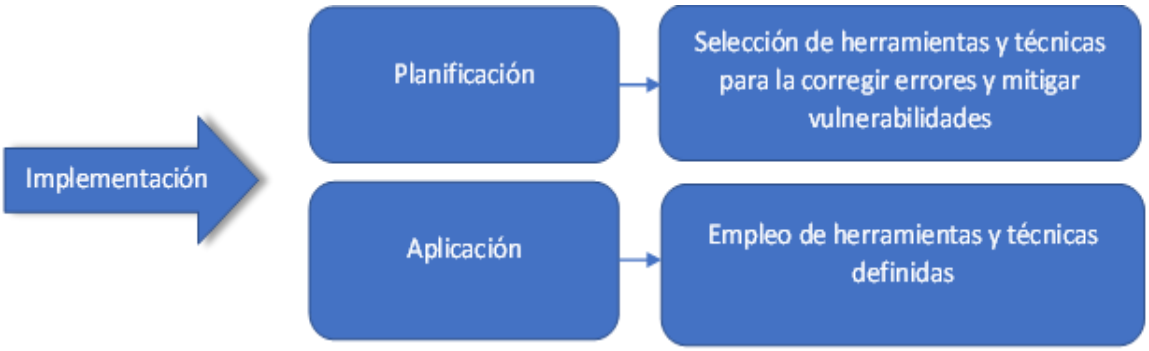


Fuente: elaboración propia.

2.3.2 Implementación

Con la información obtenida en la fase anterior es momento de definir e implementar técnicas y herramientas a utilizar para corregir fallas y/o mitigar vulnerabilidades encontradas. Es preciso tener presente que al existir herramientas de pago que permitan realizar este proceso de manera óptima, se tiene como alternativa otras opciones propuestas que ayuden a este proceso, esto depende de la parte económica de la institución. La importancia de esta etapa esta basada en la implementación de técnicas y ejecución instrumentos que mejoren la ciberseguridad de la institución, para cumplir con este objetivo se definen dos fases como se observa en la figura 67.

Figura 67: Etapa de Implementación



Fuente: elaboración propia.

2.3.2.1 Planificación

Esta fase tiene como finalidad registrar toda la información relativa a los puntos vulnerables, fallas, errores y/o problemas detectados en la etapa anterior, acompañados de soluciones que mitiguen las vulnerabilidades encontradas, para cumplir con este objetivo, se elaboran dos tablas, en donde especifican campos con la siguiente información:

Tabla de determinación de vulnerabilidades basados en herramientas

- Herramienta: Seleccionar el instrumento utilizado en la fase anterior: encuestas, *checklist* y tipo de aplicación de escaneo de vulnerabilidades
- Problema: Resumen del problema o vulnerabilidad localizada

- Afectación: Definir si el problema afecta a la integridad, confidencialidad y/o disponibilidad de información y/o servicio
- Gravedad: Los incidentes son asociados a las recomendaciones que dan las normas estándares ISO 27001, IEEE 80211, ANSI/TIA/EIA-568-569-606 y a los siguientes niveles de gravedad:
    - Alto: Interrupción de servicio, cuentas sin control de privilegios, acceso no autorizado a equipos o información, infraestructura considerada como crítica, software sin licenciamiento, ausencia de controles, vulnerabilidades que afecten la integridad, confidencialidad y disponibilidad de información y de los servicios
    - Medio: Mala configuración de equipos, documentación inexistente, equipos obsoletos, ausencia de personal, funcionarios sin conocimiento en temas de ciberseguridad
    - Bajo: Configuraciones de equipos o infraestructura que no interrumpan el servicio o pongan en riesgo la información,
- Mitigación: Establecer las medidas o acciones a aplicarse para minimizar o eliminar la vulnerabilidad localizada

Tabla de determinación de vulnerabilidades basados en CVE (vulnerabilidades y exposiciones comunes)

- Equipo: Detalle del equipo en donde se encuentra la vulnerabilidad.
- Puerto: Especificar el número de puerto del equipo vulnerable.
- CVE – ID: Especificar el número de identificación del CVE.
- Descripción: Explicación resumida de la vulnerabilidad
- Afectación: Definir si el problema afecta a la integridad, confidencialidad y/o disponibilidad de información y/o servicio
- Gravedad: La gravedad de la vulnerabilidad la determina la Autoridad de Numeración de CVE (CNA)
- Mitigación: Establecer las medidas o acciones a aplicarse para minimizar o eliminar la vulnerabilidad localizada
- CNA: Especificar la Autoridad de Numeración de CVE (CNA) de donde se extrajo la información de la vulnerabilidad basadas en ID-CVE

Es importante recalcar que existen instituciones u organismos de investigación que son Autoridad de Numeración de CVE (CNA), como el Instituto Nacional de Ciberseguridad (INCIBE), MITRE Corporation, entre otros, cuyas competencias son la asignación efectiva de los identificadores CVE, designación y divulgación de vulnerabilidades a nivel internacional.

Los diferentes tipos de instrumentos definidos y aplicados en la etapa de diagnóstico (encuestas, *checklist* y herramientas de escaneo de vulnerabilidades), permitieron el reconocimiento, detección y análisis especifico de errores y puntos vulnerables presentes en el recurso humano, tecnológico, *networking* y de comunicación de la institución, los resultados obtenidos son resumidos, detallados, clasificados y plasmados como se observa en las tablas 6-7

Tabla 6: Tabla de determinación de vulnerabilidades.

No.	Herramienta	Problema	Afectación	Gravedad	Mitigación
1	Encuestas	Falta de capacitación y/o personal TI especializado en seguridad informática	Integridad y disponibilidad de servicios	MEDIO	Implementar o capacitar al personal en seguridad informática
2	Encuestas	Falta de auditorias y controles de ciberseguridad	Integridad, confidencialidad y disponibilidad de información y servicios	ALTO	Control periódico y/o auditorias internas o externas de ciberseguridad
3	Encuestas Checklist	Documentación inexistente sobre planes de contingencia, políticas de respaldos, correo electrónico, gestión de contraseñas, uso del wifi, prevención de riesgos informáticos, control de accesos, instalación de software, uso del internet	Integridad, confidencialidad y disponibilidad de información	MEDIO	Elaboración de reglamentos u otros documentos que regulen el uso de correo electrónico, wifi, gestión de contraseñas, prevención de riesgos informáticos, políticas de respaldos, control de accesos
4	Encuestas	Clasificación de información inexistente	Integridad, confidencialidad y disponibilidad de información	MEDIO	Elaboración de Reglamento interno de clasificación de información
5	Encuestas	Desconocimiento sobre temas generales ciberseguridad.	Integridad, confidencialidad y disponibilidad de información	MEDIO	Capacitaciones y envío de información de manera periódica a funcionarios y autoridades en temas de ciberseguridad
6	Checklist	Equipos informáticos y comunicación con software y hardware obsoletos	Integridad, confidencialidad y disponibilidad de información y servicios	MEDIO	Cambio de equipos que permitan la instalacion de software actual
7	Checklist	Cableado no cuenta con etiquetado de identificación	Disponibilidad de servicios	BAJO	Cumplir con la norma ANSI/TIA/EIA - 606 A - etiquetado de identificacion
8	Checklist	Equipos informáticos sin software licenciado	Integridad, confidencialidad y disponibilidad de información	ALTO	Adquisicion de sofware licenciado para administracion de servicios, utilitarios y control de virus
9	Checklist	Falta de equipos y aplicaciones de control perimetral Firewall - IPS - IDS	Integridad, confidencialidad y disponibilidad de información y servicios	ALTO	Adquisicion o cotratacion de equipos o aplicaciones de control perimetral Firewall - IPS - IDS
10	Checklist	Utiliza el nombre del departamento en el SSID.	Disponibilidad de servicios	BAJO	Cambio de nombres SSID
11	Checklist	Configuración de fabrica en dispositivos de comunicaciones (Router - Access Point)	Confidencialidad y disponibilidad de servicios	ALTO	Cambio de configuraciones de fabrica de ingreso
12	Checklist	No dispone de un inventario de equipos informáticos y networking	Disponibilidad de servicios	BAJO	Elaboracion de equipos informaticos, tecnologicos y de comunicacion
13	Checklist	Autenticacion de wifi debiles	Disponibilidad de servicios	ALTO	Establecer protocolos de autenticación, como está establecido en el estándar IEEE 802.11i (Norma Inalámbrica)
14	Checklist	Inexistentes controles de accesos a las instalaciones y cuarto de equipos	Confidencialidad y disponibilidad de servicios	ALTO	Establecer controles de accesos mediante equipos y verificacion del personal que ingresa a las instalaciones y cuarto de equipos

Fuente: elaboración propia.

Tabla 7: Tabla de determinación de vulnerabilidades basados en CVE

No.	Equipo	Puerto	CVE - ID	Descripción	Afectación	Gravedad	CNA	Mitigación
1	SERVIDOR WEB	80	Posible CSRF CWE-352	Falsificación de solicitudes entre sitios (CSRF). El atacante engaña a la víctima para que haga una solicitud que la víctima no tenía la intención de hacer	Integridad del sistema	BAJO	INCIBE	Redireccionamiento a puerto 443
2	SERVIDOR WEB	80	CVE-2005-3299	Inclusión de archivos PHP en grab_globals.lib.php en phpMyAdmin. Permite a atacantes remotos incluir archivos locales a través del parámetro de redireccionamiento $ __, posiblemente involucrando la matriz de subformulario	Integridad del sistema	MEDIO	INCIBE	Redireccionamiento a puerto 443
3	SERVIDOR WEB	443	Posible CSRF CWE-352	Falsificación de solicitudes entre sitios (CSRF). Atacante engaña a la víctima para que haga una solicitud que la víctima no tenía la intención de hacer	Integridad del sistema	BAJO	INCIBE	Deshabilitacion protocolos SSL 2, SSl 3, TLS1.0 y TLS 1.1 de Apache en incremento cifrado fuerte
4	SERVIDOR WEB	2222	CVE-2019-6111	Vulnerabilidad en OpenSSH. Un servidor SCP (Secure Copy Protocol) malicioso (o atacante Man-in-the-Middle) puede sobrescribir archivos arbitrarios en el directorio objetivo del cliente SCP	Integridad del sistema	MEDIO	INCIBE	Incrementar cifrado fuerte
5	SERVIDOR WEB	10000	Posible CSRF CWE-352	Falsificación de solicitudes entre sitios (CSRF). El atacante engaña a la víctima para que haga una solicitud que la víctima no tenía la intención de hacer	Integridad del sistema	BAJO	INCIBE	Eliminacion de aplicacion Webmin y Usermin
6	SERVIDOR WEB	10000	CVE-2005-3299	Inclusión de archivos PHP en grab_globals.lib.php en phpMyAdmin. Permite a atacantes remotos incluir archivos locales a través del parámetro de redireccionamiento $ __, posiblemente involucrando la matriz de subformulario	Integridad del sistema	MEDIO	INCIBE	Eliminacion de aplicacion Webmin y Usermin
7	SERVIDOR WEB	10000	CVE-2007-6750	Vulnerabilidad en Apache. Denegación de servicio (interrupción del demonio) a través de solicitudes HTTP parciales	Disponibilidad del sistema	MEDIO	INCIBE	Eliminacion de aplicacion Webmin y Usermin
8	SERVIDOR WEB	10000	CVE-2006-3392	Vulnerabilidad Webmin y Usermin. Permite a atacantes remotos leer ficheros arbitrarios	Confidencialidad del sistema	MEDIO	INCIBE	Eliminacion de aplicacion Webmin y Usermin
9	ZIMBRA		CVE-2019-9621	Vulnerabilidad en Zimbra . Permite vulnerabilidad de tipo SSRF (Server-side request forgery / falsificación de solicitudes del lado del servidor) por medio del componente ProxyServlet.	Confidencialidad del sistema	MEDIO	INCIBE	Actualizacion ZIMBRA
10	ZIMBRA		CVE-2018-20160	Vulnerabilidad en ZeChat (o ZeXtras Chat) . Permite ataques de tipo XXE (inyección de código en una aplicación que analiza datos XML), como demuestra una petición XML creada al componente buzón mailboxd.	Integridad, confidencialidad y disponibilidad del sistema	ALTO	INCIBE	Actualizacion ZIMBRA
11	ZIMBRA	7443	CVE-2015-4000	Vulnerabilidad en el protocolo TLS / Logjam. Diseño de la negociación de claves Diffie-Hellman (DH) implementado en TLS. El fallo puede ser explotado para realizar ataques Man in the Middle.	Integridad del sistema	ALTO	INCIBE	Deshabilitacion protocolos SSL 2, SSl 3, TLS1.0 y TLS 1.1
12	CENTRAL TELEFONICA	80	CVE-2007-6750	Vulnerabilidad en Apache. Denegación de servicio (interrupción del demonio) a través de solicitudes HTTP parciales	Disponibilidad del sistema	MEDIO	INCIBE	Deshabilitar el puerto 80
13	CENTRAL TELEFONICA	8089	CVE-2015-4000	Vulnerabilidad en el protocolo TLS. Falla en transmitir correctamente una opción de conjunto de cifrado DHE_EXPORT	Integridad del sistema	MEDIO	INCIBE	Cambio de puerto

Fuente: elaboración propia.

2.3.2.2 Aplicación

Esta etapa consecuentemente con la fase antes descrita, consiste en la aplicación de herramientas y ejecución de acciones necesarias que permitan minimizar o eliminar cada una de las vulnerabilidades localizadas. Es recomendable realizar la ejecución de instrumentos o acción de solución acorde a las tablas elaboradas anteriormente, se incrementa un campo denominado acción, el cual, se determina si el objetivo se llevó a cabo o es recomendado para su cumplimiento.

2.3.2.2.1 Mitigación de vulnerabilidades basadas en herramientas

Se ejecutan acciones que permiten mitigar las vulnerabilidades localizadas con el uso de encuestas y *checklist* como se observa en la tabla 8.

Tabla 8: Recomendaciones y cumplimiento de Mitigaciones basadas en herramientas

No.	Herramienta	Problema	Afectación	Gravedad	Mitigación	Accion
1	Encuestas	Falta de capacitación y/o personal TI especializado en seguridad informática	Integridad y disponibilidad de servicios	MEDIO	Implementar o capacitar al personal en seguridad informática	Recomendado
2	Encuestas	Falta de auditorias y controles de ciberseguridad	Integridad, confidencialidad y disponibilidad de información y servicios	ALTO	Control periódico y/o auditorias internas o externas de ciberseguridad	Recomendado
3	Encuestas Checklist	Documentación inexistente sobre planes de contingencia, políticas de respaldos, correo electrónico, gestión de contraseñas, uso del wifi, prevención de riesgos informáticos, control de accesos, instalación de software, uso del internet	Integridad, confidencialidad y disponibilidad de información	MEDIO	Elaboración de reglamentos u otros documentos que regulen el uso de correo electrónico, wifi, gestión de contraseñas, prevención de riesgos informáticos, políticas de respaldos, control de accesos	Cumplido
4	Encuestas	Clasificación de información inexistente	Integridad, confidencialidad y disponibilidad de información	MEDIO	Elaboración de Reglamento interno de clasificación de información	Cumplido
5	Encuestas	Desconocimiento sobre temas generales ciberseguridad.	Integridad, confidencialidad y disponibilidad de información	MEDIO	Capacitaciones y envio de información de manera periódica a funcionarios y autoridades en temas de ciberseguridad	Cumplido
6	Checklist	Equipos informáticos y comunicación con software y hardware obsoletos	Integridad, confidencialidad y disponibilidad de información y servicios	MEDIO	Cambio de equipos que permitan la instalacion de software actual	Recomendado
7	Checklist	Cableado no cuenta con etiquetado de identificación	Disponibilidad de servicios	BAJO	Cumplir con la norma ANSI/TIA/EIA - 606 A - etiquetado de identificacion	Cumplido
8	Checklist	Equipos informáticos sin software licenciado	Integridad, confidencialidad y disponibilidad de información	ALTO	Adquisicion de sofware licenciado para administracion de servicios, utilitarios y control de virus	Recomendado
9	Checklist	Falta de equipos y aplicaciones de control perimetral Firewall - IPS - IDS	Integridad, confidencialidad y disponibilidad de información y servicios	ALTO	Adquisicion o cotratacion de equipos o aplicaciones de control perimetral Firewall - IPS - IDS	Recomendado
10	Checklist	Utiliza el nombre del departamento en el SSID.	Disponibilidad de servicios	BAJO	Cambio de nombres SSID	Cumplido
11	Checklist	Configuración de fabrica en dispositivos de comunicaciones (Router - Access Point)	Confidencialidad y disponibilidad de servicios	ALTO	Cambio de configuraciones de fabrica de ingreso	Cumplido
12	Checklist	No dispone de un inventario de equipos informáticos y networking	Disponibilidad de servicios	BAJO	Elaboracion de inventario de equipos informaticos, tecnologicos y de comunicacion	Cumplido
13	Checklist	Autenticacion de wifi debiles	Disponibilidad de servicios	ALTO	Establecer protocolos de autenticación, como está establecido en el estándar IEEE 802.11i (Norma Inalámbrica)	Cumplido
14	Checklist	Inexistentes controles de accesos a las instalaciones y cuarto de equipos	Confidencialidad y disponibilidad de servicios	ALTO	Establecer controles de accesos mediante equipos y verificacion del personal que ingresa a las instalaciones y cuarto de equipos	Recomendado

Fuente: elaboración propia.

- Al determinarse que existe un solo funcionario en la unidad de Tecnologías de la Información y Comunicación de la Institución, es recomendable implementar más funcionarios o capacitar en seguridad informática al personal TI.

- Mediante la recolección de datos, se determina que, en la Gobernación de Tungurahua, existen documentos realizaos y otros que continúa en etapa de elaboración y aprobación, en cuales, se establecen políticas de respaldos, correo electrónico, gestión de contraseñas y control de accesos, los mismos están ubicados en los archivos de las oficinas de TIC's y secretaria de la Institución.

De manera general mencionados documentos establecen:

- Lineamientos generales aplicables a los sistemas de información y a la infraestructura de servidores ubicados en la Gobernación de Tungurahua, en lo referente a los procedimientos para resguardar respaldos de información, software y sistemas, asegura su permanente

integridad, confidencialidad y disponibilidad, en conformidad al Sistema de Seguridad de la información institucional.

- Políticas de correo electrónico institucional que proveen los lineamientos a las y los servidores públicos de la Gobernación de Tungurahua de utilizar este recurso para disminuir riesgos de seguridad por manejo indebido, así como, también, controlar y precautelar el rendimiento de la red institucional para evitar su saturación y mantener la disponibilidad de los servicios.

- Normar, controlar y aplicar de manera eficiente los protocolos establecidos para el ingreso, salida, tránsito y permanencia de funcionarios, usuarios y visitantes a las instalaciones de la Gobernación de Tungurahua con la finalidad de establecer medidas de seguridad en los controles de acceso y edificio que dispone la Institución.

- Clasificar información que genera, almacena y envía la Gobernación de Tungurahua (Reglamento interno por aprobarse)

- El analista de Gestión de TIC de la entidad, realiza capacitaciones virtuales y envía información mediante redes sociales y correo electrónico institucional a funcionarios y a autoridades sobre temas de manejo de contraseñas y ciberseguridad.

- Los dispositivos informáticos, tecnológicos y comunicación de la institución son de tecnología obsoleta, cuentan con software que no tienen soporte por parte del fabricante y son considerados altamente vulnerables de ataques, en tal virtud, se recomienda la adquisición de equipos informáticos, comunicación, software y antivirus licenciado. La adquisición de equipos de comunicación capa 3 que cumplan con las funciones de control *Firewall* y/o aplicaciones, IPS, IDS, consecuente con la aplicación de VPN y junto con la configuración de VLAN como medida de seguridad, es una recomendación prioritaria y urgente, ya que, se considera como método de ciberseguridad perimetral encargado de proteger sistemas y dispositivos conectados a la red.

- En la infraestructura *networking,* se realiza el etiquetado de identificación del cableado, como se observa en la figura 68, configuración de dispositivos de comunicación, establecimiento contraseñas robustas y cambios de nombres SSID

Figura 68: Etiquetado de identificación del cableado

Fuente: elaboración propia.

- Se recomienda incrementar los niveles de seguridad con sistemas de control de acceso que restrinja el ingreso de personal no autorizado a cuartos de equipos.

- **Mitigación de vulnerabilidades basadas en CVE**

Se ejecutan acciones que permiten mitigar las vulnerabilidades basadas en CVE como se observa en la tabla 9.

Tabla 9: Cumplimiento de Mitigaciones basadas en CVE

No.	Equipo	Puerto	CVE - ID	Descripción	Afectación	Gravedad	CNA	Mitigación	Acción
1	SERVIDOR WEB	80	Posible CSRF CWE-352	Falsificación de solicitudes entre sitios (CSRF). El atacante engaña a la víctima para que haga una solicitud que la víctima no tenía la intención de hacer	Integridad del sistema	BAJO	INCIBE	Redireccionamiento a puerto 443	Cumplido
2	SERVIDOR WEB	80	CVE-2005-3299	Inclusión de archivos PHP en grab_globals.lib.php en phpMyAdmin. Permite a atacantes remotos incluir archivos locales a través del parámetro de redireccionamiento $ __, posiblemente involucrando la matriz de subformulario	Integridad del sistema	MEDIO	INCIBE	Redireccionamiento a Puerto 443	Cumplido
3	SERVIDOR WEB	443	Posible CSRF CWE-352	Falsificación de solicitudes entre sitios (CSRF). Atacante engaña a la víctima para que haga una solicitud que la víctima no tenía la intención de hacer	Integridad del sistema	BAJO	INCIBE	Deshabilitacion protocolos SSL 2, SSL 3, TLS1.0 y TLS 1.1 de Apache en incremento cifrado fuerte	Cumplido
4	SERVIDOR WEB	2222	CVE-2019-6111	Vulnerabilidad en OpenSSH. Un servidor SCP (Secure Copy Protocol) malicioso (o atacante Man-in-the-Middle) puede sobrescribir archivos arbitrarios en el directorio objetivo del cliente SCP	Integridad del sistema	MEDIO	INCIBE	Incrementar cifrado fuerte	Cumplido
5	SERVIDOR WEB	10000	Posible CSRF CWE-352	Falsificación de solicitudes entre sitios (CSRF). El atacante engaña a la víctima para que haga una solicitud que la víctima no tenía la intención de hacer	Integridad del sistema	BAJO	INCIBE	Eliminación de aplicación Webmin y Usermin	Cumplido
6	SERVIDOR WEB	10000	CVE-2005-3299	Inclusión de archivos PHP en grab_globals.lib.php en phpMyAdmin. Permite a atacantes remotos incluir archivos locales a través del parámetro de redireccionamiento $ __, posiblemente involucrando la matriz de subformulario	Integridad del sistema	MEDIO	INCIBE	Eliminación de aplicación Webmin y Usermin	Cumplido
7	SERVIDOR WEB	10000	CVE-2007-6750	Vulnerabilidad en Apache. Denegación de servicio (interrupción del demonio) a través de solicitudes HTTP parciales	Disponibilidad del sistema	MEDIO	INCIBE	Eliminación de aplicación Webmin y Usermin	Cumplido
8	SERVIDOR WEB	10000	CVE-2006-3392	Vulnerabilidad Webmin y Usermin. Permite a atacantes remotos leer ficheros arbitrarios	Confidencialidad del sistema	MEDIO	INCIBE	Eliminación de aplicación Webmin y Usermin	Cumplido
9	ZIMBRA		CVE-2019-9621	Vulnerabilidad en Zimbra . Permite vulnerabilidad de tipo SSRF (Server-side request forgery / falsificación de solicitudes del lado del servidor) por medio del componente ProxyServlet.	Confidencialidad del sistema	MEDIO	INCIBE	Actualización ZIMBRA	Cumplido
10	ZIMBRA		CVE-2018-20160	Vulnerabilidad en ZxChat (o ZeXtras Chat) . Permite ataques de tipo XXE (inyección de código en una aplicación que analiza datos XML), como demuestra una petición XML creada al componente buzón mailboxd.	Integridad, confidencialidad y disponibilidad del sistema	ALTO	INCIBE	Actualización ZIMBRA	Cumplido
11	ZIMBRA	7443	CVE-2015-4000	Vulnerabilidad en el protocolo TLS / Logjam. Diseño de la negociación de claves Diffie-Hellman (DH) implementado en TLS. El fallo puede ser explotado para realizar ataques Man in the Middle.	Integridad del sistema	ALTO	INCIBE	Deshabilitacion protocolos SSL 2, SSL 3, TLS1.0 y TLS 1.1	Cumplido
12	CENTRAL TELEFONICA	80	CVE-2007-6750	Vulnerabilidad en Apache. Denegación de servicio (interrupción del demonio) a través de solicitudes HTTP parciales	Disponibilidad del sistema	MEDIO	INCIBE	Deshabilitar el puerto 80	Cumplido
13	CENTRAL TELEFONICA	8089	CVE-2015-4000	Vulnerabilidad en el protocolo TLS. Falla en transmitir correctamente una opción de conjunto de cifrado DHE_EXPORT	Integridad del sistema	MEDIO	INCIBE	Cambio de puerto	Cumplido

Fuente: elaboración propia.

- En el sitio *web,* se realiza la redirección de HTTP a la versión HTTPS para evitar y mitigar la vulnerabilidad del puerto 80 como se observa en la figura 69.

Figura 69: Redireccionamiento a https

```
<VirtualHost *:80>
   ServerAdmin root@gobernaciontungurahua.gob.ec
   DocumentRoot /var/www/html
   ServerName www.gobernaciontungurahua.gob.ec
   <Directory /var/www/html>
   #  Options FollowSymLinks
     AllowOverride All
   </Directory>
   ErrorLog /var/log/httpd/gobernaciontungurahua.gob.ec-error_log
   CustomLog /var/log/httpd/gobernaciontungurahua.gob.ec-access_log common
   <Location /control>
     order deny,allow
     allow from all
   </Location>
   Redirect permanent / https://www.gobernaciontungurahua.gob.ec
</VirtualHost>
```

Fuente: elaboración propia.

- De manera predeterminada el servidor web utiliza los protocolos TLS 1 y TLS 1.1, al igual algoritmos de cifrado débiles, lo que, se consideran factores vulnerables, por lo que, para mitigar esta vulnerabilidad, se procede con la restricción de los puertos mencionados y se incrementa la seguridad en los algoritmos de cifrado como se observa en la figura 70.

Figura 70: Restricción de protocolos TLS e incremento de seguridad en algoritmos de cifrado

```
SSLEngine on
SSLProtocol all -SSlv3 -TLSv1 -TLSv1.1 +TLSv1.2
SSLCompression off
SSLHonorCipherOrder on
SSLCipherSuite "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:EC
A256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-
ES:!MD5:!PSK:!RC4"

SSLCertificateFile /etc/pki/tls/certs/STAR_gobernaciontungurahua_gob_ec.crt
SSLCertificateKeyFile /etc/pki/tls/private/commercial.key
SSLCACertificateFile /etc/pki/ca-trust/extracted/pem/My_CA_Bundle.crt
</VirtualHost>
<VirtualHost *:443>
DocumentRoot /var/www/html
ServerName mail.gobernaciontungurahua.gob.ec
SSLEngine on
SSLProtocol -TLSv1 -TLSv1.1 +TLSv1.2
SSLCertificateFile /etc/pki/tls/certs/STAR_gobernaciontungurahua_gob_ec.crt
SSLCertificateKeyFile /etc/pki/tls/private/commercial.key
SSLCACertificateFile /etc/pki/ca-trust/extracted/pem/My_CA_Bundle.crt
#SSLVerifyClient none
</VirtualHost>
```

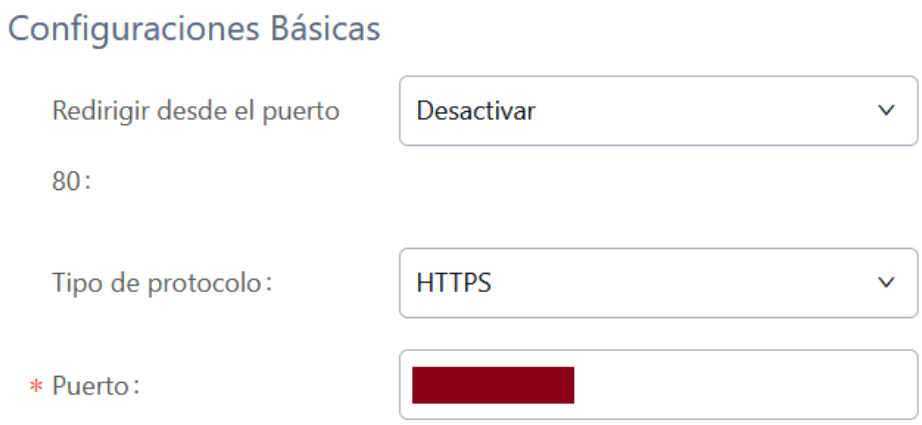
Fuente: elaboración propia.

- La aplicación *Web*min y Usermin que utiliza el puerto 10000, se considera como herramientas de administración de servidores, y dado que, actualmente no existe una actualización de seguridad disponible, que haya sido liberada por el fabricante, se elimina la aplicación para que el servidor sea administrado mediante consola de comandos.

- El servicio de correo electrónico Zimbra presentaba vulnerabilidades debido a la versión 8.7.6 instalada, por lo que, se procede a su actualización con la finalidad de solucionar y reducir las vulnerabilidades encontradas.

- La central telefónica presentaba vulnerabilidades a través de sus puertos, por lo que, se procede a desactivar el puerto 80, cambiarlo al tipo de protocolo https y modificar el puerto 8089, como se observa en la figura 71, con la aplicación de estas acciones, se soluciona las vulnerabilidades presentadas

Figura 71: Desactivación de puerto 80 y cambio de puerto



Fuente: elaboración propia.

2.3.3 Fase de Control

La ejecución de esta etapa requiere acciones y procedimientos que fusionadas en un solo proceso permiten la correcta gestión y control de la información de los componentes de la infraestructura de red, comunicaciones, servidores, aplicaciones *web*, estaciones de trabajo y factor humano de la Institución.

Este proceso constante y dinámico, se lleva a cabo con la aplicación de herramientas y técnicas utilizadas en la fase de diagnóstico, la información resultante del empleo de estos instrumentos permite comparar el estado inicial con la situación actual que se encuentra la entidad, de tal manera que, al descubrirse vulnerabilidades o falencias, se tomen medidas correctivas que ejecutan acciones en pro de la mejora continua del estado de la ciberseguridad de la institución.

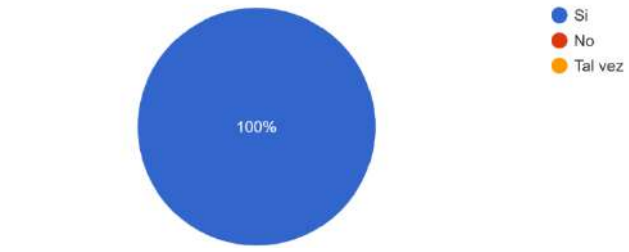
2.3.3.1 Aplicación de Encuestas:

Se emplea cuestionarios dirigidos a funcionarios y autoridades de la Gobernación de Tungurahua, para determinar su grado de conocimiento sobre ciberseguridad, el resultado obtenido se resume con la siguiente información:

- **Encuestas aplicadas a autoridades**

1. ¿Conoce usted si la institución cuenta con personal especializado en seguridad informática o un equipo de respuesta a incidentes de seguridad informática (CSIRT- Computer Security Incident & Response Team)?

Figura 72: Tabulación pregunta 1 Autoridades



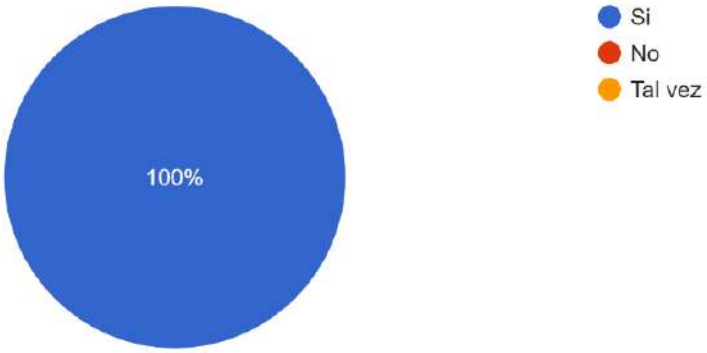
Fuente: elaboración propia

Interpretación:

Según las respuestas obtenidas, se concluye que al interior de la Gobernación existe personal especializado en seguridad informático o la existencia de un equipo de respuesta a incidentes de seguridad informática.

2. ¿Conoce usted si la Institución posee con una metodología para el análisis de vulnerabilidades y/o gestión de riesgo de ciberseguridad?

Figura 73: Tabulación pregunta 2 Autoridades



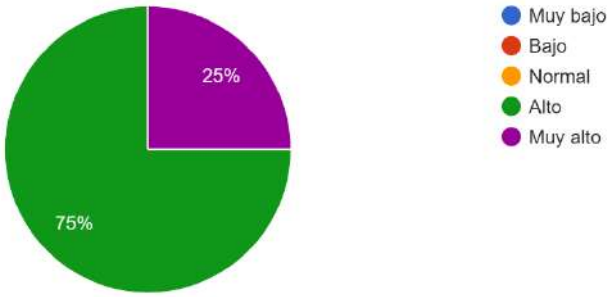
Fuente: elaboración propia

Interpretación:

Según las respuestas obtenidas, se concluye que, al interior de la Gobernación de Tungurahua, existe ya una metodología que permite el análisis de vulnerabilidades y/o gestión de riesgo de ciberseguridad.

3. ¿Cuál cree usted que es el nivel de seguridad que actualmente dispone la gobernación de Tungurahua?

Figura 74: Tabulación pregunta 3 Autoridades



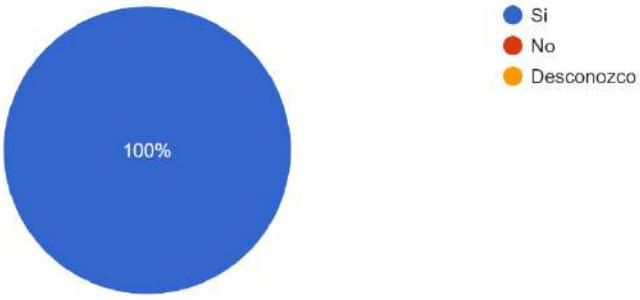
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por las autoridades, se concluye que, al interior de la Gobernación de Tungurahua, el nivel de seguridad de la información es Alto.

4. ¿Conoce usted si la Institución cuenta con planes de contingencia, políticas de seguridad, reglamentos u otros documentos que regulen el uso de correo electrónico, gestión de contraseñas, uso del wifi, prevención de riesgos informáticos, entre otros?

Figura 75: Tabulación pregunta 4 Autoridades



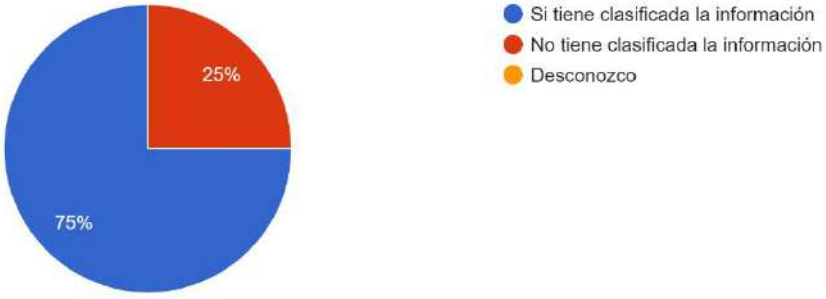
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por las autoridades, se concluye que, la Gobernación de Tungurahua, cuenta ya con planes de contingencia, políticas de seguridad, reglamentos u otros documentos que regulen el uso de correo electrónico, gestión de contraseñas, uso del wifi, prevención de riesgos informáticos, entre otros.

5. ¿Conoce usted si la Institución tiene una correcta clasificación de la información producida, recibida y almacenada (Confidencial, pública, etc.)?

Figura 76: Tabulación pregunta 5 Autoridades



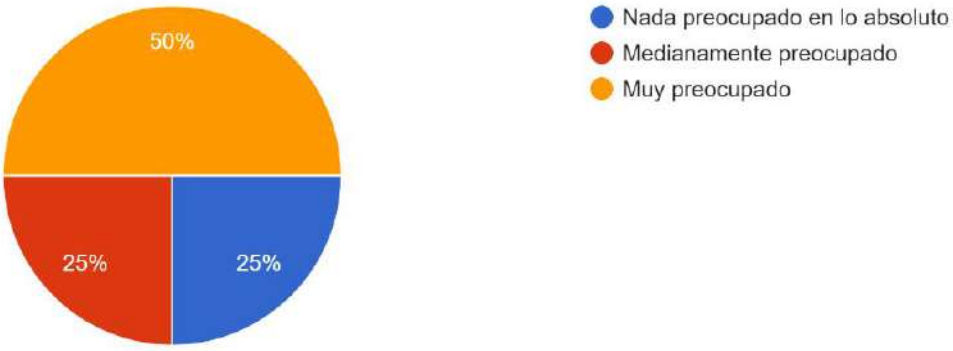
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por las autoridades, se concluye que, la Gobernación de Tungurahua, mantiene una correcta clasificación de la información producida.

6. ¿Cuál es su nivel de preocupación sobre los ciberataques a instituciones públicas?

Figura 77: Tabulación pregunta 6 Autoridades



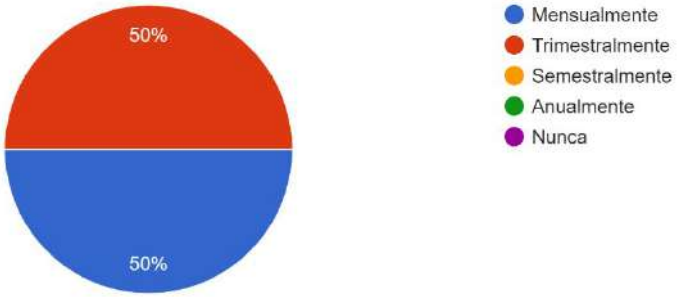
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por las autoridades Se concluye que, al interior de la Gobernación de Tungurahua, se tiene un nivel muy preocupado de ciberataques a Instituciones Públicas.

7. ¿Con que periodo la institución realiza capacitaciones a los funcionarios sobre temas de ciberseguridad?

Figura 78: Tabulación pregunta 7 Autoridades



Fuente: elaboración propia

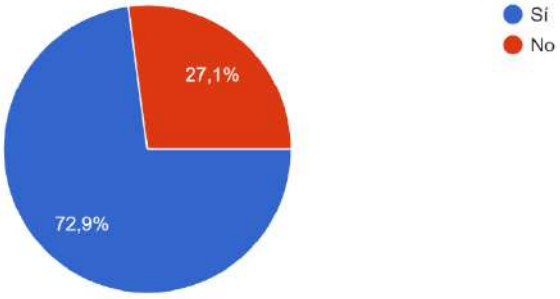
Interpretación:

Según las respuestas proporcionadas, se concluye que, las capacitaciones sobre temas de ciberseguridad se desarrollan de manera mensual o semestral.

- **Encuestas aplicadas a funcionarios**

1. ¿Usted es capaz de identificar los efectos producidos por virus/*malware* informático?

Figura 79: Tabulación pregunta 1 funcionarios.



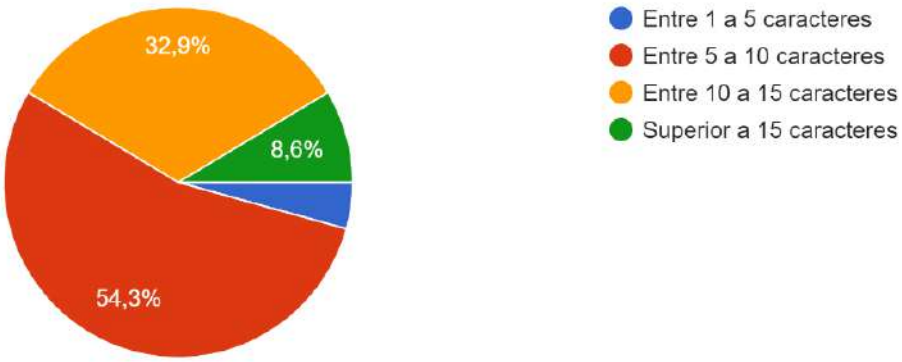
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por los funcionarios, se concluye que, el 73% de los trabajadores reconocen los efectos que producen los virus/*malware* informático.

2. ¿Las contraseñas que usted usa tienen una longitud normalmente de?

Figura 80: Tabulación pregunta 2 funcionarios.



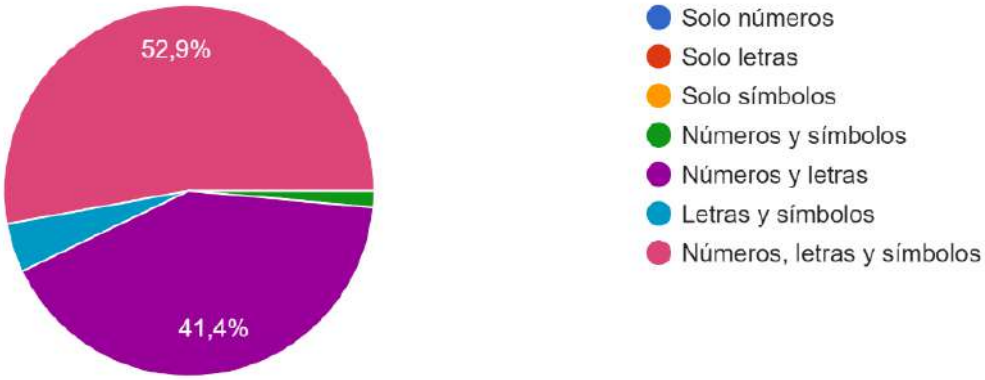
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por los funcionarios, se concluye que, la longitud de las contraseñas usadas va desde los 5 a los 10 caracteres y que llegan incluso a un nivel mayor.

3. ¿Las contraseñas que usted implementa por lo general están compuestas de?

Figura 81: Tabulación pregunta 3 funcionarios.



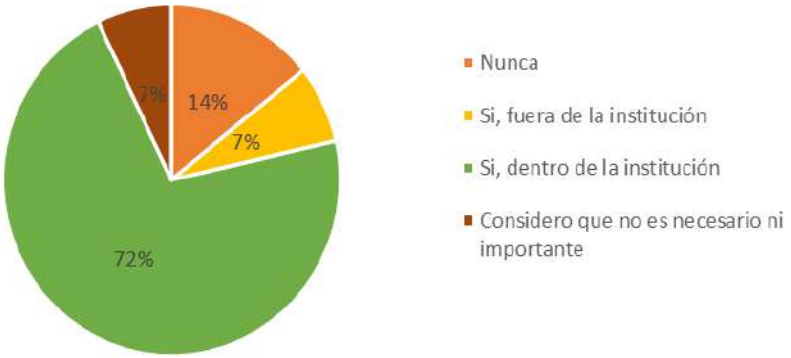
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por los funcionarios, se concluye que, las contraseñas en su mayoría están compuestas por la mezcla de números, letras y símbolos.

4. ¿Ha recibido capacitación en temas relacionados a ciberseguridad?

Figura 82: Tabulación pregunta 4 funcionarios.



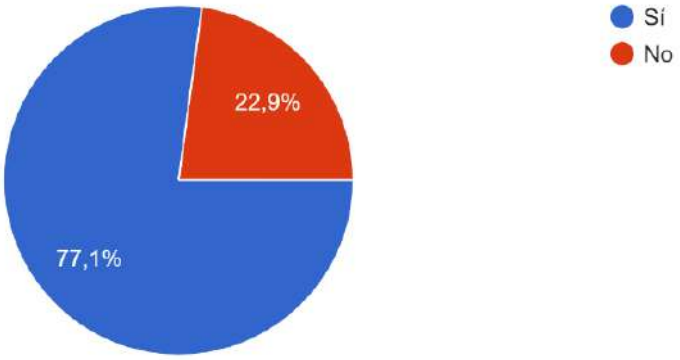
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por los funcionarios, se concluye que, el 79% ha recibido capacitaciones sobre ciberseguridad.

5. ¿Conoce los principales peligros asociados con el uso del internet y tecnologías de la información?

Figura 83: Tabulación pregunta 5 funcionarios.



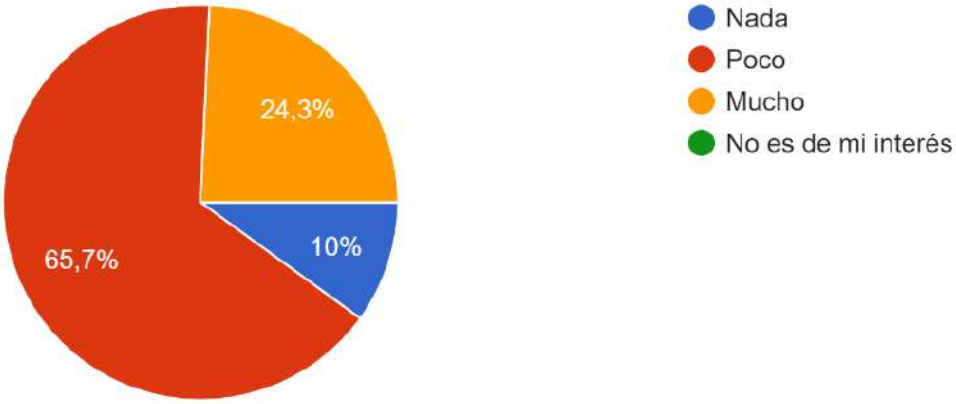
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por los funcionarios, se concluye que, el 77% conoce sobre los principales peligros que están asociados el uso del internet y tecnologías de la información.

6. ¿Cuál es el grado de conocimiento que usted posee sobre ciberseguridad?

Figura 84: Tabulación pregunta 6 funcionarios



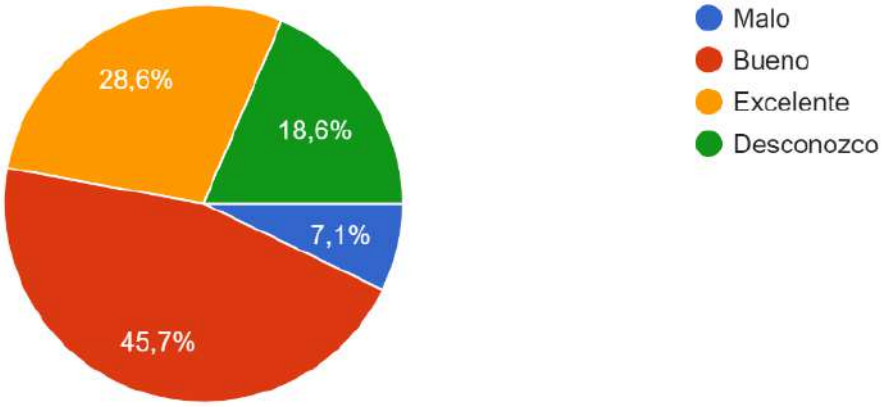
Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por los funcionarios, se concluye que, el 90% tiene cierto nivel de conocimiento sobre ciberseguridad.

7. ¿Según su criterio, el nivel de ciberseguridad en la institución es?

Figura 85: Tabulación pregunta 7 funcionarios



Fuente: elaboración propia

Interpretación:

Según las respuestas proporcionadas por los funcionarios, se concluye que, el 74% considera que el nivel actual de ciberseguridad es bueno a excelente.

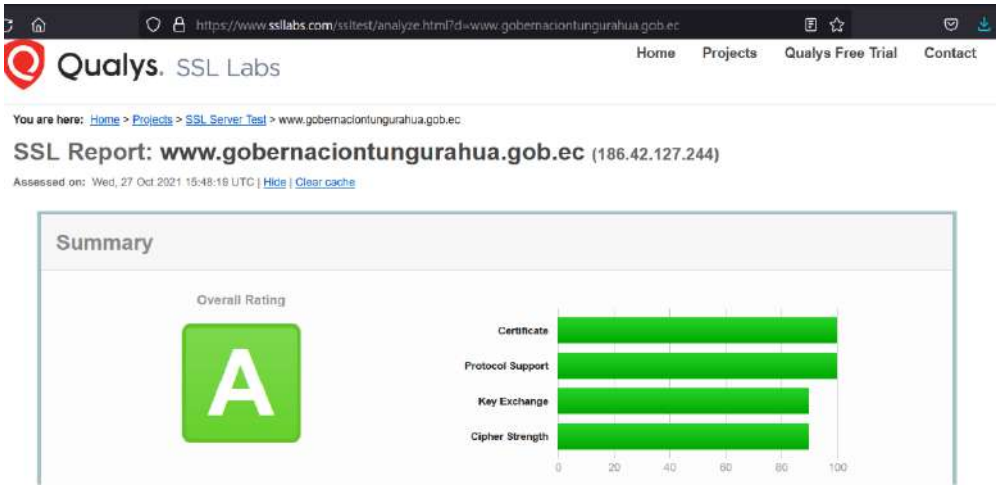
2.3.3.2 Aplicación de *Checklist*:

Con el empleo nuevamente de esta herramienta, se obtiene información que permite obtener resultados del estado actual en la administración e instalaciones de espacios de telecomunicaciones, cuartos de equipos, dispositivos informáticos, condiciones de seguridad física, implementación de controles, entre otros. Tal como se observa en el Anexo 2.

Escaneo de vulnerabilidades:

- Se aplican escáner online y herramientas de Kali Linux como se visualiza en las imágenes 86-90, con la finalidad de conocer el estado actual del servidor y sitio *web* de la Gobernación de Tungurahua.

Figura 86: Reporte de escaneo de sitio *web* con la herramienta Ssllabs (Qualys)

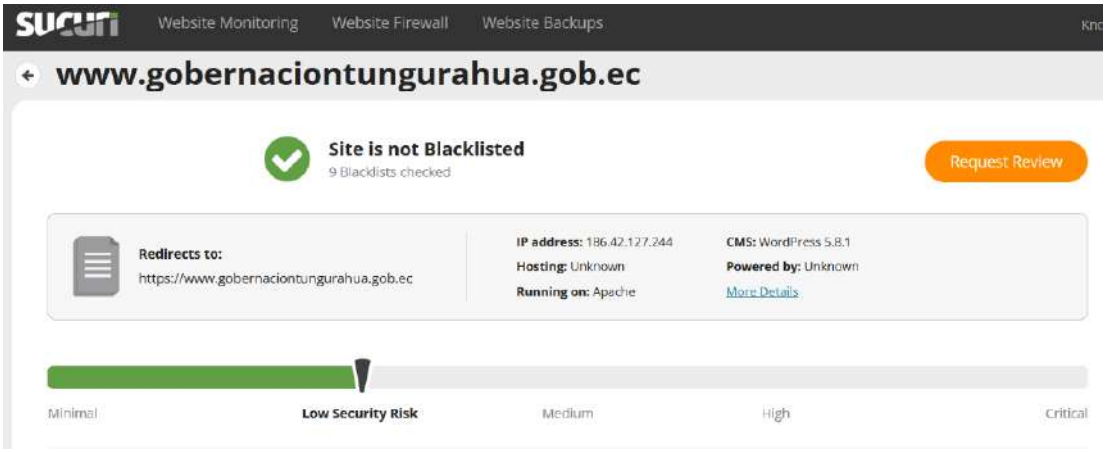


Fuente: elaboración propia

Figura 87: Reporte de escaneo de protocolos del sitio *web* con Qualys

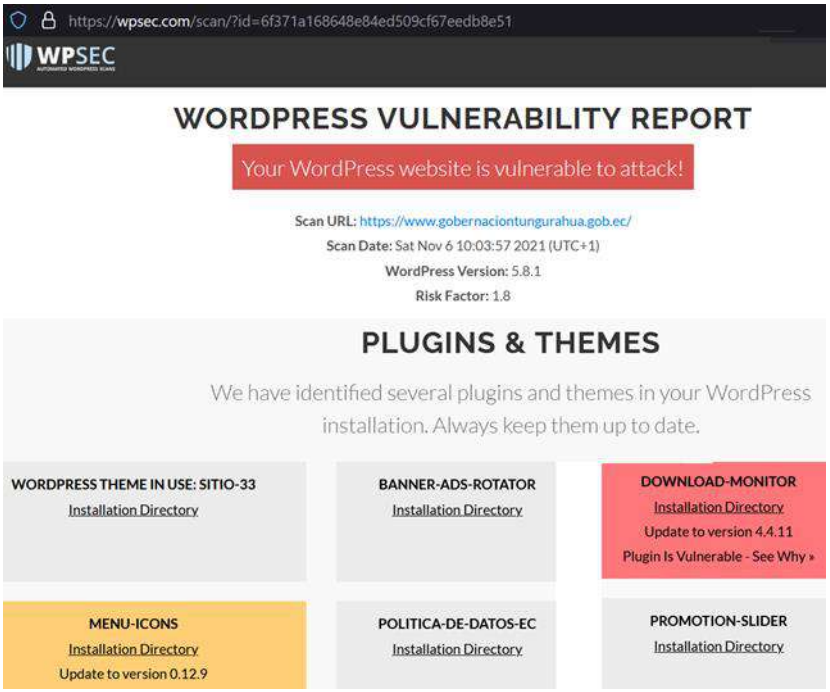
Fuente: elaboración propia

Figura 88: Reporte de escaneo de sitio *web* con la herramienta Sucuri



Fuente: elaboración propia

Figura 89: Reporte de escaneo de sitio *web* con la herramienta WPsec



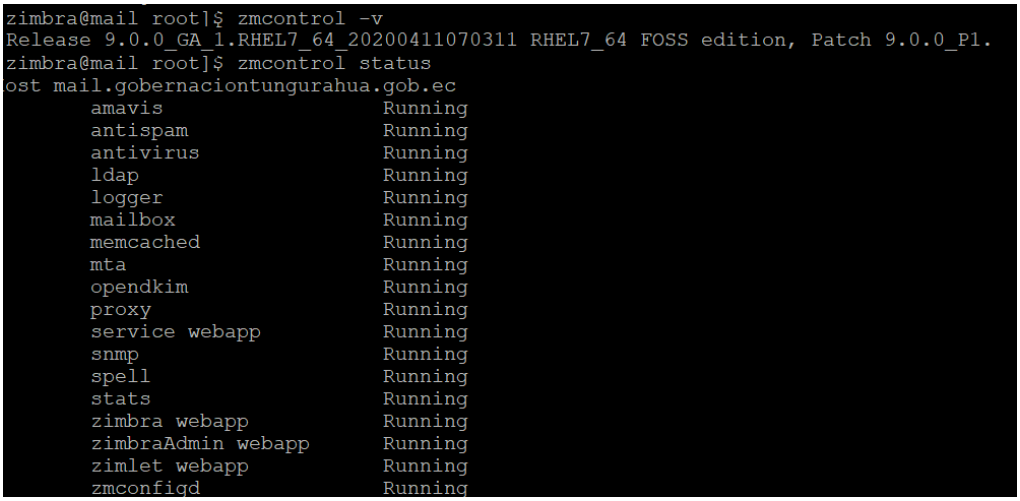
Fuente: elaboración propia

Figura 90: Reporte de escaneo de sitio *web* con la herramienta What*web*

Fuente: elaboración propia

Se aplica herramientas correspondientes en el servidor para determinar la versión actual del correo electrónico Zimbra como se observa en la imagen 91.

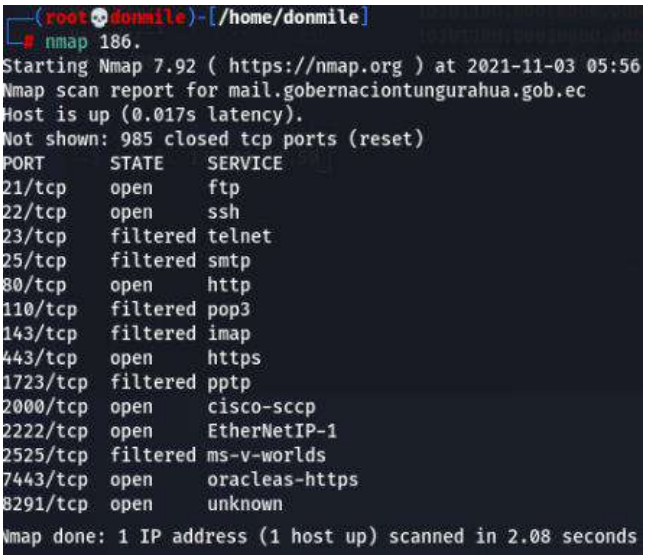
Figura 91: Zimbra actualizado



Fuente: elaboración propia

Mediante la herramienta nmap de Kali Linux, como se observa en la figura 92, se visualiza los puertos abiertos del servidor en el que se distingue que el puerto 10000 que utiliza la aplicación *web*min y usermin no se encuentra abierto.

Figura 92: Puertos 10000 del servidor cerrado



Fuente: elaboración propia

Aplicación de nmap de Kali Linux con el parámetro *script* vuln, para detectar vulnerabilidades en los puertos del servidor, como se observa en la Figura 93.

Figura 93: nmap con el parámetro *script* vuln

Fuente: elaboración propia

2.3.4 Ciclo del modelo

El modelo de mejora del estado de la ciberseguridad de la Gobernación de Tungurahua, se considera de ejecución cíclica y recursiva, en vista que las etapas vuelven a aplicarse repetidamente, hasta cumplir con el objetivo de diagnosticar, detectar, planificar, responder y por consecuencia mejorar en nivel de ciberseguridad institucional.

3 CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS

3.1 ANÁLISIS DE RESULTADOS

Los análisis de definiciones relacionados con el proceso de Ciberseguridad, es una necesidad en la actualidad, porque permiten una mejor comprensión de la seguridad de la información.

En cuanto a la ciberseguridad en la Gobernación de Tungurahua no se evidencia la utilización de métodos de protección a nivel de software o hardware, entonces existe la necesidad de optar nuevos medios seguridad con la finalidad de garantizar la seguridad integral y que genere la protección de información.

A continuación, se presenta los resultados obtenidos en cada una de las fases, en donde se constata como el desarrollo de un modelo de mejora de la ciberseguridad, permite garantizar protección de información que radica en la Gobernación de Tungurahua.

3.1.1 Fase de diagnóstico

3.1.1.1 Resultados del estado actual de la Institución

Los datos obtenidos a partir de las herramientas aplicadas, permitieron determinar que el estado de la ciberseguridad institucional es considerada como crítica, debido al incumplimiento de las normas y estándares ISO 27001, IEEE 80211, ANSI/TIA/EIA-568-569-606, la alta de gestión en los recursos, presencia de fallas en la protección y gestión de permisos que permiten el control de acceso en espacios considerados como vitales dentro de la institución y negligencias humanas causadas por la carencia de documentación, planes y políticas que regulen el uso y manejo tanto de la información como de la infraestructura tecnológica y de comunicaciones, dan como resultado la presencia de vulnerabilidades que la hacen susceptible a amenazas y son consideradas potencialmente peligrosas, porque, ponen en riesgo la seguridad de la información ya que comprometen su integridad, disponibilidad o confidencialidad.

Conclusión de las Encuestas

En base a las respuestas recopiladas mediante las encuestas, es preocupante observar que desde las autoridades de la gobernación no se ha preparado al personal sobre el peligro potencial que tienen un ciberataque a un equipo utilizado para realizar las labores correspondientes por los funcionarios. Además, los diferentes tipos de medidas de seguridad tomadas por varias personas causan una seria preocupación, las personas que utilizan métodos de autenticación extremamente seguros como la autenticación de dos pasos y la copia de seguridad están por debajo del 30%. Con el nivel actual de amenazas cibernéticas, el uso de solo una contraseña o un PIN provocan graves violaciones de seguridad.

La mentalidad de la mayoría de los usuarios tiende a subestimar la importancia de prevenir el uso no autorizado. Además, la implementación de prácticas de restricción y monitoreo son consideradas trabajos altamente técnicos según los comentarios de los participantes. Por lo tanto, es necesario proporcionar suficientes planes de capacitación técnicos para la implantación de software de monitoreo como parte del marco de concientización.

El objetivo principal de las encuestas fue evaluar la conciencia sobre las preocupaciones de seguridad de la información y las responsabilidades de los usuarios. De los resultados que se obtuvieron, es evidente que es necesario crear más conciencia para comprender mejor los diversos aspectos de seguridad y su implementación.

El conocimiento sobre la recopilación de datos y las características de seguridad incorporadas es muy bajo, probablemente debido a la dificultad de uso o menos publicidad. Según los comentarios de la mayoría de los participantes, el antivirus es el único método para proteger la información, la privacidad y la seguridad.

Estos resultados sobre las preocupaciones de seguridad generan una fuerte advertencia temprana sobre cómo los usuarios no poseen ciberseguridad en la Gobernación de Tungurahua.

3.1.1.2 Resultados del levantamiento y evaluación de la información

En el marco del proceso de evaluación de la ciberseguridad, se efectúo un conjunto de actividades que se ejecutaron mediante el uso de distintas herramientas con el objetivo de identificar y analizar vulnerabilidades, el análisis realizado en la aplicación *web*, servidores, equipos informáticos y de comunicaciones de la institución. Las vulnerabilidades halladas presentan riesgos de distinta naturaleza para la institución, algunas de estas, se las categoriza como severas, sin embargo, ciertas vulnerabilidades tienen el grado de peligrosas. A continuación, se presentan los resultados obtenidos de este proceso.

- **Vulnerabilidades del Servidor**
- El servidor presenta datos sobre la información interna de la institución, así como las versiones de software utilizadas, esta revelación es útil para planificar ataques potenciales.
- Se detectan errores en la configuración TLS, el servidor *web* utiliza TLS 1.0 y TLS 1.1, lo que produce varias situaciones que ponen en riesgo la privacidad y seguridad de los usuarios.
- La versión 8.7 de Zimbra utilizado en la institución, se encuentra expuesta a vulnerabilidades (CVE-2019-9621, CVE-2018-20160), su riesgo está en el manejo de los request de zimbra, el cual, el atacante realiza un bypass del sanitizado de los documentos XHTML, que deriva en un XXE, lo que repercute sobre la confidencialidad, integridad y disponibilidad de la información

- **Vulnerabilidades del sitio *web***
- El sitio *web* es desarrollado con el sistema de administración de contenido (CMS) WordPress, el mismo tiene la versión 5.2.4, considerada como obsoleta, presenta la vulnerabilidad referenciada en el CVE (nomenclatura estándar para identificación de la vulnerabilidad de forma inequívoca) CVE-2019-20043 que manifiesta: “Un usuario sin privilegios haría que una publicación sea pegajosa a través de la API REST. Los usuarios autenticados que no tienen los derechos para publicar una publicación pudieron marcar las publicaciones como pegajosas o no adhesivas a través

de la API REST. Por ejemplo, el rol de colaborador no tiene tales derechos, pero esto les permitió omitir eso.

- Los *plugin* desactualizados como es el caso del complemento Download Monitor que se ve afectado por múltiples vulnerabilidades XSS consideradas peligrosas, como se referencia en el CVE-2013-5098 que manifiesta “La vulnerabilidad de secuencias de comandos entre sitios (XSS) en admin / admin.php en el complemento Download Monitor antes de 3.3.6.2 para WordPress permite a los atacantes remotos inyectar secuencias de comandos *web* arbitrarias o HTML a través del parámetro de ordenación.
- Enlaces rotos como es el caso de las páginas accesibilidad y transparencia presentan error 404 (página no encontrada), falla considerada como vulnerabilidad debido a que los atacantes modifican las páginas con este error para llegar a las víctimas que simulan formularios con inicios de sesión falsos.
- Se detecta que el sitio *web* institucional no posee *Firewall*, haciéndolo vulnerable de ataques más comunes que aprovechan la inyección SQL, el cross-site *script*ing y la ejecución de archivos maliciosos.
- El sitio *web* no tiene ninguna redirección de HTTP a la versión HTTPS para evitar la advertencia del navegador no seguro.

- **Vulnerabilidades Infraestructura *networking***
- Con la aplicación de la herramienta Aircrack-ng, se determinó, que está comprometida la seguridad en las conexiones Wifi, debido a la falta de robustez de la estructura de las contraseñas, logrando descifrar claves, por lo que, se concluye que están compuestas solamente por dígitos numéricos, lo que hace vulnerable al servicio Wifi y que puede generar incursiones de terceros no autorizados a la red institucional
- Dispositivos de comunicaciones, equipos tecnológicos e información que son considerados para los funcionarios y autoridades como un activo importante dentro de la Gobernación, son componentes de la infraestructura *networking* institucional que se desarrollan en cada una de sus etapas y/o capas en un ambiente no confiable y con un enfoque de ciberseguridad vulnerable y altamente expuesto a riesgos informáticos. La ausencia de

herramientas *Firewall* perimetral que brinden la protección contra amenazas internas y externas procedentes de la red o internet, exposición de equipos ante la infección con virus, *malware* o gusanos, direcciones Ip no controladas, ausencia de gestión de accesos, filtrado de paquetes, puertos y aplicaciones e información comprometida por diversas amenazas como el robo, falsificación, fraude divulgación o eliminación, se consideran como una vulnerabilidad alto riego que ponen en peligro la seguridad tanto de los equipos como de la confidencialidad, integridad y disponibilidad de la información.

- **Vulnerabilidades en equipos informáticos**
- Los equipos objetivo, están expuestos a fallas de software, hardware y sistema, con la aplicación de las diferentes herramientas descritas anteriormente, su resultados describen que las vulnerabilidades encontradas son producidas por la antigüedad del hardware y sistemas operativos con los que trabajan, en su gran mayoría utilizan Windows 7, considerado como una vulnerabilidad de alto riesgo como lo referencia el CVE-2018-8589 que manifiesta “Existe una vulnerabilidad de elevación de privilegios si Windows maneja incorrectamente las llamadas a Win32k.sys, también, conocido como "Windows Win32k *Elevation of Privilege Vulnerability*". Esto afecta a Windows Server 2008, Windows 7, Windows Server 2008 R2”
- Los computadores presentan fallas en sus configuraciones como la falta de control de acceso con contraseña, ausencia de antivirus y privilegios totales de configuración del sistema al usuario, estos problemas, hacen que las vulnerabilidades se conviertan en un riesgo potencialmente peligroso y susceptible a un ataque informático.

- **Vulnerabilidades Telefonía IP**
- La telefonía IP que dispone la institución, presenta vulnerabilidades que son susceptibles a ataques que provocan interrupciones en el servicio, intercepción de líneas para hacer llamadas, intrusión a los dispositivos, entre otros, esto es causado porque los equipos conservan las configuraciones predeterminadas de fábrica para inicios de sesión y por la ausencia de

herramientas *Firewall* que incrementen la ciberseguridad en el servicio y equipamiento de telefonía IP.

3.1.2 Fase de control

3.1.2.1 Encuestas posteriores.

Los resultados arrojados con el empleo de las mismas herramientas aplicadas en la primera fase, reportan la disminución considerable de vulnerabilidades en comparación con la información producida en el estado inicial, tanto en el servidor, equipos de comunicación, infraestructura *networking* y factor humano, hay que tomar en consideración que, las anomalías no mitigadas son por causa del uso de *plugin* en el caso de WordPress, son lineamientos ministeriales y a la falta de recursos económicos que arrastran un problema considerado como crítico debido a que dificultan o limitan el uso de equipos y software que brinde seguridad en la infraestructura de red, comunicaciones y dispositivos informáticos. En términos generales, se concluye que existe mejora en el estado de la ciberseguridad de la Gobernación de Tungurahua.

3.1.2.2 *Checklist* posterior.

Luego de realizar la implementación, se realizó el *checklist* que permite obtener la información sobre resultados del estado actual en la administración e instalaciones de espacios de telecomunicaciones, cuartos de equipos, dispositivos informáticos, condiciones de seguridad física.

3.1.2.3 Vulnerabilidades.

Los resultados arrojados con la implementación de las mismas herramientas aplicadas en la primera fase, reportan la disminución considerable de vulnerabilidades en comparación con la información producida en el estado inicial, tanto en el servidor, equipos de comunicación, infraestructura *networking* y factor humano, se toma en consideración que, las anomalías no mitigadas son consecuencia del uso de *plugin* en el caso de WordPress, son lineamientos ministeriales y a la falta de recursos económicos que arrastran un problema considerado como crítico debido a que dificultan o limitan el uso de equipos y software que brinde seguridad en la infraestructura de red, comunicaciones y

dispositivos informáticos. En términos generales, se concluye que existe mejora en el estado de la ciberseguridad de la Gobernación de Tungurahua

CONCLUSIONES

- Mediante la identificación de los modelos existentes, se logra obtener un modelo que permita mejorar el nivel de ciberseguridad de forma ordenada y sistematizada, además, permite poseer herramientas de seguridad de la información, así como lineamientos que permitan actuar ante posibles ataques.
- El análisis realizado ha permitido encontrar las diferencias entre los procedimientos realizados a nivel mundial para la selección e infraestructuras críticas que toma en cuenta la realidad de la institución, y concluye que la ciberseguridad es gestionada a través del área que maneja información de vital importancia en este caso específico el departamento de Tics de la Gobernación de Tungurahua.
- Luego de haber identificado los estándares más utilizados, se estructuro un modelo de mejora de la ciberseguridad basada en cuatro etapas, que se ajusta a las necesidades de la institución, el cual, brinda las pautas necesarias para hacer frente a cualquier tipo de ataque que pudiese materializar.
- Luego de la validación realizada, el modelo permite evidenciar que las fases escogidas se complementan de tal manera que brindan las herramientas tecnológicas necesarias para mitigar y/o contrarrestar vulnerabilidades y amenazas, debido a que, con ellas se encuentra un apoyo en el uso de las normativas al comprender qué herramienta o estrategia usar para cada caso en específico, tomando en cuenta cada fase presente dentro de una posible materialización de algún ataque.

RECOMENDACIONES

- Se recomienda que el departamento de TIC implemente todas las consideraciones que en este proyecto se estipulan, tomar en cuenta los estándares como una referencia para proteger la información a través del uso de modelos.
- Para complementar las fases del modelo de mejora, se recomienda como actividad anual de la Unidad de TIC, elaborar planes de capaciones sobre el manejo de información, ciberseguridad y ciberataques, involucrando la participación de autoridades, funcionarios y demás personas encargadas del manejo de la información al interior de la Gobernación de Tungurahua.
- La ciberseguridad de la Gobernación de Tungurahua depende de diversos factores tanto tecnológicos como humanos, por lo tanto, es de vital importancia la elaboración, actualización o modificación continua de reglamentos u otros documentos que regulen el uso de correo electrónico, wifi, gestión de contraseñas, prevención de riesgos informáticos, políticas de respaldos, control de accesos, en general, instrumentos que contribuyan a la mejora de la ciberseguridad institucional
- Como prioridad institucional, se considera la gestión de recursos económicos para implementar acciones, capacitaciones, contratos para aumento de personal, herramientas o equipos que refuercen la mejora de ciberseguridad de la entidad

BIBLIOGRAFÍA

27001:2013, I. (2013). Information technology-Security techniques-Information security management systems-Requirements. *ISO/IEC 27001:2013*.

AETecno. (2016). *AETecno*. Retrieved from AETecno: http://tecno.americaeconomia.com/articulos/america-latina-el-nuevo-paraisode-los-ciberataques

Altamirano, & Bayona. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 112-134.

Ciberseguridad, I. E. (2016). *Ciberseguridad.*

Costas, S. (2011). Seguridad Informática (Ediciones). *Seguridad Informática*.

Erreyes, D. (2017). METODOLOGÍA PARA LA SELECCIÓN DE HERRAMIENTAS EFICIENTES Y PROTOCOLOS ADECUADOS PARA MEJORAR LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES. *UNIVERSIDAD DE CUENCA FACULTAD DE INGENIERÍA*.

Gartner. (2018). *Uso del marco de ciberseguridad del NIST*. Retrieved from Uso del marco de ciberseguridad del NIST: www.gartner.com/*web*inar/3163821/player?commId=180719&channelId=5500&srcld=1–4730952011.

Gasca G. (2010). Estudio de Similitud del Proceso de Gestión de Riesgos en Proyectos de Outsourcing de Software: Utilización de un Método. *Ingenierías Universidad de Medellín*, 119-129.

ISACA. (2014). The Cybersecurity Fundamentals Study Guide. *The Cybersecurity Fundamentals Study Guide*.

ISDEFE S.A., I. d. (n.d.). *ISDEFE S.A., I. d. (s.f.).* . Retrieved from ISDEFE S.A., I. d. (s.f.). : https://www.isdefe.es/.

Kaspersky Lab. (2017). *Ciberamezana, mapa en tiempo real*. Retrieved from https://cybermap.kaspersky.com/es/stats#country=35&type=vul&period=m

Kaspersky, L. (2017). *Fileless attacks against enterprise networks.* Retrieved from Fileless attacks against enterprise networks.: https://securelist.com/fileless-attacks-against-enterprise-networks/77403/

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo. *Revista Latinoamericana de Ingeniería de Software*, 161-176.

López, F., & Kirk, B. (2017). Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad. *UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL* .

López, M. J. (2013). Criptografía y Seguridad de Computadores. *Criptografía y Seguridad de Computadores*.

Manzano, V., & Andréu, J. (2000). Formatos para items en las encuestas electrónicas, antecedentes y propuestas. *Metodología de Encuestas*, 61-101.

Martín, A. (2011). *La encuesta: una perspectiva general metodológica .* MADRID: CASLON, S.I.

Ministerio de Justicia, D. H. (2014). *Código Orgánico Integral Penal del Ecuador (Primera). Quito: Gráficas Ayerve C. A.* . Retrieved from http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Ministerio de Telecomunicaciones, d. l. (2020). *ENCS ESTRATEGIA NACIONAL DE CIBERSEGURIDAD*. Retrieved from ENCS ESTRATEGIA NACIONAL DE CIBERSEGURIDAD: https://www.gobiernoelectronico.gob.ec/estrategia-nacional-de-ciberseguridad/

Naudi. (2016). *El Segundo informe de seguridad de la aplicación web Acunetix.* Retrieved from El Segundo informe de seguridad de la aplicación *web* Acunetix.: https://www.acunetix.com/blog/news/*web*-app-security-report-2016/

Netcloud, E. (2017). *Netcloud Engineering*. Retrieved from Netcloud Engineering: https://netcloudengineering.com/ciberseguridad-amenaza-vulnerabilidad/

Philco, L. (2017). Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad. *UNIVERSIDAD CATOLICA DE SANTIAGO DE GUAYAQUIL*.

Pinzón, D. M. (2018). Metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles.

Question Pro. (2018). *Questionpro*. Retrieved from https://www.questionpro.com/blog/es/formato-de-encuesta/

Ramírez Atehortúa, F. H., & Zwerg Villegas, A. M. (2012, Junio 06). Metodología de la investigación: más que una receta. *AD-minister*(20), 91-111. Retrieved Junio 06, 2019, from http://publicaciones.eafit.edu.co/index.php/administer/article/view/1344/1215

Symantec Corporation. (2016). *Informe de Symantec sobre las amenazas para la seguridad de los sitios web*. Retrieved from https://*web*sitesecurity.symantec.com/campaigns/17290/current/landing/assets/Symantec-WSTR-Report-ES.pdf

Tates, C., & Recalde, L. (2019). LA CIBERSEGURIDAD EN EL ECUADOR UNA PROPUESTA DEORGANIZACIÓN. *Revista de Ciencias de Seguridad y Defensa*, 156-159.

Tirumala, S., Valluri, M., & Babu, G. (2019). Una encuesta sobre preocupaciones, prácticas y medidas conceptuales de concientización sobre ciberseguridad. *Conferencia Internacional sobre Comunicación e Informática por Computadora (ICCCI) 2019*, 1-6.

Tungurahua, G. d. (2018). *Gobernación de Tungurahua*. Retrieved from http://docplayer.es/91467920-Plan-estrategico-de-la-gobernacion-de-tungurahua.html?cv=1

ANEXOS

1. *Checklist* 1

No.	PREGUNTA	SI	NO	N/A	OBSERVACIONES
ANSI/TIA/EIA-568-B Cableado de Telecomunicaciones en Edificios Comerciales					
1	¿El armado del patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B? Norma EIA/TIA 568-A	x			
2	¿La longitud de cada cableado horizontal no excede de los 90 metros?	x			
3	Existe fibra óptica en algún punto de la red ANSI/TIA/EIA-568-B.3		x		
4	Las redes o sección de red implementadas con fibra óptica van de acuerdo al estándar 802.3? ANSI/TIA/EIA-568-C.3			x	No posee fibra óptica
ANSI/TIA/EIA - 568 C.2 Requisitos mínimos para componentes reconocidos de UTP, usados en cableados para redes de telecomunicaciones (cable, conectores, hardware de conexión, cordones y jumpers).					
5	Utiliza cable UTP para Back-Bone	x			Cat 5e
6	Utiliza cable Fibra Óptica para Back-Bone			x	
7	Dispone de paneles de interconexión (Patch Panel) para distribución horizontal	x			Cat 5e
8	Dispone de equipos activos (Switch) para distribución horizontal	x			Obsoletos Dlink - TPLink - HP
9	Utiliza cable UTP para distribución horizontal	x			Cat 5e
10	Utiliza cable Fibra Óptica para distribución horizontal			x	
ANSI/TIA/EIA 569-C Estándar de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales. Dispone de:					
11	Instalaciones de Entrada	x			
12	Canalizaciones Montantes (“Back-bone”)	x			Metálicas
13	Canalizaciones horizontales	x			Plásticas sobre techo
14	La longitud del cableado horizontal no excede los 90 m	x			
15	Sala de Telecomunicaciones (central)	x			
16	Sala de Telecomunicaciones (por piso)	x			
ANSI/TIA/EIA - 606 A Norma de Administración para la Infraestructura de Telecomunicaciones Comerciales					
17	Clase 1: Edificio con un espacio de telecomunicaciones		x		
18	Clase 2: Edificio con varios espacios de telecomunicaciones	x			
19	Clase 3: Campus con múltiples edificios		x		
20	Clase 4: Institución con múltiples campus	x			Oficinas en cantones y parroquias
21	El etiquetado de la red cuenta con códigos de colores para facilitar su identificación		x		sin etiquetado
22	La red está dividida conforme al servicio que brindan (voz, datos, CCTV)	x			
ANSI/TIA/EIA 607-B1 Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales					
23	Cumple con los Requerimientos para instalaciones a tierra de los sistemas de Telecomunicaciones en Edificios Comerciales.	x			
EQUIPAMIENTO					
24	Dispone de Circuito Cerrado de TV (CCTV)	x			
26	El CCTV es administrable desde el data center	x			

26	Dispone de telefonía IP	x			
27	Telefonía IP Es administrable desde el data center	x			
28	Cuenta con dispositivos de comunicaciones que permitan la conexión WIFI (Router - Access Point)	x			Obsoletos (año 2000)
CONTROL DE ACCESO					
29	La edificación cuenta con puertas de seguridad con sistemas de control de acceso		x		
30	La institución cuenta con protocolo de control de acceso para el personal y visitantes		x		
31	Las Salas de Telecomunicaciones están protegidos de acceso no autorizado		x		Comparten oficinas
32	Dispone con un registro de control de usuarios que acceden a la red		x		Sin control para funcionarios y visitantes
SEGURIDAD					
33	La red cuenta con equipo *Firewall* físico para protección		x		
34	La red cuenta con equipos y aplicaciones (IDS, IPS, NIDS)		x		
35	Para evitar vulnerabilidades en las WLAN ¿Usan protocolos de autenticación, como está establecido en el estándar IEEE 80211i (Norma Inalámbrica)?	x			
36	Utiliza el nombre de la entidad o departamento en el SSID.	x			
37	La configuración predeterminada (fabrica) de los dispositivos de comunicaciones (Router - Access Point) ha sido cambiada		x		User - password (fabrica)
38	Considera que los password para ingreso a los dispositivos de comunicaciones (Router - Access Point) son seguros		x		Igual password (inseguros) para todos los dispositivos
39	Dispone de VLAN's con el objetivo de tener una mayor administración en cada una de los servicios de red		x		
40	Las direcciones IP´S de los equipos son fijas	x			
41	Los equipos informáticos cuentan con antivirus licenciados		x		
42	Utilizan herramientas software de diagnóstico para Identificar vulnerabilidades en los sistemas que utiliza la institución		x		
43	Monitorea y registra periódicamente la red para la prevención de errores o situaciones anómalas		x		
POLITICAS - PLANES – DOCUMENTACION					
44	Existe políticas para control de acceso para dispositivos de red y comunicaciones		x		
45	Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red		x		
46	Existe políticas de control de acceso y uso de los servicios de la red		x		
47	Existe una política de copias de respaldo o backups		x		
48	Existe política para controlar la instalación de software en sistemas operativos.		x		
49	Existe políticas o procedimientos de ingreso seguro para usuarios de los computadores en sistemas y aplicaciones		x		
50	Dispone de un inventario actualizado de los equipos informáticos y *networking*	x			Equipos obsoletos (años 2000 - 2004)
51	Dispone de política o documentación para la implementación y configuración de los dispositivos de red		x		Configuración a criterio del responsable

2. *Checklist 2*

No.	PREGUNTA	SI	NO	N/A	OBSERVACIONES
ANSI/TIA/EIA-568-B Cableado de Telecomunicaciones en Edificios Comerciales					
1	¿El armado del patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B? Norma EIA/TIA 568-A	x			
2	¿La longitud de cada cableado horizontal no excede de los 90 metros?	x			
3	Existe fibra óptica en algún punto de la red ANSI/TIA/EIA-568-B.3		x		
4	Las redes o sección de red implementadas con fibra óptica van de acuerdo al estándar 802.3? ANSI/TIA/EIA-568-C.3			x	No posee fibra óptica
ANSI/TIA/EIA - 568 C.2 Requisitos mínimos para componentes reconocidos de UTP, usados en cableados para redes de telecomunicaciones (cable, conectores, hardware de conexión, cordones y jumpers).					
5	Utiliza cable UTP para Back-Bone	x			Cat 5e
6	Utiliza cable Fibra Óptica para Back-Bone			x	
7	Dispone de paneles de interconexión (Patch Panel) para distribución horizontal	x			Cat 5e
8	Dispone de equipos activos (Switch) para distribución horizontal	x			Obsoletos Dlink - TPLink - HP
9	Utiliza cable UTP para distribución horizontal	x			Cat 5e
10	Utiliza cable Fibra Óptica para distribución horizontal			x	
ANSI/TIA/EIA 569-C Estándar de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales. Dispone de:					
11	Instalaciones de Entrada	x			
12	Canalizaciones Montantes (“Back-bone”)	x			Metálicas
13	Canalizaciones horizontales	x			Plásticas sobre techo
14	La longitud del cableado horizontal no excede los 90 m	x			
15	Sala de Telecomunicaciones (central)	x			
16	Sala de Telecomunicaciones (por piso)	x			
ANSI/TIA/EIA - 606 A Norma de Administración para la Infraestructura de Telecomunicaciones Comerciales					
17	Clase 1: Edificio con un espacio de telecomunicaciones		x		
18	Clase 2: Edificio con varios espacios de telecomunicaciones	x			
19	Clase 3: Campus con múltiples edificios		x		
20	Clase 4: Institución con múltiples campus	x			Oficinas en cantones y parroquias
21	El etiquetado de la red cuenta con códigos de colores para facilitar su identificación	x			sin etiquetado
22	La red está dividida conforme al servicio que brindan (voz, datos, CCTV)	x			
ANSI/TIA/EIA 607-B1 Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales					
23	Cumple con los Requerimientos para instalaciones a tierra de los sistemas de Telecomunicaciones en Edificios Comerciales.	x			
EQUIPAMIENTO					
24	Dispone de Circuito Cerrado de TV (CCTV)	x			
26	El CCTV es administrable desde el data center	x			
26	Dispone de telefonía IP	x			

27	Telefonía IP Es administrable desde el data center	x			
28	Cuenta con dispositivos de comunicaciones que permitan la conexión WIFI (Router - Access Point)	x			Obsoletos (año 2000)
CONTROL DE ACCESO					
29	La edificación cuenta con puertas de seguridad con sistema de control de acceso		x		
30	La institución cuenta con protocolo de control de acceso para el personal y visitantes	x			
31	Las Salas de Telecomunicaciones están protegidos de acceso no autorizado		x		Sin dispositivos de control de accesos
32	Dispone con un registro de control de usuarios que acceden a la red	x			
SEGURIDAD					
33	La red cuenta con equipo *Firewall* físico para protección	x			No Recomendado Mikrotik
34	La red cuenta con equipos y aplicaciones (IDS, IPS, NIDS)		x		
35	Para evitar vulnerabilidades en las WLAN ¿Usan protocolos de autenticación, como está establecido en el estándar IEEE 802?11i (Norma Inalámbrica)?	x			
36	Utiliza el nombre de la entidad o departamento en el SSID.		x		
37	La configuración predeterminada (fabrica) de los dispositivos de comunicaciones (Router - Access Point) ha sido cambiada	x			
38	Considera que los password para ingreso a los dispositivos de comunicaciones (Router - Access Point) son seguros	x			
39	Dispone de VLAN’s con el objetivo de tener una mayor administración en cada una de los servicios de red	x			
40	Las direcciones IP´S de los equipos son fijas	x			
41	Los equipos informáticos cuentan con antivirus licenciados		x		
42	Utilizan herramientas software de diagnóstico para Identificar vulnerabilidades en los sistemas que utiliza la institución	x			
43	Monitorea y registra periódicamente la red para la prevención de errores o situaciones anómalas	x			
POLITICAS - PLANES - DOCUMENTACION					
44	Existe políticas para control de acceso para dispositivos de red y comunicaciones	x			
45	Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red		x		
46	Existe políticas de control de acceso y uso de los servicios de la red	x			
47	Existe una política de copias de respaldo o backups	x			
48	Existe política para controlar la instalación de software en sistemas operativos.		x		
49	Existe políticas o procedimientos de ingreso seguro para usuarios de los computadores en sistemas y aplicaciones	x			
50	Dispone de un inventario actualizado de los equipos informáticos y *networking*	x			Equipos obsoletos (años 2000 - 2004)
51	Dispone de política o documentación para la implementación y configuración de los dispositivos de red	x			

3. Políticas de uso del correo institucional

GOBERNACIÓN DE
LA PROVINCIA DE TUNGURAHUA

POLÍTICAS DE USO
CORREO ELECTRÓNICO INSTITUCIONAL
GOBERNACIÓN DE TUNGURAHUA

Este documento contiene información de propiedad exclusiva de Gestión de Tecnologías de la Información y Comunicaciones de la Gobernación de Tungurahua. La información que contiene este documento se mantendrá de forma confidencial y reservada, no pudiendo ser divulgada a personal interno o externo que no sean servidores públicos de la Gobernación de Tungurahua.

Gestión de Tecnologías de la Información y Comunicaciones
Ambato, Julio/ 2020

INDICE

4. Capacitación firma electrónica

ASUNTO: Capacitación Firma Electrónica

De mi consideración:

Reciba un cordial y atento saludo, en virtud al Decreto Presidencial No.981, de 28 de enero de 2020, en el cual manifiesta en la segunda cláusula de Disposiciones Generales lo siguiente "Las autoridades, funcionarios y servidores públicos que en el ejercicio de sus funciones suscriban documentos, deberán contar obligatoriamente, a su costo, con un certificado de firma electrónica...", por tal motivo, como Analista de Tics en coordinación con la Abg. Mónica Durán, Analista de Talento Humano, se gestionó la capacitación sobre la Firma Electrónica, con el siguiente temario que contempla:

1. Que es la firma electrónica.
2. Como firmar documentos electrónicos.
3. Validación de documentos firmados electrónicamente.
4. Vigencia de la Firma Electrónica.
5. Tipos de Firma Electrónica, diferencias.
6. Cómo verificar la caducidad de mi firma.
7. Instalación de la firma electrónica en archivo.
8. Costos de la firma electrónica.
9. Aplicativos gratuitos para firmar electrónicamente.

El curso es impartido por el Ing. Marlon Bedón, profesional avalado por la SETEC, a través de la plataforma Zoom, tiene una duración aproximada de 1 hora.

Fecha: 16 de Octubre de 2020
Hora: 10:00
Link de enlace:
https://us02web.zoom.us/j/81726411237?pwd=RXFyelJPTnlNNTUyUTlicmkxd1d3UT09

ID: 817 2641 1237
Contraseña: 781698

Para la constancia de la participación se hará entrega de un Certificado de asistencia luego de obtener un puntaje mínimo de 7/10 en el cuestionario virtual que se tomará al finalizar. Es importante que los participantes se registren en el formulario: para que reciban las preguntas a contestar vía móvil.

Formulario de Registro: http://firmasecuador.com/BE-VA/

5. Manual de usuario del Correo Electrónico Institucional

GOBERNACIÓN DE
LA PROVINCIA DE TUNGURAHUA

MANUAL DE USUARIO
CORREO ELECTRÓNICO INSTITUCIONAL

zimbra®

Este manual de usuario está enfocado a los usuarios finales del correo Web Institucional Zimbra.

La información que contiene este documento se mantendrá de forma confidencial, reservada y no debe ser divulgada a personal que no pertenezca a la Gobernación de Tungurahua.

GOBERNACIÓN DE TUNGURAHUA
Ambato, Noviembre/ 2020

ÍNDICE DE CONTENIDOS

6. Manual de Uso del Correo Electrónico Institucional Zimbra

ASUNTO: Manual de Uso del Correo Electrónico Institucional - Zimbra

De mi consideración:

Reciban un cordial y atento saludo, la presente tiene por objeto hacerle llegar el Manual de Uso del Correo Electrónico Institucional - Zimbra, en donde se detalla la manera adecuada y correcta de utilizar esta herramienta, tomando en cuenta las siguientes consideraciones:

El nombre del correo electrónico para funcionarios de Planta Central, está compuesto de la letra del nombre, seguido del signo punto (.), seguido el apellido y la identificación de la institución (@gobernaciontungurahua.gob.ec).

Ejemplo: v.robayo@gobernaciontungurahua.gob.ec
i.sanchez@gobernaciontungurahua.gob.ec

h.lopez@gobernaciontungurahua.gob.ec

El nombre del correo electrónico para las dependencias, Jefaturas, Tenencias Políticas y Comisarías está compuesto por el nombre de la dependencia (jefatura, comisaria. tenencia), seguido del signo punto (.), seguido del nombre del cantón o el nombre de la parroquia a la que pertenece la dependencia y la identificación de la institución (@gobernaciontungurahua.gob.ec).

Ejemplo: comisaria.patate@gobernaciontungurahua.gob.ec
jefatura.banos@gobernaciontungurahua.gob.ec
tenencia.ulba@gobernaciontungurahua.gob.ec

Listas de Contactos

Es un conjunto de correos electrónicos almacenados en un solo nombre. Puede ser utilizada cuando el remitente desee enviar emails a contactos frecuentes de manera simultánea, en una lista de contactos, al enviar un mensaje a la dirección de la lista, este llegará a la dirección de todas las personas inscritas en ella

La institución cuenta con tres listas de contactos que incluyen todos los contactos de las dependencias, tanto de comisaria, jefaturas y tenencias políticas.

- comisarias@gobernaciontungurahua.gob.ec
- jefaturas@gobernaciontungurahua.gob.ec
- tenencias@gobernaciontungurahua.gob.ec

Los nombres de los correos electrónicos no contienen vocales con tildes ni caracteres especiales como espacios en blanco o la letra ñ. el único carácter que contiene el nombre del correo electrónico es el signo punto (.)

Se adjunta la lista de correo electrónico de todos los funcionarios y dependencias de la Gobernación de Tungurahua

Es menester aclarar que la información del directorio de los funcionarios y dependencias de la Institucion se encuentra en la página web:

https://gobernaciontungurahua.gob.ec/?page_id=28

Particular que pongo en su conocimiento para los fines pertinentes

Con sentimientos de distinguida consideración.

7. Obtención de respaldos del Sistema de Gestión Documental Quipux y Respaldos de seguridad o Backups de las computadoras

ASUNTO: Obtención de respaldos del Sistema de Gestion Documental Quipux y Respaldos de seguridad o Backups de las computadoras

De mi consideración:

Reciban un cordial y afectuoso saludo, por medio de la presente pongo en su

conocimiento el instructivo adjunto, elaborado por la Subsecretaría de Gobierno Electrónico, que permitirá dar a conocer el proceso que se debe seguir para la obtención de respaldos de los documentos generados en el Sistema de Gestión Documental Quipux, para el caso de los usuarios tipo "servidor público" que se encuentren **activos** en dicho sistema.

Para efectos de este instructivo se denominará "Activo" al funcionario público que tenga las siguientes características:

- Se encuentre laborando en la Gobernación de Tungurahua
- La institución pública se encuentre registrada y haciendo uso del Sistema de Gestión Documental Quipux en forma institucional.
- Posea un usuario y contraseña válida en Quipux.
- Su acceso o ingreso al sistema Quipux (inicio de sesión) sea exitoso.

Estas solicitudes de respaldos se realizarán exclusivamente en los casos donde el funcionario público activo se encuentre en el proceso de desvinculación de la institución.

Respaldos de seguridad o Backups: Es el proceso mediante el cual se copian todos los archivos importantes de un usuario almacenados en el computador a otro medio con el fin de poder recuperarlos en caso de pérdida de la información. Esto es muy importante debido a que existen múltiples causas por las cuales un usuario podría experimentar este problema. Por ejemplo, los discos duros suelen tener una vida útil limitada debido al desgaste natural del motor. Las memorias poseen una cantidad de escrituras de datos limitada y por otro lado, un computador portátil está expuesto al extravío o robo. Además, los virus también pueden contribuir a que una persona pierda información de su computadora.

Para evitar la perdida de información en los equipos tecnológicos, una solución bastante efectiva es hacer un 'backup' o copia de seguridad. Esta práctica consiste en hacer un guardado de los documentos o archivos importantes que se encuentran almacenados en su computador para que no se nos pierdan y que podamos acceder a ellos de una u otra forma si tenemos algún problema.

Es importante establecer la periodicidad con la que se debe realizar la copia de seguridad. Esta decisión debe adoptarse considerando la frecuencia con que se modifican, eliminan y crean archivos. Si se trabaja todos los días en un archivo, será necesario realizar una copia de seguridad a diario. En cambio, una carpeta con imágenes debe ser nuevamente respaldada solo cuando se agreguen fotografías.

El medio de almacenamiento de las copias de seguridad será el espacio físico en donde se guarde la información a ser respaldada, por ejemplo: