



**UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD DE
ADMINISTRACIÓN, FINANZAS E INFORMÁTICA**

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA

PRÁCTICA PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

**ANÁLISIS DE POLÍTICAS DE SEGURIDAD APLICABLES A
INFRAESTRUCTURAS TECNOLÓGICAS DEL GOBIERNO AUTÓNOMO
DESCENTRALIZADO DEL CANTÓN BABAHOYO**

ESTUDIANTE:

ADONIS DARÍO NARVÁEZ CEREZO

TUTOR:

ING. ERICK MAGNO RICAURTE ZAMBRANO

NOVIEMBRE 2022 - ABRIL 2023

ANÁLISIS DE POLÍTICAS DE SEGURIDAD APLICABLES A INFRAESTRUCTURAS TECNOLÓGICAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN BABAHOYO

RESUMEN

La seguridad de la información es un pilar fundamental para que los municipios funcionen sin inconvenientes informáticos y sus operaciones y transacciones sean adecuadas y fructíferas, existen normativas que les exigen buenas prácticas de control de la seguridad de la información.

El no seguir normativas sujetas a supervisión y control puede desencadenar en errores administrativos básicos, pero además puede tener consecuencias de gran Impacto, pues la información en los gobiernos autónomos descentralizados es uno de los activos más preciados.

Las políticas bien definidas posibilitarán verificar la persistencia de los servicios, es decir, comprender si las regulaciones pueden establecer demandas para la sostenibilidad de los servicios, incluso en momentos de emergencia. Las empresas pueden estar obligadas a ejecutar planes de emergencia, copias de seguridad y sistemas de recuperación de catástrofes para asegurar que los sistemas tecnológicos estén siempre disponibles.

PALABRAS CLAVES

POLITICAS, NORMAS, ISO, NCI, GAD

PLANTEAMIENTO DEL PROBLEMA

La seguridad es un Pilar fundamental que los gobiernos en el territorio como lo es el GAD de Babahoyo, poco lo aplican teniendo además normativas que les exigen que se apeguen a normas de control interno relacionadas con buenas prácticas de control de la seguridad de la información.

El no seguir normativas sujetas a supervisión y control puede desencadenar en errores administrativos básicos, pero además puede tener consecuencias de gran Impacto, pues la información en los gobiernos autónomos descentralizados es uno de los activos más importantes y el hecho que esta no esté amparada en normativas que permitan su seguridad es un riesgo que claramente no deberían tener.

En general, el Gobierno Autónomo Descentralizado Cantonal de Babahoyo cuenta con una baja elaboración de lo que corresponde a Políticas de seguridad relacionadas con sus infraestructuras tecnológicas, esto al no tener conocimiento por parte de los coordinadores de tecnologías y directores que rigen los procesos informáticos en las diferentes instituciones descentralizadas y no aplicar normas obligatorias de control

interno que exigen la aplicabilidad de reglamentación para incidir en el cuidado de la infraestructura soporte a los usuarios y sobre todo políticas que permitan el buen uso de las tecnologías y su seguridad en las organizaciones.

Esto suele conllevar a que el crecimiento tecnológico en las organizaciones no sea eficiente por lo que requiere inversión frecuente para solventar problemas que debieron haber sido mitigados con anterioridad al tener las reglas claras y los diseños de procesos en tiempos oportunos.

Justificación

Con este trabajo de titulación, se garantiza eficazmente que se realizará un análisis apegado a lo que requiere el Gobierno Autónomo Descentralizado de Babahoyo en materia de seguridad de la información, ya que las políticas relacionadas con la Seguridad informática pueden establecer requisitos para la protección de la información y los sistemas informáticos.

Las normas de control interno de la Contraloría General del Estado pueden tener un impacto significativo en el uso y la implementación de la tecnología en las organizaciones sujetas a su supervisión y control.

En general, las políticas de seguridad aplicables buscan garantizar la eficiencia, eficacia, transparencia y responsabilidad en la gestión pública, y la tecnología puede ser una herramienta importante para lograr estos objetivos. Las normas pueden establecer requisitos específicos en relación con el uso de la tecnología, tales como:

Las organizaciones pueden estar obligadas a implementar medidas de seguridad informática, tales como firewalls, sistemas de autenticación, encriptación, entre otros, para garantizar la integridad y la confidencialidad de la información, todo debe estar amparado en políticas que permitan un mejor desempeño y garantía de disponibilidad.

Además, con políticas bien claras se pueden mejorar el control de procesos, es decir, las normas pueden establecer requisitos para el control de los procesos de la organización, incluyendo los procesos relacionados con la tecnología. Las organizaciones pueden estar obligadas a establecer controles de calidad y de cumplimiento de los procesos para garantizar la eficacia y eficiencia en el uso de la tecnología y sus infraestructuras tecnológicas en general.

El análisis de las políticas, permitirán comprobar la continuidad de los servicios, esto es, comprender o verificar si las normas pueden establecer requisitos para la continuidad de los servicios, incluso en situaciones de contingencia. Las organizaciones pueden estar obligadas a implementar planes de contingencia, respaldos y sistemas de recuperación de desastres para garantizar la disponibilidad de los sistemas de tecnología en todo momento.

Así mismo, puede decirse que este trabajo es pertinente y justificable, porque además la seguridad aplicable a las infraestructuras puede influir en el GAD de Babahoyo para verse bien en lo referente a la rendición de cuentas, ya que las normas pueden establecer requisitos para la rendición de cuentas en relación con el uso de la tecnología. Las organizaciones pueden estar obligadas a mantener registros de auditoría, informes de gestión y otros documentos que permitan la evaluación de la gestión de la tecnología y la rendición de cuentas a las autoridades competentes.

De modo general, este análisis desarrollado en este caso de estudio, puede influir en la adopción y el uso de la tecnología en las organizaciones sujetas a su supervisión y control, al establecer requisitos específicos relacionados con la seguridad informática, el control de procesos, la continuidad de los servicios y la rendición de cuentas; el sector público en general debe cumplir normas de control interno para lograr garantizar una gestión efectiva y responsable de la tecnología en el sector público.

Objetivos

General

Analizar las políticas de seguridad aplicables al Gobierno Autónomo Descentralizado de Babahoyo para un mejor control y uso de la información.

Específicos

Fundamentar teorías inherentes a las políticas informáticas para tener mejores prácticas de seguridad de la infraestructura tecnológica.

Recopilar datos y aspectos relacionados con las normas aplicadas en Gobierno Autónomo Descentralizado de Babahoyo que permitan demostrar su impacto.

Plasmar la discusión de resultados para recomendar buenas prácticas orientadas a normas de mejoramiento de la seguridad de la infraestructura tecnológica.

Línea de investigación

Este documento se refiere o se enfoca a la línea de investigación relacionado con los Sistemas de información y comunicación, emprendimiento e innovación; y se complementa además con una sub línea de investigación que se relaciona con las redes y las telecomunicaciones que son afines a la carrera de sistemas de información pues los especialistas en esta profesión requieren de elementos fundamentales que les permitan comprender la lógica y la funcionalidad para aplicar normativas y políticas afines a las tecnologías de forma general.

MARCO CONCEPTUAL

LOS GOBIERNOS AUTONOMOS DESCENTRALIZADOS

Los GAD's o los Gobiernos Autónomos Descentralizados, son organizaciones gubernamentales o empresas de gobierno que permiten administrar un territorio local esto es un cantón una parroquia o una provincia, están rígidamente por el código de ordenamiento territorial y cada uno de ellos tiene sus competencias apegados al estamento legal que es el COIP; y están organizados de la siguiente forma:

- Gobiernos Provinciales

- Gobiernos Cantonales

- Gobiernos Parroquiales

El modelo existente hace esfuerzos para ya no ser dependiente siempre de la capital de la república es decir de forma descentralizada todo trabaja mejor ha sido una de las cualidades de estos gobiernos descentralizados que en cierta parte han logrado su autonomía con sus competencias únicas, esto conlleva a:

Administración eficiente de recursos: Esto es una de las mejores estrategias que tiene los gobiernos autónomos descentralizados es la administración eficiente de recursos. Estos gobiernos tienen la responsabilidad de administrar los recursos públicos de manera efectiva y transparente para garantizar el desarrollo y bienestar de sus comunidades.

Participación ciudadana: Es importante que los gobiernos autónomos descentralizados fomenten la participación ciudadana en la toma de decisiones. Deben crear canales para que los ciudadanos puedan expresar sus opiniones y sugerencias sobre políticas públicas y programas.

Desarrollo sostenible: Los gobiernos autónomos descentralizados también tienen la responsabilidad de promover el desarrollo sostenible en sus comunidades. Esto implica equilibrar el desarrollo económico con la conservación del medio ambiente y el bienestar social, Borja, J., & Castells, M. (1997).

Fortalecimiento institucional: Para que los gobiernos autónomos descentralizados funcionen de manera efectiva, es fundamental contar con instituciones sólidas y transparentes. Esto requiere de una planificación estratégica y una gestión adecuada de los recursos humanos y financieros.

Lucha contra la corrupción: La corrupción es un problema que afecta a muchos gobiernos en todo el mundo, y los gobiernos autónomos descentralizados no son una excepción. Es importante que estos gobiernos implementen medidas para prevenir y combatir la corrupción en todas sus formas.

Según Foa Torres y González González (2019), Todos los estudios indican que son necesarias las descentralizaciones, porque son realidades diferentes a causa de necesidades diferentes; no es lo mismo solucionar un problema surgido en Vinces que es un cantón de Los Ríos, comparado con Salinas que es un cantón de la provincia de Santa Elena, aunque ambos son de la costa, pero tienen realidades distintas porque su uso de suelo es distinto en la configuración social también, así como en su economía.

De acuerdo con Ojeda Segovia (2020), la descentralización es un proceso complejo y costoso, que ha generado conflictos desde su inicio y ha afectado a ciertos grupos tanto a nivel local como nacional. La implementación de este proceso requiere de herramientas legales y de la voluntad incondicional y decidida de los tres actores principales: el gobierno central, los gobiernos autónomos y la sociedad. En este sentido,

el las referencias del Código Orgánico de Organización Territorial, como proyecto y Ley de Autonomía y Descentralización establece un marco legal que busca impulsar la descentralización y el cumplimiento de la obligatoriedad de transferir competencias y recursos de acuerdo a lo establecido por la Constitución Política de 2008. Por lo tanto, la descentralización en Ecuador representa un desafío grande para las planificaciones de transformación democrática, social y económica y de recompensación institucional del Ecuador (Código Orgánico de Organización Territorial, Autonomía y Descentralización, exposición de motivos).

Importancia de la seguridad informática de las empresas

De acuerdo con Uni Assignment Centre (2019), la seguridad informática surge alrededor del año 1980, cuando se incrementó el uso de computadoras en centros computacionales. En un principio, la seguridad informática abordaba solo los aspectos de infraestructura, pero con la utilización de sistemas de redes, y especialmente el internet, surgieron nuevas amenazas para la informática. La apertura mundial del internet permitió la expansión a millones de personas, muchas de ellas anónimas, lo que obligó a las empresas a mejorar estrategias de seguridad, no se puede ver a la seguridad informática simplemente como un simple cambio de contraseñas o tal vez como la colocación de un antivirus potente en una PC, la seguridad informática va más allá pues cada día se descubren múltiples formas de defraudar y echar a perder sistemas de información y bases de datos, cada día se descubren muchas nuevas amenazas y por ello es muy necesario mantener un esquema de seguridad que pueda influir en el mantener la información bien resguardada y disponible sobre todo. (Techopedia, 2021).

Y una de las características de un sistema o buenas prácticas para lograr la seguridad informática es iniciar primero con políticas estandarizadas y bien introducidas así como muy socializadas dentro de la institución o empresa; por lo que debe ser protegida de forma adecuada (Perez, 2019), y la seguridad informática es una parte esencial de esa protección.

Seguridad informática en las empresas

La seguridad informática es vital para las empresas debido a las graves consecuencias que pueden surgir de la utilización maliciosa de sus sistemas de información y recursos internos. En consecuencia, es importante contar con personal experto en tecnologías informáticas capaz de predecir las amenazas y los riesgos.

De acuerdo con Southern New Hampshire University (2019), el 62% jefes o directores de informática, encargados de la seguridad en las empresas afirman sentirse medianamente seguros o nada seguros, respecto de los sistemas informáticos de las organizaciones donde estos se desempeñan; mientras que solamente un 7% se siente extremadamente seguro. Como resultado, las empresas están invirtiendo más en seguridad informática, asignando mayores fondos de su presupuesto a esta área para hacer frente a las amenazas de ciberseguridad en constante cambio (Southern New Hampshire University, 2019).

Herramientas de seguridad informática

En la actualidad, es esencial que las herramientas tecnológicas de seguridad informática comúnmente se enfocan en la detección constante y la ejecución redundante para detectar vulnerabilidades técnicas y operativas en los ambientes tecnológicos de la información (TI) de las organizaciones, realizándose escaneos y mediciones desde plataformas digital que permiten una visualización general de los distintos procesos de la

organización. Según información del portal especializado en tecnología, Tech Target, estas medidas preventivas permiten anticipar los riesgos y minimizar los daños ante posibles ataques informáticos que pongan en peligro la información privada de las empresas. Por esta razón, contar con este tipo de herramientas se convierte en una necesidad y en una inversión a corto, mediano y largo plazo para cualquier organización que busque proteger su información y recursos. Tech Target. (2021)

Para que sirve una política de seguridad

Una política de seguridad informática es una herramienta esencial para establecer lineamientos y procedimientos que permitan proteger la información y los recursos informáticos de una organización. Según Mendoza y Mendoza (2020), una política de seguridad informática tiene como objetivo principal establecer directrices para el uso de la tecnología de la información y la comunicación (TIC) dentro de la empresa, para garantizar la disponibilidad, confidencialidad e integridad de la información.

Además, una política de seguridad informática ayuda a las organizaciones a cumplir con las leyes y regulaciones que rigen el uso de la información, así como a prevenir y gestionar los riesgos asociados con la seguridad de la información (Mendoza y Mendoza, 2020). Según los autores, una política de seguridad informática debe incluir aspectos tales como la identificación y autenticación de usuarios, la gestión de contraseñas, el control de acceso a la información, la gestión de riesgos, la seguridad de la red, la seguridad física y la gestión de incidentes.

En resumen, una política de seguridad informática es una herramienta esencial para proteger la información y los recursos informáticos de una organización, garantizar la disponibilidad, confidencialidad e integridad de la información, cumplir con las leyes y regulaciones, y prevenir y gestionar los riesgos asociados con la seguridad de la información.

Políticas informáticas de seguridad aplicables a instituciones publicas

Según Castañeda, Grados, y Taboada (2017), en el contexto de las instituciones públicas, la política de seguridad informática juega un papel fundamental en la protección de la información y sistemas que manejan. La implementación de estas políticas permite establecer un marco de referencia para la gestión de la seguridad informática, establecer normas, procedimientos y buenas prácticas, así como también mejorar la cultura de seguridad informática en la organización.

Además, las políticas de seguridad informática en instituciones públicas deben cumplir con los lineamientos y estándares establecidos por las normativas y leyes en materia de seguridad informática, como la Ley N° 30309 - Ley de Delitos Informáticos en el Perú.

Castañeda, Grados y Taboada (2017) también señalan que la implementación de políticas de seguridad informática en instituciones públicas debe considerar la capacitación constante de los colaboradores, el monitoreo y actualización constante de los sistemas, y la evaluación periódica de la eficacia de las políticas implementadas.

En la actualidad, la tecnología se ha vuelto esencial en todos los ámbitos de la vida, tanto personal como profesional. Sin embargo, con la tecnología también han llegado nuevos riesgos y amenazas en forma de ciberataques y ciberdelitos que pueden poner en peligro la seguridad de la información y los datos de las empresas y organizaciones.

Es por eso que la ciberseguridad se ha convertido en una necesidad crítica para cualquier empresa u organización que quiera proteger sus sistemas y datos contra los ciberataques. Según un informe de la firma de investigación Markets and Markets, se espera que el mercado global de ciberseguridad crezca a una tasa compuesta anual del 10,2% hasta el año 2023, alcanzando un valor de \$ 231,94 mil millones.

Además, el cumplimiento de las normativas de seguridad y privacidad también se ha vuelto cada vez más importante, especialmente para las empresas que manejan datos sensibles de los clientes y usuarios. En muchos países, existen regulaciones como la RGPD en la Unión Europea o la Ley de Protección de Datos Personales en México, que establecen requisitos específicos para la protección de los datos personales y la seguridad informática.

En tal sentido, la ciberseguridad es fundamental en la era digital actual, y las empresas y organizaciones deben implementar políticas y prácticas efectivas para proteger sus sistemas y datos contra los ciberataques y cumplir con las regulaciones de seguridad y privacidad.

Las normas de control interno de la Contraloría de Ecuador y la seguridad informática

El control interno se define como un conjunto de políticas, procedimientos y medidas adoptadas por la gerencia para garantizar la eficiencia, eficacia, transparencia y rendición de cuentas en el uso de los recursos públicos (Pizarro, 2018). Entre los objetivos del control interno en las instituciones públicas se encuentra la protección de los activos, incluyendo la información, contra posibles riesgos y amenazas.

La seguridad informática se refiere a la protección de la información contra posibles amenazas, como el acceso no autorizado, la manipulación, la divulgación o la destrucción (ISO/IEC, 2018). Las instituciones públicas manejan grandes cantidades de información sensible y crítica, por lo que es necesario implementar medidas de seguridad informática adecuadas para protegerla.

En resumen, la implementación de normas de control interno en las instituciones públicas, incluyendo medidas de seguridad informática, es esencial para garantizar la transparencia, la eficiencia y la protección de los recursos públicos y la información.

Las Normas de Control Interno 410 son un conjunto de estándares emitidos por la Contraloría General del Estado de Ecuador

Las Normas de Control Interno 410 son un conjunto de estándares emitidos por la Contraloría General del Estado de Ecuador que establecen las políticas y procedimientos necesarios para asegurar la eficacia, eficiencia y transparencia de las operaciones gubernamentales. En relación a la seguridad informática, estas normas establecen la necesidad de contar con controles de seguridad adecuados para proteger la información y los sistemas de información de la entidad.

Según la Norma de Control Interno 410.13, se debe establecer un "Plan de Continuidad del Negocio" que contemple la protección y recuperación de la información y sistemas de información críticos de la entidad ante eventos que puedan interrumpir o comprometer su funcionamiento normal. Asimismo, la Norma de Control Interno 410.15 establece la necesidad de contar con un "Plan de Contingencia" para enfrentar situaciones de emergencia que puedan afectar la integridad de los datos y sistemas informáticos.

Estas normas de control interno son fundamentales para garantizar la seguridad informática en las entidades gubernamentales de Ecuador y cumplir con las regulaciones y leyes de protección de datos. Es importante que las instituciones públicas se adhieran a estas normas y establezcan medidas adecuadas para proteger su información y sistemas de información.

La norma de control interno 410 establece que la máxima autoridad de la entidad debe aprobar las políticas y procedimientos para organizar adecuadamente el área de tecnología de información, asignar el talento humano calificado y proveer la infraestructura tecnológica necesaria. Además, la Unidad de Tecnología de Información debe definir, documentar y difundir políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, los cuales deben ser actualizados periódicamente e incluir tareas, responsables, procesos de excepción, enfoque de cumplimiento y control de los procesos normados, así como sanciones administrativas en caso de incumplimiento.

Las políticas y procedimientos deben estar apegadas a estas normas de control interno de contraloría, ya que permiten tener una injerencia directa sobre la mejora continua de la infraestructura tecnológica en las instituciones de gobierno siendo que hay una sección completa enfocada a brindar una guía de mejores prácticas en relación a la conectividad a los equipos a las bases de datos y a la informática en general de las instituciones públicas, esta norma es muy poco conocida pues personas con experiencia han comentado que recién la conocen luego de que les llega un llamado de atención por

no cumplir cierto punto de la norma, en tal sentido supone que la contraloría debería capacitar de forma permanente en el cumplimiento de sus normas a los gobiernos autónomos descentralizados en sus diferentes niveles.. (Contraloría General del Estado, 2017)

Las normas iso y la seguridad informática en las instituciones publicas

Las Normas ISO proporcionan a las organizaciones un marco para el establecimiento, implementación, mantenimiento y mejora continua de los sistemas de gestión de seguridad de la información. Las normas ISO 27001 y 27002 son especialmente relevantes para las instituciones públicas que buscan garantizar la protección y confidencialidad de los datos que manejan. Estas normas proporcionan un conjunto de controles y mejores prácticas que pueden ser implementados en una organización para gestionar los riesgos de seguridad de la información de manera eficaz y consistente.

Según Jaramillo et al. (2018), "las normas ISO 27001 y 27002 ofrecen a las instituciones públicas una guía detallada sobre cómo establecer y poder mantener un sistema de gestión de la seguridad de la información siempre efectivo y eficiente; estableciendo medidas para asegurar la confidencialidad, integridad y alta disponibilidad de los datos e información" (p. 21).

MARCO METODOLOGICO

Cuando se decide llevar a cabo una investigación científica sobre políticas de seguridad aplicables a infraestructuras tecnológicas de los gobiernos autónomos descentralizados cantonales, es fundamental elegir una metodología adecuada que sea relevante para los objetivos y problemas de la investigación. Existen diversas metodologías de investigación en el ámbito de las políticas relacionadas con la seguridad de la información e infraestructuras.

Una posible opción es utilizar un enfoque de estudio de casos para examinar de manera minuciosa uno o varios casos y comprender mejor los desafíos que conlleva implantar políticas de seguridad en las infraestructuras de las organizaciones descentralizadas cantonales.

Asimismo, este enfoque puede ayudar a identificar posibles soluciones para abordar estos desafíos de manera efectiva. Además, se pueden emplear técnicas de entrevistas con expertos en seguridad informática para obtener información relevante sobre las necesidades y desafíos de implantar políticas adecuadas de seguridad. Esto permite recopilar datos de profesionales con experiencia en el tema y obtener información valiosa sobre los problemas de vulnerabilidades, entre otros aspectos relevantes.

Otra opción es emplear una metodología de análisis de documentos para recopilar información relacionada con el uso de políticas aplicables a tecnologías y seguridad de infraestructuras en el Gobierno Autónomos Descentralizados Cantonal de Babahoyo. Esta metodología se enfocará en documentos especializados en el tema, como informes, libros y artículos.

Cuando se requiera abordar cuestiones que no se pueden cuantificar, se puede utilizar una metodología cualitativa. Esto permitirá recopilar información sobre las experiencias y percepciones de expertos en el ámbito de la tecnología en relación con la seguridad de la información.

Para validar y comparar los resultados obtenidos mediante el análisis de documentos, se llevarán a cabo entrevistas con especialistas en la materia. Luego, se analizarán y discutirán los resultados obtenidos para confirmar las contribuciones de los expertos involucrados en la investigación.

RESULTADOS

Se han realizado entrevistas a diferentes funcionarios de Gobiernos Autónomos Descentralizados Municipales, todos ellos conocedores de su institución y con amplia experiencia en informática, en relación a: **Como conocedor del funcionamiento de la infraestructura de seguridad en un GAD Cantonal y técnico informático de amplia experiencia, indicar por favor cuáles son las políticas de seguridad aplicables a las infraestructuras tecnológicas de los municipios;** Responde el Ing. García (Anexo1), La política de seguridad de la información establece reglas y pautas para proteger la gestión, clasificación, tratamiento, almacenamiento y protección de la información de una organización. Además, es importante que las infraestructuras tecnológicas de los municipios tengan políticas de gestión de accesos y contraseñas, backup y recuperación de datos, seguridad de red y gestión de dispositivos móviles. Estas políticas deben definir medidas de seguridad necesarias para proteger la información y los dispositivos de posibles ataques, así como establecer procedimientos para la gestión y el acceso de usuarios.

Así mismo, responde **el Ing. Rizo indicó:** Es esencial controlar el acceso a los sistemas, redes y datos de la infraestructura tecnológica de un municipio y establecer políticas para su gestión y control. Las políticas de contraseñas también son importantes, estableciendo requisitos de complejidad, frecuencia de cambio y gestión por parte de los usuarios y administradores.

El Ing. Meza Contesta: Las políticas de seguridad informática de un municipio deben incluir políticas de accesos para controlar quiénes pueden acceder a los sistemas, redes y datos. También deben establecer políticas de contraseñas para garantizar contraseñas seguras y una gestión adecuada de las mismas. Además, se necesitan políticas de seguridad física para proteger la infraestructura tecnológica de daños o intrusiones, incluyendo la ubicación física y la protección contra robos e incendios.

En lo relacionado con : **Como la Norma de control interno influye en las políticas informáticas relacionadas con la de seguridad la infraestructura tecnológica;** el Ing.

García indicó: La NCI tiene una gran influencia en las políticas de seguridad informática relacionadas con la infraestructura tecnológica, ya que establece los requisitos y lineamientos necesarios para proteger la información y los activos de la organización. Las políticas de seguridad deben estar alineadas con la NCI para garantizar controles de seguridad efectivos, así como contar con políticas y procedimientos documentados para la gestión de la información, la gestión de riesgos y la gestión de incidentes de seguridad.

Así mismo, responde el **Ing. Rizo:** La Norma de Control Interno (NCI) es una guía que proporciona un marco de referencia para la gestión de riesgos y el control interno en las organizaciones. La NCI establece una serie de principios y lineamientos que deben ser aplicados por la alta dirección de una organización para garantizar la eficacia y eficiencia de sus procesos, la integridad de su información y el cumplimiento de las leyes y regulaciones aplicables.

El **Ing. Meza Contesta:** La NCI y la tecnología están relacionadas para fortalecer y mejorar el control interno. La NCI establece los requisitos para el diseño y evaluación del control interno, mientras que la tecnología puede ser utilizada para identificar y evaluar los riesgos y para supervisar y monitorear los controles necesarios.

En lo relacionado con **Que estrategias considera importantes para desarrollar e implantar políticas que permitan brindar seguridad a las infraestructuras tecnológicas en una institución municipal;** Responde el Ing. García (Anexo1), lo siguiente: Para garantizar la seguridad de la infraestructura tecnológica es necesario identificar los riesgos, establecer políticas claras y documentadas, implementar controles de acceso, capacitar al personal, implementar soluciones de seguridad, realizar pruebas y auditorías de seguridad y mantenerse actualizado sobre las últimas amenazas y soluciones de seguridad. Todo esto permitirá proteger la infraestructura y los datos de posibles amenazas y vulnerabilidades.

Así mismo, responde el **Ing. Rizo:** Identificar los riesgos de seguridad informática.

Establecer políticas de seguridad que permitan mitigar los riesgos y proteger la información de la organización.

Comunicar las políticas de seguridad a todos los empleados.

Implementar controles de seguridad tecnológicos.

Capacitar a los empleados en las políticas de seguridad.

El **Ing. Meza Contesta**: La evaluación de riesgos es importante para identificar las amenazas y vulnerabilidades de la organización y determinar los controles de seguridad necesarios. Las políticas de seguridad deben establecer los procedimientos y responsabilidades y ser claras y comprensibles para todos los empleados. La capacitación de los empleados es clave para que comprendan la importancia de la seguridad informática y sepan cómo manejar situaciones de riesgo.

En lo relacionado con los componentes de infraestructuras tecnológicas a las que hay que aplicarles políticas de seguridad con un enfoque mas cuidadoso; contesta García: Las políticas de seguridad deben aplicarse a diferentes componentes de la infraestructura tecnológica, como servidores, redes, dispositivos de almacenamiento, aplicaciones y software, dispositivos móviles y sistemas de control industrial. Es importante asegurar la disponibilidad, integridad y confidencialidad de los datos almacenados y procesados en estos componentes y protegerlos de posibles pérdidas, robos o accesos no autorizados. También es fundamental aplicar políticas de seguridad específicas para proteger los sistemas de control industrial utilizados en infraestructuras críticas y garantizar la continuidad de las operaciones críticas.

El **Ing. Meza Indica**: Las políticas de seguridad deben cubrir aspectos como autenticación, cifrado, gestión de contraseñas, monitorización del tráfico y prevención de intrusiones en redes y sistemas de comunicación. Además, se deben establecer políticas de seguridad para servidores y sistemas operativos, y medios de almacenamiento, cubriendo aspectos como configuración segura, encriptación de datos, control de acceso y monitorización de actividad del usuario.

El **Ing. Rizo** comenta que: Los Servidores, Los Firewalls, Los Sistemas Operativos de Los Usuarios Haciéndoles Hardening

DISCUSION DE RESULTADOS

Las políticas de seguridad aplicables a las infraestructuras tecnológicas de los municipios incluyen la política de seguridad de la información, gestión de accesos y contraseñas, backup y recuperación de datos, seguridad de red y gestión de dispositivos móviles.

La Norma de control interno (NCI) influye en estas políticas y es necesario alinearlas con los requisitos y lineamientos de la NCI. Para desarrollar e implantar políticas de seguridad efectivas, es importante identificar los riesgos, establecer políticas claras, implementar controles de acceso, capacitar al personal, implementar soluciones de seguridad, realizar pruebas y auditorías de seguridad y mantenerse actualizado sobre las últimas amenazas y soluciones de seguridad.

Los componentes de infraestructuras tecnológicas a los que se deben aplicar políticas de seguridad con un enfoque más cuidadoso incluyen servidores, redes, dispositivos de almacenamiento, aplicaciones y software, dispositivos móviles y sistemas de control industrial, especialmente en infraestructuras críticas.

El control interno se refiere a un conjunto de políticas, procedimientos y medidas adoptadas por la gerencia para garantizar la eficiencia, eficacia, transparencia y rendición de cuentas en el uso de los recursos públicos, y la protección de los activos, incluyendo la información, contra posibles riesgos y amenazas.

La seguridad informática se refiere a la protección de la información contra posibles amenazas, como el acceso no autorizado, la manipulación, la divulgación o la destrucción. En las instituciones públicas, es necesario implementar medidas de seguridad informática adecuadas para proteger la información sensible y crítica que manejan.

Las Normas de Control Interno 410 brindan unos estándares emitidos por la Contraloría General del Estado de Ecuador que establecen las políticas y procedimientos necesarios para asegurar la eficacia, eficiencia y transparencia de las operaciones gubernamentales, incluyendo la seguridad informática. La norma de control interno 410 establece la necesidad de contar con controles de seguridad adecuados para proteger la información y los sistemas de información de la entidad, y establece procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización.

Las Normas ISO, como la ISO 27001 y 27002, proporcionan un marco para el establecimiento, implementación, mantenimiento y mejora continua de los sistemas de gestión de seguridad de la información, y son especialmente relevantes para las instituciones públicas que buscan garantizar la protección y confidencialidad de los datos que manejan.

CONCLUSIONES

La información es un activo muy valioso para las instituciones públicas como lo es para el Gobierno Autónomo Descentralizado de Babahoyo, es decir la municipalidad, ya que estos manejan servicios ciudadanos necesarios para que un territorio funcione, el pretender no cuidarla o no tener reglas claras que fortalezcan su seguridad puede ser un error grave.

Para lograr tener mejores resultados de seguridad en toda la infraestructura tecnológica pueden combinarse políticas informáticas con controles provenientes de normas como las ISO 27001 y 27002, ya que estas ofrecen a las instituciones públicas una guía detallada sobre cómo establecer y sistemas de gestión de seguridad de la información efectivo y eficiente.

El Gobierno Autónomo Descentralizado de Babahoyo deben apearse a Normas de Control Interno, ya que en las normativas de contraloría como la NCI 410-10 Seguridad de tecnología de información, donde se hace referencia a que se debe implementar medidas para proteger y preservar la información y los medios físicos procesados por sistemas informáticos, a fin de evitar pérdidas o fugas.

Estas medidas incluyen la ubicación adecuada y el control de acceso físico a áreas críticas como servidores, desarrollo y bibliotecas, la definición de procedimientos para hacer respaldos periódicos, la migración de información a medios físicos adecuados y con estándares abiertos en caso de actualización de tecnologías de soporte, el almacenamiento de respaldos críticos en lugares externos a la organización, la implementación y administración de medidas de seguridad a nivel de software y hardware con monitoreo y pruebas periódicas, instalaciones físicas adecuadas para controlar fuego, temperatura, humedad relativa y energía, la disposición de sitios alternativos de procesamiento y la

definición de procedimientos de seguridad para el personal que trabaja en turnos nocturnos o de fin de semana.

RECOMENDACIONES

Es recomendable que las instituciones públicas, específicamente en el Gobierno Autónomo Descentralizado de Babahoyo, tomen medidas efectivas para proteger y preservar su información, ya que ésta es un activo muy valioso y esencial para el buen funcionamiento de los servicios ciudadanos que prestan, esto es Creando Políticas Informáticas para lograr mantener los servicios sin interrupciones.

Se recomienda que el Gobierno Autónomo Descentralizado de Babahoyo combin políticas informáticas con controles provenientes de normas reconocidas como las ISO 27001 y 27002 para lograr mejores resultados en la seguridad de su infraestructura tecnológica, ya que estas normas ofrecen una guía detallada y efectiva para establecer sistemas de gestión de seguridad de la información.

Es recomendable que el Gobierno Autónomo Descentralizado de Babahoyo se apegue a las Normas de Control Interno y en particular a la NCI 410-10 Seguridad de Tecnología de Información, que establece medidas específicas para proteger y preservar la información y los medios físicos procesados por sistemas informáticos.

Para lograr una mayor seguridad de la información, se recomienda que el Gobierno Autónomo Descentralizado de Babahoyo implemente medidas como la ubicación adecuada y el control de acceso físico a áreas críticas, la definición de procedimientos para hacer respaldos periódicos, la implementación de medidas de seguridad a nivel de software y hardware, y la definición de procedimientos de seguridad para el personal que trabaja en turnos nocturnos o de fin de semana, entre otras.

REFERENCIAS BIBLIOGRÁFICAS

Borja, J., & Castells, M. (1997). *Local y global: La gestión de las ciudades en la era de la información*. Madrid: Taurus.

Velasco, J. (2019). La Descentralización y la Autonomía en el Ecuador. *Revista Jurídica de la Universidad Autónoma de Madrid*, (33), 37-58.
<https://doi.org/10.15366/rjua.2019.33.003>

Ojeda Segovia, L. (2019). Descentralización en Ecuador: análisis y perspectivas. *Revista de Investigación Académica*, 20(2), 1-16. <https://doi.org/10.18272/ria.v20i2.1434>

Uni Assignment Centre. (2020). What is computer security? Uni Assignment Centre.
<https://www.uniassignment.com/essay-samples/information-technology/what-is-computer-security>.

Shanbhag, G. (2018). The importance of cyber security in modern Internet age. *International Journal of Engineering and Technology*, 7(3), 53-55.
<https://doi.org/10.14419/ijet.v7i3.36.19745>.

Kumar, A., Gupta, R., & Sharma, R. (2019). An overview of cyber security challenges and solutions. *Proceedings of the 2019 5th International Conference on Computing*

<https://doi.org/10.1109/COMPUTINGSCIENCES.2019.8921604>.

Uni Assignment Centre. (2019). An Introduction to Cyber Security. Uni Assignment Centre. <https://www.uniassignment.com/essay-samples/information-technology/an-introduction-to-cyber-security>

Southern New Hampshire University. (2019). The Growing Importance of Cybersecurity in Business. Southern New Hampshire University. <https://www.snhu.edu/about-us/newsroom/2019/03/the-growing-importance-of-cybersecurity-in-business>

Tech Target. (2021). Vulnerability management (administración de vulnerabilidades). Recuperado de <https://searchsecurity.techtarget.com/definition/vulnerability-management>

Mendoza, C. A. y Mendoza, L. A. (2020). Políticas de seguridad informática. Revista Científica de Administración, 8(2), 15-26. <https://doi.org/10.52292/rca.v8i2.296>

Castañeda, J., Grados, D., & Taboada, J. (2017). Políticas de seguridad informática aplicables en las instituciones públicas. Revista del Instituto de Investigación FIGMMG, 20(40), 54-62.

ISO/IEC. (2018). ISO/IEC 27001:2018 - Information technology - Security techniques - Information security management systems - Requirements. <https://www.iso.org/standard/54534.html>

Pizarro, R. (2018). Control interno en las instituciones del sector público. Universidad de San Martín de Porres. https://repositorio.usmp.edu.pe/bitstream/handle/usmp/3922/Control_interno_en_las_instituciones_del_sector_publico_Ronald_Pizarro_Cervantes.pdf?sequence=1&isAllowed=y

Contraloría General del Estado de Ecuador. (2017). Normas de control interno 410. Recuperado de <https://www.funcionjudicial.gob.ec/wp-content/uploads/2017/08/CGE-2017-Normas-de-Control-Interno.pdf>

Banco Central del Ecuador. (2015). Norma de Control Interno No. 410 para el sector público. Quito, Ecuador: Banco Central del Ecuador.

Jaramillo, M. A., López, L. F., & Trujillo, R. E. (2018). Análisis de la norma ISO 27001 en la gestión de seguridad de la información. *Tecnura*, 22(57), 18-29. <https://doi.org/10.14483/22487638.12247>

ANEXOS

ANEXO 1 FORMULARIO DE ENTREVISTAS

UNIVERSIDAD TECNICA DE BABAHOYO

ENTREVISTA RELACIONADA CON: ANÁLISIS DE POLÍTICAS DE SEGURIDAD APLICABLES A INFRAESTRUCTURAS TECNOLÓGICAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN BABAHOYO

NOMBRE: ING. GALO GARCIA

EMPRESA: MUNICIPIO DE BABAHOYO CARGO: DIRECTOR

1 Como conocedor del funcionamiento de la infraestructura de seguridad en un GAD Cantonal y técnico informático de amplia experiencia, indicar por favor cuáles son las políticas de seguridad aplicables a las infraestructuras tecnológicas de los municipios:

2 Como la Norma de control interno influye en las políticas informáticas relacionadas con la de seguridad la infraestructura tecnológica

3 Que estrategias considera importantes para desarrollar e implantar políticas que permitan brindar seguridad a las infraestructuras tecnológicas en una institución municipal.

4 Cuáles son los componentes de infraestructuras tecnológicas a las que hay que aplicarles políticas de seguridad con un enfoque mas cuidadoso.

ENTREVISTAS REALIZADAS:

UNIVERSIDAD TECNICA DE BABAHOYO

ENTREVISTA RELACIONADA CON: ANÁLISIS DE POLÍTICAS DE SEGURIDAD APLICABLES A INFRAESTRUCTURAS TECNOLÓGICAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN BABAHOYO

NOMBRE: ING. GALO GARCIA

EMPRESA: MUNICIPIO DE BABAHOYO CARGO: DIRECTOR

1 Como conocedor del funcionamiento de la infraestructura de seguridad en un GAD Cantonal y técnico informático de amplia experiencia, indicar por favor cuáles son las políticas de seguridad aplicables a las infraestructuras tecnológicas de los municipios:

Una política de seguridad de la información es un conjunto de reglas y pautas que establecen los procedimientos de seguridad para la gestión de información, su clasificación, tratamiento, almacenamiento y protección. Esta política debe definir las medidas de seguridad necesarias para proteger la información de la organización, así como el acceso a esta información y la responsabilidad de los empleados en la gestión de la misma.

Gestión de accesos y contraseñas: Las infraestructuras tecnológicas de los municipios deben contar con un sistema de gestión de accesos y contraseñas robusto. Esto implica que se deben definir políticas de contraseñas seguras, establecer políticas de gestión de usuarios y grupos de usuarios, así como políticas de gestión de accesos y permisos.

Política de backup y recuperación: Es fundamental que las infraestructuras tecnológicas de los municipios cuenten con un sistema de backup y recuperación de datos

para garantizar la disponibilidad y la continuidad de los servicios. La política de backup y recuperación debe definir los procedimientos para la copia de seguridad, la frecuencia de los backups y la estrategia de recuperación de datos en caso de fallos o desastres.

Política de seguridad de red: Las políticas de seguridad de red son fundamentales para proteger la infraestructura tecnológica de los municipios de posibles ataques externos. Estas políticas deben establecer las medidas necesarias para prevenir el acceso no autorizado a la red, la detección y la respuesta ante intrusiones, así como la gestión de dispositivos y servicios de red.

Política de gestión de dispositivos móviles: Es necesario establecer políticas de seguridad para la gestión de dispositivos móviles, como smartphones o tablets, que se utilicen en la infraestructura tecnológica del municipio. Estas políticas deben incluir la gestión de accesos, la protección de datos y la configuración de dispositivos móviles.

2 Como la Norma de control interno influye en las políticas informáticas relacionadas con la de seguridad la infraestructura tecnológica

En el caso de las políticas informáticas relacionadas con la seguridad de la infraestructura tecnológica, la NCI influye de manera significativa, ya que establece los requisitos y lineamientos que deben seguir las entidades públicas para garantizar la protección de la información y los activos de la organización.

La NCI establece la necesidad de diseñar e implementar controles de seguridad adecuados para proteger los activos de la entidad, incluyendo los sistemas de información. Esto implica que las políticas informáticas relacionadas con la seguridad de la infraestructura tecnológica deben estar alineadas con los requisitos de la NCI para garantizar la eficacia de los controles de seguridad.

Además, la NCI también establece la necesidad de contar con políticas y procedimientos documentados y actualizados para la gestión de la información, la gestión de riesgos y la gestión de incidentes de seguridad. Estas políticas y procedimientos deben estar diseñados para asegurar la confidencialidad, integridad y disponibilidad de la información y los sistemas de información.

3 Que estrategias considera importantes para desarrollar e implantar políticas que permitan brindar seguridad a las infraestructuras tecnológicas en una institución municipal.

Identificar los riesgos: Es fundamental realizar una evaluación de riesgos de la infraestructura tecnológica para determinar los puntos vulnerables y las amenazas potenciales. Esta evaluación permitirá establecer las medidas de seguridad necesarias para proteger la infraestructura y los datos.

Definir políticas claras y documentadas: Es necesario establecer políticas de seguridad claras y documentadas que incluyan los procedimientos y responsabilidades en la gestión de la seguridad de la infraestructura tecnológica. Estas políticas deben ser comunicadas de manera efectiva a todo el personal y deben ser revisadas y actualizadas de manera periódica.

Establecer controles de acceso: La implementación de controles de acceso adecuados es fundamental para evitar el acceso no autorizado a la infraestructura tecnológica. Esto implica la implementación de contraseñas seguras, autenticación de usuarios, gestión de usuarios y permisos, entre otros.

Capacitar al personal: Es importante capacitar al personal sobre las políticas y procedimientos de seguridad y su responsabilidad en la gestión de la seguridad de la infraestructura tecnológica. Esto permitirá mejorar la conciencia sobre la importancia de la seguridad de la información y reducir los errores humanos que puedan poner en riesgo la seguridad de la infraestructura.

Implementar soluciones de seguridad: Es fundamental contar con soluciones de seguridad adecuadas, como antivirus, firewalls, sistemas de detección de intrusos, sistemas de copias de seguridad y recuperación de desastres, entre otros. Estas soluciones permitirán detectar y mitigar los posibles riesgos de seguridad.

Realizar pruebas y auditorías: Es necesario realizar pruebas y auditorías de seguridad de manera periódica para evaluar la eficacia de las políticas y soluciones de seguridad implementadas y detectar posibles vulnerabilidades y amenazas.

Mantenerse actualizado: Es importante mantenerse actualizado sobre las últimas amenazas y soluciones de seguridad y actualizar las políticas y soluciones de seguridad en consecuencia.

4 Cuáles son los componentes de infraestructuras tecnológicas a las que hay que aplicarles políticas de seguridad con un enfoque mas cuidadoso.

Servidores: Los servidores son componentes críticos de la infraestructura tecnológica, ya que almacenan y procesan datos importantes y sensibles. Es necesario aplicar políticas de seguridad estrictas para asegurar la disponibilidad, integridad y confidencialidad de los datos almacenados en los servidores.

Redes: Las redes son el medio por el cual los dispositivos de la infraestructura tecnológica se conectan y comunican entre sí. Es fundamental aplicar políticas de seguridad para proteger la red de posibles ataques y asegurar la privacidad de la información transmitida.

Dispositivos de almacenamiento: Los dispositivos de almacenamiento, como discos duros, memorias USB y discos externos, pueden contener datos importantes y sensibles. Es necesario aplicar políticas de seguridad para proteger estos dispositivos de posibles pérdidas, robos o accesos no autorizados.

Aplicaciones y software: Las aplicaciones y software utilizados en la infraestructura tecnológica pueden contener vulnerabilidades y errores de seguridad que pueden ser explotados por atacantes. Es necesario aplicar políticas de seguridad para asegurar la confidencialidad, integridad y disponibilidad de los datos procesados por estas aplicaciones y software.

Dispositivos móviles: Los dispositivos móviles, como teléfonos inteligentes y tabletas, se utilizan cada vez más para acceder a la infraestructura tecnológica. Es necesario aplicar políticas de seguridad para proteger los datos almacenados y transmitidos por estos dispositivos y evitar su pérdida o acceso no autorizado.

Sistemas de control industrial: Los sistemas de control industrial, como los utilizados en infraestructuras críticas, como plantas de energía y sistemas de transporte, son objetivos de ataques cibernéticos cada vez más frecuentes. Es necesario aplicar políticas de seguridad específicas para proteger estos sistemas y asegurar la continuidad de las operaciones críticas.



ING. GALO GARCIA

DIRECTOR DE TECNOLOGIAS (E)

UNIVERSIDAD TECNICA DE BABAHOYO

ENTREVISTA RELACIONADA CON: ANÁLISIS DE POLÍTICAS DE SEGURIDAD APLICABLES A INFRAESTRUCTURAS TECNOLÓGICAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN BABAHOYO

NOMBRE: ING. GABRIEL MEZA

EMPRESA: GADM BUENA FE

CARGO: COORD TICS

1 Como conocedor del funcionamiento de la infraestructura de seguridad en un GAD Cantonal y técnico informático de amplia experiencia, indicar por favor cuáles son las políticas de seguridad aplicables a las infraestructuras tecnológicas de los municipios:

Políticas de accesos: estas establecen quiénes tienen acceso a los sistemas, redes y datos de la infraestructura tecnológica del municipio, y cómo se gestiona y controla ese acceso.

Políticas de contraseñas: Estas indican los requisitos de complejidad y longitud de las contraseñas, la frecuencia de cambio y la gestión de contraseñas por parte de los usuarios y administradores.

Políticas de seguridad física: Establecen los requisitos para proteger los equipos y la infraestructura tecnológica del municipio de daños o intrusiones, incluyendo la ubicación física, la protección contra incendios y la protección contra robos.

2 Como la Norma de control interno influye en las políticas informáticas relacionadas con la de seguridad la infraestructura tecnológica

La Norma de Control Interno (NCI) y la tecnología están estrechamente relacionadas ya que la tecnología puede ser utilizada como herramienta para fortalecer y mejorar el control interno en las organizaciones.

La NCI establece los requisitos para el diseño, implementación y evaluación del control interno en las organizaciones, incluyendo la evaluación de los riesgos, la identificación de los controles necesarios y la supervisión y seguimiento de los mismos. La tecnología, por su parte, puede ser utilizada para facilitar la identificación y evaluación de los riesgos

3 Que estrategias considera importantes para desarrollar e implantar políticas que permitan brindar seguridad a las infraestructuras tecnológicas en una institución municipal.

El primer paso es identificar los riesgos de seguridad informática a los que está expuesta la organización. Esto se puede hacer mediante la realización de una evaluación de riesgos, que permitirá conocer las vulnerabilidades y amenazas que pueden afectar a la seguridad de los sistemas de información.

Una vez identificados los riesgos, se deben establecer políticas de seguridad que permitan mitigarlos y proteger la información de la organización. Estas políticas deben incluir medidas de seguridad física, lógica y administrativa, y deben ser comunicadas a todos los empleados para que las conozcan y las apliquen.

Se deben implementar controles para garantizar su cumplimiento. Estos controles pueden incluir medidas de seguridad tecnológicas, como firewalls, antivirus, sistemas de detección de intrusiones, entre otros.

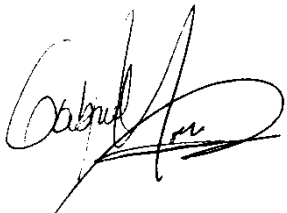
La capacitación es fundamental para que los empleados conozcan las políticas de seguridad.

4 Cuáles son los componentes de infraestructuras tecnológicas a las que hay que aplicarles políticas de seguridad con un enfoque mas cuidadoso.

Las redes y los sistemas de comunicación son fundamentales para la interconexión y el intercambio de información en una organización. Las políticas de seguridad deben cubrir aspectos como la autenticación, el cifrado, la gestión de contraseñas, la monitorización del tráfico y la prevención de intrusiones.

Los servidores y los sistemas operativos son esenciales para alojar aplicaciones y datos empresariales. Las políticas de seguridad deben cubrir aspectos como la configuración segura de los servidores.

Los medios de almacenamiento como discos duros, unidades USB y discos externos también son objetivos importantes para los ataques informáticos. Las políticas de seguridad deben cubrir aspectos como la encriptación de datos, el control de acceso y la monitorización de la actividad del usuario.



ING. ING. GABRIEL MEZA

DIRECTOR DE TECNOLOGIAS (E)

UNIVERSIDAD TECNICA DE BABAHOYO

ENTREVISTA RELACIONADA CON: ANÁLISIS DE POLÍTICAS DE SEGURIDAD APLICABLES A INFRAESTRUCTURAS TECNOLÓGICAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN BABAHOYO

NOMBRE: ING. FRANCIS RIZZO

EMPRESA: GADM BABA CARGO: TICS -COORDINADOR

1 Como conocedor del funcionamiento de la infraestructura de seguridad en un GAD Cantonal y técnico informático de amplia experiencia, indicar por favor cuáles son las políticas de seguridad aplicables a las infraestructuras tecnológicas de los municipios:

Controlar quiénes son los que tienen acceso a los sistemas, redes y datos de la infraestructura tecnológica del municipio, y cómo se gestiona y controla ese acceso.

Todo lo relacionado con contraseñas, estas indican los requisitos de complejidad, apegados a su frecuencia de cambio y la gestión de contraseñas por parte de los usuarios y administradores.

2 Como la Norma de control interno influye en las políticas informáticas relacionadas con la de seguridad la infraestructura tecnológica

La Norma de Control Interno (NCI) es una guía que proporciona un marco de referencia para la gestión de riesgos y el control interno en las organizaciones. La NCI establece una serie de principios y lineamientos que deben ser aplicados por la alta dirección de una organización para garantizar la eficacia y eficiencia de sus procesos, la integridad de su información y el cumplimiento de las leyes y regulaciones aplicables.

3 Que estrategias considera importantes para desarrollar e implantar políticas que permitan brindar seguridad a las infraestructuras tecnológicas en una institución municipal.

Antes de desarrollar cualquier política de seguridad, es importante realizar una evaluación de riesgos para identificar las amenazas y vulnerabilidades que enfrenta la organización. Esta evaluación puede ayudar a determinar qué controles de seguridad son necesarios y cuáles son las áreas críticas que requieren una mayor protección.

Luego exponerlas en un documento de formas claras y concisas, y deben establecer claramente los procedimientos y las responsabilidades de todos los empleados de la organización. Deben ser redactadas de manera sencilla y fácilmente comprensible por todos los miembros de la organización.

Y capacitación de los empleados, estas son clave para garantizar que los empleados comprendan la importancia de la seguridad informática y sepan cómo cumplir con las políticas de seguridad establecidas. Los empleados deben estar capacitados para reconocer los riesgos de seguridad y saber cómo manejar situaciones de riesgo.

4 Cuáles son los componentes de infraestructuras tecnológicas a las que hay que aplicarles políticas de seguridad con un enfoque mas cuidadoso.

Los Servidores

Los Firewalls

Los Sistemas Operativos de Los Usuarios Haciéndoles Hardening



ING. FRANCIS RIZZO
TICS SERVIDOR PUBLICO 4

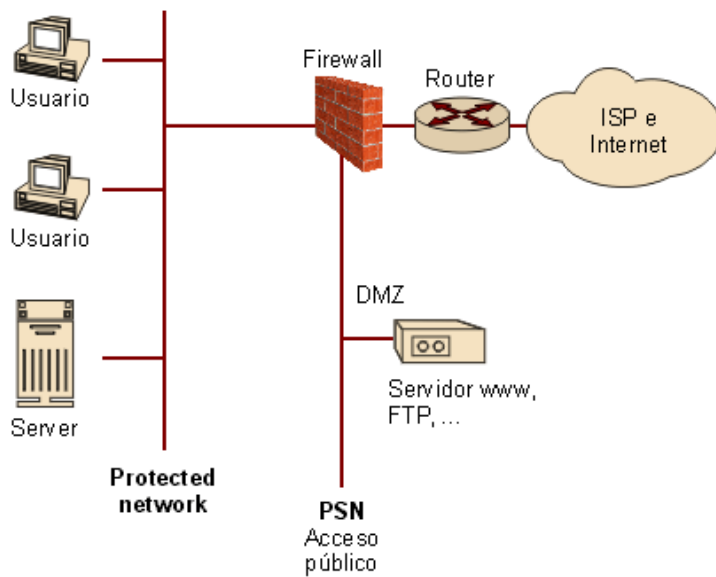
**ANEXO 2 ESQUEMAS DE INFRAESTRUCTURA Y SEGURIDAD
CONSULTADOS**

**ANEXO 2: ESQUEMA DE FUNCIONAMIENTO DE ALGUNOS MUNICIPIOS
Y SU ESTRUCTURA DE SEGURIDAD CON FIREWALLS**

PROVEEDORES DE INTERNET DE CADA CANTON

BABA

CNT: ESQUEMA GENERAL:

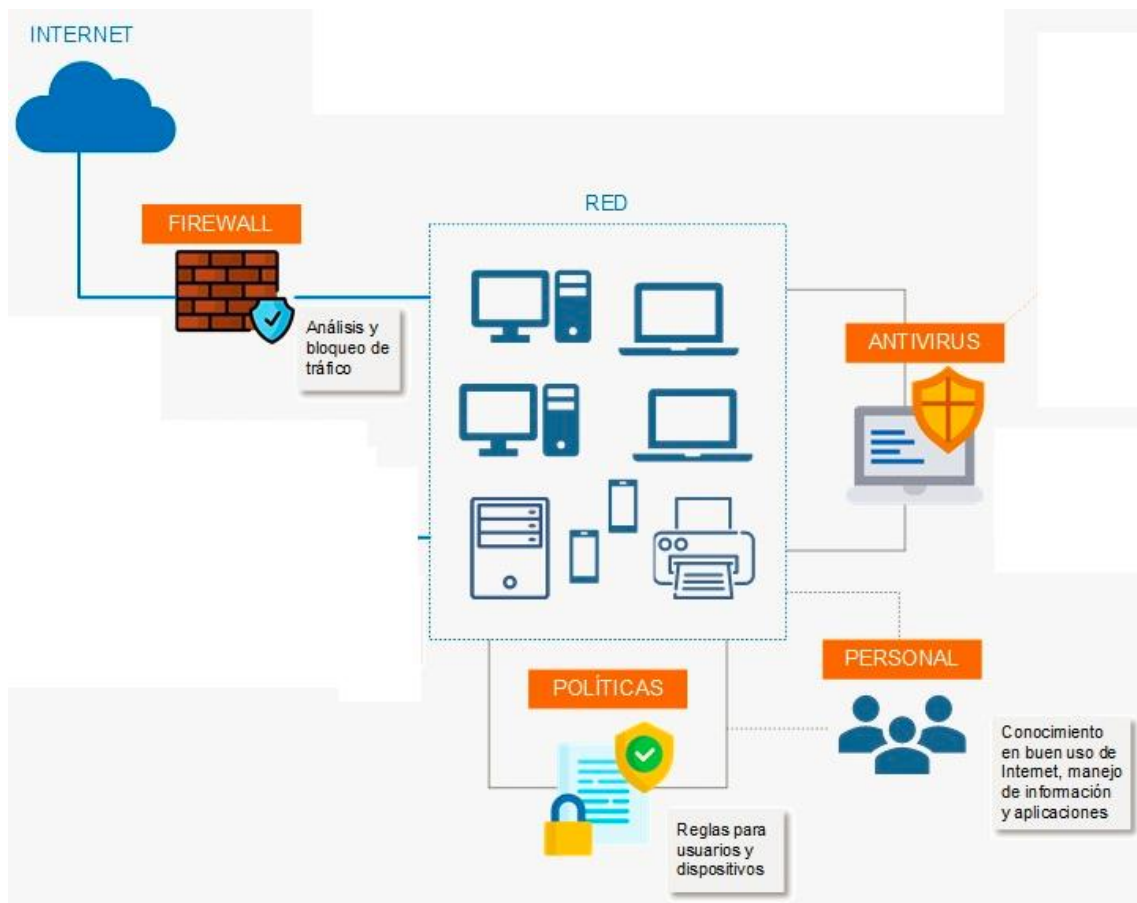


REFERENC ING. FRANCIS RIZZO

BUENA FE

TELCONET: ESQUEMA GENERAL

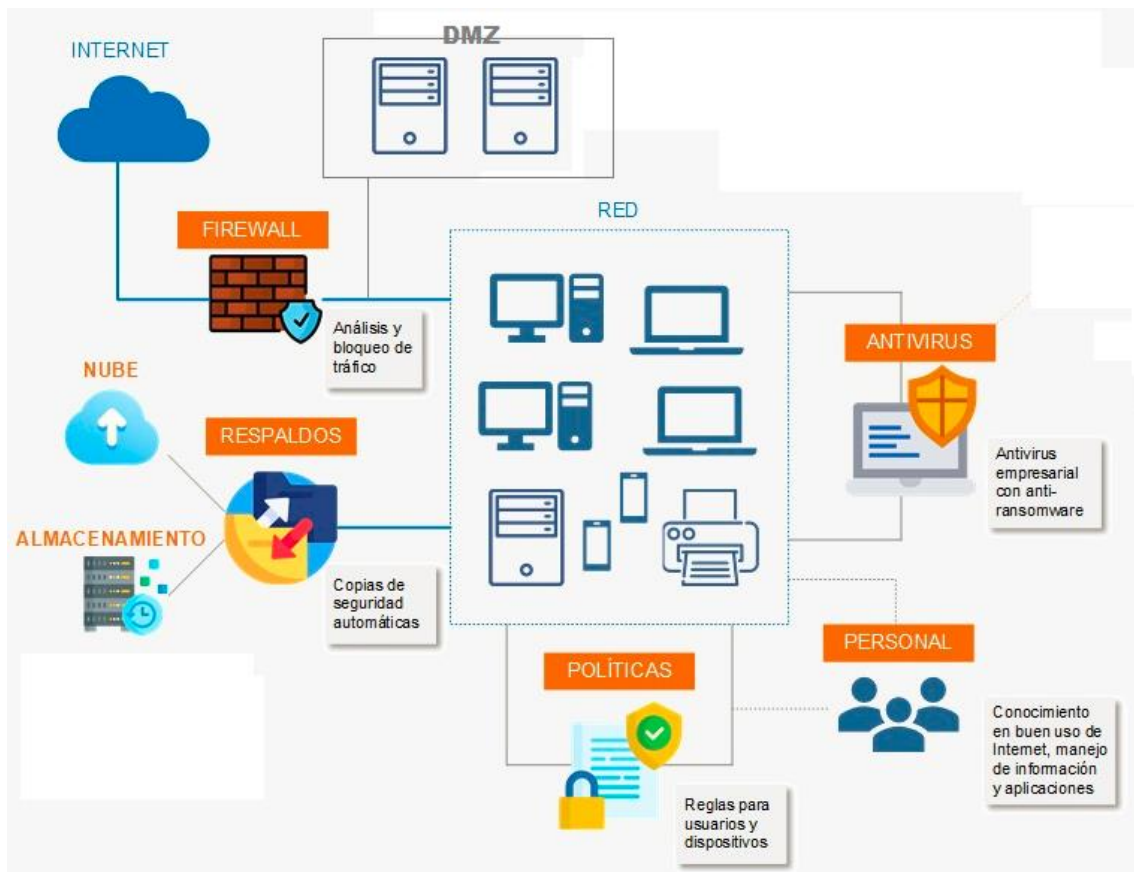
REFERENCI] ING. GABRIEL MEZA



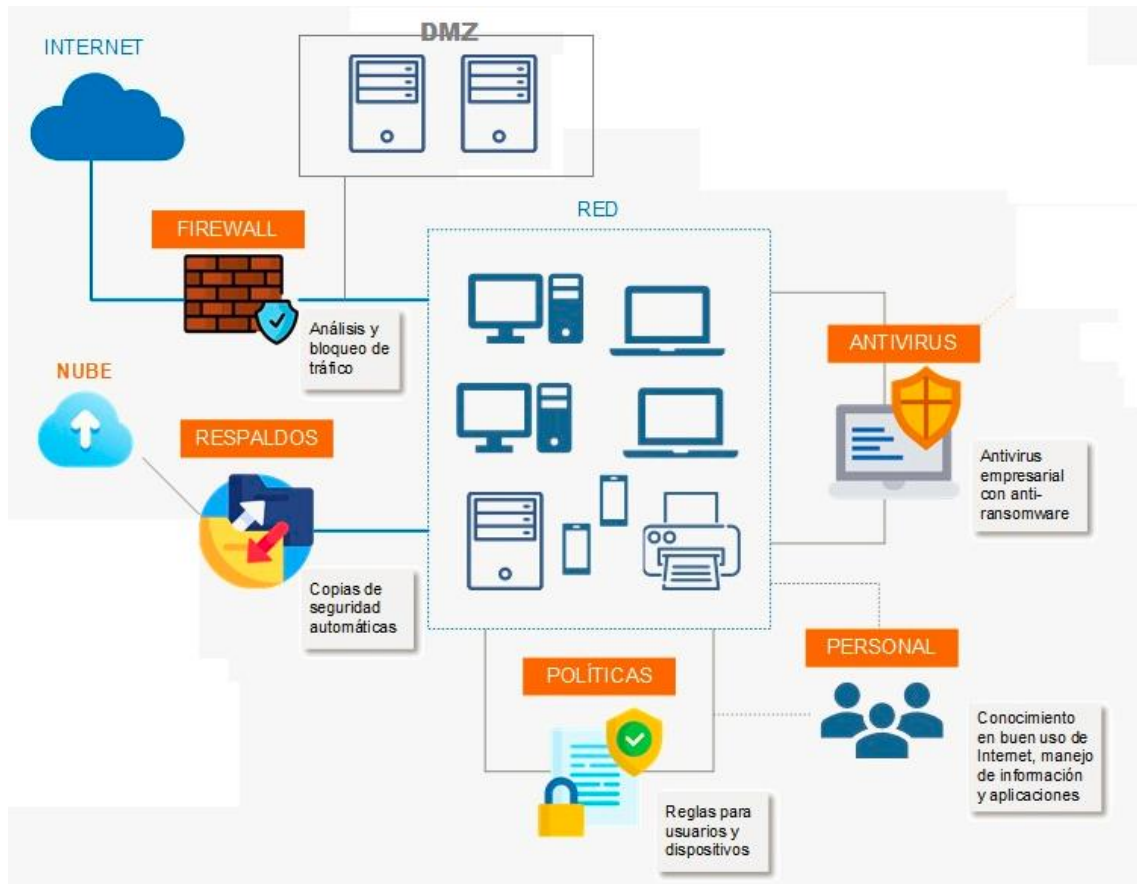
QUEVEDO

MUNICIPIO: PROVEEDOR TELCONET

REFERENCING. DANIEL FERRIN



MUNICIPIO DE BABAHOYO
PROVEEDOR TELCONET
REFERENCIA : ING GALO GARCIA



ENTREVISTA



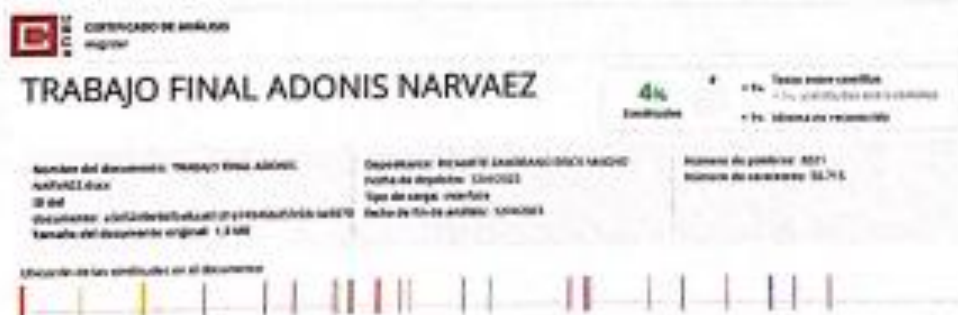


Babahoyo, 13 de abril de 2023

**CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES
EN EL SISTEMA DE ANTIPLAGIO**

En mi calidad de Tutor del Trabajo de la Investigación del Sr. **NARVAEZ CEREZO ADONIS DARIO**, cuyo tema es: **ANÁLISIS DE POLÍTICAS DE SEGURIDAD APLICABLES A INFRAESTRUCTURAS TECNOLÓGICAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN BABAHOYO**, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio COMPILATIO, obteniendo como porcentaje de similitud de [4%], resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.



Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

Ing. Erick Ricuarte Zambrano, MSIG, MBA.
DOCENTE DE LA FAFI.