UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

JUNIO –SEPTIEMBRE 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERÍA EN SISTEMAS

TEMA:

Aplicación de Normas ISO 27005 mediante un análisis de Seguridad de la Información en el Departamento de la Jefatura Política del Cantón Alfredo Baquerizo Moreno (Jujan).

EGRESADA:

Carla Andreina Pérez Laz

TUTOR:

Ing. Raúl Armando Ramos Morocho

AÑO 2020

INTRODUCCIÓN

Hoy en día la seguridad de la información es considerada como un pilar fundamental de cada empresa u organización, donde dicha información está expuesta cada día a diferentes amenazas al no establecer normas de seguridad, esto es causado debido a la falta de conocimiento o interés acerca de este tema.

Con el pasar de los años esto ha causado el aprovechamiento de grandes vulnerabilidades y riesgos dentro de lo que es la seguridad de cada uno de los sistemas, incluyendo lo que son pérdidas de información que han sido de gran importancia tanto para las empresas públicas como privadas y por ende afecta a la integridad y confidencialidad de la misma, esto es muy importante ya que la seguridad es considerada como un factor esencial para cada empresa en si un elemento indispensable para de esta manera garantizar la confianza en el uso de este tipo de tecnologías de información.

La Jefatura Política del cantón Alfredo Baquerizo Moreno (Jujan) es una Institución muy importante dentro del Cantón dedicada a la organización pública cantonal, esta maneja una cantidad considerable de información muy relevante de cada uno de los problemas de la comunidad, como sabemos cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes actualmente atentan contra la seguridad y privacidad de la información las cuales representan un riesgo que pueden afectar a las mismas.

Este caso de estudio tiene como objetivo aplicar normas ISO 27005 para realizar un análisis de la situación actual de la información y que de esta manera dicha institución tenga un cierto grado de confidencialidad, integridad ya que de esta manera ayudaría a proporcionar mejores habilidades en la gestión de la seguridad de la información.

El principal problema que se presenta en el departamento de Jefatura Política del cantón Alfredo Baquerizo Moreno es la falta de gestión de seguridad de la información lo que significa que es necesario la implementación de normas de seguridad para de esta manera tener una debida protección de información.

Para llevar a cabo el caso de estudio, se utilizó una metodología inductiva la misma que es utilizada para conseguir información necesaria mediante las diferentes técnicas entrevista y encuestas y así poder descubrir respuestas a las diferentes causas que se generan en dicho departamento.

El presente caso de estudio está vinculado con la línea de investigación sistema de gestión de seguridad de la información de la carrera de Ingeniería en sistemas de la Facultad de Administración, Finanzas e informática, en base a las normativas de seguridad de la información que determinan el riesgo operacional en este caso el departamento de la Jefatura Política.

DESARROLLO

La Jefatura Política del Cantón Alfredo Baquerizo Moreno ubicada en las calles José Domingo Delgado y Jaime Roldós junto con su representante cantonal trabajando por muchos años con el objetivo de ofrecer el bienestar de su comunidad y además controlar la parte administrativa de dicha organización cantonal.

La información que se maneja dentro de la Jefatura Política del cantón Alfredo Baquerizo Moreno se encuentra archivada en cada una de los ordenadores que se encuentran en dicho departamento esta información debe ser integra y confidencial por lo cual se plantea realizar un análisis de la situación actual de la información del departamento y así poder evaluar las amenazas y vulnerabilidades de la misma.

Es necesario la implementación de normas ISO 27005 para la seguridad de la información ya que cada vez existen más vulnerabilidades de ataques mal intencionado cada vez son más especializadas, complejas y avanzadas es por dicho motivo que la mayoría de empresas aplican este tipo de normativas para así poder establecer y mantener segura la información.

Con respecto a las normas ISO 27005 se puede establecer un contexto el cual indica una orientación e impacto acerca del riesgo de la información , en la cual se describen alcances y límites, es importante tener en cuenta que el análisis de riesgo dentro de cualquier entidad ya sea pública o privada, es de suma importancia ya que de esta manera nos ayuda a verificar en la situación que se encuentra y así tener niveles altos en la seguridad de cada uno de los datos y que tengan una mayor eficiencia, confiabilidad, disponibilidad e integridad.

En cuanto al personal encargado de la Jefatura Política se dedica a realizar las diferentes actividades en base a sus roles asignados a cada uno de ellos por lo general la mayoría de veces se mantiene reuniones entre las diferentes autoridades de dicho cantón con

la finalidad de verificar las situaciones desfavorables y así poder brindar un buen servicio a la comunidad.

Tabla 1 *Personal Encargado*

Fuente: *Elaboración propia*

Nombre	**Cargo**
Ing Juan de Dios Villamar	Jefe Político
Lcda. Fabiola Lizarzaburo Castro	Secretaria del departamento de Sistemas
Ing Yomaira Alcívar Molina	Analista en sistemas
Abg. Belén García	Comisaria
Abg. Cinthya Hernández Sánchez	Abogada

Para evaluar el departamento de la Jefatura política en la seguridad de la información se empleara la metodología margerit ,según los autores (Amutio Gómez & Candau, 2012)la metodología margerit permite responde a lo que se denomina "Proceso de Gestión de los Riesgos" (pag.7).además de esta manera realizar un análisis de la gestión de riesgo para así poder conocer los diferentes peligros ,amenazas y poder obtener una planificación de medidas para mantener los conflictos bajo control.

Sistema de Gestión de Seguridad de la Información – SGSI

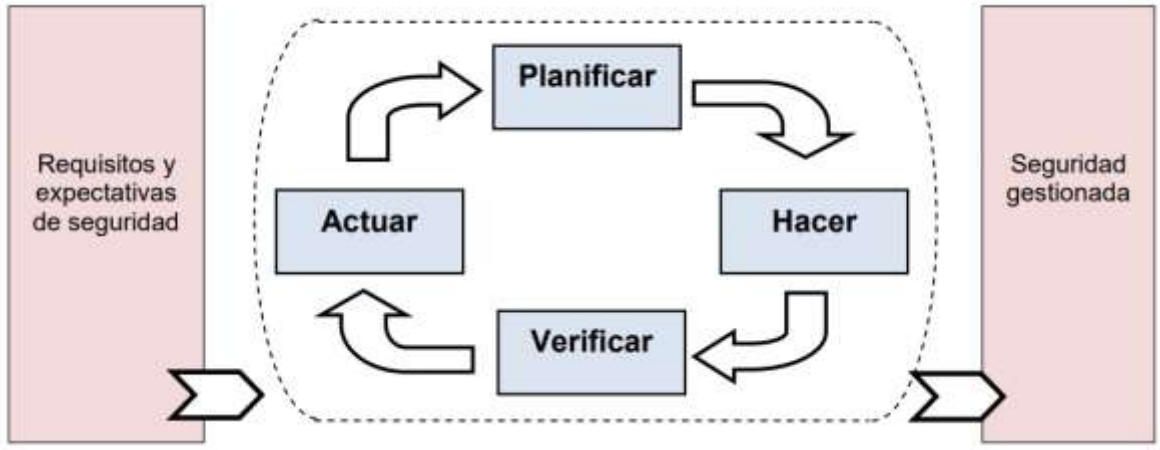
El SGSI, tiene un establecimiento de los mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro de un conjunto de estándares previamente determinados para evaluar la seguridad.

El objetivo principal es identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a los procesos y servicios que presta la organización con apoyo de TI, además de verificar la existencia de controles de seguridad que permitan integrarlos a las políticas y procedimientos para mitigar

los riesgos encontrados. (Javier Solarte, ENRIQUEZ ROSERO, & Benavides Ruano, 2015, pág. 498)

Figura 1 *Modelo PHVA aplicado a los Procesos de SGSI*

Fuente*: (Metodología psi ,2013)*



Seguridad

La seguridad se encarga de la protección de cada uno de los bienes informáticos los cuales son importante proteger. Entre ellos se encuentran el hardware; el software y los datos los cuales son considerados los más expuestos a riesgos, son los datos los cuales se pierden rápidamente por lo cual el tiempo de vida útil es corto y sobre todo pierden su valor antes que el hardware, cuyo tiempo de vida es entre 2 o 3 años, mientras que la vida del software en diferentes ocasiones con los diferentes mantenimientos oportunos realizados, pueden operar durante más de 5 años. (Travieso, 2003)

La seguridad física es empleada frecuentemente para referirse a las medidas de protección externas. Normalmente, estas son implementadas mediante los diferentes dispositivos eléctricos, electrónicos y son las primeras que se introducen en todas las instalaciones informáticas dentro de las cuales existen dos factores; la ocurrencia de un desastre las pérdidas serían completas, por otro, estas medidas de protección son generalmente las más fáciles de tomar. Su costo no es considerado muy alto (con la

excepción de los sistemas de continuidad eléctrica) y su mantenimiento no presenta dificultades especiales. (Travieso, 2003)

Por otra parte, se menciona a las medidas de seguridad técnicas y lógicas son aquellas que hacen referencia a lo que es la protección del software dentro de una empresa u organización lo cual esto puede involucrar lo que son la identificación de cada uno de los usuarios con todos los requerimientos al momento de ingresar a un sistema con son las contraseñas acceso de autenticación estas son medidas las cuales ayudarían a que solo ingresen usuarios autorizados.

Seguridad Informática

La seguridad informática es considerada como una disciplina que con base a las políticas y normas internas y externas de una empresa, además se encarga de proteger la integridad y reserva de la información la cual se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas minimizando los riesgos tantos físicos como lógicos a lo que están expuestas las características dentro de las cuales están : efectividad ,eficiencia confidencialidad, integridad ,disponibilidad y confiabilidad .. (Urbina, 2016, págs. 12,13)

Las principales áreas que cubre la Seguridad de la Información son:

Disponibilidad: la disponibilidad puede hacer referencia como una habilidad la cual permite asegurar que los usuarios puedan ser autorizados a acceder ya sea a sistemas o diferentes programas que contengan la información que ellos necesiten.

Confidencialidad: la confidencialidad es aquella que permite asegura que solo tenga acceso a la información personal autorizado.

Integridad: la integridad es la que permite salvaguarda la información con una gran precisión y completitud de manera que no contenga fallas ni errores.

Valoración de Activos.

Es de vital importancia dentro de la fase de Análisis de Riesgo, se lo realiza con el objetivo de establecer el valor de afectación de estos activos en cuanto al beneficio de los servicios y procesos de negocio de la empresa. La base para la valoración de los activos del departamento de TIC es el costo en que se incurre debido a la perdida de la confidencialidad, integridad y disponibilidad como resultado de un incidente. Esta valoración proporciona las dimensiones que tienen los elementos importantes para el valor del activo. (Mejía Viteri , Gonzáles Valero, & España Leon , 2019)

Tabla 2 *Escala de Valor de cada activo*

Fuente: *Elaboración propia*

Valorización de los Activos		**Descripción**
1	Alto	Grave
2	Medio	Medio Grave
3	Bajo	Importante
4	Depreciable	Insignificante

Tabla 3 *Valoración de los Activos*

Fuente: *Elaboración propia*

Activos	**Función**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Promedio**
PC´s de escritorios	Permiten el acceso a cada uno de los servicios	4	4	3	4
1 impresora	Permite imprimir documentos	3	4	4	4

	necesarios y certificados por el departamento				
Cableado Estructurado	Es la que provee conectividad a cada una de las estaciones de trabajo	2	2	5	3
Servidores	Son los que contienen la información	4	3	3	3

Seguridad de la Información

De acuerdo a la asociación española para la calidad (Calidad, 2020), "la seguridad de la información tiene como finalidad de la protección de la información y de los sistemas de la información de acceso, uso, divulgación, interrupción o en si la destrucción no autorizada".

Vulnerabilidad Informática

Son las posibilidades de que se dan en el mismo ambiente, en el cual las características propician y se vuelven susceptibles a una potencial amenaza, por lo tanto, se puede considerar como la capacidad de reacción ante la presencia de un componente que pueda posibilitar una amenaza o un ataque. Se puede decir que es vulnerable ante cualquier suceso, sin importar su ambiente ya sea interno o externo que pueda afectar cada uno de los activos informáticos ante la posibilidad de la presencia de un ataque o no, por parte del personal interno o externo a la organización. (Javier Solarte, ENRIQUEZ ROSERO, & Benavides Ruano, 2015, pág. 497)

Las vulnerabilidades son consideradas como un mecanismo que se encuentra en la parte interna de un sistema por lo cual los responsables de detectarlas son los administradores y personal encargado.

Algunas de las áreas en las que se puede identificar las Vulnerabilidades son:

Organización: es considerado como un lugar físico donde trabajan un conjunto de personas tanto internas como externas dentro de las mismas.

Procesos y procedimientos: estos se verán afectados por la participación en cada manejo de la información.

Personal: son los principales responsables de que las vulnerabilidades afecten a la organización porque trabaja y sobre todo manipula la información ya sean física o lógicas.

Ambiente: este se verá afectado cuando no se siga un adecuado lineamiento para de esta manera mantener un espacio estable y libre de cada una de las amenazas.

Amenazas Informáticas

Las amenazas informáticas están relacionadas con la posibilidad de que algún tipo de evento se pueda dar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial sobre cada uno de los activos informáticos y de los sistemas de información. Las amenazas son estimadas como los ataques que son realizados por personas internas o externas, que pueden ocasionar daños a equipos tecnológicos, a los sistemas de información o a la misma información que recorre en la organización.

Las amenazas pueden presentarse por las diferentes acciones criminales en las que actúan seres humanos violando las normas y las leyes, o sucesos de orden físico por eventos naturales que puedan presentar, los diferentes eventos en los que el ser humano propicia las condiciones para determinar un hecho físico, o por negligencia que son las omisiones, decisiones o acciones que pueden realizar algunas personas por desconocimiento,

falta de capacitación y/o abuso de autoridad. (Javier Solarte, ENRIQUEZ ROSERO, & Benavides Ruano, 2015, pág. 498)

Generalmente podemos decir que estas se dividen en tres grupos:

Criminalidad: desde el punto de vista estas son consideradas amenazas en la que intervienen los humanos provocando así un robo de información las cuales violan la ley y los involucrados de estas acciones pueden ser penadas por las mismas ya que no son considerados personales autorizados para obtener este tipo de información.

Sucesos de Origen Físico: están son aquellas acciones en las cuales intervienen cada uno de los eventos naturales y sobre todo técnicos los cuales se puede mencionar a los incendios, sobrecarga eléctricos entre otros estos son causados directamente por la intervención humana.

Negligencia y decisiones Institucionales: son consideradas como una de las amenazas menos predecibles ya que estas se relación directamente con el actuar del humano.

Tabla 4 *Probabilidad de Amenazas*

Fuente: *Elaboración propia*

Parámetros de Valorización		**Descripción**
1	Bajo	Amenazas cuya probabilidad de explotar vulnerabilidades es muy baja
2	Medio	Amenazas que con poca frecuencia explotan vulnerabilidades
3	Alto	Amenazas que frecuentemente explotan vulnerabilidades

Tabla 5 *Cálculo que ocurra Amenazas*

Fuente: *Elaboración propia*

Activos	Amenazas	Vulnerabilidades	Nivel de ocurrencia	Facilidad de explotación
PC´s de escritorios	Falta de mantenimiento preventivo o correctivo	No existe adecuado mantenimiento	Alta	Alta
	Robo de información	Falta de control en contraseñas	Alta	Alta
impresora	Falta de mantenimiento	No existe mantenimiento adecuado	Media	Baja
Cableado Estructurado	Daños por suministro de energía errores de conectividad	Cortes o insuficiencia de energía	Bajo	Bajo
Servidores	Incumplimiento en el mantenimiento	Mantenimiento no adecuado	Alta	Media

Tabla 6 *Ejemplo de Amenazas*

Fuente: *Elaboración propia*

Tipo	Amenaza
Deliberadas	Acceso no autorizado
	Manipulación de configuraciones
	Robo de información
	Manipulación de programas
	Alteración de información
	Polvo

Naturales	Sismo
Accidentales	Sobrecarga Eléctrica
	Errores de mantenimiento/ Actualizaciones
	Falla de corriente (Apagones)
	Incendios
	Falta de Antivirus
	Fallas de Equipos
	Errores de Usuarios

Riesgos Informáticos

Los riesgos informáticos son considerados problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo por ende si no se cuenta con las medidas convenientes para de esta manera salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento, por lo tanto los riesgos se pueden clasificar en: Riesgos de integridad, Riesgos de relación, Riesgos de acceso, Riesgos de utilidad, Riesgo de infraestructura (Javier Solarte, ENRIQUEZ ROSERO, & Benavides Ruano, 2015, pág. 498)

Riesgos de Integridad: estos son considerados como procesos los cuales se enfrenta a una empresa u organización a causa de una mala gestión de vulnerabilidades es por aquello que hoy en día cada una de las empresas buscan en si mejorar estas gestiones y mantener la información fuera de riesgos.

Riesgos de Relación: estos riesgos son considerados como aquellos que están relacionados con la toma de decisiones siendo así de una manera oportuna que se lo realiza mediante la información recolectada y sobre todo en un momento preciso esta información debería ser de manera íntegra para así poder tomar una decisión de manera adecuada.

Riesgos de Acceso: estos riesgos son aquellos que debido a una inadecuada configuración del sistema o utilización de normativas para salvaguardar la información estos están cada día más expuestos a las vulnerabilidades que hace deficiente la integridad y confidencialidad de la información.

Análisis de Riesgos Informáticos

Es considerado como un proceso el cual permite identificar cada uno de los activos informáticos con lo que cuenta una empresa u organización además nos permite descubrir mediante una investigación sobre las diferentes vulnerabilidades y amenazas en las que se puede encontrar expuesta sin importar el tipo de empresas ya sean tanto públicas como privadas , en donde se identifica el impacto que cada una de estas pueden provocar esto se realiza con el fin de implementar cada uno de los controles y medidas preventivas que sean necesarias para evitar el riesgo identificado mediante el análisis realizado.

Tabla 7 *Niveles de Riesgo*

Fuente: *Elaboración propia*

Nivel de Riesgo	**Rango**
Bajo	8-10
Medio	5-8
Alto	0-4

Tabla 8 *Cálculo de Riesgo*

Fuente: *Elaboración propia*

Activos	**Amenazas**	**Vulnerabilidades**	**Nivel de ocurrencia**	**Facilidad de explotación**	**Riesgo**
PC´s de escritorios	Falta de mantenimiento preventivo o correctivo	No existe adecuado mantenimiento	Alta	Alta	8
	Robo de información	Falta de control en contraseñas	Alta	Alta	7
1 impresora	Falta de mantenimiento	No existe mantenimiento adecuado	Media	Baja	3
Cableado Estructurado	Daños por suministro de energía errores de conectividad	Cortes o insuficiencia de energía	Bajo	Bajo	5
Servidores	Incumplimiento en el mantenimiento	Mantenimiento no adecuado	Alta	Media	6

En el proceso de análisis de riesgo se puede diferenciar dos aspectos:

La Evaluación de Riesgo: conducente a establecer cada uno de los sistemas que, en su conjunto o en cualquiera de sus partes, pueden verse afectados directa o indirectamente por amenazas, valorando los riesgos y estableciendo cada uno de los niveles que se realizan a partir de las diferentes amenazas o vulnerabilidades existentes y el impacto que puedan

causar a la entidad. Consiste en el proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar la importancia.

La Gestión de Riesgo: involucra la identificación**,** selección, aprobación y manejo de los diferentes controles a establecer para eliminar o reducir los riesgos evaluados a niveles aceptables, con acciones destinadas a:

- Sujetar la probabilidad de que una amenaza ocurra
- Limitar el impacto de una amenaza
- Reducir o eliminar una vulnerabilidad existente
- Permitir la recuperación del impacto o transferencia a terceros

La gestión de riesgo involucra la clasificación a las alternativas para manejar los riesgos a que puede estar sometido un bien informático dentro de los procesos de una identidad. (contienen., 2013)

ISO

La Organización Internacional de Normalización, es una federación de alcance mundial integrada por cuerpos de estandarización nacionales de 157 países. La ISO es una organización no gubernamental, cuya misión es promover el progreso de la estandarización y las actividades relacionadas, con el fin de facilitar el intercambio de servicios y bienes y promover la cooperación científico, tecnológico y económico. (Tola & Freire , 2019)

La Serie ISO 27000

La familia de las normas ISO/IEC 27000, son la seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, son los que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización estas normas permiten especificar los requerimientos que deben desempeñar las

organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

La ISO 27000 es un conjunto de estándares que permiten explicar cómo implantar un Sistema de Gestión de Seguridad de la Información en una empresa. La utilización de una norma ISO 27000 dentro de una organización permite proteger la información, de una forma más fiable posible. (Valencia-Duque & Orozco-Alzate, 2017, pág. 5)

Norma ISO/IEC 27005

Denominada formalmente como Tecnología de la información o Técnicas de seguridad, Gestión del riesgo en la seguridad de la información es la norma que proporciona directrices para la gestión del riesgo de la seguridad de la información, para de esta manera proporcionar metodologías específicas para tal fin. El componente de gestión del riesgo, es uno de los insumos esenciales para desarrollar un SGSI existen múltiples marcos de referencia, que en su mayoría presentan los mismos elementos. (Valencia-Duque & Orozco-Alzate, 2017, pág. 5)

CONCLUSIONES

Luego de haber realizado un análisis de riesgo mediante la implementación de las normas ISO 27005 en el departamento de la Jefatura Política del cantón ABM(Jujan) se obtuvo las siguientes conclusiones:

- La implementación de la norma ISO 27005 es una herramienta la cual permite realizar un análisis de la seguridad de la información y sobre todo realizar una correcta valorización de los activos que se encuentran en el departamento además permite la identificación de cada una de las amenazas y vulnerabilidades que se enfrentan a cada uno de estos activos.

- Con respecto al análisis realizado se pudo establecer el nivel de riesgo en cada uno de los activos que posee dicho departamento en donde los resultados obtenidos es que la mayor parte de estos poseen niveles altos y medios, dentro del departamento no existe un control adecuado de autentificación ya que en su mayoría deja a visibilidad las contraseñas que son ingresadas a sus equipos de cómputo, lo cual esto hace posible que personas no autorizadas puedan ingresar libremente y de esta manera tomar o alterar información que sea importante.

- Tomando en cuenta los resultados obtenidos de la entrevista realizada en el departamento de la Jefatura Política del cantón ABM(Jujan) nos pudimos dar cuenta que no existe un mantenimiento frecuente en cada uno de los equipos de cómputo del departamento lo cual esto provoca fallos habituales en los ordenadores y además molestias en su adecuado funcionamiento.

Bibliografía

Javier Solarte, F., ENRIQUEZ ROSERO, E., & Benavides Ruano, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL* , 507.

Amutio Gómez, M., & Candau, J. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid .

Arias, J. E., & Rieto Sarmiento, E. J. (2016). *" sistema de gestión de seguridad de la información". Trabajo de grado, universidad distrital francisco José de caldas.* Bogota .

Calidad, A. E. (27 de 05 de 2020). Seguridad de la Informacion. *revista AEC*. Obtenido de https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

contienen., U. p. (08 de 2013). *Una política de seguridad informática es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.* Obtenido de Una política de seguridad informática es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.

Libre, U. (10 de Junio de 2015). *Seguridad de Información.* Obtenido de Universidad Libre: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

Magazines, U. (Julio de 2016). *Magazine* . Obtenido de Informática y Computación: Concepto, Relación y Diferencia: http://universitariosmagazine.com/site/index.php/eventos/universitarios-travel/informatica-y-computacion-concepto-relacion-y-diferencia

Mejía Viteri , J., Gonzáles Valero, M., & España Leon , A. (2019). *METODOLOGÍA PARA ANÁLISIS DE RIESGO DE LA INFORMACIÓN APOYANDO EN ISO 27005 .* Los Rios Babahoyo: Universidad Técnica de Babahoyo.

Tola , D., & Freire , L. (2019). *IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE.* Guayaquil-Ecuador.

Travieso, I. Y. (2003). La Criptografía como elemento de la seguridad informática. *SciELO*.

Urbina, G. B. (2016). *Introducción a la seguridad informática.* Grupo Editorial Patria.

Valencia-Duque , F., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, 22.

ANEXO # 1

1. **¿El departamento de la Jefatura Política del cantón Alfredo Baquerizo Moreno posee algún plan de contingencia ante cualquier eventualidad?**

Si ☐

No ☐

2. **¿De qué manera son los mecanismos de autentificación que utiliza la Jefatura Política?**

Clave de acceso ☐

Firma electrónica digital ☐

No posee ☐

3. **¿Disponen de servidores centrales?**

Si ☐

No ☐

4. **¿Las claves de acceso a las computadoras son visibles a otros usuarios?**

Si ☐

No ☐

5. **¿Con que frecuencia se realizan los respaldos de información del departamento de la Jefatura Política?**

Diario ☐ **Mensual** ☐

Semanal ☐ **Anual** ☐

6. **¿Al realizar cada una de las actividades diarias los equipos de cómputo responden de manera rápida a cada uno de los procesos?**

Si ☐

No ☐

7. **¿Se capacita al personal encargado en el manejo de los equipos de cómputo del departamento de la Jefatura Política?**

Si ☐

No ☐

8. **¿Se realiza algún tipo de mantenimiento en cada uno de los equipos de cómputo que se encuentran en el departamento de la Jefatura Política?**

Si ☐

No ☐

9. **¿Los programas que se utilizan en el departamento de la Jefatura Política habitualmente poseen su respectiva licencia?**

Si ☐

No ☐

10. **¿Se realiza actualización de software habitualmente?**

Si ☐

No ☐

Análisis de los resultados de la encuesta

1. **¿El departamento de la Jefatura Política del cantón Alfredo Baquerizo Moreno posee algún plan de contingencia ante cualquier eventualidad?**

Tabla 9*. Plan de Contingencia*

Opciones	Frecuencia	Porcentaje
Si	0	0%
No	5	100%
Total	**5**	**100%**

Fuente *Departamento de la Jefatura Política de ABM(Jujan)*

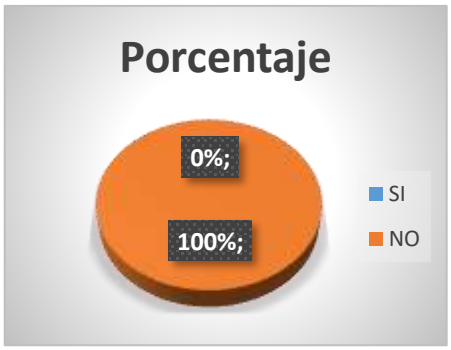


Figura 2*Plan de Contingencia*

Fuente: *Elaboración propia*

Análisis. De acuerdo a la encuesta realizada al personal del departamento de la Jefatura Política, el 100% de los encuestados dijo que no existe un plan de contingencia ante cualquier eventualidad ya que esto ocasiona que no se pudieran solucionar los diferentes inconvenientes

2. **¿De qué manera son los mecanismos de autentificación que utiliza la Jefatura Política?**

Tabla 10 *Mecanismos de Autentificación*

Opciones	Frecuencia	Porcentaje
Clave de Acceso	5	100%
Firma electrónica Digital	0	0%
No posee	0	0%
Total	**5**	**100%**

Fuente *Departamento de la Jefatura Política de ABM (JUJAN)*

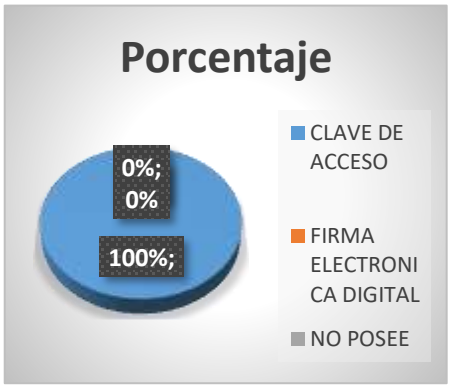


Figura 3 *Mecanismos de Autentificación*

Fuente: *Elaboración propia*

Análisis. Mediante la encuesta efectuada de acuerdo a los mecanismos de autentificación. El 100% del personal del departamento de la Jefatura indican que se realiza por medio de claves de acceso a cada una de las computadoras de dicho departamento.

3. ¿Disponen de servidores centrales?

Tabla 11 *Servidores Centrales*

Opciones	Frecuencia	Porcentaje
Si	1	20%
No	4	80%
Total	**5**	**100%**

Fuente *Departamento de la Jefatura Política de ABM (JUJAN)*

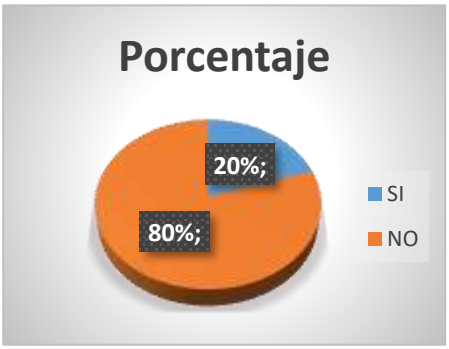


Figura 4 *Servidores Centrales*

Fuente: *Elaboración propia*

Análisis Con respecto al uso de servidores centrales dentro de la jefatura el 20% de los encuestados dijeron que, si contaban con servidores para el almacenamiento de la información dentro del departamento de la Jefatura Política, mientras el 80% indica que no cuentan con servidores.

4. ¿Las claves de acceso a las computadoras son visibles a otros usuarios?

Tabla 12 *Acceso a las Computadoras*

Opciones	Frecuencia	Porcentaje
Si	3	60%
No	2	40%
Total	**5**	**100%**

Fuente *Departamento de la Jefatura Política de ABM (JUJAN)*

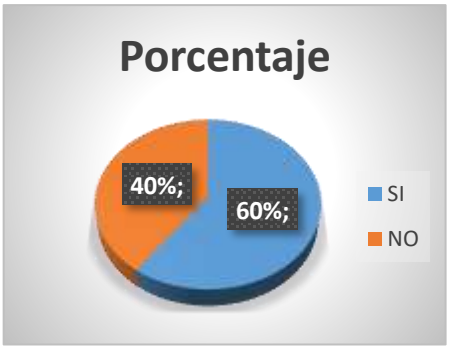


Figura 5*Acceso a las Computadoras*

Fuente: *Elaboración propia*

Análisis con respecto a los resultados de los encuestados el 60%indica que las claves del acceso a cada computadora son visibles mientras el 40% indica que sus claves de acceso son personales por lo tanto se considera que los encargados que muestran sus claves facilitan la infiltración de usuarios.

5. **¿con que frecuencia se realizan los respaldos de información del departamento de la Jefatura Política?**

Tabla 13 *Respaldo de Información*

Opciones	**Frecuencia**	**Porcentaje**
Diario	3	60%
Semanal	1	20%
Mensual	1	20%
Anual	0	0%
Total	**5**	**100%**

Fuente *Departamento de la Jefatura Política de ABM (JUJAN)*

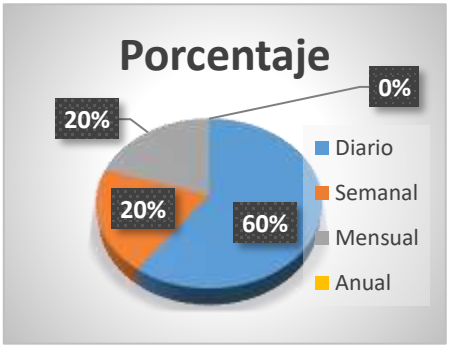


Figura 6*Respaldo de Información*

Fuente: *Elaboración propia*

Análisis. Con respecto a los resultados obtenidos de las 5 personas encuestadas el 60% indica que el respaldo de la información lo hacen a diario mientras que el 20% indica que lo realizan semanalmente mientras que el otro 20% indica que realizan el respaldo cada mes.

6. **¿Al realizar cada una de las actividades diarias los equipos de cómputo responden de manera rápida a cada uno de los procesos?**

Tabla 14 *Rendimiento del Computador*

Opciones	**Frecuencia**	**Porcentaje**
Si	3	60%
No	2	40%
Total	**5**	**100%**

Fuente *Departamento de la Jefatura Política de ABM (JUJAN)*

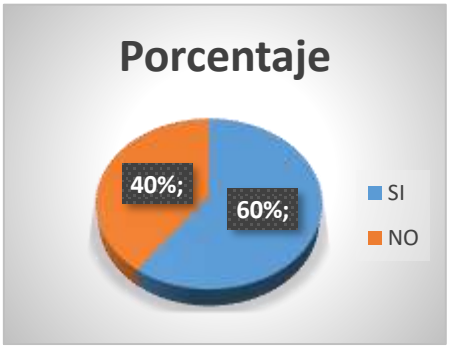


Figura 7 *Rendimiento del Computador*

Fuente: *Elaboración propia*

Análisis. Con respecto a los datos obtenidos de la encuesta realizada el 60% indica que los equipos responden de manera ágil mientras que el 40% indica que sus equipos tecnológicos son pocos lentos para poder trabajar con agilidad**.**

7. **¿Se capacita al personal encargado en el manejo de los equipos de cómputo del departamento de la Jefatura Política?**

Tabla 15 *Manejo de Equipos de Computo*

Opciones	Frecuencia	Porcentaje
Si	1	20%
No	4	80%
Total	**5**	**100%**

Fuente *Departamento de la Jefatura Política de ABM (JUJAN)*

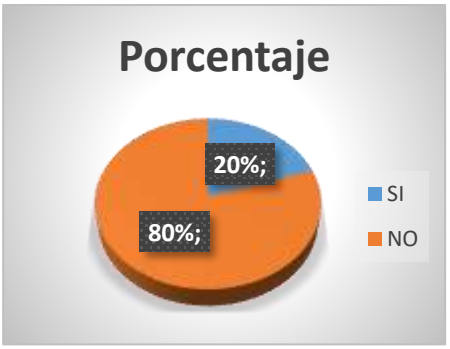


Figura 8 *Manejo de Equipos de Computo*

Fuente: *Elaboración propia*

Análisis. Con respecto a los datos obtenidos de la encuesta el 80% indica que no se los capacita en el área de la tecnología mientras que el 20% indica que si están capacitados en dicha área ya que se recomienda que se realicen dichas capacitaciones para que así los encargados tengan conocimiento de aquello.

8. **¿se realiza algún tipo de mantenimiento en cada uno de los equipos de cómputo que se encuentran en el departamento de la Jefatura Política?**

Tabla 16 *Mantenimiento Periódico*

Opciones	Frecuencia	Porcentaje
Si	1	20%
No	4	80%
Total	**5**	**100%**

Fuente *Departamento de la Jefatura Política de ABM (JUJAN)*

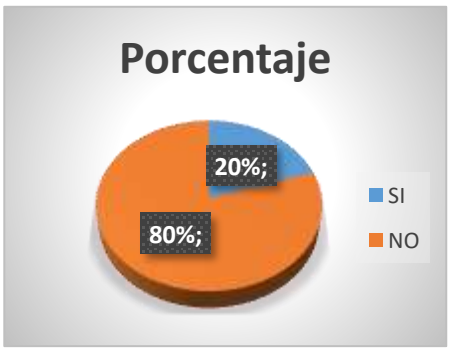


Figura 9 *Mantenimiento Periódico*

Fuente: *Elaboración propia*

Análisis. con respecto a los datos obtenidos de la encuesta el 80% indica que no se realizan frecuentemente el mantenimiento mientras el 20% indica que si se realizan mantenimiento lo cual es muy importante realizarlo para que así funcionen de manera correcta sus equipos.

9. ¿los programas que se utilizan en el departamento de la Jefatura Política habitualmente poseen su respectiva licencia?

Tabla 17 *Programas Utilizados*

Opciones	Frecuencia	Porcentaje
Si	3	60%
No	2	40%
Total	**5**	**100%**

Fuente *Departamento de la Jefatura Política de ABM (JUJAN)*

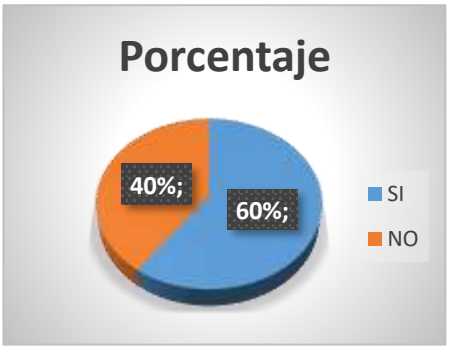


Figura 10 *Programas Utilizados*

Fuente: *Elaboración propia*

Análisis. Con respecto a los datos obtenidos en la encuesta el 60% indica que cada uno de los programas a utilizar cuenta con su respectiva licencia mientras que el 40% indica que no tienen su respectiva licencia se manifiesta que al no mantener licencia es considerado como programas ilegales.

10. ¿se realiza actualización de software habitualmente?

Tabla 18 *Utilización De Software*

Opciones	Frecuencia	Porcentaje
Si	0	0%
No	5	100%
Total	**5**	**100%**

Fuente *Departamento de la Jefatura Política de ABM (JUJAN)*

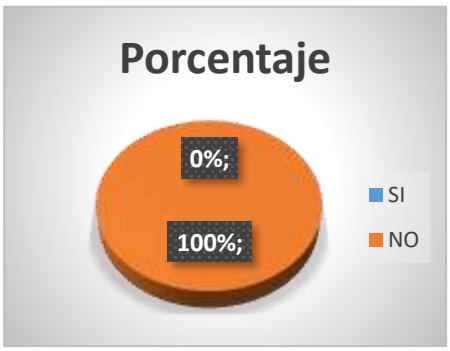


Figura 11 *Utilización De Software*

Fuente: *Elaboración propia*

Análisis. Con respecto a los datos obtenidos de las encuestas el 100% indica que no se realiza la actualización del software en cada uno de los equipos informáticos dentro del departamento de la Jefatura Política.