
# UNIVERSIDAD TÉCNICA DE BABAHOYO

## FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

## EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

**PRUEBA PRÁCTICA**

**INGENIERÍA EN SISTEMAS**

**PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN SISTEMAS**

## TEMA:

# ANÁLISIS DE RIESGO Y FUNCIONAMIENTO DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA EL COMERCIAL SU ECONOMÍA DEL CANTÓN BABA


## EGRESADA(O):

## LITARDO VERA RAFAEL ANGEL

## TUTOR:

## ING. LEON ACUARIO JOFFRE VICENTE


## AÑO 2021

# INTRODUCCIÓN

En la presente investigación se refiere al análisis de riesgo y funcionamiento de un plan de seguridad informática para el comercial su economía del cantón Baba, donde se indicará si existiera los riesgos que refleja la empresa, cuáles serían los planes de contingencia en caso que sea necesario.

Sus características principales de este análisis es la metodología de riesgo que se implementaría para saber cuáles son su factibilidad en este caso.

Para analizar la problemática se debe de indicar cuáles son sus causas. Una de ella son el riesgo de información y el riesgo operativo en caso de factores externos; este tipo de riesgos serán analizados con las metodologías, cualitativo y cuantitativo. Para que, de esta manera, se pueda evitar problemas futuros y se tenga un plan de contingencia con el interés de mantener la seguridad de la información que se está usando en la empresa, haciendo confiable a la misma y que sus clientes se sientan satisfechos.

Vale recalcar, que el interés académico de este caso de estudio es con el fin de solucionar los riesgos de la empresa y así ver su factibilidad de mejoras en problema futuros.

El objetivo de este caso de estudio, es encontrar los análisis de riesgos en caso que se encuentre en comercial Economía haciendo que se tome decisiones favorables para evitar los daños que podría generar si no se aplica las prevenciones necesarias.

# Desarrollo

## Proyecto de inversión

La información que se tratara en este caso de estudio, es para elaborar las ventajas y desventajas que reflejan a la analizar los riesgos informáticos que existen en la empresa su Economía y ayudar a que existan mejoras para el mismo, siendo así una ayuda que se verá reflejada con acontecimientos a futuros, haciendo que se vuelva incierta.

La información que se ejecute en cualquier empresa debe siempre cumplir con las reglas establecidas en lo que es la seguridad informática.

La seguridad informática se debe de medir en dos aspectos, en lo que se debe de cumplir y lo que se debe de evitar.

Lo que se debe de cumplir. - esta lo que es usar sistema de software de sistema antivirus y mantener una contraseña periódicamente cambiante, mantener un respaldo de la información que se tiene de los usuarios, cifrar archivos muy importantes

Cuando nos referimos a lo que se debe de evitar, tenemos tener en cuenta el uso de las wifis abiertas, que son un peligro par información que se mantiene, estar ejecutando link que son de índoles sospechosas o estar obsequiando la wifi del internet del local.

## Riesgos

Cuando se refiere a riesgos nos damos cuenta que es la falta de toma de decisiones al manejo de la misión y visión que se tiene cuando uno ejecuta algún proyecto y no toma las medidas preventivas del caso y hace que existan fallas dentro de lo que se está ejecutando. (Pacheco, 2015). A firma. “El riesgo es la probabilidad que ocurra una amenaza que explota una vulnerabilidad de un activo informático, causando un impacto, comprometiendo la confidencialidad, integridad y/o disponibilidad”. Es por ello, que es necesario analizar los riesgos para evitar problemas futuros.

## Seguridad Informática

Como indica (YESID GONZALEZ DUQUE, JORGE ELIÉCER JURADO SAPUYES, CARLOS ALBERTO ORTÍZ AUX, DIEGO GUZMÁN IRAGORRI, & EFRAIN ALFONSO HOYOS, 2017)Es brindar seguridad y estabilidad a la información institucional que se manipula por parte de usuarios internos y externos de la Corporación, implementando mecanismos de seguridad informática que garanticen la confidencialidad, integridad y disponibilidad de los sistemas de información.

Es por ello que se debe de precautelar en mantener la información de manera que la empresa brinde la confianza, integridad y sobretodo la seguridad de lo que reposa en ella.

A demás la seguridad de la información, ayuda que la empresa esté preparada para algún ataque cibernético y pueda atender paulatinamente, lo que le está sucediendo y darle prioridad a las cosas paulatinamente, como lo indica (Empresas, 2018) “el plan de seguridad informática para la empresa podrá determinar cuál emergencia atender en primer lugar, y de manera sucesiva” aportando así un manejo oportuno y cauteloso al toma de decisiones.

## Riesgos de Proyecto de Inversión

Como primer plano tenemos el riesgo informático, cuyo inconveniente existe en el control de mantener la información con respaldo en un servidor en caso de que se produzca inconvenientes técnicos, se debe de aprovechar los avances de la tecnología para implementar en un servidor web, haciendo que estos en caso que falle la maquina se pueda ingresar por medio de un dispositivo móvil y seguir manteniendo el control de la información que se necesita en la empresa.

También pueden surgir fallas eléctricas, donde afectarían en uso de las máquinas y no nos permitirá tener el seguimiento de las ventas, se indicará como sugerencia llevar

el control con un libro diario o mantener una generadora portátil de energía, haciendo así una continúa venta de la empresa Económica.

Otro riesgo que se puede ver afectado la empresa, es cuando pueda existir falla en el programa, haciendo no se mantengan el control de sus ventas en forma virtual, en esos casos mantener un técnico informático operativo, que solucione el inconveniente que está afectando a la empresa y se podría llevar la información en un Excel hasta que esté solucionado el problema.

Existen otros tipos de riesgos como son los naturales y huelgas de personas, que influirían también la parte del manejo de las ventas, donde se podría aplicar la tecnología como las ventas por redes sociales, creación de páginas web ente otras alternativas que ayudarían a que la empresa tenga su plan de contingencia.

Como se pudo notar en los análisis anteriores se pudo constatar que en la tabla 1, nos reflejaba los riegos que se tiene si no se mantiene un plan de contingencia, teniendo datos favorables en resolver los riesgos que se tendría en el comercial Economía, en la tabla de fuego que ese encuentra en la imagen 1 ella nos indica, que si mantiene las estructura de riesgo igual, su impacto de que exista problema de riesgos van a ser extremadamente altos, pero si se aplican las mejoras, su nivel disminuyen, de un nivel medio a un nivel bajo, que sería lo que toda empresa en su máximo pico desearía que pase, que exista menos riesgo y más producción.

**Políticas de Seguridad de protección y respaldo a la Información**

De la empresa comercial “Su Economía” que se encuentra ubicada en el cantón Baba de la provincia de Los Ríos.

Esquema del acuerdo 166

De acuerdo con el acuerdo ministerial 166, se estipula (Peñaherrera, 2013) “Que, es importante adoptar políticas, estrategias, normas, procesos, procedimientos,

tecnologías y medios necesarios para mantener la seguridad en la información que se genera y custodia en diferentes medios y formatos de las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.” Es por ello que se debe de aplicar las normas estipuladas en la gestión de seguridad informática para evitar que exista la vulnerabilidad al momento de guardar información y que sean atacados por Hackers.

En este caso de estudio se aplicaría lo que es la norma ISO/IEC 27002:2005 – Código para la Práctica de la Gestión de la Seguridad de la Información (A.D, 2018). El cual ayudaría a que la información que está siendo procesada en la Empresa la Economía sea protegida evitando perdidas de información.

**ISO 27005**

También se podría aplicar lo que es la norma (ISO27000.es, 2016)“I**SO 27005:** es una guía de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones. No especifica ninguna metodología de análisis y gestión de riesgos concreta, pero incluye ejemplos de posibles amenazas, vulnerabilidades e impactos.” Se mantiene la información segura y se analizaría y se gestionaría los riesgos concretos, haciendo que se defina la vulnerabilidad del caso y su impacto de lo que podría suceder, si o se toma en cuenta las medidas de prevención para la empresa Economía.

Se puede hacer una estimación de algún problema que puede surgir, ejemplo en un incendio dentro de las horas laborables.

Como indica el literal C. del esquema (Peñaherrera, 2013), se debe

- Identificar el incendio
- Notificar a las oficinas de Seguridad de la Información de la Institución.

- Resolver y restaurar el servicio afectado por el incidente debido a la par de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes (Peñaherrera, 2013)

**ITIL**

Otra forma de aplicar una gestión de seguridad de informática es usando ITIL, según su propósito (interpolados, 2020), es de "proteger la información que necesita la organización para realizar sus actividades comerciales."

Haciendo que se comprendan y se gestione los riesgos. Manteniendo una prevención, detención y corrección.

**GRi**

Según (Cordoba, Viña , & Coria, 2017) "GRi tecnológico busca evitar las pérdidas de información ante fallas en los sistemas que pueden ser de cualquier tipo (naturales, accidentales, intencionales, etc.), y también considera los fraudes internos o externos (en este sentido, involucra al riesgo legal y al reputacional ante esas amenazas)."

Con esta aplicación de riesgo, indica que también es una forma de prevenir los riesgos ya sean existente o futuros con el fin de evitar nuevas vulnerabilidades.

**Como metodologías también tenemos**

**MAGERIT**

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT Implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. (Amutio Gómez, Candau, & Mañas,,

2012) es una norma que apoya a las normas ISO 27005 detectando la amenazas y la información crítica del sistema, afirma (Bailón-Lourido, 2019).

**PMBOK**

Según lo que indica (TAYO, 2017)PMBOK, el Riesgo de un proyecto es un evento o condición incierta que, de producirse, tiene un efecto positivo o negativo en uno o más de los objetivos del proyecto, tales como el alcance, el cronograma, el costo y la calidad. Con esta forma en cambio indica la parte positiva o negativa que se gestiona la seguridad de la información haciendo un impacto de una o más causas.

**OSINT**

Una de las formas de tener un buen resultado en la búsqueda de información, se podría aplicar la herramienta de OSINT significa Open Source Intelligence (en español Inteligencia de Fuentes Abiertas), y se trata de un conjunto de técnicas y herramientas para recopilar información pública, correlacionar los datos y procesarlos. (Pastorino, 2019)

**COBIBT 2019**

También encontramos la metodología de COBIT 2019, (Ritegno, 2019) como indica, es una herramienta, que permiten una orientación adicional para adaptar un sistema de gobierno a las necesidades de la empresa, es una fuente de marco abierta con el fin de informar actualizaciones futuras, con las nuevas guías y herramientas hace el COBIT 2019 sea más prescriptivo/preceptivo.

**Herramienta Pilar**

Como indica (Nacional, 2020)PILAR es una herramienta de Entorno de Análisis de Riesgos (EAR), que soporta el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit (Metodología de Análisis y Gestión de

Riesgos de los Sistemas de Información). Haciendo que al momento de utilizar esta herramienta dirija su análisis a la metodología de Magerit, para que cumpla con lo que la Metodología indica.

**Balanced Scorecard**

Otro método que también se puede aplicar al momento de gestionar levantamiento de información es el uso de Balanced Scorecard o en español Cuadro de Mando Integral, como o indican (Roncancio, 2018) "Es una metodología de gestión estratégica utilizada para definir y hacer seguimiento a la estrategia de una organización". Haciendo así que la metodología sea evaluable y medible, generando su propio indicador de factibilidad.

## PROCESO METODOLOGICO APLICADO DESCRIPCION DE LA EMPRESA CASO DE ESTUDIO

Para realizar el análisis del caso de estudio en la Empresa Económica ubicada en el cantón Baba indica que su proceso de aplicar las sugerencias de análisis de riesgo, tendría un avance de unos tres años. La función principal de la empresa es de la venta de productos de primera necesidad de la canasta básica, es una empresa conocida a nivel local, su evaluación de la empresa es con la finalidad de crecer por verse con una buena acogida y en un futuro ampliarse si es necesario.

A continuación, nos enfocaremos en las metodologías que se implementarían:

En este análisis se aplicaría la metodología cualitativa o cuantitativa, o se aplicaría las dos, todo depende de lo que se requiera.

- Cuando nos referimos a la cualitativa es más para la toma de decisiones de la empresa y se puede hacer por medio de entrevistas y encuestas.
- Cuando nos referimos a cuantitativas ella se encarga de calcular el riesgo que se puede generar el proyecto, eso haciendo énfasis a la factibilidad de la misma.

**Valoración de probabilidad de accidente**

| Riesgos | Amenaza | Control | Vulnerabilidad | Valoración de consecuencia |
|---|---|---|---|---|
| **Riesgo Informático** | Falla de respaldo al servidor | Servidor en una nube | El servidor no esté protegido | Perdida de conexión |
| **Riesgo Eléctrico** | Falla de apagones. | Generador de energía. | No funciones la máquina. | Las ventas del día no está ingresadas al sistema. |
| **Riesgo en el programa** | Que el programa falle. | Llevar el registro en el Excel. | Que mantenga fallos el sistema. | Tener un Técnico disponible. |
| **Riesgos naturales y huelgas de personas** | Que el computador falle y las personas no puedan acudir a la empresa hacer sus compras. | Ventas por medio, de redes sociales, páginas web, entrega a domicilio. | Que no se tenga internet o un vehículo de movilización. | Disponibilidad de internet datos y vehículos alquilados. |

*Tabla 1: Valoración de probabilidad*

Luego del análisis de los riesgos que podrían ocasionar y las evaluaciones que podrían ocurrir y como se las puede manejar se puede aplicar la metodología cualitativa y cuantitativa.

**Rango de estimación de riesgos**

Se debe estimar los rangos de riesgos para poder sacar la información necesaria.

- La estimación del riesgo se valora de forma numérica con una escala del 1 al 2.
- La estimación de consecuencias de valor en forma monetaria, con una escala menor de $200 y hasta mayor que el capital.
- La probabilidad se valora con los tiempos, con valores desde un mes hasta 2 años.

| Posibilidad | Efectos |
|---|---|
| **1 caso en 2 años** | Menor $400 |
| **1 caso en 1 año** | Mayor $200 y menor a $1.000 |
| **1 caso en 9 meses** | Mayor $400 y menor a $2.000 |
| **2 casos por 6 meses** | Mayor a $800 y menor a $4.000 |
| **1 vez por mes** | Mayor al patrimonio |

*Tabla 2: Rango de estimación de riesgo*

**Tabla de fuego**

También aplicamos el grafico de fuego, donde nos indica la probabilidad de riesgo si es extra alto, alto, moderado o bajo.


*Imagen 1 Tabla de fuego P- 98: http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/39396/D-103191.pdf?sequence=-1&isAllowed=y*

**Valoración de Matriz de Riesgo**

| Nro. | Riesgo Inherente | | Riesgo Residual | | Riesgo residual deseado | |
|---|---|---|---|---|---|---|
| | Posibilidad | Efecto | Posibilidad | Efecto | Posibilidad | Efecto |
| **1** | 5 | 4 | 3 | 3 | 1 | 1 |
| **2** | 2 | 1 | 1 | 1 | | |
| **3** | 4 | 3 | 2 | 2 | 1 | 1 |
| **4** | 2 | 1 | 1 | 1 | | |

*Tabla 3: Matriz de Riesgo*

En esta matriz calculamos los niveles de probabilidad que pueden surgir en caso que exista un acontecimiento y los efectos que pueda sea poco favorables, siendo así un riesgo residual deseado que no coexista riesgo sería muy favorable, pero como no todo puede ser perfecto, tenemos una probabilidad de riesgo medio o riesgo residual, que nos indica un balance en término medio con un efecto manejable.

**Análisis de encuesta**

En base la encuesta que se le realizo a la empresa la Economía por la falta de una buena aplicación de gestión de riesgos con un plan información, fue que para la empresa es que existe la falta de capital y la complejidad para cumplir las normativas.

**Informe de análisis de riesgos**

Bajo la herramienta de PILAR, la normativa de análisis de riesgo emite lo siguiente resultados:

El riesgo de impacto y la dimensión que indica la amenaza de activos refleja una leve amenaza de riesgo, por lo que indica la tabla 4.

| Amenaza | Impacto | Dimensión | Riesgo | |
|---|---|---|---|---|
| **Acceso no autorizado** | 7 | c | 6,2 | 5,8 |
| **Manipulación de la información** | 8 | a | 6,4 | 5,6 |

*Tabla 4: Informe de Análisis de Riesgo*

A continuación, se mostrará en la siguiente tabla 5 que sucedería usando un firewall, como ejemplo para evolución de la amenaza de riesgos haciendo que la denegación, se desaparezca en esta nueva tabla.

| Amenaza (Firewall) | Impacto | Dimensión | Riesgo |
|---|---|---|---|
| Acceso no autorizado | 7 | C y A | 5,8 6,2 |
| Manipulación de información | 7 | B | 5,4 6,6 |
| Denegación se acceso la información | 7 | D | 0 |

*Tabla 5: Usando un Firewall*

**Inversión**

Para poder implementar un sistema de gestión confiable y seguro, cumpliendo las normativas estipuladas en el sistema informático se indicará lo que debería invertir económicamente la Empresa “Su Economía” a continuación, se indicará lo siguiente:

**Impedimento**

El impedimento, del porque no aplicaría sería más por la falta de conocimiento de no saber que existían normativas para implementación de un sistema de seguridad informático para evitar riesgos,

**Factibilidad económica**

Se resolvería haciendo un plan de inversión desde caja chica, con el fin de cumplir de a poco con sus normativas, para evitar riesgo de pérdida de información, de ataques informáticos, de mantener la seguridad apropiada de vigilancia entre otras falencias que indica la empresa.

| Necesidades | Valores a Invertir |
|---|---|
| **Firewall Open Source** | 000 |
| **Antivirus Open Source** | 000 |
| **Cámara de Seguridad** | $450 |
| **Sistema de detección de Incendio** | $2.000 |
| **Sistema de Archivos Owncloud Computer Open Source** | 000 |
| **Computador de escritorio** | $800 |
| **Sistema de Cableado** | $1000 |
| **Total** | $4.250 |

*Tabla 6: Estimación de los valores de la implementación de las necedades de la Empresa Su Economía*

Estos son las inversiones que se indicarían para el plan de la gestión de seguridad de riesgo en la Empresa Su Economía, con un valor de los $4,250, teniendo en cuenta que, si mantiene algunos recursos, quedaría en un valor de $3,800.

# Conclusión

Una vez concluida este caso de estudio la factibilidad del análisis de riesgo y un plan de seguridad informático para el comercial Economía del cantón Baba, nos da como resultado satisfactorio por lo que en la empresa Su Economía se reflejan en aceptar los cambios.

Dentro del caso de estudio se pudo observar que debido a los riesgos que se representan en la empresa, ellos se encuentran con la necesidad de un plan de contingencia para evitarse perdidas mayores y mantener el crecimiento de la empresa y su información respaldada y segura.

# Bibliografía


A.D. (2018). POLÍTICAS DE SEGURIDAD DE PROTECCIÓN Y RESPALDO DE INFORMACIÓN . *Universidad Administrativa Especial de Rehabilitacíon y MantenimientoVial*, 9.

Amutio Gómez, M., Candau, J., & Mañas,, J. (2012). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En M. A. Amutio Gómez, J. C. Candau, & ,. J. Mañas, *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (págs. 7-127). Madrid: © Ministerio de Hacienda y Administraciones Públicas; Secretaría General Técnica; Subdirección General de Información, Documentación y Publicaciones Centro de Publicacione.

Bailón-Lourido, W. A. (2019). Gestión de riesgos del área informática de las empresas exportadoras de pesca. *Polo de Conocimiento*, 165-189.

Cordoba, M., Viña , M., & Coria, M. (2017). *Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje.* La Plata: Universidad de La Plata Argentina.

Empresas, B. d. (22 de Julio de 2018). *Plan de seguridad informática para una empresa: ¿cómo se lleva a cabo?* Obtenido de uss: https://uss.com.ar/corporativo/plan-de-seguridad-informatica-para-una-empresa/

interpolados. (16 de Sep de 2020). *interpolados*. Obtenido de interpolados: https://interpolados.wordpress.com/2020/09/16/itil-4-practicas-de-gestion-de-itil-gestion-de-seguridad-de-la-informacion/

ISO27000.es. (2016). ISO 27000 y el conjunto de estándares de Seguridad de la Información. *intedya*, S.P.

Molina Miranda, M. (2015). *PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA APLICADO EN LA ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.* Madrid: Universidad Politécnica de Madrid .

Nacional, C. C. (29 de Julio de 2020). *ccn-cert*. Obtenido de ccn-cert: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/10388-nuevo-portal-de-pilar-la-solucion-de-analisis-y-gestion-de-riesgos-del-ccn.html#:~:text=La%20soluci%C3%B3n%20PILAR%20es%20una,de%20los%20Sistemas%20de%20Informaci%C3%B3n).

Pacheco, J. L. (2015). *"DESARROLLO DE UN PLAN DE PRUEBAS DE VULNERABILIDAD A LA RED DE DATOS DE UNA EMPRESA PÚBLICA DE DISTRIBUCIÓN ELÉCTRICA CNEL EP.* Guayaquil- Ecuador: Escuela Superior Politecnica del Litoral ESPOL.

Pastorino, C. (7 de Octubre de 2019). *welivesecurity*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2019/10/07/tecnicas-herramientas-osint-investigacion-internet/#:~:text=OSINT%20significa%20Open%20Source%20Intelligence,correlacionar%20los%20datos%20y%20procesarlos.&text=Estas%20gu%C3%ADas%20son%20muy%20%C3%BAtiles,a

Peñaherrera, C. C. (2013). *ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI.* SECRETARIO NACIONAL DE LA ADMINISTRACION PUBLICA.

Ritegno, E. O. (S.F de S.F de 2019). *iaia*. Obtenido de iaia: https://iaia.org.ar/wp-content/uploads/2019/07/COBIT2019-IAIA.pdf

TAYO, L. P. (2017). *MAESTRA EN DIRECCIÓN Y GESTIÓN DE PROYECTOS DE INGENIERIA.* SANTIAGO DE QUERETARO: Centro de Tecnología Avanzada, CIATEQ.

YESID GONZALEZ DUQUE, JORGE ELIÉCER JURADO SAPUYES, CARLOS ALBERTO ORTÍZ AUX, DIEGO GUZMÁN IRAGORRI, & EFRAIN ALFONSO HOYOS. (2017). *PLAN DE SEGURIDAD INFORMÁTICA.* Popayán: CORPORACIÓN AUTÓNOMA REGIONAL DEL CAUCA.


# ANEXO

Universidad Técnica de Babahoyo

Facultad de Administración, Finanzas e Informáticas

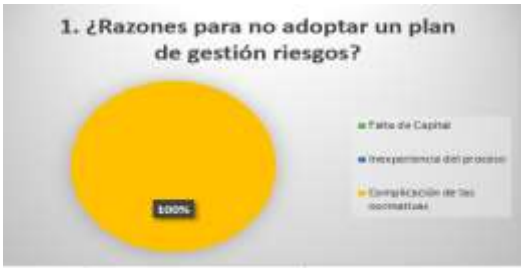
Encuesta dirigida a la Empresa Economía que se encuentra ubicada en el cantón Baba, de la provincia de Los Ríos.

1. ¿Razones para no adoptar un plan de gestión riesgos?

    a) Falta de Capital

    b) Inexperiencia del proceso

    c) Complicación de las normativas




2. ¿Causa que Ud. considera para no ser implementadas la gestión de riesgos y su seguridad informática en su empresa?

    a) No existir incidencias mayores

    b) No se considera una buena estrategia de información

    c) Complicación de las normativas

    d) Falta de presupuesto

Encuesta dirigida a la Empresa Economía que se encuentra ubicada en el cantón Baba, de la provincia de Los Ríos.

3. ¿Razones para no adoptar un plan de gestión riesgos?

    d) Falta de Capital

    e) Inexperiencia del proceso

    f) Complicación de las normativas

4. ¿Causa que Ud. considera para no ser implementadas la gestión de riesgos y su seguridad informática en su empresa?

    e) No existir incidencias mayores

    f) No se considera una buena estrategia de información

    g) Complicación de las normativas

    h) Falta de presupuesto

**UNIVERSIDAD TECNICA DE BABAHOYO**
**FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA**
**DECANATO**

Babahoyo, febrero 22 de 2021
D-FAFI-UTB-057-UT-2021

Ingeniera
Liliana Isabel Litardo Vera
**REPRESENTANTE LEGAL DE LA EMPRESA "SU ECONOMÍA"**
Ciudad. –

De mis consideraciones:

La Universidad Técnica de Babahoyo y la Facultad de Administración, Finanzas e Informática (FAFI), con la finalidad de formar profesionales altamente capacitados busca prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El Señor **LITARDO VERA RAFAAEL ANGEL,** con cédula de identidad No. 120520236-7, Estudiante de Ingeniería en Sistemas, matriculado en el proceso de titulación en el periodo Noviembre 2020 – Mayo 2021, trabajo de titulación modalidad Estudio de Caso para la obtención del grado académico profesional universitario de tercer nivel como **INGENIERO EN SISTEMAS.** El Estudio de Caso: **ANÁLISIS DE RIESGOS Y FUNCIONAMIENTO DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA EL COMERCIAL SU ECONOMÍA DEL CANTON BABA.**

Es por esta razón, solicito a usted, si es posible se sirva autorizar el permiso respectivo para que el Señor Litardo pueda desarrollar la investigación en la institución de su acertada dirección.

Por su gentil atención al presente, se extiende el agradecimiento institucional.

Atentamente.

**Lcdo. Eduardo Galeas Guijarro MAE.**
**DECANO**

c.c Archivo

Litardo
Recibido
16/03/2021.


Comercial
Su Economia


REDMI NOTE 9S
AI QUAD CAMERA


REDMI NOTE 8S
AI QUAD CAMERA