REVISTA CIENCIAS DE LA INGENIERÍA Y APLICADAS
ISSN: 2602-8255
Volumen 5, número 2, diciembre de 2021

Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador

Importance of IT security policies in accordance with ISO 27001 for small and medium-sized companies in Ecuador.

Alex Christian Llano Casa[1],Mónica Lisseth Gaibor Gavilanez.[2], Carla Cristina Cruz Caiza.[3], José Augusto Cadena Moreano.[4]

RESUMEN:

El presente artículo presenta la importancia de ejecutar buenas prácticas informáticas mediante el uso de normas ISO 27001 en las pequeñas y medianas empresas del Ecuador, incorporando una buena gestión en las TIC's, minimizando los riesgos y amenazas sobre la información empresarial, así como de sus activos informáticos. Los niveles de madurez para la gestión de los sistemas de información deben se desarrollados por clientes internos y externos, permitiendo elevar su prestigio y rentabilidad con la mejora en los procesos empresariales, garantizando la óptima operación de los servicios informáticos para cumplir con los objetivos de negocio de las empresas públicas, privadas y PYMES. Para medir las vulnerabilidades informáticas se usó la matriz de análisis de riegos de tecnología de información, permitiendo identificar las amenazar y riesgos, estos serán solventados con la elaboración de políticas de seguridad informática para garantizar la confiabilidad, integridad, disponibilidad de la información y recursos informáticos.

Palabras claves: Políticas de seguridad informática; gestión; confidencialidad; disponibilidad; integridad.

Recibido 2 de mayo de 2021; revisión aceptada 5 de agosto de 2021

ABSTRACT:

This article presents the importance of executing good computer practices through the use of ISO 27001 standards in small and medium-sized companies in Ecuador, incorporating good management in TIC's, minimizing risks and threats to business information, as well as its

[1] Universidad Técnica de Cotopaxi, Latacunga, Cotopaxi, Ecuador, alex.llano9864@utc.edu.ec
[2] Universidad Técnica de Cotopaxi, Latacunga, Cotopaxi, Ecuador, monicagaibor1996@gmail.com
[3] Universidad Técnica de Cotopaxi, Latacunga, Cotopaxi, Ecuador, carlita.cruz409@gmail.com
[4] Universidad Técnica de Cotopaxi, Latacunga, Cotopaxi, Ecuador, jose.cadena@utc.edu.ec

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

computer assets. The maturity levels for the management of information systems must be developed by internal and external clients, allowing them to increase their prestige and profitability with the improvement in business processes, guaranteeing the optimal operation of computer services to meet business objectives of compalies public, private and PYMES. To measure computer vulnerabilities, the information technology risk analysis matrix was used, allowing to identify threats and risks, these will be solved with the development of computer security policies to guarantee the reliability, integrity, availability of information and computer resources.

Keywords: Computer Security Policies, Threats, Confidentiality, Availability, Integrity.

1. INTRODUCCIÓN

Uno de los grandes problemas que enfrentan las pequeñas y medianas empresas son las vulnerabilidades informáticas, que se van formando en la ejecución de sus actividades diarias, estas vulnerabilidades al no ser combatidas, con el tiempo puede causar daños en el funcionamiento laboral de la empresa, dichas vulnerabilidades se las puede combatir mediante el diseño e implementación de políticas de seguridad informáticas mediante la ISO 27001.

En la actualidad la inseguridad informática puede producir en las empresas la pérdida o alteración de la información, que conlleva a ataques cibernéticos para el robo de información, así mismo afectar en el buen funcionamiento de los servicios informáticos y por ende el prestigio de las empresas. En virtud de ello, si se diseña Políticas de Seguridad Informática de acuerdo al estándar ISO 27001, entonces se podrá apoyar a la gestión de la seguridad de la información. Es importante el análisis de las normas ISO 27001 en pequeñas y medianas empresas, aplicando investigación de campo y bibliográfica para que las organizaciones hagan uso de las buenas prácticas informáticas. Además de concientizar la gestión de la información de una manera segura evitando pérdidas económicas y permitiendo precautelar el uso adecuado de todos los servicios informáticos.

Las políticas de seguridad informáticas son medidas que toman una organización o institución para proteger sus datos. Es por eso cuando la institución requiera una certificación, demanda tener esta documentación con el propósito de controlar lo que suceda en la Gestión de Seguridad de la Información, por esta razón se debe conocer a detalle las cláusulas de la ISO 27001 [1] en

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

donde se menciona que los objetivos de negocio sean medibles, puesto que debe tener los principios claves como: confidencialidad, integridad y disponibilidad [2].

Es viable poder implementar el modelo conocido como PDCA (Plan, Do, Check, Act) para captar la participación de todo el personal, quienes participarán activamente en las 4 etapas con un periodo de gestión 6 meses a 1 año [3].

En [4] mencionan que "las amenazas están relacionadas con la posibilidad de que algún tipo de evento se puede presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial sobre los activos informáticos y sistemas de información. Estas amenazas pueden clasificar en función del daño como: modificación, interpretación, interrupción, fabricación, accidentales o intencionales".

La vulnerabilidad se considera el punto más débil en la seguridad informática que puede producir falencias en la confidencialidad, integridad y disponibilidad de la información, afectando el normal funcionamiento de los servicios informáticos al ejecutar los tipos de vulnerabilidades como: física, natural, software, humana [5].

Objetivo

Identificar las amenazar y riesgos, con la elaboración de políticas de seguridad informática para garantizar la confiabilidad, integridad, disponibilidad de la información y recursos informáticos.

2. METODOLOGÍA

La estimación de riesgo permitió dar paso a esta investigación, ya que las empresas están vulnerables a ciertos riesgos que pueden provocar daños a corto y mediano tiempo, [6] relata que la estimación de riesgos "permite determinar cuáles serán los factores de riesgo que potencialmente tendrá un impacto significativo dentro de la organización". Finalmente, una vez que se haya identificado los activos, sus vulnerabilidades y las amenazas a las que están expuestos como siguiente paso es estimar el riesgo, esto permitirá determinar los controles que se debe implementar en el sistema.

De esta manera se puede utilizar dos métodos las cuales son: cuantitativos y semi-cuantitativos, pues generan un análisis más detallado y por lo tanto más confiable para las empresas. Se puede usar también un método cualitativo solo cuando no se puede hacer un análisis detallado o cuando no se pueda cuantificar la amenaza por falta de tiempo.

2.1. Tipo de investigación

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

La investigación de campo ayudó a diagnosticar y ratificar la problemática encontrada de 10 empresas de la región sierra centro del Ecuador, extrayendo los datos directamente de la realidad a través el banco de preguntas ejecutadas a los encargados de los departamentos de TIC's, comprendiendo las vulnerabilidades y necesidades a la que están expuestos.

A demás se utilizó la investigación bibliográfica que permitió revisar y recopilar la información por medio de la lectura de libros, artículos o tesis, a fin de poder sustentar y obtener las bases necesarias para el desarrollo de la investigación de políticas de seguridad informática mediante las ISO 27001. En virtud de la expresado acerca de la investigación de campo y bibliográfica se puede indicar que para generar la información se realizó una entrevista a los líderes departamentales de Sistemas de Información de las pequeñas y medianas empresas, las cuales colaboraron con total normalidad, ayudando a resolver las inquietudes que poseíamos para la realización de la propuesta de políticas de seguridad informática. Por tanto, se ejecutó la observación, esta investigación nos facilitó conocer la factibilidad en la que se encuentra la seguridad en las empresas, igualmente analizar las diferentes vulnerabilidades y amenazas que podrían poseer, causando que los activos informáticos no trabajen satisfactoriamente, la ejecución de ambas metodologías nos ayudó a conocer la realidad de las empresas frente a la investigación.

2.2. Enfoque Cualitativa

Para lograr un mayor conocimiento y poder cumplir con el objetivo de la investigación se utilizó la modalidad cualitativa, en vista que se realizó la entrevista a los ingenieros encargados de los departamentos informáticos, logrando conocer la gestión de la información y control de los activos de las empresas.

2.3. Métodos de investigación

Se empleó el método Inductivo-Deductivo, permitiendo conocer a profundidad el impacto positivo que tendrá las políticas de seguridad informática, así evaluar si las empresas consideran implementar nuestra propuesta en un futuro.

3. ANÁLISIS DE RESULTADOS

Este trabajo está basado en el Análisis de riesgos para la creación de políticas de seguridad informática usando ISO 27001. La aplicación práctica de la investigación para el diseño del plan de mitigación analizando diferentes riesgos, tanto internos como externos de las instituciones, lo que ha permitido conocer las vulnerabilidades.

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

Tabla 1: Riesgos Internos y Externos.

RIESGO INTERNO	
Control de acceso a equipos	Los equipos no cuentan con solicitud de usuario y contraseña para ingresar a realizar sus actividades, por ello, tampoco tiene protector de pantalla que bloquee el acceso después de un tiempo de 3 a 5 minutos.
Respaldo a los equipos	No se respalda la información de los equipos, si no existe una disposición que identifique lo realice.
Navegación en internet	Algunos equipos no cuentan con restricciones a ciertas páginas de internet, que no compete a sus actividades laborales, como a Facebook, WhatsApp, YouTube, entre otras.
Correo electrónico	Los funcionarios no hacen uso de su correo electrónico corporativo, el destino de la información laboral son sus correos electrónicos personales.
Datacenter	Las empresas no cuentan con un Datacenter, los servidores se encuentran alojados en los departamentos de los encargados de TI.
Seguridad física en equipos de computo	Las portátiles propiedades de las empresas, no cuentan con un candado cuando estas no están siendo utilizadas por los responsables.
RIESGO EXTERNO	
Control de salida e ingreso de equipos	No se controla el acceso de equipos por parte de los visitantes, así como de los funcionarios que ingresan a laborar con sus equipos personales o equipos propiedad de las empresas.

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

3.1. Matriz de factores Interno y Externo

Continuando como parte del proceso de la investigación realizada, se procede a realizar una matriz a los factores internos y externos, FODA. Este proceso ayudará también a la elaboración del plan de mitigación de riesgos.

Para realizar la matriz de factores [7] explica la asignación del campo valor que corresponde al impacto que ese factor tiene, se acerca a 1 si es muy importante y 0 es de poca importancia. Así mismo el campo clasificación que corresponde al tipo de respuesta que la empresa está en capacidad de dar, va de 1 a 4, siendo 4 el nivel en el que mejor preparado se encuentra, dando valor como lo indica el siguiente cuadro:

Tabla 2: Factores Interno y Externo.

		CLASIFICACIÓN
FACTORES INTERNOS	FORTALEZAS	ENTRE 3-4
	DEBILIDADES	ENTRE 1-2
FACTORES EXTERNOS	OPORTUNIDADES	ENTRE 3-4
	AMENAZAS	ENTRE 1-2

Para sacar el total del valor ponderado [8] menciona que se suma los valores, estos valores deben estar entre 1.0 y 4.0. Donde 1 es el valor más bajo, 4 el valor más alto y 2.5 es el valor promedio ponderado. Si el valor ponderado está por debajo de la media, significa que la marca es débil internamente, mientras si el valor ponderado está por encima, señala fortaleza.

Tabla 3: Factores Internos.

FACTORES INTERNOS			
FORTALEZAS	**VALOR**	**CLASIFICACIÓN**	**VALOR PONDERADO**
Base de datos respaldadas	0,17	4	0,68
Antivirus de software gratuito	0,15	3	0,45
Red física en cascada.	0,15	3	0,45
DEBILIDADES			

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

Carencia de plan de mantenimiento preventivo.	0,09	1	0,09
No cuenta con plan de contingencia para cambio de equipo.	0,09	1	0,09
No se realizan respaldos a los equipos.	0,17	2	0,34
Acceso a redes sociales, streaming y otras páginas.	0,18	1	0,18
TOTAL	**1,00**		**2,28**

3.2. Análisis de la tabla 3: Factores Internos

El valor ponderado de los factores internos es de 2,28 se puede deducir que la situación no es tan favorable pues está por debajo del valor ponderado, lo que quiere decir que la empresa no tiene una fuerte posición interna. Pero se puede decir que los factores externos más relevantes y que pueden hacer una diferencia son: Los respaldos semanales a las bases de datos asimismo el contar con antivirus, estos factores internos pueden hacer competitividad.

Tabla 4: Factores Externos.

FACTORES EXTERNOS			
OPORTUNIDADES	**VALOR**	**CLASIFICACIÓN**	**VALOR PONDERADO**
Presupuesto no muy elevado, destinado a TIC's.	0,18	3	0,54
Página segura.	0,16	3	0,48
AMENAZAS			
Carencia de políticas de seguridad informática.	0,18	1	0,18

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

No cuenta con acuerdos que garantice la confidencialidad de la información.	0,16	1	0,16
Nivel de seguridad baja, en el control de acceso a equipos.	0,16	1	0,16
No cuenta con plan de contingencia ante desastres naturales.	0,16	1	0,16
TOTAL	**1**		**1,68**

3.3. Análisis de la tabla 4: Factores Externos

El valor ponderado la tabla de factores es externa es de 1,68 valor aún más por debajo de media ponderada, que da por conclusión que existe debilidad de igual forma en los factores externos. Existen mayores oportunidades que amenazas estos factores como el presupuesto y la página segura, puede hacer la diferencia ante otras instituciones.

3.4. Matriz para el análisis de riesgos

Según [9], indica que "la matriz de riesgo se trata de una herramienta ampliamente utilizada como un proceso en la descripción organizada y calificada de sus actividades o rubros para permitir un apoyo al seguimiento y/o gerenciamiento de los riesgos."

La matriz de riesgo evalúa el riesgo de una institución, de manera que se realiza un diagnóstico objetivo de la situación de la institución, se calcula utilizando la formula Riesgo= Probabilidad de Amenaza x Magnitud de Daño.

En virtud de esto, se debe realizar la identificación de las actividades principales además de los riesgos a la que puede estar expuesta. Seguidamente desde su concepción metodológica las matrices se componen de dos vectores, uno de impacto y otro de probabilidad, cuya combinación define el riesgo de un factor en particular. Estos vectores tienen valores que están en un rango de 1 a 4, en la que 1 es insignificante, 2 baja, 3 media y 4 alta, tanto para la magnitud de daño como para la probabilidad de amenaza, al multiplicar estos rangos dan como resultado el valor del riesgo que significa:

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

Tabla 5: Vectores del Riesgo.

RIESGO	VALOR	COLOR
Bajo	1-6	Verde
Medio	8-9	Amarillo
Alto	12-16	Rojo

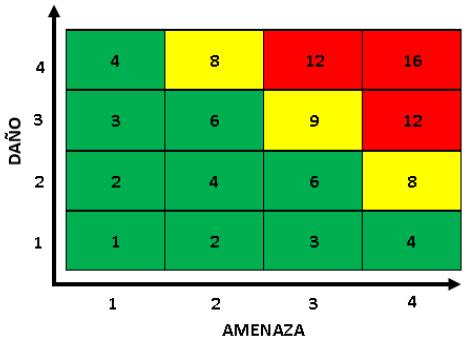

Figura 1: Resultado del Riesgo.

3.5. Clasificación y valoración de "Magnitud de Daño"

3.5.1. Clasificación: se marca con una "x", una o varias opciones a la lista, caso que no aplique se deja en blanco.

3.5.2. Magnitud de Daño: Se realiza la valoración según la siguiente escala:

Tabla 6: Calificación y Valoración de Magnitud de Daño.

Calificación de la probabilidad	Significado de la magnitud de daño
Insignificante	No causa ningún tipo de impacto o daño a la organización.
Bajo	Causa daño aislado, es decir que no perjudica a ningún componente de la organización.
Mediano	Provoca la desarticulación de un componente de la institución. Si no atiende a tiempo, a largo plazo puede provocar la desarticulación de la organización.
Alto	Es decir que en el corto plazo desmoviliza o desarticula a la organización.

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

3.5.3. Valoración de "Probabilidad de Amenaza"

Consiguientemente se valora la probabilidad de amenaza que podría causar perjuicio a la confidencialidad, integridad, disponibilidad y autenticidad de la información de la institución. La tabla 7 muestra la valoración según la escala:

Tabla 7: Valoración de Probabilidad de Amenazas.

Calificación de la probabilidad	Significado de probabilidad de Amenaza
Insignificante	No existen condiciones que impliquen riesgo o ataque.
Bajo	Existen condiciones que hacen muy lejana la posibilidad del ataque.
Mediano	Existen condiciones que hacen probable un ataque en el corto plazo, pero que no son suficientes para evitarlo en el largo plazo.
Alto	La realización del ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque.

En virtud de lo investigado acerca de la matriz de análisis de riesgo, se procede a realizar la matriz tomando en consideración la información que se tiene acerca de las empresas.

Tabla 8: Matriz de análisis de Riesgo de datos e Información.

Matriz de Análisis de Riesgo		**Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]**																								
Sistemas de Información	**Magnitud de Daño: [1 = Insignificante, 2 = Bajo, 3 = Mediano 4 = Altol**	**Actos originados por la criminalidad común y motivación política**									**Sucesos de origen físico**								**Sucesos derivados de la impericia, descuido de usuarios/as y decisiones institucionales**									
		Allanamiento (ilegal, legal)	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro	Falta de inducción, capacitación y sensibilización sobre riesgos	Utilización de programas no autorizados / software 'pirateado'	Perdida de datos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Falta de normas y reglas claras (no institucionalizar el estudio de los	Transmisión de contraseñas por teléfono	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Ausencia de documentación
		3	3	3	3	3	4	4	3	3	3	1	3	3	3	3	4	3	4	3	4	4	4	4	4	3	3	3
Datacenter	3	9	9	9	9	9	12	12	9	9	9	3	9	9	9	9	12	9	12	9	12	12	12	12	12	12	9	9	9
Seguridad física en equipos de cómputo (Candado en Portátiles, otros)	3	9	9	9	9	9	12	12	9	9	9	3	9	9	9	9	12	9	12	9	12	12	12	12	12	12	9	9	9
Control de acceso a equipos de cómputo (login)	4	12	12	12	12	12	16	16	12	12	12	4	12	12	12	12	16	12	16	12	16	16	16	16	16	16	12	12	12

Correo electrónico	3	9	9	9	9	9	12	12	9	9	9	3	9	9	9	9	12	9	12	9	12	12	12	12	12	9	9	9
Cableado estructurado de datos	3	9	9	9	9	9	12	12	9	9	9	3	9	9	9	9	12	9	12	9	12	12	12	12	12	9	9	9
Respaldos de la información	4	12	12	12	12	12	16	16	12	12	12	4	12	12	12	12	16	12	16	12	16	16	16	16	16	12	12	12
Uso del servicio de internet	3	9	9	9	9	9	12	12	9	9	9	3	9	9	9	9	12	9	12	9	12	12	12	12	12	9	9	9
Control de salida e ingreso de equipos	4	12	12	12	12	12	16	16	12	12	12	4	12	12	12	12	16	12	16	12	16	16	16	16	16	12	12	12

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

3.5.4. Análisis de riesgo promedio

La valoración de la probabilidad de amenaza según sus resultados es la siguiente:

Baja: Es decir que existen condiciones que hacen muy lejana la posibilidad de un ataque.

Mediana: Sostiene que existen condiciones que hacen poco probable un ataque en corto plazo, pero no son suficientes para evitarlo en largo plazo.

Alta: El ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque.

		Probabilidad de Amenaza		
		Criminalidad	**Sucesos de origen físico**	**Institucional**
Magnitud de Daño	**Sistemas de Información**	**10.9**	**9.7**	**12.2**

Tabla 9: Análisis de riesgo promedio.

Como resultado del análisis de riesgo, se percibe una probabilidad de riesgo alto con relación a criminalidad y al área de TI de las instituciones, es decir que el ataque es inminente, no existen condiciones internas y externas que impidan el desarrollo del ataque. La probabilidad de amenaza en sucesos de origen físico es medio lo que significa que existen condiciones que hacen poco probable un ataque en corto plazo, pero no son suficientes para evitarlo en largo plazo. En virtud de ello se puede decir que las políticas de seguridad informáticas, son necesarias y se recomendaría las PYMES tome en consideración implementarlas en un futuro, para que sus actividades no se vean afectadas.

4. DISCUSIÓN

Luego de la valoración de riesgos y amenazas en las 10 empresas se pudo evidenciar la necesidad de adoptar Políticas de Seguridad Informática que permitan regular los procesos y gestión de los servicios informáticos más comunes a nivel empresarial.

4.1 Estructura del documento de políticas de seguridad informática

Antes de explicar la estructura de las políticas de seguridad informática de acuerdo a las normas ISO 27001, se requiere dar a conocer que para el desarrollo de las políticas de seguridad se ha percibido conveniente englobar a todas las políticas de seguridad informática dentro de un

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

proceso, el cual se ha denominado PR-01 Sistemas de Información, para su gestión deben cumplir con las siguientes actividades:

- Mantener y administrar las redes.
- Prestar soporte técnico a usuarios en todo lo referente a la plataforma computacional.
- Supervisar todo el proyecto informático.
- Generar propuestas para facilitar el acceso y uso de la tecnología.
- Velar por la integridad y la seguridad de la información.
- Desarrollar, investigar y adaptar nuevas técnicas para mejorar la gestión interna y externa de la municipalidad.

De acuerdo a la investigación realizada, la manera más adecuada de generar la documentación, para la gestión de información es la siguiente:

Encabezado: Al lado izquierdo de la tabla se destina el logo de la Institución para quien va dirigido el diseño de las políticas de seguridad; intermedio de la tabla se especifica el nombre de la política; al lado derecho se define el código de la política, seguido de la versión y finalmente en el último recuadro el número de página.

Objetivo: Posee un conjunto de metas que se propone alcanzar según el tema o referencia de la política.

Alcance: Define a las personas que se verán involucradas acatar las políticas descritas.

Definiciones: Es un glosario de palabras que se asume el usuario desconozca, pretendiendo mejorar la comprensión de lectura de las políticas a los usuarios.

Documentos de referencia: Son documentos que se recomienda utilizar a fin de acatar las políticas, estos documentos pueden ser registros o anexos, se recomienda llamarla o identificarla de la siguiente forma: para registros se identifica anticipando el RE, seguido del código y finalmente el nombre del registro (RE-1A Carta de Aceptación de políticas de seguridad) y para los anexos se recomienda anticipar ANEXO, seguido del código y el nombre del anexo (ANEXO-1A Cronograma de mantenimiento preventivo de equipos).

Descripción de la política Aquí abarca los lineamientos que se propone según las necesidades de la institución, para mejorar la calidad de la seguridad informática, se detalla lo más claro posible de forma que sea comprensible para el lector.

Registros: Puede ser representada mediante una tabla que contiene:

- Código que es el nombre del documento.

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

- Nombre es el título del documento.
- Responsable será la persona encargada de llevar esta documentación.
- Ubicación es el lugar donde se pueda alojar el documento.
- Archivos especifica la fecha en la que ha sido aprobado.
- Actualización indica la fecha del tiempo que estará vigente el modelo del anexo o registro, pasado el tiempo estipulado se podrá realizar los cambios que se crean convenientes.
- Retención es el tiempo que se estima, se tendrá los documentos impresos.
- Destino final habitualmente los registros van hacer los documentos físicos.
- Acceso es quien va a poder ver, revisar o administrar las políticas físicas.

Anexos: Indica el listado de documentos en los que ya está estipulada cierta información, se vuelve a ubicar los anexos descritos en Documentos de Referencia, en caso que la política no requiera anexos, no hay que dejar el espacio vacío se debe usar N/A (No aplica). Cabe aclarar que los registros tanto como los anexos pueden ser llamados en otras políticas de acuerdo a la necesidad.

Pie de Página: Posee las firmas de quienes son los responsables de gestionar la política y de quien aprueba para su ejecución.

Esta documentación se debe imprimir asimismo reposar en cada uno de los departamentos para cualquier auditoría ya sea informática, auditoría de calidad, auditoría de procedimientos, entre otras. Finalmente, es necesario elaborar un plan de mitigación de riesgos como una propuesta estratégica para reducir la probabilidad de incidencias e impactos sobre los servicios informáticos que apoyan a la operación de las pequeñas y medianas empresas.

Tabla 11: Plan de mitigación de riesgos

OBJETIVO	RIESGO	ACCIONES A TOMAR	RESPONSABLE	TIEMPO DE MITIGAR EL RIESGO
Incrementar la seguridad de la información en los equipos, para estar listos ante cualquier eventualidad.	F. Interno: Respaldo a los equipos	Generar como Anexo un listado de usuarios para la ejecución de Backups siendo el medio de verificación un registro (RE-1F Bitácora de respaldos de usuarios).	Líder de los procesos de Infraestructura, aplicaciones de sistemas de información.	6 meses luego de la implementación
	F. Externo: No cuenta con acuerdos que garantice la confidencialidad de la información.	Firmar una Carta de aceptación de políticas de seguridad informática, registro que compromete a cumplir a los empleados con los lineamientos de confidencialidad de información enlistados.	Líder del proceso de sistemas de información.	6 meses luego de la implementación
Controlar los equipos que		Generar como Anexo un listado de categorías de acceso a internet, enuncia a las categorías	Líder del proceso de Infraestructura de sistemas de información	7 meses luego de la implementación

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

ingresen a la institución además de reducir la saturación de la red por mal uso del internet.	F. Interno: Acceso a redes sociales, streaming y otras páginas.	de accesos según las funciones de cada departamento.		
	F. Externo: Nivel de seguridad baja, en el control de acceso a equipos.	Elaborar registros como la solicitud de creación de nuevos usuarios de red, en el cual se crearán usuarios y contraseñas. De igual forma se da seguimiento a la actualización con una Bitácora de actualización de contraseñas.	Líder del proceso de Infraestructura de sistemas de información. Líder del proceso de Recursos Humanos.	8 meses luego de la implementación
Diseñar políticas de seguridad informática para proteger los activos del municipio.	F. Interno: Carencia de plan de mantenimiento preventivo.	Elaborar como Anexo el Cronograma para mantenimiento preventivo de equipos, dando seguimiento con el registro de la Bitácora de mantenimiento preventivo de equipos.	Líder del proceso de Infraestructura de sistemas de información.	6 meses luego de la implementación
	F. Externo: Carencia de políticas de seguridad informática.	Generar la gestión de procesos organizacionales para los Sistemas de Información, que aplica lineamiento para protección de la información como de los recursos informáticos.	Líder del proceso de sistemas de información. Líder del proceso de Gestión por Procesos.	8 meses luego de la implementación

5. CONCLUSIONES

Conclusiones

El presente trabajo de investigación permitió analizar a profundidad el estado en que se encuentran los servicios informáticos de las empresas públicas, privadas. PYMES del centro del país, como la operación de las herramientas, aplicaciones y equipos informáticos.

Es indispensable aplicar la matriz de análisis de riegos de tecnología de información, para identificar las amenazar y riesgos en cada empresa, además de justificar la necesidad de adoptar las políticas de seguridad informática para garantizar la confiabilidad, integridad, disponibilidad de la información y recursos informáticos.

Finalmente se ha iniciado un proceso de diseño del modelo de las políticas de seguridad informáticas en las 10 medianas y pequeñas empresas, aplicando los estándares de la ISO 27001, que permitan gestionar los servicios de TIC’s garantizando su operación confiable, íntegra y disponible.

ISSN: 2602-8255
Volumen 4, número 1, febrero 2022

6. BIBLIOGRAFÍA

[1] Iván Salvadori, “Los delitos contra la confidencialidad, la disponibilidad y la integridad de los datos y sistemas informát,” 2011. Accessed: Dec. 07, 2020. [Online]. Available: http://www.

[2] L. Y. B. Moreno, K. M. Tamara, and B. E. S. Carvajalino, “Creación de un manual de políticas de seguridad de la información para la dependencia secretaria de la institución educativa nuestra señora de belen de cúcuta,” 2017. Accessed: Dec. 07, 2020. [Online]. Available: http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/1688.

[3] ICA, “Manual del Sistema de Gestión de Seguridad de la Información SGSI AGOSTO 2018 El presente Manual es parte integral del Manual del Sistema de Gestión Oficina Tecnologías de la Información,” Colombia, Aug. 2018. Accessed: Aug. 12, 2020. [Online]. Available: https://www.ica.gov.co/getattachment/Modelo-de-P-y-G/Eficiencia-Administrativa/Procesos-y-Procedimientos/ManualSGSI-Agosto-2018.pdf.aspx?lang=es-CO.

[4] F. N. J. Solarte Solarte, E. R. Enriquez Rosero, and M. del C. Benavides Ruano, “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001,” *Tecnológica ESPOL–RTE* , vol. 28, pp. 1–16, Dec. 2015, Accessed: Sep. 03, 2020. [Online]. Available: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321.

[5] M. I. Romero Castro *et al.*, “Introducción a la seguridad informática y el análisis de vulnerabilidades,” Manabí, 2018. Accessed: Jun. 05, 2020. [Online]. Available: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf.

[6] J. E. Guanoluisa Huertas and I. F. Maldonado Soliz, “ANÁLISIS DE RIESGOS Y DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CONSEJO NACIONAL DE IGUALDAD DE DISCAPACIDADES ‘CONADIS’.,” Quito, May 2015. Accessed: Jun. 07, 2020. [Online]. Available: https://bibdigital.epn.edu.ec/bitstream/15000/10499/1/CD-6217.pdf.

[7] K. E. López Carranza, “Diseño de un plan de mitigación de riesgos empresariales identificando los riesgos internos y externos de comercial novedades leydi en el cantón la troncal del año 2014.,” 2015. Accessed: Sep. 07, 2020. [Online]. Available: http://186.5.103.99/handle/reducacue/7293.

[8] Yi Min Shum, “Matriz de evaluación de factores internos (Matriz EFI - MEFI),” 2018. https://yiminshum.com/matriz-evaluacion-factores-internos-mefi/ (accessed Sep. 07, 2020).

[9] K. Cárdenas Posada, J. D. Fernández Vásquez, and L. Hernández Aros, “Matriz de riesgos en el desarrollo del encargo,” p. 22, 2018, Accessed: Sep. 06, 2020. [Online]. Available: https://repository.ucc.edu.co/bitstream/20.500.12494/5166/1/Matriz de riesgo en el desarrollo del encargo %282%29.pdf.