DISEÑO DE UN SGSI QUE PERMITA EL CONTROL ADECUADO EN EL MANEJO DE LA INFORMACIÓN Y SU SEGURIDAD EN UNA PYME DE GESTION DE EVENTOS Y ESPECTACULOS DE LA CIUDAD DE CALI

LUIS FERNANDO MUÑOZ BOJORGE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E NGENIERÍA

ESPECIALIZACION EN SEGURIDAD INFORMÁTICA

POPAYÁN

2021

DISEÑO DE UN SGSI QUE PERMITA EL CONTROL ADECUADO EN EL MANEJO DE LA INFORMACIÓN Y SU SEGURIDAD EN UNA PYME DE GESTION DE EVENTOS Y ESPECTACULOS DE LA CIUDAD DE CALI

LUIS FERNANDO MUÑOZ BOJORGE

PROYECTO APLICADO

YENNY STELLA NÚÑEZ
DIRECTORA DE PROYECTO DE GRADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E NGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
POPAYÁN
2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Ciudad y Fecha (día, mes, año) (Fecha de entrega)

A mis padres, porque su fuerza me ha inspirado y me inspirará toda la vida.

AGRADECIMIENTOS

Dedicado a mi familia, a mis amigos y en especial a mis hijos, como motor de cada uno de mis pasos.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

En la actualidad la información es el activo más importante en una Organización, un elemento crucial para poder ser competitivos frente a las demás empresas que hacen parte de los mercados, por lo que se deben analizar e implementar los mecanismos necesarios para protegerla. Bajo esta premisa se llevó a cabo este estudio que pretende identificar los activos informáticos en las PYMES dedicadas a la gestión de eventos y espectáculos en la ciudad de Cali y determinar los riesgos a los que se encuentran expuestos, ya que debido en muchas ocasiones se presenta desorganización en el área de Sistemas y la falta de gestión de la plataforma informática.

Este análisis se realiza en varias etapas las cuales comprenden entrevistas, observación directa y la aplicación de Magerit, como metodología para analizar riesgos y poder así reconocer vulnerabilidades y amenazas. Como resultado se pretende generar un modelo del manual de políticas de seguridad informática de una empresa y el listado de los activos informáticos, así como las recomendaciones para mejorar la confidencialidad apoyándose en posibles auditorías ya realizadas anteriormente, que puedan haber generado hallazgos para ser verificados mediante esta herramienta en pro de brindar el tratamiento correspondiente.

PALABRAS CLAVE: Amenaza, estrategia, información, riesgo, seguridad, vulnerabilidad.

ABSTRACT

Information is currently the most important asset in an Organization, a crucial element in order to be competitive with other companies that are part of the markets, so the necessary mechanisms to protect it must be analyzed and implemented. Under this premise, this study was carried out, which aims to identify the IT assets in SMEs dedicated to the management of events and shows in the city of Cali and determine the risks to which they are exposed, since on many occasions it occurs disorganization in the Systems area and lack of management of the IT platform.

This analysis is carried out in several stages which include interviews, direct observation and the application of Magerit, as a methodology to analyze risks and thus be able to recognize vulnerabilities and threats. As a result, it is intended to generate a model of a company's computer security policy manual and the list of computer assets, as well as recommendations to improve confidentiality based on possible audits already carried out previously, which may have generated findings to be verified through this tool in order to provide the corresponding treatment.

KEY WORDS: Threat, strategy, information, risk, security, vulnerability.

INTRODUCCIÓN

Los diferentes avances tecnológicos y las actuales exigencias en las comunicaciones hacen que sea de gran importancia mantener nuestra información protegida ante posibles accesos no autorizados que pueda acarrear fraudes o ilícitos.

Vivimos en un mundo en el que el uso masivo de los recursos de información y el constante procesamiento de los datos han creado un estado de riesgo, donde nuestra información es un elemento de interés para terceros que buscan lucrarse al violar sus propiedades de confidencialidad o exclusividad. Esta problemática exige mecanismos de protección cada vez más robustos y planificados, los cuales parten de análisis exhaustivos que buscan determinar las características que deben tener estas herramientas para cumplir a cabalidad su objetivo.

La finalidad de este documento es entregar un análisis de los riegos informáticos existentes actualmente en las PYMES que generan eventos y espectáculos, que sirva como precedente en la implementación a futuro de un Sistema de Gestión de la Seguridad de la información y como diagnóstico exhaustivo de las condiciones de confidencialidad de los recursos informáticos que allí coexisten, como parte del procesamiento de datos exigido por la operación de las Organizaciones.

1. DEFINICION DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La PYME de gestión de eventos y espectáculos está ubicada en la ciudad de Cali, donde se encuentra su única sede, en el sur de la ciudad. Actualmente cuenta con una edificación alquilada de dos niveles, en donde el primer piso está dedicado a la recepción de los clientes, proveedores y un salón de eventos, así mismo como las oficinas del área jurídica, diseño y comunicaciones, la Gerencia General y una pequeña sala de juntas. En el segundo nivel se encuentran las oficinas administrativas, Tesorería, Talento humano, Contabilidad, Gestión de eventos, Sistemas y telecomunicaciones, Compras, Producción, una segunda sala de juntas y el cuarto de Tecnologías de información.

La PYME está dedicada a la gestión y producción de eventos artísticos, culturales y deportivos, propios y contratados por terceros, labor que ha hecho que su crecimiento en la ciudad haya sido precipitado, llegando a convertirse en una empresa de gran importancia para la ciudad. A pesar de su crecimiento y envergadura de sus operaciones, cabe mencionar que ha evolucionado dejando de un lado la atención a sus sistemas tecnológicos, convirtiéndose en una Organización cuya estructura informática presenta notables atrasos, a los cuales apenas se les está brindando atención. Por este motivo, se puede afirmar que este documento es el único análisis de riesgos relacionado a la seguridad de la información que se ha desarrollado.

1.2 DESCRIPCIÓN DEL PROBLEMA

Definiendo la problemática, podemos decir que actualmente se presentan fallas con el manejo de la información que han repercutido seriamente en los objetivos del negocio, además de que nunca ha existido una persona capacitada para analizar e identificar los riesgos existentes, esto ha causado incidentes de seguridad bastante graves, como la pérdida de información de los servidores de la empresa.

Aunque existen algunos mecanismos para salvaguardar la información, estos no son eficientes ya que no hay una persona encargada para esta labor, ni para el control de la plataforma tecnológica que simplemente crece por la contratación desordenada de múltiples proveedores de tecnología que trabajan individualmente sobre los servidores, los dispositivos de red y telecomunicaciones, provocando que estos sean configurados de manera independiente por cada persona en pro de que sus aplicativos funcionen, pero

sin tener el debido cuidado de no exponer la seguridad de estos equipos al hacer sus configuraciones.

La falta de control sobre los activos y sobre la información que fluye a través de ellos es tan evidente, que todos los datos permanecen expuestos en carpetas compartidas en la red, sin control de acceso ni manejo de permisos adecuados, así mismo, aunque existen cuartos de telecomunicaciones dotados de corriente regulada y de racks, se evidencia desorden y poca seguridad física que evite que personas inescrupulosas accedan a los equipos ubicados en esta área, pudiendo causar daños, robo o sabotaje a los equipos que permiten que los servicios informáticos sean utilizados por los usuarios, lo cual tendría un impacto altísimo en la Organización, debido a que se detecta que no hay un plan efectivo de Backups que respalde la información y que permita salvaguardar información importante de las diferentes áreas o definir un plan de contingencia en caso de materializarse los riesgos existentes, los cuales no han sido definidos ni analizados, a pesar de que en el pasado la empresa ha realizado algunas inversiones en tecnología como la compra de servidores, de una buena conexión a Internet y equipos de cómputo de última tecnología, se hace necesaria una gran capacidad de almacenamiento y procesamiento de información para satisfacer las diferentes áreas de la empresa.

1.3 FORMULACION DEL PROBLEMA

¿De qué manera el diseño de un SGSI en una PYME de gestión de eventos y espectáculos puede ayudar al correcto manejo y la seguridad de la información?

2. JUSTIFICACIÓN

En la actualidad la información de una empresa es su activo más importante por ende debe ser protegida. En un mundo de conectividad creciente y donde las amenazas aumentan de manera constante, debemos protegernos no solo de personas inescrupulosas que quieran robar nuestros datos o destruirlos, sino de aquellas debilidades que nos exponen a ser blanco fácil de ataques o de errores internos que nos dejen a merced de los riesgos latentes en nuestro entorno. Analizar la implementación de un SGSI permitirá aprovechar oportunidades para trazar un camino seguro y eficiente hacia la meta empresarial, aprovechando las nuevas tecnologías existentes y permitiéndonos ver nuestro estado actual lo que serviría como un pequeño paso para poder evaluar si realmente estamos siguiendo el mejor camino hacia el crecimiento y el desarrollo organizacional.

La actividad de la PYME tiene como pilar absoluto la comunicación que se tiene entre las dependencias de la misma, estos son entes generadores de información a cada segundo y, por tanto, el tratamiento que se dé a estos datos es de vital importancia en la velocidad y calidad de los procesos para proveer a la Gerencia de informes que sean un mecanismo eficiente al momento de realizar cambios en el esquema empresarial, en el manejo de presupuestos y de recursos. Desde este enfoque se puede trabajar para mejorar, ya que si se puede garantizar que estos procesos de comunicación son óptimos y seguros los servicios que presta la empresa también lo serán, incidiendo directamente en la calidad que se muestra ante el cliente interno y externo de la empresa, logrando un impacto mucho mayor en los mercados donde se participa.

La clave para poder mejorar los procesos internos de la PYME radica en conocer que se tiene, que se hace y cómo se hace, y en el proceso garantizar los mecanismos que permitan asegurar y respaldar la información que se maneja día a día.

La importancia de realizar la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) es que permitirá gestionar de manera adecuada y constante la seguridad de los datos y en una mejora continua, dándole al área directiva de la empresa las herramientas para poder tomar decisiones que la acerquen a sus objetivos empresariales. Cabe resaltar que entre los mayores beneficios que este proceso traerá para la PYME está el involucrar la Gerencia en la protección de la información, concientizando y creando una cultura informática general que logre cambiar el pensamiento de las personas, en especial de los directivos con respecto a la falta de importancia que se da hoy en día al mejoramiento y la gestión sobre los diferentes sistemas informáticos que se tienen, un cambio que sea consecuente en el cuidado y protección de los datos que cada persona maneja y que una a todos en un solo pensar, el de tratar los datos empresariales y personales como lo que realmente son, una parte

vital en las operaciones de la empresa y como tal se debe garantizar la colaboración permanente para contrarrestar las actuales situaciones presentadas.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de la seguridad informática en una PYME de gestión de eventos y espectáculos de la ciudad de Cali, mediante la aplicación de la metodología MAGERIT, utilizando los controles de la norma ISO27001:2013

3.2 OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico general de la seguridad informática para determinar el nivel de riesgo al que se encuentran expuestos los recursos informáticos de la Organización.

- Identificar mediante la metodología MAGERIT los activos informáticos para evidenciar amenazas, vulnerabilidades a los que se encuentran expuestos con el fin de determinar acciones de mejora o mecanismos que permitan mitigar los posibles riesgos.

- Aplicar la declaración de aplicabilidad de los controles del anexo A de la ISO 27001:2013 como referencia para la implementación de medidas de protección de la información.

- Crear el manual de políticas de seguridad informática para la PYME.

4. MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

Actualmente las Organizaciones dependen exclusivamente de la información que procesan convirtiéndola en el principal activo que poseen. Bajo esta premisa se debe garantizar la aplicación de los conceptos de seguridad de la información que permitan alcanzar los niveles de confidencialidad, integridad y disponibilidad deseados. A continuación, se enuncia algunos conceptos relevantes en la seguridad de la información.

Sistema de gestión de la información (SGSI).

Un Sistema de Gestión de la seguridad de la información es un conjunto de políticas establecidas para poder administrar la información, cuyo concepto claves es el diseño, implantación y mantenimiento de un grupo de procesos, definidos con la finalidad de poder gestionar el acceso a la información de manera que se pueda asegurar la confidencialidad, integridad y disponibilidad de los activos de información mediante la mitigación de los riesgos existentes[1]. Su propósito es garantizar que los riesgos en materia de seguridad de la información sean conocidos, asumidos, gestionados y minimizados, de manera documentada y organizada por parte de las empresas.

Un SGSI es útil para muchos aspectos, como el cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno y la protección de los objetivos del negocio en pro del aprovechamiento de nuevas oportunidades de negocio.

Un SGSI es el elemento más importante de la norma ISO27001, en donde se unifican todos aquellos criterios para evaluar los riesgos relacionados al manejo de información. Estos son algunos de los beneficios que trae su implementación:

- Brinda confianza y satisfacción sobre los requisitos de seguridad de la información.
- Permite una adecuada gestión de los activos de información de las Organizaciones
- Reducción de riesgo de pérdida de información con la opción de poder continuar con la operación después de un siniestro o de incidentes graves.
- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.

[1] ISO Tool excellence, 2016

Ventajas de la implementación de un SGSI

- Reducción del riesgo de pérdida de información
- Se establece una metodología para gestión de la seguridad de la información
- Implanta medidas de seguridad que conllevan a mejora continua.
- Permite ofrecer una garantía para con los clientes y socios.
- Operación normal en las Organizaciones
- Permite integrarse con otros sistemas de gestión
- Cumplimiento de legislación vigente relacionada

Seguridad informática

Es el proceso de prevenir y detectar el uso no autorizado de los diferentes sistemas informáticos, protegiéndolos contra intrusos que puedan cometer fraudes, ilícitos con la finalidad de obtener ganancias. [2]

Áreas principales de la Seguridad Informática

- Confidencialidad: Se trata de que sólo los usuarios autorizados para acceder a la información puedan acceder a ella.
- Integridad: Solo los usuarios autorizados pueden modificar la información cuando así lo determinen.
- Disponibilidad: Los datos siempre deben estar disponibles para los usuarios cuando estos los necesiten.
- Autenticación: Poder confiar en que los usuarios con los que se comunica son realmente quienes dicen ser.[3]

La Seguridad informática busca proteger los activos de la información, a saber:

Información: Mayor activo de las empresas, conjunto de datos organizados.
Equipos: Software o Hardware.
Usuarios: Personas que usan los sistemas informáticos

[2] Equipo de expertos – Universidad de Valencia, 2016

[3] Equipo de expertos – Universidad internacional de Valencia, 2016 (https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf)

La importancia de la Seguridad informática radica en que permite prevenir ilícitos que se pueden desprender de las acciones que realizamos día a día, en el manejo de nuestra información.[4]

Seguridad de la información

Son el conjunto de medidas preventivas y reactivas definidas por la Organizaciones para resguardar la información manteniendo la confidencialidad, disponibilidad e integridad de los datos[5].
El objetivo de la Seguridad de la información es mantener un ambiente relativamente seguro, que permita proteger los activos de información de la empresa, así como el uso adecuado de los recursos y la gestión del riesgo.

Ciclo PHVA

Es una herramienta que permite mejorar continuamente los procesos de una Organización, esencial por su efectividad y eficacia ya que es un modelo dinámico y flexible que ayuda a reducir costos y al mejoramiento de la productividad.

El ciclo PHVA funciona a partir de 4 pasos:

- Planificar

Se establecen objetivos y se identifican procesos con el fin de lograr objetivos de acuerdo a las políticas de la Organización.

- Hacer

Se ejecutan las acciones determinadas con la finalidad de conseguir los objetivos definidos.

- Verificar

[4] Equipo de expertos – Universidad internacional de Valencia, 2016
[5] Universidad Libre, 2015

Se tiene un periodo de prueba para poder definir si los cambios implementados han sido eficientes.

- Actuar

En el caso de que los cambios no sean suficientes o se ajusten a las expectativas se realizan acciones correctivas.
Beneficios del ciclo PHVA:

- Reducir costos
- Aumentar productividad
- Ganar cuota de mercado
- Incrementar rentabilidad
- Mejora integral de la competitividad, de los productos y servicios
- Mejora continua de la calidad

Vulnerabilidad: Es una debilidad o fallo de los sistemas informáticos que pone en riesgo la seguridad de la información, permitiendo que un atacante pueda comprometer la confidencialidad, integridad y disponibilidad de los datos. [6]

Amenaza:

Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Toda amenaza tiene una consecuencia, que puede llegar a ser ataques (fraudes, robos, ilícitos), sucesos físicos (incendios, inundaciones, o negligencia y malas decisiones institucionales, como por ejemplo mal manejo de contraseñas, no utilizar cifrado, etc. [7]

Riesgo informático:

Se define como la dificultad que interviene en el cumplimiento de una meta o una amenaza a la pérdida de documentos.[8]

[6] Incibe – Instituto Naciona de Ciberseguridad, 2017
[7] Incibe – Instituto Naciona de Ciberseguridad, 2017

[8] Uniminuto, Facultad de Contaduría pública, 2014

Activo informático:

Es cualquier componente, dispositivo o dato del entorno que ejecuta actividades relacionadas con la generación de información. [9]

Impacto:

Es la consecuencia sobre un activo que tiene la materialización de una amenaza. [10]

MAGERIT:

Es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para el análisis de los riesgos que se derivan del uso de las TICs e implementar las medidas más adecuadas que logren mitigar esos riesgos.[11]

Magerit se basa en identificar el impacto que tendría violar la seguridad en la empresa, mostrando las amenazas que pueden llegar a afectar y las vulnerabilidades usadas por estas amenazas.

Magerit está dividida en 3 libros. El primero hace referencia al método, en él se describe la estructura que debe tener el modelo de gestión de riesgos, el segundo es un catálogo de elementos que puede verse como un inventario que la empresa puede utilizar para enfocar el análisis de riesgo. El tercer libro es una guía de técnicas, lo cual lo convierte en un elemento que lo diferencia de otras metodologías.

MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, MAGERIT es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico.

Objetivos de MAGERIT

[9] Widefense, Seguridad sin miedo, Keneth Daniels, 2018
[10] Incibe – Instituto Nacional de Ciberseguridad, 2017
[11] Ministerio de Hacienda y Administraciones públicas, Gobierno de España - Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012

MAGERIT persigue los siguientes Objetivos Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Libro 1 – Método

- El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.
- El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.
- El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.
- El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.
- El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.
- El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.
- El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

Libro 2 – Catálogo

Marca unas pautas en cuanto a:

- Tipos de activos
- Dimensiones de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de información
- Salvaguardas que considerar para proteger sistemas de información

Se persiguen dos objetivos:

Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.
Cada sección incluye una notación XML que se empleará para publicar regularmente los elementos en un formato estándar capaz de ser procesado automáticamente por herramientas de análisis y gestión.
Si el lector usa una herramienta de análisis y gestión de riesgos, este catálogo será parte de la misma; si el análisis se realiza manualmente, este catálogo proporciona una amplia base de partida para avanzar rápidamente sin distracciones ni olvidos.

Libro 3 – Guía de técnicas

Aporta luz adicional y orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos:

- Técnicas específicas para el análisis de riesgos
- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Técnicas gráficas
- Sesiones de trabajo: entrevistas, reuniones y presentaciones

Sistema de información:

Es un conjunto de elementos que son utilizados para la administración de datos y que están coordinados entre sí. [12]

Tipos de Sistemas de información

Existen diferentes tipos:

- Sistemas de procesamiento de transacciones
- Sistema de información Gerencial
- Sistema de apoyo a decisiones
- Sistemas expertos e inteligencia artificial
- Sistema de apoyo a decisiones de grupo
- Sistema de información a ejecutivos

Análisis de riesgo:

Es un estudio que se realiza para evaluar los peligros potenciales y sus posibles consecuencias en una Organización o en un proyecto, con el objeto de establecer medidas de prevención y de protección. Éstos ayudan a tomar decisiones que permiten implementar medidas de prevención y así evitar peligros potenciales o reducir su impacto.[13]

Malware

Es un software cuyos fines son maliciosos, entre los cuales pueden incluirse infectar y dañar un sistema informático. El objetivo es invadir, dañar o deshabilitar sistemas, asumiendo el control parcial de las operaciones e interfiriendo en el funcionamiento normal. [14]

[12] Victor Manuel Vázquez López, 2017
[13] Juan Pablo Calle, 2020
[14] Malwarebytes, 2015

Tipos de malware:

- Adware:

Es un software no deseado diseñado para mostrar anuncios en la pantalla, normalmente en los exploradores.

- Spyware:

Es un software que se dedica a monitorear las acciones de un usuario dentro de un dispositivo para luego comunicarlas a un tercero, previamente definido.

- Virus informático:

Es un software que se adjunta a otro programa y cuando este es ejecutado realiza acciones no deseadas modificando archivos o aplicaciones.

- Gusanos informáticos:

Es un software similar a los virus informáticos con la diferencia de que se replican por sí mismos a través de otros ordenadores o redes.

- Troyanos:

Es uno de los más peligrosos pues es un malware que se oculta tras algo útil para el usuario, cuando está en el sistema víctima puede dar acceso a los atacantes.

- Ramsomware:

Es un malware que bloquea el acceso a dispositivos o cifra la información del usuario para posteriormente exigir un pago para devolvérselos.

- Rootkit:

Es un programa maligno que proporciona al atacante acceso con permisos de administración a los sistemas.

Ingeniería Social:

Son un conjunto de técnicas utilizadas por los ciberdelincuentes para engañar a los usuarios incautos y que estos envíen datos confidenciales, infecten sus sistemas con malware o abran enlaces a sitios infectados. [15]

4.2 MARCO CONTEXTUAL

ASEGURÉMONOS es una empresa vallecaucana, ubicada en la ciudad de Santiago de Cali, con instalaciones que albergan casi a 100 personas en temporadas altas, como los meses de noviembre y diciembre. Posee una sede principal en donde se encuentran dos niveles o pisos, en el primero funciona la recepción y un salón de reuniones y en el segundo las oficinas que contienen las diferentes áreas administrativas y de producción.

La empresa está dedicada a la producción de eventos socioculturales y deportivos, entre los cuales tenemos la feria de Cali y el festival de macetas entre otros, eventos que se han institucionalizado a lo largo del tiempo en la ciudad, que espera año tras año estos eventos para participar de manera activa y ordenada.

4.3 MARCO LEGAL

ASEGURÉMONOS es una empresa mixta, constituida por capital privado y recursos del estado, que recibe apoyo económico de la alcaldía de Cali. Las sociedades de economía mixta se sujetan a las reglas del derecho privado y a la jurisdicción ordinaria, según el artículo 461 del código de Comercio.

[15] Kaspersky, 2016

Según la constitución nacional colombiana: “Son sociedades de comercio sujetas al derecho mercantil, con las limitaciones expresas que la constitución y la ley establezcan”.[16]

El Decreto 3130 de 1968 alude igualmente a este tipo de empresas en su artículo 1º, cuando al referirse a las entidades descentralizadas menciona que los institutos y empresas oficiales a que se refiere la Ley 65 de 1967, son, conforme al Decreto 1050 de 1968, de tres tipos: Establecimientos Públicos, Empresas Industriales y Comerciales del Estado y Sociedades de Economía Mixta, las cuales desarrollan una actividad específica, gozan de autonomía administrativa y se encuentran bajo el control del poder central, comúnmente conocido como control de tutela.

Así, se pueden señalar como sus características:

- Son de creación o autorización legal, amén de que surgen del contrato de sociedad
- Tienen el carácter de sociedades comerciales
- Cumplen actividades industriales o comerciales
- El capital está integrado por aportes del Estado y de los particulares, por este motivo la legislación que la cobija es amplia, con algunas excepciones debido a su naturaleza privada.

El artículo 97 de la ley 489 de 1998 define las características que las sociedades de economía mixta deben cumplir para considerarse como tal menciona que dichas sociedades forman parte de la rama ejecutiva del poder público en el sector descentralizado por servicios y que están vinculadas a ministerios o a departamentos administrativos.
En el artículo 14 de ley 1150 de 2007, modificado por el artículo 93 de la ley 1474 de 2011 se dispone que las sociedades de economía Mixta donde el estado tenga participación superior al 50% estarán sometidas al Estatuto general de contratación de la administración pública.

4.4 MARCO NORMATIVO

La serie ISO 27000 es la que abarca toda la normativa en lo relacionado a la Seguridad de la Información, a continuación, se relacionan:

[16] Wikipedia. Definición de Sociedad mercantil. 2013.

Tabla 1: Normatividad relacionada a Seguridad Informática

Norma	Descripción
ISO 27000	Es un conjunto de estándares internacionales sobre la Seguridad de información que contiene una serie de buenas prácticas para el establecimiento, implementación, mantenimiento y mejoras de Sistemas de gestión de seguridad de la información (SGSI).
ISO 27001	Norma internacional que permite el aseguramiento, confidencialidad e integridad de los datos y de la información, así como de los sistemas que los procesan.
ISO 27002	Esta norma se centra en las buenas prácticas para la gestión de la Seguridad de la Información. Describe como se pueden establecer los controles, los cuales son escogidos con base a una evaluación de riesgos de los activos más importantes de las empresas. Esta norma tiene como principal objetivo establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la Seguridad de la información.
ISO 27003	Es una norma que pretende servir como guía de implementación de un SGSI. Contiene una descripción del proceso de delimitación del SGSI, además del diseño e ejecución de distintos planes de implementación.
ISO 27004	Sistema de métricas e indicadores Este estándar especifica como estructurar el sistema de medición, define cuales son los parámetros a medir, cuántos son y como medirlos. Ayuda a las empresas al establecimiento de objetivos relacionados con el rendimiento y los criterios del éxito.
ISO 27005	Guía de análisis y gestión de riesgos Contiene diferentes recomendaciones y directrices para la gestión del riesgo en Sistemas de gestión de seguridad de la información.
ISO 27006	Especificaciones para Organismos certificadores del SGSI Contiene las definiciones y términos que se usarán durante toda la serie 27000. Contiene el vocabulario perfectamente definido para evitar malos entendidos o malas interpretaciones de conceptos.
ISO 27007	Guía para auditar el SGSI Contiene una guía para las organizaciones certificadas para auditar SGSI.
ISO/IEC TR 27008	Es un estándar que suministra orientación acerca de la implementación y operación de los controles.
ISO/IEC 27010	Guía para la gestión de la Seguridad de la Información cuando se comparte entre sectores u organizaciones

Norma	Descripción
Ley 1273 de 2009	Ley de delitos informáticos en Colombia En esta ley se modifica el código penal creando un nuevo bien jurídico relacionado a la información, y se penaliza los delitos que atenten contra su confidencialidad, integridad y disponibilidad.
Ley 1581 de 2012	Ley de protección de datos personales. En esta ley se especifican los limitantes para la transferencia de datos considerados como personales. En ella se define como las personas tienen el derecho de conocer, actualizar y rectificar la información que tienen las diferentes entidades sobre ella.

Fuente: El autor

Origen de la NTC ISO 27001

Esta norma es la evolución de diferentes estándares[17]:

1901 – Normas "BS": La British Standards Institution publica normas con el prefijo "BS" con carácter internacional. Estas son el origen de normas actuales como ISO 9001, ISO 14001 u OHSAS 18001.

1995- BS 7799-1:1995: Mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información.

1998 – BS 7799-2:1999: Revisión de la anterior norma. Establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.

1999 – BS 7799-1:1999

2000 – ISO/IEC 17799:2000: La Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799, sin experimentar grandes cambios.

2002 – BS 7799-2:2002: Se publicó una nueva versión que permitió la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países.

2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005: Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.

[17] ISO Tools Excellence, 2013

2007 – ISO 17799: Se renombra y pasa a ser la ISO 27002:2005

2007 – ISO/IEC 27001:2007: Se publica la nueva versión.

2009 – Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M:2009.

4.5 ANTECEDENTES

Actualmente en la PYME y de manera anual se realiza una auditoría al área de Sistemas, la cual es ejecutada por un tercero, el grupo Millán y asociados. En este proceso se verifican las condiciones en que la información es manejada dentro de la Organización y cómo se protegen los diferentes equipos que albergan los datos.

Como resultado de estas auditorías se obtiene un informe, el cual contiene los hallazgos identificados y posibles riesgos que pueden llegar a materializarse, estos puntos deben ser resueltos por personal del área de Sistemas en el menor tiempo posible y de igual manera se debe reportar a la Gerencia el tratamiento que se brinda para poder cerrar de manera satisfactoria lo encontrado en las auditorías.

Actualmente la auditoria tuvo lugar en el mes de febrero del presente año, así mismo, se dio solución a los puntos del documento para mitigar algunos de los riesgos existentes en el momento.

5. DISEÑO METODOLOGICO

5.1 METODOLOGIA

Actualmente el método PHVA parte de una mejora continua sobre los procesos que se van a aplicar y es una de las principales herramientas para el mejoramiento continuo de la calidad dentro de las empresas.[18] Sus etapas son:

Modelo PHVA de un SGSI

- Planificación: En esta etapa se establece la política, objetivos, procesos y los procedimientos que permitan mejorar la Seguridad de la información.
- Hacer: Esta etapa está destinada a realizar la ejecución de los procedimientos establecidos.
- Verificar: En esta etapa se evalúa la efectividad de los mecanismos diseñados e implementados con la finalidad de presentar un informe a la Dirección que permita determinar acciones de mejora y retroalimentación.
- Actuar: Se emprenden acciones correctivas que garanticen la mejora de la Seguridad de la información.

Debido a que en el presente proyecto se realizará únicamente el análisis del SGSI para la PYME, se definen los siguientes elementos para la etapa involucrada:

PLANEAR:

- Definir los objetivos del SGSI
- Definir el alcance para el SGSI
- Realizar un inventario de los activos informáticos de la Organización
- Identificar las posibles amenazas para los activos
- Identificar las vulnerabilidades existentes.
- Identificar el impacto de las vulnerabilidades
- Realizar un análisis y evaluación de los riesgos
- Realizar una selección de los controles

[18] ISOTOOLS. En que consiste el ciclo PHVA. Modelos de gestión y excelencia. 2015

5.2 POBLACIÓN

Debido al tamaño de la PYME de gestión de eventos y espectáculos se toma la totalidad de las dependencias existentes en las cuales se aplicó una encuesta con el objetivo de identificar la problemática actual.
Actualmente la PYME cuenta con 70 colaboradores, distribuidos en sus 10 dependencias relacionadas a continuación:

- Recepción
- Comunicaciones
- Contabilidad
- Tesorería
- Producción
- Gestión humana
- Gerencia
- Compras
- Calidad
- Financiera

5.3 INSTRUMENTOS

Se elabora una encuesta y se aplica a los diferentes colaboradores de la PYME, definiendo una muestra de la totalidad de personas por área, de esta manera:

- Recepción 1
- Comunicaciones 1
- Contabilidad 1
- Tesorería 1
- Producción 2
- Gestión humana 2
- Gerencia 1
- Compras 2
- Calidad 1
- Financiera 2

Total personas encuestadas: 13

5.3.1 APLICACIÓN DEL INSTRUMENTO

Las encuestas se aplican el día 11 de febrero del año 2020 desde las 8 a.m. hasta las 4 p.m. mediante formulario escrito.

6. DISEÑO DEL SGSI

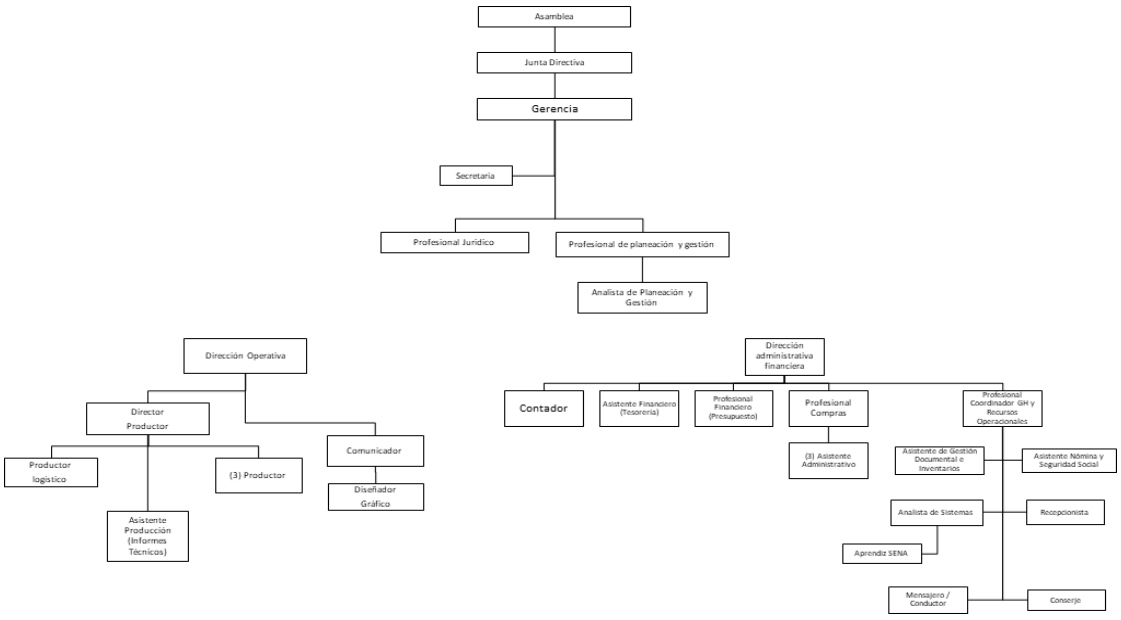
6.1 ANÁLISIS DE LA SITUACION ACTUAL

6.1.1 DIAGNÓSTICO

Actualmente la PYME posee una sede principal ubicada en la ciudad de Cali ubicada en el sur de la ciudad, es una edificación que consta de 2 pisos. En el primer piso funcionan las áreas de Recepción, Comunicaciones, Secretaría de Gerencia, Gerencia y el área Jurídica. En el segundo piso están las áreas de Producción, Tesorería, Gestión humana y administrativa, Compras, Gestión documental y la Dirección financiera. Además de esto, se encuentra el cuarto de telecomunicaciones, donde están los equipos técnicos y de comunicaciones como el Rack, switches, routers, Servidores, UPS, entre otros. Es de aclarar que la sede no es propiedad de la PYME, es tomado en alquiler por la Organización.

6.1.2 ORGANIGRAMA

Ilustración 1 Organigrama de la PYME



Fuente. PYME objeto de análisis.

6.1.3 ANÁLISIS DE RECURSOS TECNOLÓGICOS

6.1.3.1 INVENTARIO DE ACTIVOS DE LA PYME

Los Activos son todo lo que la empresa posee para realizar el procesamiento de la información, tales como Hardware, Software, recursos humanos y otros[19]. La clasificación de los Activos se realiza de acuerdo con la siguiente tabla:

Inicialmente se definen los siguientes dominios para la PYME:

Tabla 2 Listado de dominios

CODIGO	DOMINIO
BASE	Personal
HW	Hardware
RD	Red
INT	Instalaciones
SV	Servicios
EA	Equipamiento auxiliar
SW	Software o aplicación
AI	Activo de información
INS	Instalaciones

Fuente: El autor

Teniendo en cuenta estos dominios se definen los siguientes Activos informáticos para la PYME, los cuales fueron obtenidos al realizar el inventario correspondiente.

Tabla 3 Listado de activos

CODIGO	DETALLE
IS	**SERVICIOS INTERNOS**
INT	Internet
COELE	Correo electrónico
FICHE	Almacenamiento de ficheros
E	**EQUIPAMIENTO**

[19] DANIELS, K. Ciberseguridad sin miedo: Activo informático: lo que todo buen Gerente quiere cuidar.2020.

CODIGO	DETALLE
SW	***APLICACIONES***
SCPROV	Contratación de proveedores
APOT	Apoteosys
WIN	Windows
OFI	Ofimática
XEN	Xenserver
FREE	Freenas
CEN	Centos
AV	Antivirus
HW	***EQUIPOS***
PCS	Equipos de cómputo
SER	Servidores
IMP	Impresoras
PSP	Equipos de cómputo portátiles
TELIP	Teléfonos IP
DDB	Discos duros externos
COM	***COMUNICACIONES***
AP	Access Point
SWITCH	Switches
ROU	Routers
B	**ACTIVOS ESENCIALES**
INFONEG	Información del negocio
L	**INSTALACIONES**
CAEST	Cableado estructurado
INSELEC	Instalaciones eléctricas
EDI	Edificio
P	**PERSONAL**
INGSIS	Ingeniero de sistemas
GER	Gerente
ABO	Abogado
TES	Tesorero
CON	Contador
PROD	Productor
DIRFINAN	Director financiero
COORDGESHUMAN	Coordinador de gestión humana
COORDCOMPRAS	Coordinador de compras
COORDPROD	Coordinador de producción

CODIGO	DETALLE
AUXPROD	Auxiliar de producción
GESEVEN	Gestor de eventos
AUXADMIN	Auxiliar administrativo
SERASEO	Servicio de aseo
DISE	Diseñador
SECGER	Secretaria de Gerencia
EQAUX	**EQUIPAMIENTO AUXILIAR**
PLAELEC	Planta eléctrica
UPS	UPS

Fuente: El autor

6.1.3.2 VALORACIÓN DE LOS ACTIVOS

Para valorar los activos se tomarán las siguientes dimensiones de seguridad de la metodología Magerit:

- [D] Disponibilidad.
- [I] Integridad de los datos.
  - [C] Confidencialidad de la información.
- [A] Autenticidad.
- [T] Trazabilidad.

Tabla 4 Dimensiones de valoración de Activos de la PYME

Valor	**Criterio**	
10	Muy Alto	Daño muy grave a la Organización
7-9	Alto	Daño grave a la Organización
4-6	Medio	Daño importante a la Organización
1-3	Bajo	Daño menor a la Organización
0	Despreciable	Irrelevante a efectos prácticos

Fuente: El autor

Se realiza la correspondiente valoración de los Activos de la PYME.

Tabla 5 Valoración de activos

CODIGO	DETALLE	D	I	C	A	T
IS	**SERVICIOS INTERNOS**					
INT	Internet	9	9	9	9	9
COELE	Correo electrónico	9	9	9	9	9
FICHE	Almacenamiento de ficheros	10	10	10	10	10
E	**EQUIPAMIENTO**					
SW	***APLICACIONES***					
SCPROV	Contratación de proveedores	8	8	7	8	7
APOT	Apoteosys	8	9	9	9	10
WIN	Windows	6	7	9	8	9
OFI	Ofimática	6	7	8	7	9
XEN	Xenserver	10	10	10	10	9
FREE	Freenas	10	10	9	8	9
CEN	Centos	10	9	10	10	10
AV	Antivirus	9	8	9	9	9
HW	***EQUIPOS***					
PCS	Equipos de cómputo	7	9	9	8	8
SER	Servidores	10	10	10	10	10
IMP	Impresoras	7	5	4	4	4
PSP	Equipos de cómputo portátiles	5	6	8	7	7
TELIP	Telefónos IP	5	4	3	4	4
DDB	Discos duros externos	10	9	10	9	9
COM	***COMUNICACIONES***					
AP	Access Point	5	4	4	7	6
SWITCH	Switches	9	9	9	8	8
ROU	Routers	8	8	8	8	8
B	**ACTIVOS ESENCIALES**					
INFONEG	Información del negocio	9	10	10	10	10
L	**INSTALACIONES**					
CAEST	Cableado estructurado	9	9	9	8	8
INSELEC	Instalaciones eléctricas	9	9	4	9	9
EDI	Edificio	8	8	8	8	7
P	**PERSONAL**					
INGSIS	Ingeniero de sistemas	5	7	9	9	1
GER	Gerente	9	7	9	9	9
ABO	Abogado	5	9	9	9	1

CODIGO	DETALLE	D	I	C	A	T
TES	Tesorero	9	9	7	9	1
CON	Contador	7	9	9	9	1
PROD	Productor	9	3	7	9	0
DIRFINAN	Director financiero	7	1	1	1	1
COORDGESHUMAN	Coordinador de gestión humana	1	1	1	1	1
COORDCOMPRAS	Coordinador de compras	1	1	1	1	1
COORDPROD	Coordinador de producción	1	1	1	1	1
AUXPROD	Auxiliar de producción	1	1	1	1	1
GESEVEN	Gestor de eventos	1	1	1	1	1
AUXADMIN	Auxiliar administrativo	1	1	1	1	1
SERASEO	Servicio de aseo	1	1	1	1	1
DISE	Diseñador	1	1	1	1	1
SECGER	Secretaria de Gerencia	1	1	1	1	1
EQAUX	**EQUIPAMIENTO AUXILIAR**					
PLAELEC	Planta eléctrica	10	NA	NA	9	7
UPS	UPS	10	NA	NA	NA	7

Fuente: El autor

6.1.3.3 IDENTIFICACIÓN DE VULNERABILIDADES

Las vulnerabilidades se definen como debilidades en los Activos que pueden ser aprovechadas por las amenazas para afectarlos. A continuación, se define una escala de probabilidad que ayuda a determinar el nivel de cada vulnerabilidad encontrada.

Tabla 6 Escala de probabilidad de vulnerabilidades

Probabilidad	Descripción	Valor	
Muy frecuente	A diario	75-100%	**Crítico**
Frecuente	Una vez al mes	50-75%	**Alto**
Frecuencia Normal	Una vez al año	25-50%	**Medio**
Poco frecuente	Cada varios años	0-25%	**Bajo**

El autor

A continuación, se muestra las vulnerabilidades de los Activos informáticos de la PYME, obtenidas mediante un análisis realizado en conjunto con el área de Sistemas de la Organización y como complemento a la auditoría realizada en el mes de enero de 2020 al proceso de Sistemas y Telecomunicaciones por parte del grupo Millán y asociados.

Tabla 7 Identificación de vulnerabilidades

Vulnerabilidad	Valor	Impacto
Falta de documentación sobre la plataforma informática de la empresa	Crítico	La falta de documentación actualizada sobre los activos que posee la empresa, tales como el Hardware, Software y los diferentes recursos y servicios con los que se cuenta imposibilita la adecuada gestión de la plataforma informática, haciendo que procesos que se ejecutan por parte del personal de TI sean lentos, poco asertivos, poco oportunos y sin una adecuada definición de oportunidades de mejora
Falta de capacitación de los empleados en su cargo	Crítico	El recurso humano debe permanecer capacitado y actualizado en las labores que son de su correspondencia, esto evita que se presente bajo rendimiento, poca productividad y demoras en los procesos para corregir problemáticas propias del flujo de información de cada dependencia.
No existen acuerdos de confidencialidad	Crítico	No existe una concientización adecuada para lograr que los colaboradores actúen bajo premisas éticas y actitudes apropiadas.
Ausencia de logs de ataques de intrusos y errores humanos en el procesamiento de la información	Crítico	No existe un registro de ataques ni de intrusiones, motivo por el cual no se puede determinar que problemas se presentan.
Ausencia de un plan claro para hacer frente a incidentes de seguridad que comprometan información	Crítico	Al no existir soportes de la información que permitan definir un plan de respaldo para hacer frente a incidentes se afectan todos los servicios, ya que hay pérdida de tiempo al intentar corregir el incidente.
Ausencia de políticas de seguridad informática	Crítico	No existen políticas que permitan proteger la información de la empresa, motivo por el cual está expuesta a malos manejos, incidentes de seguridad, fraudes e ilícitos.
No existen procesos disciplinarios para quienes ocasionen incidentes de seguridad informática	Alto	Existe la posibilidad de que personas inescrupulosas accedan y corrompan los sistemas de información de la empresa, ocasionando graves daños a la plataforma, el problema radica en que no existen sanciones si se detectan este tipo de comportamientos.
No existe un software para auditorias de control	Alto	Es importante ejecutar labores de auditoría en el manejo de procesos de información de todas las áreas para garantizar que se haga buen uso de estos

Vulnerabilidad	Valor	Impacto
Ausencia de control de accesos serios y eficientes	Alto	No se tiene un control claro para el control de accesos de los empleados a recursos Hardware y Software, motivo por el cual las personas pueden acceder a todo tipo de información compartida en la red interna, sin restricción alguna y sin la debida gestión por parte de los responsables de los recursos TI
Ausencia de personal especialista en cada área	Alto	Las diferentes dependencias de la empresa deben contar con la capacidad y conocimientos adecuados para la función que desempeña en la misma, además, contar con formación en manejo de ofimática.
Ausencia de procedimientos serios para creación y eliminación de usuarios nuevos o retirados de la empresa	Crítico	Esto trae consigo que personal que ha laborado en la empresa anteriormente pueda seguir teniendo acceso a información crítica o a los diferentes recursos y servicios de la plataforma informática
No existen controles sobre el tiempo de sesión en aplicativos de alta criticidad	Crítico	Al no realizarse gestión sobre sesiones en este tipo de aplicaciones se incrementa la posibilidad que personas ajenas a las dependencias o a la empresa puedan usar estas sesiones para acceder a información confidencial o realizar procesos que perjudiquen la Organización
Falta de controles físicos a áreas importantes en la empresa	Crítico	La falta de controles en el acceso físico a las dependencias pone en riesgo la confidencialidad de la información que se maneje en ellas ya que personas ajenas pueden acceder a los equipos informáticos.
Algunas aplicaciones no poseen contraseñas seguras	Crítico	No hay procedimientos que obliguen a los empleados a utilizar contraseñas adecuadas para evitar problemas de seguridad.
Los equipos de la red no tienen restricción al uso de unidades de DVD, USB	Crítico	La falta de restricción en el uso de unidades CD, DVD, USB puede involucrar infecciones de malware por la falta de precaución en el manejo por parte de empleados y colaboradores
Existe exposición de información sin cifrado expuesta a terceros no autorizados	Crítico	No existen mecanismos de cifrado para información confidencial que pueda ser servida para fraudes o ilícitos
Falta de políticas de buenas prácticas	Alto	La falta de cultura informática en la empresa puede aumentar la probabilidad de que haya incidentes de seguridad informática
No existen planes de respaldo periódicos de la información	Alto	Falta definir un esquema de Backups eficiente, oportuno y que permita restaurar servicios y recursos informáticos en caso de incidentes en la plataforma informática

Vulnerabilidad	Valor	Impacto
No existe control en el acceso a páginas web	Crítico	No existen lineamientos claros en el uso del Internet dentro de la empresa, motivo por el cual hay una alta probabilidad de infecciones de malware que puede afectar la plataforma informática de la Organización.
Alta rotación de personal de TI	Crítico	Existe un alto nivel de rotación del personal de TI, lo que ocasiona que haya retrasos en la gestión de la plataforma de TI debido a que cada vez que ingresa nuevo personal hay necesidad de capacitación, inducción y adecuación a los cargos.

Fuente: El autor.

6.1.3.4 AMENAZAS

Las amenazas son situaciones que se pueden presentar que traen consigo problemas de seguridad, están clasificadas en cuatro grupos:

- Desastres naturales
- Desastres industriales
- Errores y fallos no intencionados
- Ataques intencionados

La siguiente tabla muestra una descripción de amenazas que pueden llegar a afectar los activos de la PYME.

Tabla 8 Descripción de amenazas

GRUPO	AMENAZA	Dimensión Afectada					Activos Afectados						
		A	C	I	D	T	I	H	A	D	R	S	P
Desastres Naturales	Fuego				X		X	X					
	Daños por agua				X		X	X					
	Contaminación				X		X	X		x			
	Siniestro mayor				X		X	X		x			
	fenómeno climático				X		X	X		x			
	Fenómeno de origen volcánico				X		X	X		x			

GRUPO	AMENAZA	Dimensión Afectada					Activos Afectados						
		A	C	I	D	T	I	H	A	D	R	S	P
	Fenómeno meteorológico				X		X	X		x			
	Inundación				X		X	X		x			
	Otros desastres Naturales				X		X	X					
Desastres de Origen Industrial	Fuego				X		X	X					
	Daños por agua				X		X	X					
	Contaminación Mecánica				X			X					
	Contaminación electromagnética				X			X					
	Avería de origen físico o lógico				X			X	X				
	Corte del suministro eléctrico				X			X					
	Condiciones inadecuadas de temperatura o humedad				X			X					
	Fallo de servicios de comunicaciones				X						X		
	Interrupción de otros servicios y suministros esenciales				X					X			
	Degradación de los soportes de almacenamiento de la información				X					X			
	Emanaciones electromagnéticas Errores y fallos no intencionados		x				X	X					
	Errores de los usuarios		X	X	X				X	X		x	
	Errores del administrador		X	X	X			X	X	X	X	X	
	Errores de monitorización (log)			X		X				X			
	Errores de configuración			X						X			
	Deficiencias en la organización				X								X
	Difusión de software dañino		X	X	X				X				
	Errores de [re-]encaminamiento		X						X		X	X	

GRUPO	AMENAZA	Dimensión Afectada					Activos Afectados						
		A	C	I	D	T	I	H	A	D	R	S	P
Errores y fallos no intencionados	Errores de secuencia			X					X		X	X	
	Escapes de información		X							X			
	Alteración accidental de la información			X			x		X	X	X	X	
	Destrucción de información				X		x		X	X	X	X	
	Fugas de información		X				x		X	X	x	X	X
	Vulnerabilidades de los programas (software)		X	X	X				X				
	Errores de mantenimiento / actualización de programas (software)			X	X				X				
	Errores de mantenimiento / actualización de equipos (hardware)				X			X					
	Caída del sistema por agotamiento de recursos				X			X	X		X		
	Pérdida de equipos		X		X			X					
	Indisponibilidad del personal				X								X
ataques intencionados	Manipulación de los registros de actividad (log)			X		X				X			
	Manipulación de la configuración	X	X	X						X			
	Suplantación de la identidad del usuario	x	X	X	X			X	X	X	X	X	
	Abuso de privilegios de acceso		X	X	X			X	X	X	X	X	
	Uso no previsto		X	X	X			X	X	X	X	X	
	Difusión de software dañino		X	X	X				X				
	[Re-]encaminamiento de mensajes		X						X		X	X	
	Alteración de secuencia			X					X		X	X	

GRUPO	AMENAZA	Dimensión Afectada					Activos Afectados						
		A	C	I	D	T	I	H	A	D	R	S	P
	Acceso no autorizado		X	X			X	X	X	X	X	X	
	Análisis de tráfico		X								X		
	Repudio			X		X				X		X	
	Interceptación de información (escucha)		X								X		
	Modificación deliberada de la información			X				X	X	X	X	X	
	Destrucción de información				X				X	X	X	X	
	Divulgación de información		X						X	X	X	X	
	Manipulación de programas		X	X	X				X				
	Manipulación de los equipos		X		X			X					
	Denegación de servicio				X			X	X	X	X	X	
	Robo		X		X			X		X			
	Ataque destructivo				X		X	X					
	Ocupación enemiga		X		X		X						
	Indisponibilidad del personal				X								X
	Extorsión		X	X	X								X
	Ingeniería social		X	X	X								X

Fuente: El autor

6.1.3.4.1 IDENTIFICACIÓN DE AMENAZAS

Se identifican las siguientes amenazas para la PYME.

Tabla 9 Listado de amenazas

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
IS	**SERVICIOS INTERNOS**

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
INT	**Internet**
[E.2]	Errores del Administrador del sistema / de la seguridad
[E.9]	Errores de [re-] encaminamiento
[E.10]	Errores de secuencia
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.5]	Suplantación de la identidad
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.9]	[Re-] encaminamiento de mensajes
[A.11]	Acceso no autorizado
[A.12]	Análisis de tráfico
[A.14]	Interceptación de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
COELE	**Correo electrónico**
[E.2]	Errores del Administrador del sistema / de la seguridad
[E.19]	Fugas de información
[A.5]	Suplantación de la identidad
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.15]	Modificación de la información
[A.19]	Revelación de la información
SW	***APLICACIONES***
SCPROV	**Contratación de proveedores**
[E.1]	Errores de los usuarios
[E.2]	Errores del Administrador del sistema / de la seguridad
[E.8]	Difusión de software dañino
[E.15]	Alteración de la información
[E.19]	Fugas de información
[E.20]	Vulnerabilidades de los programas (software)
[A.5]	Suplantación de la identidad
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.8]	Difusión de software dañino

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
[A.11]	Acceso no autorizado
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.22]	Manipulación de programas
APOT	**Apoteosys**
[E.1]	Errores de los usuarios
[E.2]	Errores del Administrador del sistema / de la seguridad
[E.8]	Difusión de software dañino
[E.15]	Alteración de la información
[E.19]	Fugas de información
[E.20]	Vulnerabilidades de los programas (software)
[A.5]	Suplantación de la identidad
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.8]	Difusión de software dañino
[A.11]	Acceso no autorizado
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.22]	Manipulación de programas
WIN	**Windows**
[E.1]	Errores de los usuarios
[E.2]	Errores del Administrador del sistema / de la seguridad
[E.8]	Difusión de software dañino
[E.15]	Alteración de la información
[E.19]	Fugas de información
[E.20]	Vulnerabilidades de los programas (software)
[A.5]	Suplantación de la identidad
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.8]	Difusión de software dañino
[A.11]	Acceso no autorizado
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.22]	Manipulación de programas
XEN	**Xenserver**
[E.1]	Errores de los usuarios

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
[E.2]	Errores del Administrador del sistema / de la seguridad
[E.8]	Difusión de software dañino
[E.15]	Alteración de la información
[E.19]	Fugas de información
[E.20]	Vulnerabilidades de los programas (software)
[A.5]	Suplantación de la identidad
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.8]	Difusión de software dañino
[A.11]	Acceso no autorizado
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.22]	Manipulación de programas
CEN	**Centos**
[E.1]	Errores de los usuarios
[E.2]	Errores del Administrador del sistema / de la seguridad
[E.8]	Difusión de software dañino
[E.15]	Alteración de la información
[E.19]	Fugas de información
[E.20]	Vulnerabilidades de los programas (software)
[A.5]	Suplantación de la identidad
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.8]	Difusión de software dañino
[A.11]	Acceso no autorizado
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.22]	Manipulación de programas
HW	***EQUIPOS***
PCS	**Equipos de cómputo**
[E.11]	Emanaciones electromagnéticas
[E.2]	Errores del administrador del sistema / de la seguridad
[E.25]	Pérdida de equipos
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos
SER	**Servidores**
[I.11]	Emanaciones electromagnéticas
[E.2]	Errores del administrador del sistema / de la seguridad
[E.25]	Pérdida de equipos
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos
IMP	**Impresoras**
[E.11]	Emanaciones electromagnéticas
[E.2]	Errores del administrador del sistema / de la seguridad
[E.25]	Pérdida de equipos
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos
PSP	**Equipos de cómputo portátiles**
[E.11]	Emanaciones electromagnéticas
[E.2]	Errores del administrador del sistema / de la seguridad
[E.25]	Pérdida de equipos
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos
TELIP	**Teléfonos IP**
[E.11]	Emanaciones electromagnéticas
[E.2]	Errores del administrador del sistema / de la seguridad
[E.25]	Pérdida de equipos
[A.7]	Uso no previsto
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
DDB	**Discos duros externos**
[I.11]	Emanaciones electromagnéticas
[E.1]	Errores de los usuarios
[E.2]	Errores del administrador del sistema / de la seguridad
[E.15]	Alteración de la información
[E.19]	Fugas de información
[E.25]	Pérdida de equipos
[A.5]	Suplantación de la identidad
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos
COM	***COMUNICACIONES***
AP	**Access Point**
[E.11]	Emanaciones electromagnéticas
[E.2]	Errores del administrador del sistema / de la seguridad
[E.25]	Pérdida de equipos
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos
SWITCH	**Switches**
[E.11]	Emanaciones electromagnéticas
[E.2]	Errores del administrador del sistema / de la seguridad
[E.25]	Pérdida de equipos
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos
ROU	**Routers**
[E.11]	Emanaciones electromagnéticas

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
[E.2]	Errores del administrador del sistema / de la seguridad
[E.25]	Pérdida de equipos
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos
B	**ACTIVOS ESENCIALES**
INFONEG	**Información del negocio**
[E.1]	Errores de los usuarios
[E.2]	Errores del administrador del sistema / de la seguridad
[E.15]	Alteración de la información
[E.18]	Destrucción de la información
[E.19]	Fugas de información
[A.11]	Acceso no autorizado
[A.15]	Modificación de la información
[A.18]	Destrucción de la información
[A.19]	Revelación de la información
L	**INSTALACIONES**
CAEST	**Cableado estructurado**
[I.8]	Fallo de servicios de comunicaciones
[E.2]	Errores del administrador del sistema / de la seguridad
[E.9]	Errores de [re-] encaminamiento
[E.10]	Errores de secuencia
[E.15]	Alteración de la información
[E.19]	Fugas de información
[E.24]	Caída del sistema por agotamiento de recursos
[A.5]	Suplantación de la identidad
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.9]	[Re-] encaminamiento de mensajes
[A.10]	Alteración de secuencia
[A.11]	Acceso no autorizado
[A.12]	Análisis de tráfico
[A.14]	Interceptación de información (escucha)
[A.15]	Modificación de la información

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
[A.18]	Destrucción de la información
[A.19]	Revelación de la información
[A.24]	Denegación del servicio
INSELEC	**Instalaciones eléctricas**
[N.1]	Fuego
[N.2]	Daños por agua
[N.*]	Desastres naturales
[I.1]	Fuego
[I.2]	Daños por agua
[I.*]	Desastres naturales
[I.3]	Contaminación medioambiental
[I.4]	Contaminación electromagnética
[I.6]	Corte del suministro eléctrico
[I.7]	Condiciones inadecuadas de temperatura o humedad
[E.25]	Pérdida de equipos
[A.57]	Acceso no autorizado (a través del perímetro físico)
[A.58]	Destrucción del perímetro físico
EDI	**Edificio**
[I.11]	Emanaciones electromagnéticas
[A.5]	Suplantación de la identidad
[A.6]	Abuso de privilegios de acceso
[A.7]	Uso no previsto
[A.11]	Acceso no autorizado
[A.27]	Ocupación enemiga
P	**PERSONAL**
INGSIS	**Ingeniero de sistemas**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
GER	**Gerente**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
ABO	**Abogado**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
TES	**Tesorero**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
CON	**Contador**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
PROD	**Productor**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
DIRFINAN	**Director financiero**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
COORDGESHUMAN	**Coordinador de gestión humana**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
COORDCOMPRAS	**Coordinador de compras**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
COORDPROD	**Coordinador de producción**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
AUXPROD	**Auxiliar de producción**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
GESEVEN	**Gestor de eventos**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
[A.30]	Ingeniería social (picaresca)
AUXADMIN	**Auxiliar administrativo**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
SERASEO	**Servicio de aseo**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
DISE	**Diseñador**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
SECGER	**Secretaria de Gerencia**
[E.15]	Alteración de la información
[E.19]	Fugas de información
[A.15]	Modificación de la información
[A.19]	Revelación de la información
[A.29]	Extorsión
[A.30]	Ingeniería social (picaresca)
EQAUX	**EQUIPAMIENTO AUXILIAR**
PLAELEC	**Planta eléctrica**
[N.1]	Fuego
[N.2]	Daños por agua
[N.*]	Desastres naturales
[I.1]	Fuego
[I.2]	Daños por agua

AMENAZAS POR ACTIVO	
CODIGO	**NOMBRE DE AMENAZA**
[I.*]	Desastres industriales
[I.3]	Contaminación medioambiental
[E.23]	Errores de mantenimiento / actualización de equipos de hardware
[A.7]	Uso no previsto
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos
[A.26]	Ataque destructivo
UPS	**UPS**
[N.1]	Fuego
[N.2]	Daños por agua
[N.*]	Desastres naturales
[I.1]	Fuego
[I.2]	Daños por agua
[I.*]	Desastres industriales
[I.3]	Contaminación medioambiental
[E.23]	Errores de mantenimiento / actualización de equipos de hardware
[A.7]	Uso no previsto
[A.23]	Manipulación del hardware
[A.25]	Robo de equipos
[A.26]	Ataque destructivo

Fuente: El autor

6.1.3.4.2 VALORACIÓN DE AMENAZAS

Mediante esta tarea, se pretende definir la probabilidad de ocurrencia de cada amenaza, para poder determinar los efectos de la materialización de éstas.

Tabla 10 Probabilidad de ocurrencia

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	MUY BAJO
MR	MUY RARA

0	---

Fuente: El autor

Tabla 11 Degradación de las amenazas

VALOR	CRITERIO
90%-100%	Degradación muy considerable del activo
25%-89%	Degradación medianamente considerable del activo
1%-24%	Degradación poco considerable del activo

Fuente: El autor

En la siguiente tabla se procede a realizar la valoración de las amenazas encontradas para cada activo informático de la PYME, especificando la probabilidad de ocurrencia y asignando un porcentaje de degradación en cuanto a disponibilidad, integridad, confidencialidad y trazabilidad.

Tabla 12 Valoración de amenazas

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
IS	**SERVICIOS INTERNOS**						
INT	**Internet**						
[E.2]	Errores del Administrador del sistema / de la seguridad	P		25%	25%		
[E.9]	Errores de [re-] encaminamiento	P			10%		
[E.10]	Errore de secuencia	P		10%			
[E.15]	Alteración de la información	P		1%			
[E.19]	Fugas de información	P			10%		
[A.5]	Suplantación de la identidad	P		10%	50%	100%	
[A.6]	Abuso de privilegios de acceso	P		10%	50%	100%	
[A.7]	Uso no previsto	P		10%	10%		
[A.9]	[Re-] encaminamiento de mensajes	P			10%		
[A.11]	Acceso no autorizado	P		10%	50%	100%	
[A.12]	Análisis de tráfico	P			2%		
[A.14]	Interceptación de información	P			5%		

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[A.15]	Modificación de la información	P		10%			
[A.19]	Revelación de la información	P			50%		
COELE	**Correo electrónico**						
[E.2]	Errores del Administrador del sistema / de la seguridad	P		10%	10%		
[E.19]	Fugas de información	P			10%		
[A.5]	Suplantación de la identidad	P		10%	50%	10%	
[A.6]	Abuso de privilegios de acceso	P		10%	50%	100%	
[A.7]	Uso no previsto	P		10%	50%	100%	
[A.11]	Acceso no autorizado	P		10%	50%	100%	
[A.15]	Modificación de la información	P		10%			
[A.19]	Revelación de la información	P			50%		
SW	***APLICACIONES***						
SCPROV	**Contratación de proveedores**						
[E.1]	Errores de los usuarios	P		10%	10%		
[E.2]	Errores del Administrador del sistema / de la seguridad	P		20%	20%		
[E.8]	Difusión de software dañino	P		10%	10%		
[E.15]	Alteración de la información	P		1%			
[E.19]	Fugas de información	P			10%		
[E.20]	Vulnerabilidades de los programas (software)	P		20%	20%		
[A.5]	Suplantación de la identidad	P		50%	50%	100%	
[A.6]	Abuso de privilegios de acceso	P		10%	10%		
[A.7]	Uso no previsto	P		10%	10%		
[A.8]	Difusión de software dañino	P		100%	100%		
[A.11]	Acceso no autorizado	P		10%	50%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	P			50%		
[A.22]	Manipulación de programas	P		100%	100%		
APOT	**Apoteosys**						
[E.1]	Errores de los usuarios	P		10%	10%		

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[E.2]	Errores del Administrador del sistema / de la seguridad	P		20%	20%		
[E.8]	Difusión de software dañino	P		10%	10%		
[E.15]	Alteración de la información	P		1%			
[E.19]	Fugas de información	P			10%		
[E.20]	Vulnerabilidades de los programas (software)	P		20%	20%		
[A.5]	Suplantación de la identidad	P		50%	50%	100%	
[A.6]	Abuso de privilegios de acceso	P		10%	10%		
[A.7]	Uso no previsto	P		10%	10%		
[A.8]	Difusión de software dañino	P		100%	100%		
[A.11]	Acceso no autorizado	P		10%	50%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	P			50%		
[A.22]	Manipulación de programas	P		100%	100%		
WIN	**Windows**						
[E.1]	Errores de los usuarios	P		10%	10%		
[E.2]	Errores del Administrador del sistema / de la seguridad	P		20%	20%		
[E.8]	Difusión de software dañino	P		10%	10%		
[E.15]	Alteración de la información	P		1%			
[E.19]	Fugas de información	P			10%		
[E.20]	Vulnerabilidades de los programas (software)	P		20%	20%		
[A.5]	Suplantación de la identidad	P		50%	50%	100%	
[A.6]	Abuso de privilegios de acceso	P		10%	10%		
[A.7]	Uso no previsto	P		10%	10%		
[A.8]	Difusión de software dañino	P		100%	100%		
[A.11]	Acceso no autorizado	P		10%	50%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	P			50%		
[A.22]	Manipulación de programas	P		100%	100%		
XEN	**Xenserver**						
[E.1]	Errores de los usuarios	P		10%	10%		

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[E.2]	Errores del Administrador del sistema / de la seguridad	P		20%	20%		
[E.8]	Difusión de software dañino	P		10%	10%		
[E.15]	Alteración de la información	P		1%			
[E.19]	Fugas de información	P			10%		
[E.20]	Vulnerabilidades de los programas (software)	P		20%	20%		
[A.5]	Suplantación de la identidad	P		50%	50%	100%	
[A.6]	Abuso de privilegios de acceso	P		10%	10%		
[A.7]	Uso no previsto	P		10%	10%		
[A.8]	Difusión de software dañino	P		100%	100%		
[A.11]	Acceso no autorizado	P		10%	50%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	P			50%		
[A.22]	Manipulación de programas	P		100%	100%		
CEN	**Centos**						
[E.1]	Errores de los usuarios	P		10%	10%		
[E.2]	Errores del Administrador del sistema / de la seguridad	P		20%	20%		
[E.8]	Difusión de software dañino	P		10%	10%		
[E.15]	Alteración de la información	P		1%			
[E.19]	Fugas de información	P			10%		
[E.20]	Vulnerabilidades de los programas (software)	P		20%	20%		
[A.5]	Suplantación de la identidad	P		50%	50%	100%	
[A.6]	Abuso de privilegios de acceso	P		10%	10%		
[A.7]	Uso no previsto	P		10%	10%		
[A.8]	Difusión de software dañino	P		100%	100%		
[A.11]	Acceso no autorizado	P		10%	50%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	P			50%		
[A.22]	Manipulación de programas	P		100%	100%		
HW	***EQUIPOS***						
PCS	**Equipos de cómputo**						

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[E.11]	Emanaciones electromagnéticas	P			1%		
[E.2]	Errores del administrador del sistema / de la seguridad	P		20%	20%		
[E.25]	Pérdida de equipos	MA			10%		
[A.6]	Abuso de privilegios de acceso	P		10%	50%		
[A.7]	Uso no previsto	P		1	10%		
[A.11]	Acceso no autorizado	P		10%	50%		
[A.23]	Manipulación del hardware	P			50%		
[A.25]	Robo de equipos	MA			10%		
SER	**Servidores**						
[I.11]	Emanaciones electromagnéticas	P	1%				
[E.2]	Errores del administrador del sistema / de la seguridad	P	20%	20%			
[E.25]	Pérdida de equipos	P			100%		
[A.6]	Abuso de privilegios de acceso	P		100%	100%		
[A.7]	Uso no previsto	P		10%	100%		
[A.11]	Acceso no autorizado	P		100%	100%		
[A.23]	Manipulación del hardware	P			50%		
[A.25]	Robo de equipos	PP			100%		
IMP	**Impresoras**						
[E.11]	Emanaciones electromagnéticas	P			1%		
[E.2]	Errores del administrador del sistema / de la seguridad	P		20%	20%		
[E.25]	Pérdida de equipos	P			10%		
[A.6]	Abuso de privilegios de acceso	P		10%	50%		
[A.7]	Uso no previsto	P		1%	10%		
[A.11]	Acceso no autorizado	P		10%	50%		
[A.23]	Manipulación del hardware	P			50%		
[A.25]	Robo de equipos	P			50%		
PSP	**Equipos de cómputo portátiles**						
[E.11]	Emanaciones electromagnéticas	P	1%				
[E.2]	Errores del administrador del sistema / de la seguridad	P	20%	20%			
[E.25]	Pérdida de equipos	P			100%		

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[A.6]	Abuso de privilegios de acceso	P		100%	100%		
[A.7]	Uso no previsto	P		10%	100%		
[A.11]	Acceso no autorizado	P		100%	100%		
[A.23]	Manipulación del hardware	P			50%		
[A.25]	Robo de equipos	PP			100%		
TELIP	**Teléfonos IP**						
[E.11]	Emanaciones electromagnéticas	P	1%				
[E.2]	Errores del administrador del sistema / de la seguridad	P	20%	20%			
[E.25]	Pérdida de equipos	P			100%		
[A.7]	Uso no previsto	P		10%	100%		
[A.23]	Manipulación del hardware	P			50%		
[A.25]	Robo de equipos	PP			100%		
DDB	**Discos duros externos**						
[I.11]	Emanaciones electromagnéticas	O			1%		
[E.1]	Errores de los usuarios	MA		10%	10%		
[E.2]	Errores del administrador del sistema / de la seguridad	P		20%	20%		
[E.15]	Alteración de la información	P		1%			
[E.19]	Fugas de información	P			10%		
[E.25]	Pérdida de equipos	P			100%		
[A.5]	Suplantación de la identidad	MA		10%	50%		
[A.6]	Abuso de privilegios de acceso	P		100%	100%		
[A.7]	Uso no previsto	P		10%	100%		
[A.11]	Acceso no autorizado	P		100%	100%		
[A.15]	Modificación de la información	MA		100%			
[A.19]	Revelación de la información	MA			100%		
[A.23]	Manipulación del hardware	P			50%		
[A.25]	Robo de equipos	P			100%		
COM	***COMUNICACIONES***						
AP	**Access Point**						
[E.11]	Emanaciones electromagnéticas	P			1%		

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[E.2]	Errores del administrador del sistema / de la seguridad	P		20%	20%		
[E.25]	Pérdida de equipos	P			10%		
[A.6]	Abuso de privilegios de acceso	P		10%	50%		
[A.7]	Uso no previsto	P		1%	10%		
[A.11]	Acceso no autorizado	P		10%	50%		
[A.23]	Manipulación del hardware	P			50%		
[A.25]	Robo de equipos	P			50%		
SWITCH	**Switches**						
[E.11]	Emanaciones electromagnéticas	P			1%		
[E.2]	Errores del administrador del sistema / de la seguridad	P		20%	20%		
[E.25]	Pérdida de equipos	P			10%		
[A.6]	Abuso de privilegios de acceso	P		10%	50%		
[A.7]	Uso no previsto	P		1%	10%		
[A.11]	Acceso no autorizado	P		10%	50%		
[A.23]	Manipulación del hardware	P			50%		
[A.25]	Robo de equipos	P			50%		
ROU	**Routers**						
[E.11]	Emanaciones electromagnéticas	P			1%		
[E.2]	Errores del administrador del sistema / de la seguridad	P		20%	20%		
[E.25]	Pérdida de equipos	P			10%		
[A.6]	Abuso de privilegios de acceso	P		10%	50%		
[A.7]	Uso no previsto	P		1%	10%		
[A.11]	Acceso no autorizado	P		10%	50%		
[A.23]	Manipulación del hardware	P			50%		
[A.25]	Robo de equipos	P			50%		
B	**ACTIVOS ESENCIALES**						
INFONEG	**Información del negocio**						
[E.1]	Errores de los usuarios	P	10%	10%	10%		
[E.2]	Errores del administrador del sistema / de la seguridad	P	20%	20%	20%		
[E.15]	Alteración de la información	P		1%			

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[E.18]	Destrucción de la información	P	10%				
[E.19]	Fugas de información	P			10%		
[A.11]	Acceso no autorizado	P		10%	50%	100%	
[A.15]	Modificación de la información	MA		50%			
[A.18]	Destrucción de la información	P	50%				
[A.19]	Revelación de la información	P				50%	
L	**INSTALACIONES**						
CAEST	**Cableado estructurado**						
[I.8]	Fallo de servicios de comunicaciones	P	50%				
[E.2]	Errores del administrador del sistema / de la seguridad	P	20%	20%	20%		
[E.9]	Errores de [re-] encaminamiento	P			10%		
[E.10]	Errores de secuencia	P		10%			
[E.15]	Alteración de la información	P		1%			
[E.19]	Fugas de información	P			10%		
[E.24]	Caída del sistema por agotamiento de recursos	P	50%				
[A.5]	Suplantación de la identidad	P		10%	50%	100%	
[A.6]	Abuso de privilegios de acceso	P		10%	50%	100%	
[A.7]	Uso no previsto	P	10%	10%	10%		
[A.9]	[Re-] encaminamiento de mensajes	P			10%		
[A.10]	Alteración de secuencia	P		10%			
[A.11]	Acceso no autorizado	P		10%	50%	100%	
[A.12]	Análisis de tráfico	P			2%		
[A.14]	Interceptación de información (escucha)	P			1%		
[A.15]	Modificación de la información	P		10%			
[A.18]	Destrucción de la información	P	50%				
[A.19]	Revelación de la información	P			50%		
[A.24]	Denegación del servicio	MA	50%				
INSELEC	**Instalaciones eléctricas**						
[N.1]	Fuego	PP	1%				

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		Prob	D	I	C	A	T
CODIGO	NOMBRE DE AMENAZA						
[N.2]	Daños por agua	PP	1%				
[N.*]	Desastres naturales	PP	1%				
[I.1]	Fuego	PP	1%				
[I.2]	Daños por agua	PP	1%				
[I.*]	Desastres naturales	PP	1%				
[I.3]	Contaminación medioambiental	PP	1%				
[I.4]	Contaminación electromagnética	PP	1%				
[I.6]	Corte del suministro eléctrico	PP	1%				
[I.7]	Condiciones inadecuadas de temperatura o humedad	PP	1%				
[E.25]	Pérdida de equipos	PP	1%				
[A.57]	Acceso no autorizado (a través del perímetro físico)	PP	1%				
[A.58]	Destrucción del perímetro físico	PP	1%				
EDI	**Edificio**						
[I.11]	Emanaciones electromagnéticas	PP			1%		
[A.5]	Suplantación de la identidad	P		10%	50%		
[A.6]	Abuso de privilegios de acceso	P		10%	50%		
[A.7]	Uso no previsto	P		10%	50%		
[A.11]	Acceso no autorizado	MA		10%	50%		
[A.27]	Ocupación enemiga	P			50%		
P	**PERSONAL**						
INGSIS	**Ingeniero de sistemas**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
GER	**Gerente**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
ABO	**Abogado**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
TES	**Tesorero**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
CON	**Contador**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
PROD	**Productor**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
DIRFINAN	**Director financiero**						

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
COORDGESHUMAN	**Coordinador de gestión humana**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
COORDCOMPRAS	**Coordinador de compras**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
COORDPROD	**Coordinador de producción**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
AUXPROD	**Auxiliar de producción**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
GESEVEN	**Gestor de eventos**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
AUXADMIN	**Auxiliar administrativo**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
SERASEO	**Servicio de aseo**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
DISE	**Diseñador**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
SECGER	**Secretaria de Gerencia**						

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[E.15]	Alteración de la información	P		10%			
[E.19]	Fugas de información	P			10%		
[A.15]	Modificación de la información	P		50%			
[A.19]	Revelación de la información	MA			20%		
[A.29]	Extorsión	P		20%	20%		
[A.30]	Ingeniería social (picaresca)	P		20%	20%		
EQAUX	**EQUIPAMIENTO AUXILIAR**						
PLAELEC	**Planta eléctrica**						
[N.1]	Fuego	PP	1%				
[N.2]	Daños por agua	PP	1%				
[N.*]	Desastres naturales	PP	1%				
[I.1]	Fuego	PP	1%				
[I.2]	Daños por agua	PP	1%				
[I.*]	Desastres industriales	PP	1%				
[I.3]	Contaminación medioambiental	PP	1%				
[E.23]	Errores de mantenimiento / actualización de equipos de hardware	PP	1%				
[A.7]	Uso no previsto	PP	1%				
[A.23]	Manipulación del hardware	PP	1%				
[A.25]	Robo de equipos	PP	1%				
[A.26]	Ataque destructivo	PP	1%				
UPS	**UPS**						
[N.1]	Fuego	PP	1%				
[N.2]	Daños por agua	PP	1%				
[N.*]	Desastres naturales	PP	1%				
[I.1]	Fuego	PP	1%				
[I.2]	Daños por agua	PP	1%				
[I.*]	Desastres industriales	PP	1%				
[I.3]	Contaminación medioambiental	PP	1%				
[E.23]	Errores de mantenimiento / actualización de equipos de hardware	PP	1%				

		DEGRADACIÓN					
AMENAZAS POR ACTIVO		**Prob**	**D**	**I**	**C**	**A**	**T**
CODIGO	**NOMBRE DE AMENAZA**						
[A.7]	Uso no previsto	PP	1%				
[A.23]	Manipulación del hardware	PP	1%				
[A.25]	Robo de equipos	PP	1%				
[A.26]	Ataque destructivo	PP	1%				

Fuente: El autor

6.1.3.5 IDENTIFICACIÓN DE RIESGOS

Los activos de la PYME de gestión de eventos y espectáculos están expuestos a muchos riesgos, se hace necesario poder identificarlos para determinar las SALVAGUARDAS necesarias para mitigarlos.

La tabla a continuación relaciona los riesgos por cada activo y el tratamiento que se puede dar para su mitigación, definiendo los responsables por proceso y los recursos involucrados.

Tabla 13 Identificación de riesgos

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
1	[E.1] Errores de los usuarios	• SCPROV Contratación de proveedores • APOT Apoteosys • WIN Windows • XEN Xenserver • CEN Centos • DDB Discos duros externos • INFONEG Información del negocio	• Capacitaciones al personal • Concientización del personal mediante charlas educativas • Procesos de contratación enfocados en las competencias reales en el manejo de sistemas relacionados a los activos involucrados.	• Área de Sistemas • Gestión humana	• Sala de juntas • Recursos audiovisuales • Tiempo • Internet	• Actas de capacitación • Perfiles de aspirantes

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
2	[E.2] Errores del Administrador del sistema / de la seguridad	• INT Internet COELE • Correo electrónico • SCPROV • Contratación de proveedores • APOT Apoteosys • WIN Windows • XEN Xenserver • CEN Centos • PCS Equipos de cómputo • SER Servidores • IMP Impresoras • PSP Equipos de cómputo portátiles • TELIP Teléfonos IP • DDB Discos duros externos • AP Access Point • SWITCH Switches • ROU Routers • INFONEG Información del negocio CAEST Cableado estructurado	• Capacitación permanente al personal de Sistemas sobre herramientas Hardware y Software • Mayor atención a las competencias de los aspirantes en los procesos de selección del personal relacionado al área de Sistemas • Documentación de Procedimientos relacionados al manejo de la plataforma informática de la empresa	• Área de Sistemas • Gestión humana	• Tiempo • Internet	• Actas de capacitación • Perfiles de aspirantes

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
3	[E.8] Difusión de software dañino	• SCPROV Contratación de proveedores • APOT Apoteosys • WIN Windows • XEN Xenserver • CEN Centos	• Uso de herramientas antimalware • Contar con un plan de acción frente a infecciones de malware • Contar con backups diarios de la información • Contar con Backups de configuración de sistemas operativos	Área de Sistemas	• Antivirus licenciados • Discos duros externos • Plan de contingencia	• Esquema de Backups • Plan de contingencia

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
4	[E.15] Alteración de la información	• INT Internet • SCPROV Contratación de proveedores • APOT Apoteosys • WIN Windows • XEN Xenserver • CEN Centos • DDB Discos duros externos • INFONEG Información del negocio • CAEST Cableado estructurado • INGSIS Ingeniero de sistemas • GER Gerente • ABO Abogado • TES Tesorero • CON Contador • PROD Productor • DIRFINAN director financiero • COORDGESHUMAN Coordinador de gestión humana • COORDCOMPRAS Coordinador de compras • COORDPROD Coordinador de producción • AUXPROD Auxiliar de producción • GESEVEN Gestor de eventos	• Establecer permisos de acceso adecuado a las necesidades de cada empleado. • Manejar usuarios con contraseñas adecuadas • Cifrar la información que se maneja en discos duros externos • Respaldar periódicamente la información de la empresa. • Firewall actualizado	Área de Sistemas	• Herramientas de cifrado • Discos duros externos • Esquema de Backups • Firewall	• Esquema de Backups • Plan de contingencia

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
		• AUXADMIN Auxiliar administrativo • SERASEO Servicio de aseo • DISE Diseñador • SECGER Secretaria de Gerencia				

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
5	[E.19] Fugas de información	• INT Internet • COELE Correo electrónico • SCPROV Contratación de proveedores • APOT Apoteosys • WIN Windows • XEN Xenserver • CEN Centos • DDB Discos duros externos • INFONEG Información del negocio • CAEST Cableado estructurado • INGSIS Ingeniero de sistemas • GER Gerente • ABO Abogado • TES Tesorero • CON Contador • PROD Productor • DIRFINAN director financiero • COORDGESHUMAN Coordinador de gestión humana • COORDCOMPRAS Coordinador de compras • COORDPROD Coordinador de producción • AUXPROD Auxiliar de producción	• Capacitación al personal • Políticas de manejo de información • Contraseñas fuertes en los aplicativos y sistemas operativos • Mantener actualizados los sistemas operativos • Cifrar la información de los discos duros externos • Manejo de usuarios con contraseña en aplicativos, cambio de clave cada 3 meses • Concientización del personal • Acuerdos de confidencialidad en los contratos del personal • Bloqueo de puertos de equipos de cómputo	Área de Sistemas	NA	• Políticas de seguridad informática • Acuerdos de confidencialidad • Actas de capacitación

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
		• GESEVEN Gestor de eventos • AUXADMIN Auxiliar administrativo • SERASEO Servicio de aseo • DISE Diseñador • SECGER Secretaria de Gerencia				

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
6	[E.20] Vulnerabilidad de los programas (Software)	• SCPROV Contratación de proveedores • APOT Apoteosys • WIN Windows • XEN Xenserver • CEN Centos	• Control en los permisos de acceso para el desarrollo de actividades de proveedores • Uso de claves robustas, cambio de las mismas cada 3 meses • Concientización de los usuarios de los sistemas informáticos • Controles de acceso adecuados por roles, por usuarios.	Área de Sistemas	Recursos audiovisuales	Listado de claves de acceso, roles y contraseñas
7	[E.24] caídas del sistema por agotamiento de recursos	• CAEST Cableado estructurado	Revisiones periódicas de las capacidad, necesidades, estado físico y velocidad de red	Área de Sistemas	Equipo de cómputo	Registro de revisión de cableado

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
8	[A.8] Difusión de software dañino	• SCPROV Contratación de proveedores • APOT Apoteosys • WIN Windows • XEN Xenserver • CEN Centos	• Uso de herramientas antimalware • Contar con un plan de acción frente a infecciones de malware • Contar con Backups diarios de la información • Contar con Backups de configuración de sistemas operativos. • Almacenamiento de instaladores en un lugar accequible	Área de Sistemas	• Discos externos para el almacenamiento de Backups • Antivirus y / o herramientas antimalware • Software de respaldo • Drivers, instaladores.	• Esquema de Backups • Plan de contingencia

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
9	[A.15] Modificación de la información	• INT Internet • COELE Correo electrónico • SCPROV Contratación de proveedores • APOT Apoteosys • WIN Windows • XEN Xenserver • CEN Centos • DDB Discos duros externos • INFONEG Información del negocio • CAEST Cableado estructurado • INGSIS Ingeniero de sistemas • GER Gerente • ABO Abogado • TES Tesorero • CON Contador • PROD Productor • DIRFINAN director financiero • COORDGESHUMAN Coordinador de gestión humana • COORDCOMPRAS Coordinador de compras • COORDPROD Coordinador de producción • AUXPROD Auxiliar de producción	• Capacitaciones al personal • Control de acceso y restricciones • Creación de usuarios y contraseñas fuertes para los recursos de la plataforma informática	Área de Sistemas	Recursos audiovisuales	Listado de claves de acceso, roles y contraseñas

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
		• GESEVEN Gestor de eventos • AUXADMIN Auxiliar administrativo • SERASEO Servicio de aseo • DISE Diseñador • SECGER Secretaria de Gerencia				

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
10	[A.19] Revelación de la información	• INT Internet COELE Correo electrónico • SCPROV Contratación de proveedores • APOT Apoteosys • WIN Windows CEN Centos • DDB Discos duros externos • INFONEG Información del negocio • CAEST Cableado estructurado • INGSIS Ingeniero de sistemas • GER Gerente • ABO Abogado • TES Tesorero • CON Contador • PROD Productor • DIRFINAN director financiero • COORDGESHUMAN Coordinador de gestión humana • COORDCOMPRAS Coordinador de compras • COORDPROD Coordinador de producción • AUXPROD Auxiliar de producción	• Agregar cláusulas de confidencialidad al contrato del personal de la empresa • Concientización del personal.	Área de Sistemas	Personal jurídico de la empresa.	• Actas de capacitación • Anexo al contrato del personal.

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
		• GESEVEN Gestor de eventos • AUXADMIN Auxiliar administrativo • SERASEO Servicio de aseo • DISE Diseñador • SECGER Secretaria de Gerencia				

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
11	[A.22] Manipulación de los programas	• SCPROV Contratación de proveedores • APOT Apoteosys • WIN Windows • XEN Xenserver • CEN Centos	• Supervisión del acceso a proveedores • Capacitación del personal	Área de Sistemas	Recursos audiovisuales	Actas de capacitación
12	[A.23] Manipulación del Hardware	• HW EQUIPOS • SER Servidores • IMP Impresoras • PSP Equipos de cómputo portátiles • TELIP Teléfonos IP • DDB Discos duros externos • AP Access Point • SWITCH Switches • ROU Routers • PLAELEC Planta eléctrica • UPS UPS	• Establecer restricciones físicas a los lugares en donde se encuentran equipo servidores y recursos Hardware	Área de Sistemas	Cerraduras, barreras	Informe de adecuación.

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
13	[A.25] Robo de equipos	• PCS Equipos de cómputo • SER Servidores • IMP Impresoras • PSP Equipos de cómputo portátiles • TELIP Teléfonos IP • DDB Discos duros externos • AP Access Point • SWITCH Switches • ROU Routers • PLAELEC Planta eléctrica • UPS UPS	• Implementar seguridad física. • Instalación de dispositivos de red en lugares altos, lejos del acceso de terceros. • Revisión por parte del guarda de seguridad de bolsos, maletas y vehículos • Uso de guayas de seguridad para equipos portátiles • Implementación de cámaras de seguridad en lugares remotos	Área de Sistemas Vigilancia y portería Área de mantenimiento del edificio	Cerraduras, barreras Guayas de seguridad Repisas	Informe de adecuación.

No.	Riesgo	Activo afectado	Tratamiento	Responsable	Recursos	Registros
14	{A.30] Ingeniería social	• INGSIS Ingeniero de sistemas • GER Gerente • ABO Abogado • TES Tesorero • CON Contador • PROD Productor • DIRFINAN director financiero • COORDGESHUMAN Coordinador de gestión humana • COORDCOMPRAS Coordinador de compras • COORDPROD Coordinador de producción • AUXPROD Auxiliar de producción • GESEVEN Gestor de eventos • AUXADMIN Auxiliar administrativo • SERASEO Servicio de aseo • DISE Diseñador • SECGER Secretaria de Gerencia	• Capacitación en seguridad informática • Capacitación en buenas prácticas • Socialización de manual de políticas de seguridad informática	Área de Sistemas Área de gestión humana	Recursos audiovisuales	Actas de capacitación

Fuente: El Autor

6.1.3.6 SALVAGUARDAS

La Salvaguardas son mecanismos que buscan detectar, prevenir y controlar una amenaza y el daño que ésta pueda provocar, reduciendo los riesgos.

En la siguiente fase se busca identificar las salvaguardas que sean efectivas para mitigar el riesgo dentro de la PYME de gestión de eventos y espectáculos.

6.1.3.6.1 IDENTIFICACIÓN DE SALVAGUARDAS

Se definen las medidas necesarias para que las amenazas no se materialicen para de esta manera disminuir el riesgo.

Tabla 14 Listado de salvaguardas

Cód	Detalle
[IA]	Identificación y autenticación
[AC]	Control de acceso lógico
[D]	Protección de la información
[K]	Protección de claves criptográficas
[S]	Protección de los servicios
[SW]	Protección de las aplicaciones informáticas (SW)
[HW]	Protección de los equipos informáticos (HW)
[COM]	Protección de las comunicaciones
[IP]	Sistema de protección de frontera lógica
[MP]	Protección de los soportes de información
[AUX]	Elementos auxiliares
[PPE]	Protección física de los equipos
[L]	Protección de las instalaciones
[PPS]	Protección del perímetro físico
[PS]	Gestión del personal
[PDS]	Servicios potencialmente peligrosos
[IR]	Gestión de incidentes
[tools]	Herramientas de seguridad
[V]	Gestión de vulnerabilidades

[A]	Registro y auditoría
[BC]	Continuidad del negocio
[G]	Organización
[E]	Relaciones externas
[NEW]	Adquisición/desarrollo

Fuente: Pilar v7.3

6.1.3.6.2 Eficacia de las salvaguardas

Identificadas las salvaguardas se procede a determinar su eficacia dentro de la Organización

Tabla 15 Eficacia de salvaguardas

Eficacia	Nivel	Madurez	Estado
0%	L0	Inexistente	Inexistente
10%	L1	Inicia/ad hoc	Iniciado
50%	L2	Reproducible, pero intuitivo	Parcialmente realizado
90%	L3	proceso definido	En funcionamiento
95%	L4	Gestionado y medible	Monitorizado
100%	L5	Optimizado	Mejora continua

Fuente: Pilar v7.3

6.1.3.6.3 VALORACIÓN DE SALVAGUARDAS

En la tabla a continuación se define la eficiencia para las salvaguardas que buscan proteger los activos informáticos de la PYME.

Tabla 16 Identificación y valoración de salvaguardas

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
A5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A5.1.1 POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	L1	10%

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	A5.1.2 REVISION DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 6.1.2 SEPARACIÓN DE DEBERES	L0	0%
	A 6.1.3 CONTACTO CON LAS AUTORIDADES	L0	0%
	A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	L0	0%
	A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	L0	0%
	A 6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	L0	0%
	A 6.2.2 TELETRABAJO	L0	0%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS			
A 7.1 ANTES DE ASUMIR EL EMPLEO	A 7.1.1 SELECCIÓN	L3	90%
	A 7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	L3	90%
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A 7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	L3	90%
	A 7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN	L1	10%
	A.7.2.3 PROCESO DISCIPLINARIO	L3	90%
A 7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	A7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	L1	10%

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
A.8 GESTION DE ACTIVOS	A 8.1.1 INVENTARIO DE ACTIVOS	L3	90%
A 8.1 RESPONSABILIDAD POR LOS ACTIVOS	8.1.2 PROPIEDAD DE LOS ACTIVOS	L3	90%
	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS	L3	90%
	A 8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	L3	90%
A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN	A 8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	L0	0%
	A 8.2.2 ETIQUETADO DE LA INFORMACIÓN	L0	0%
	A 8.2.3 MANEJO DE ACTIVOS	L0	0%
A 8.3 MANEJO DE MEDIOS	A 8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	L0	0%
	A 8.3.2 DISPOSICIÓN DE LOS MEDIOS	L0	0%
	A 8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS.	L0	0%
A.9 CONTROL DE ACCESO			
A 9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	A 9.1.1 POLÍTICA DE CONTROL DE ACCESO	L3	90%
	A 9.1.2 ACCESO A REDES Y A SERVICIOS EN RED	L3	90%
A 9.2 GESTIÓN DE ACCESO DE USUARIOS	A 9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	L3	90%
	A 9.2.2 SUMINISTRO DE ACCESO DE USUARIOS	L3	90%
	A 9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	L1	10%

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	A 9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	L0	0%
	9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	L0	0%
	A 9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.	L1	10%
A 9.3 RESPONSABILIDADES DE LOS USUARIOS	A 9.3.1 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	L0	0%
A 9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	L1	10%
	A 9.4.2 PROCEDIMIENTO DE INGRESO SEGURO	L1	10%
	A 9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS	L0	0%
	A 9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS	L1	10%
	A 9.4.5 CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS	L0	0%
A. 10 CRIPTOGRAFIA			
A 10.1 CONTROLES CRIPTOGRAFICOS	A 10.1.1 POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	L0	0%
	A 10.1.2 GESTIÓN DE LLAVES	L0	0%
A. 11 SEGURIDAD FISICA Y DEL ENTORNO			
A 11.1 ÁREAS SEGURAS	A 11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	L3	90%
	A 11.1.2 CONTROLES DE ACCESO FÍSICOS	L3	90%

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	A 11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	L3	90%
	A 11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	L1	10%
	A 11.1.5 TRABAJO EN ÁREAS SEGURAS	L1	10%
	A 11.1.6 ÁREAS DE DESPACHO Y CARGA	L3	90%
A 11.2 EQUIPOS	A 11.2.1 UBICACIÓN Y PROTECCION DE LOS EQUIPOS	L1	10%
	A11.2.2 SERVICIOS DE SUMINISTRO	L3	90%
	A 11.2.3 SEGURIDAD DEL CABLEADO	L1	10%
	A 11.2.4 MANTENIMIENTO DE EQUIPOS	L3	90%
	A 11.2.5 RETIRO DE ACTIVOS	L3	90%
	A 11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	L0	0%
	A 11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	L0	0%
	A 11.2.8 EQUIPOS DE USUARIO DESATENDIDO	L0	0%
	A 11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.	L0	0%
A.12 SEGURIDAD DE LAS OPERACIONES			
A 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	A 12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	L1	10%
	A 12.1.2 GESTIÓN DE CAMBIOS	L0	0%

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	A 12.1.3 GESTIÓN DE CAPACIDAD	L0	0%
	A 12.1.4 SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.	L0	0%
A 12.2 PROTECCION CONTRA CODIGOS MALICIOSOS	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	L3	90%
A 12.3 COPIAS DE RESPALDO	A 12.3.1 RESPALDO DE LA INFORMACIÓN	L3	90%
A 12.4 REGISTRO Y SEGUIMIENTO	A12.4.1 REGISTRO DE EVENTOS	L0	0%
	A12.4.1 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	L0	0%
	A12.4.1 REGISTROS DEL ADMINISTRADOR Y DEL OPERADOR	L0	0%
	A12.4.1 SINCRONIZACIÓN DE RELOJES	L0	0%
A 12.5 CONTROL DE SOFTWARE OPERACIONAL	A 12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	L1	10%
A 12.6 GESTION DE LA VULNERABILIDAD TÉCNICA	A 12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	L0	0%
	A 12.6.2 RESTRICCIÓN SOBRE LA INSTALACION DE SOFTWARE	L3	90%
A 12.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	L0	0%
A. 13 SEGURIDAD DE LAS COMUNICACIONES			
A 13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	A 13.1.1 CONTROLES DE REDES	L0	0%

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	A 13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	L0	0%
	A 13.1.3 SEPARACIÓN EN LAS REDES	L0	0%
A 13.2 TRANSFERENCIA DE INFORMACIÓN	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN	L0	0%
	A 13.2.2 ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	L0	0%
	A 13.2.3 MENSAJERIA ELECTRÓNICA	L0	0%
	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	L3	90%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A 14.1.1 ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN	L2	50%
	A 14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	L0	0%
	A 14.1.3 PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES	L1	10%
A 14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	A 14.2.1 POLÍTICA DE DESARROLLO SEGURO	L0	0%

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	A 14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	L0	0%
	A 14.2.3 REVISIÓN TÉCNICA DE LAS APLICACIONES DESPUES DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN	L0	0%
	A 14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	L0	0%
	A 14.2.5 PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS	L0	0%
	A 14.2.6 AMBIENTE DE DESARROLLO SEGURO	L0	0%
	A 14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE	L0	0%
	A 14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS	L0	0%
	A 14.2.9 PRUEBA DE ACEPTACIÓN DE SISTEMAS	L0	0%
	A14.3.1 PROTECCIÓN DE DATOS DE PRUEBA	L0	0%
A.15 RELACIONES CON LOS PROVEEDORES			
A. 15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	A 15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES	L0	0%
	A 15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	L0	0%

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	A 15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	L0	0%
A 15.2 GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	A 15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	L3	90%
	A 15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	L3	90%
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION			
A 16.1 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	L0	0%
	A 16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS	L0	0%
	A 16.1.5 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	L0	0%

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
	A 16.1.7 RECOLECCIÓN DE EVIDENCIA	L0	0%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO			
A 17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
A 17.2 REDUNDANCIAS	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	L1	10%
A. 18 CUMPLIMIENTO			
A 18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES	L3	90%
	A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	L3	90%
	A 18.1.3 PROTECCIÓN DE REGISTROS	L0	0%
	A 18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	L0	0%
	A 18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	L0	0%

CONTROLES NTC -ISO-IEC 27001:2013

objetivos de control	Controles	Nivel	Eficiencia
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN		
A 18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	A 18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	L0	0%
	A 18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	L0	0%

Fuente: El autor

Estos resultados se interpretan de la siguiente manera:

Tabla 17 Controles totalizados

0%	L0 - Inexistente	70	61%
10%	L1 – Iniciado	16	14%
50%	L2 - Reproducible, pero intuitivo	1	1%
90%	L3 - Proceso definido	27	24%
95%	L4 - Gestionado y medible	0	0%
100%	L5 – Optimizado	0	0%

Fuente: El autor

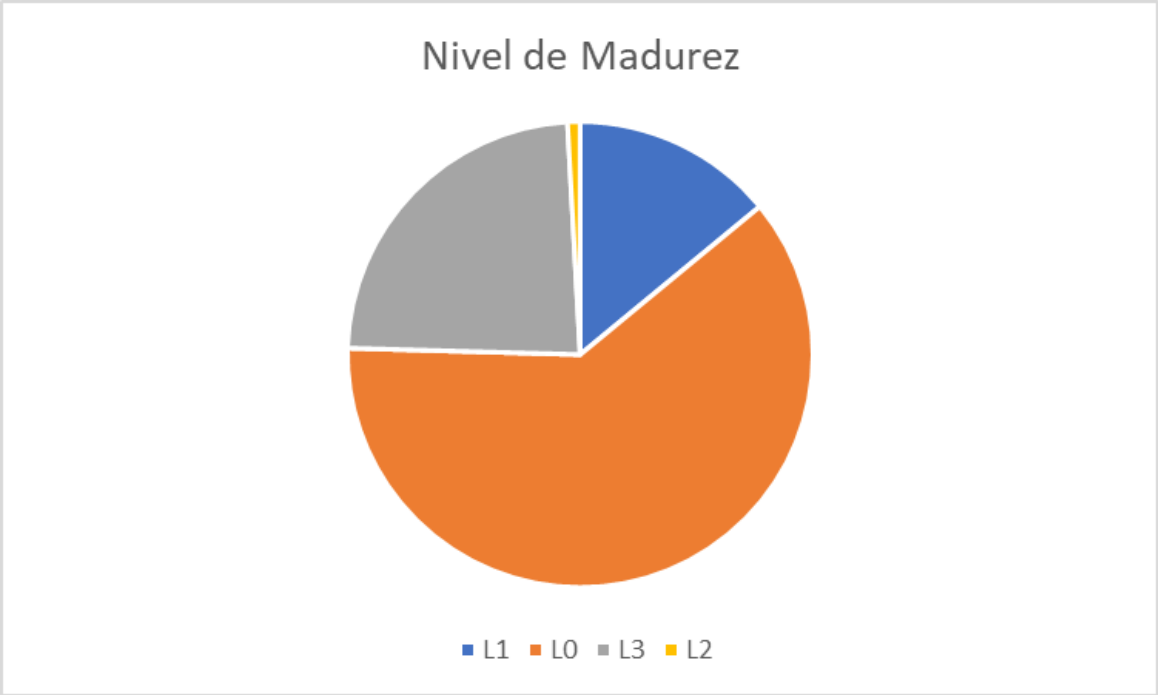


Ilustración 2 Nivel de madurez de los controles

Fuente: El autor

Análisis de la gráfica

Podemos encontrar los siguientes resultados:

El 65% de las salvaguardas no existen en la PYME, lo que permite determinar la compleja situación que se presenta. Un 14% de las salvaguardas existen, pero no se gestionan, lo que puede se considera un riesgo alto debido a que no existe una gestión adecuada que permita hacer frente a amenazas.

Un 1% de las salvaguardas dependen exclusivamente de la buena suerte y de la buena voluntad de las personas, lo que en determinado caso puede acarrear errores por desconocimiento, por falta de capacidad o de conciencia.

Un 24% de las salvaguardas se despliegan y se gestionan, existe una normatividad establecida y algunos procedimientos para garantizar reacción por parte de personal profesional ante incidentes que se puedan presentar. También hay mantenimientos regulares de las protecciones.

Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado).

No existen medidas de campo que pueda usar la Dirección de la Organización para controlar empíricamente la efectividad de las salvaguardas ni fijar metas cuantitativas de calidad. Los procesos no están bajo control, no existe mejora continua ni tecnológica incremental o innovadora.

Se puede determinar también que no se establecen objetivos cuantitativos de mejora relacionados en los objetivos del negocio que sirvan como indicadores de la gestión de los procesos.

6.1.3.7 PLAN DE TRATAMIENTO DE RIESGOS

El análisis realizado en este documento permite conocer, clasificar, evaluar y valorar las diferentes amenazas a las que están expuestos los activos de la PYME, el plan de tratamiento de riesgos define las medidas y actividades a ejecutar para dar tratamiento a los riesgos. Ver tabla 14. Identificación de riesgos.

7. RECOMENDACIONES

Con el fin de mitigar los riesgos aquí definidos se listan las siguientes recomendaciones:

- Monitoreo: Con el fin de verificar la eficacia de los controles implementados se recomienda una auditoría periódica que permita definir si las actividades de restricción y control de acceso a los sistemas se lleva a cabo de manera oportuna y eficiente.
- La valoración de los riesgos se debe revisar por lo menos una vez al año, de manera programada cada vez que se presenten cambios importantes en la organización, en los sistemas informáticos o en los procesos del negocio.
- Se deben documentar los procesos llevados a cabo por el área de TI dentro de la empresa, definiendo mecanismos para realizar una gestión documental de cada actividad realizada.
- Se debe mantener un inventario actualizado de los activos, tarea que se debe asignar a una persona en la empresa, para que registre cambios en los listados existentes, este inventario se debe verificar de manera anual como parte de proceso de auditoría.
- Todos los colaboradores de la PYME deben recibir capacitación y concientización constante acerca de buenas prácticas de seguridad informática y de los peligros a los que está expuesta la información en el entorno empresarial, por lo cual se recomienda definir un plan de inducción y reinducción anual para reforzar los conocimientos en Seguridad de la Información tanto de nuevas contrataciones como de los colaboradores ya contratados.
- La empresa debe realizar campañas de manera periódica con la finalidad de enseñar a los colaboradores y empleados acerca de los peligros de descargar archivos de Internet o de la irresponsabilidad al momento de usar deliberadamente los sistemas informáticos.
- Se deben definir filtros de Internet para evitar que los usuarios visiten webs no adecuadas o que puedan conllevar a problemas de seguridad informática en la empresa, este filtrado debe contemplar la opción de definir y restringir un conjunto de páginas y contenido web que pueda ser no adecuado para el consumo en las instalaciones de la Organización.
- Se deben definir restricciones a los usuarios para evitar el mal uso de los sistemas, tales como controles de acceso, usuarios no administradores y imposibilidad de instalación de software en los equipos, estas deben ser validadas de manera constante cada vez que ingrese o se retire algún colaborador de la empresa.

- La empresa debe mantener los equipos con soluciones antivirus, antimalware licenciadas.
- La empresa debe mantener los sistemas operativos de los equipos actualizados, para garantizar la instalación de parches que busquen corregir y proteger fallas de seguridad.
- Se debe definir un cronograma de mantenimientos preventivos para los equipos de red, de cómputo y relacionados al inventario de activos de la PYME definidos en este documento.

8. CONCLUSIONES

- Realizar un diagnóstico general que permita determinar los niveles de madurez de la seguridad en los sistemas es un proceso que permitió identificar en la PYME los niveles de madurez de los sistemas informáticos y la seguridad de la información, logrando adelantar analizar las falencias que crean vulnerabilidades.

- Identificar los activos de la empresa permitió a la corporación oportunidades para definir mecanismos que permitan reducir los riesgos que se presentan, así mismo, trazar estrategias para minimizar el impacto de la materialización de las amenazas.

- Crear un manual de políticas de seguridad informática permite que los empleados adquieran un mayor nivel de conciencia sobre la protección de los sistemas informáticos y sobre la importancia que tiene cualquier empleado sobre la seguridad informática.

9. DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación del mismo; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de Sistemas de Gestión de Seguridad de la Información, puedan acceder al documento.

BIBLIOGRAFÍA

AGUILA PLAZA, XAVIER. Análisis y diseño de un SGSI basado en el criterio de la norma NTE INEN-ISO/IEC 27001, de un modelo de negocio aplicado en la comercialización y distribución de productos químicos [en línea]. Guayaquil, [consulta 02-02-2020]. Disponible en web: https://dspace.ups.edu.ec/bitstream/123456789/10283/1/UPS-GT001168.pdf

Apartes jurídicos Supersociedades: SOCIEDADES DE ECONOMÍA MIXTA. [consultado el 16 de octubre de 2020]. Disponible en: https://www.supersociedades.gov.co/nuestra_entidad/normatividad/normatividad_conceptos_juridicos/7274.pdf

CALLE, P. 5 métodos de análisis de riesgos [en línea]. [Consultado 19 octubre de 2020]. Disponible en: https://www.riesgoscero.com/blog/5-metodos-de-analisis-de-riesgos

Centro Criptológico Nacional: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [consultado: 12 enero 2020]. https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

CORLETTI, ALEJANDRO. ISO-27001: LOS CONTROLES (Parte I). [en línea]. España, [consulta 05-08-2020]. Disponible en web: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf

DANIELS, K. Ciberseguridad sin miedo: Activo informático: lo que todo buen Gerente quiere cuidar [en línea]. [Consultado 17 octubre 2020]. Disponible en: https://www.widefense.com/recursos/ciberseguridad/activo-informatico-gerente-cuidar/

ESET TEAM. MAGERIT: metodología práctica para gestionar riesgos [en línea]. [Consultado 17 octubre 2020]. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Foro de internet. INCIBE: Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [consultado el 16 de septiembre de 2020]. Disponible en:

https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo

Foro de internet. ISO TOOLS EXCELLENCE: Descubre qué es un SGSI y cuáles son sus elementos esenciales [consultado el 10 de julio de 2020, 12:28]. Disponible en: https://www.isotools.org/2016/02/16/descubre-que-es-un-sgsi-y-cuales-son-sus-elementos-esenciales/

Foro de internet. MAGERIT V.3 : METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN [consultado el 19 de octubre de 2020, 11:00]. Disponible en: https://interpolados.wordpress.com/2018/10/02/magerit-v-3-metodologia-de-analisis-y-gestion-de-riesgos-de-los-sistemas-de-informacion/

Foro de internet. RIESGO INFORMATICO [consultado el 18 de octubre de 2020]. Disponible en: http://uniminutocontaduriapublica343875.blogspot.com/p/riesfgo-informatico.html

GALLO, C. Helinotas: ¿Qué es el ciclo PHVA, su importancia e impacto en las organizaciones? [en línea]. [Consultado 7 septiembre 2020]. Disponible en: http://heliflycolombia.com/blog/que-es-el-ciclo-phva-su-importancia-e-impacto-en-las-organizaciones/

GAVIRIA, J. Sociedades de Economía Mixta y su Régimen Contractual [en línea]. [Consultado 20 octubre de 2020]. Disponible en: https://www.asuntoslegales.com.co/consultorio/sociedades-de-economia-mixta-y-su-regimen-contratual-2867225

INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [en línea]. 2017, [citado en octubre de 2020]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo

INCIBE. Protección de la información – Colección Protege tu empresa [en línea]. [Consultado 22 de enero de 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

ISO TOOLS EXCELLENCE. ISO 27001: El método MAGERIT [en línea]. [Consultado 17 octubre de 2020]. Disponible en: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/
ISO27001.ES. [sito web]. España: ISO27001. [Consulta: 10 marzo 2020]. Disponible en: https://www.iso27000.es/sgsi.html

ISO27001.ES. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES [en línea]. España, [consulta 10-08-2020]. Disponible en web: http://www.iso27000.es/download/ControlesISO27002-2013.pdf

KASPERSKY. Ingeniería social: definición [en línea]. [Consultado 18 octubre de 2020]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

MALWARE BYTES. Todo acerca del malware [en línea]. [Consultado 12 octubre de 2020]. Disponible en: https://es.malwarebytes.com/malware/

Secretaría General de Administración Digital. MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [en línea]. [Consultado 17 octubre de 2020]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

SERRANO, CARLOS. Plan para la implementación de un SGSI en un centro educativo [en línea]. San Vicente del Raspeig, [consulta 15-08-2020]. Disponible en web:
https://rua.ua.es/dspace/bitstream/10045/93561/1/Plan_para_la_implementacion_de_un_SGSI_en_un_centro_edu_Perez_Serrano_Carlos.pdf

TAVERA, K. 7 amenazas informáticas que toda Pyme debe conocer [en línea]. [Consultado 11 octubre de 2020]. Disponible en: https://co.godaddy.com/blog/7-amenazas-informaticas-toda-pyme-debe-conocer/

Universidad Internacional de Valencia. ¿Qué es la seguridad informática y cómo puede ayudarme? [en línea]. [Consultado 22 de enero de 2021]. Disponible en: https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

Universidad Libre – Seccional Bogotá. Seguridad de la Información [en línea]. [Consultado 21 de enero de 2021]. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

UPC – DEPARTMENT DE CIENCIA I ENGINYERIA NAUTIQUES. El futuro tecnológico de las terminales marítimas de vehículos: la integración de sus sistemas de información [en línea]. [consulta 15-10-2020]. Disponible en web: < https://www.tdx.cat/bitstream/handle/10803/7001/08Jmmc08de12.pdf?sequence=8&isAllowed=y>

VASQUEZ, V. ISO 27001: Elementos de los Sistemas de Información [en línea]. [Consultado 18 octubre de 2020]. Disponible en: https://www.gestiopolis.com/elementos-los-sistemas-informacion/

MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA UNA PYME DE GESTIÓN DE EVENTOS Y ESPECTÁCULOS

Octubre 2020

INTRODUCCIÓN

Con los avances en Internet y los desarrollos de la informática y las telecomunicaciones, la Seguridad Informática, se ha convertido en figura necesaria para la protección, mantenimiento, control de acceso, confidencialidad, integridad y disponibilidad de la información, tanto para su seguridad como para la seguridad en el soporte de las operaciones de las organizaciones.

Las Políticas de Seguridad Informática son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida. El principio y final de toda red es el usuario, esto hace que las políticas de seguridad deban, principalmente, enfocarse a los usuarios, indican a las personas cómo actuar frente a los recursos informáticos de la Entidad.

Actualmente las PYMES de gestión de eventos y espectáculos cuentan con una plataforma tecnológica que almacena, procesa y transmite la información institucional, incluye equipos de cómputo de usuario y los servidores que se interconectan por medio de una red de datos, así como servicio de internet y correo electrónico institucional. Siendo la información institucional un activo valioso para la Entidad, se hace necesario no solo la implementación de herramientas de hardware y software de seguridad, sino involucrar al personal para proteger su integridad y confidencialidad.

Este compendio tiene como finalidad dar a conocer las PSI - Políticas de Seguridad Informática, que deben aplicar y acatar los empleados, contratistas y terceros de la empresa, entendiendo como premisa que la responsabilidad por la seguridad de la información es de todos y cada uno.

OBJETIVO

Definir e implementar las políticas de seguridad informática que dan las pautas y rigen para la gestión, el uso adecuado y la seguridad de la información de los sistemas informáticos y en general, sobre el ambiente tecnológico de la PYME, para su interiorización, aplicación y verificación permanente.

ALCANCE

Las políticas de seguridad informática están orientadas a toda la información almacenada, procesada y transmitida en medios electrónicos, estas políticas deben ser conocidas y cumplidas tanto por empleados de planta como por los contratistas que apoyan la gestión y por los terceros o grupos de interés que utilicen la información generada y custodiada por la PYME, y por quienes hagan uso de los servicios tecnológicos de la empresa.

DEFINICIONES

Para los efectos del presente manual, se adoptarán las siguientes definiciones:

Acceso físico: La posibilidad de acceder físicamente a un computador o dispositivos, manipularlo tanto interna como externamente.

Acceso lógico: Ingresar al sistema operativo o aplicaciones de los equipos y operarlos, ya sea directamente, a través de la red de datos interna o de Internet.

Activos de Información: Toda aquella información que la Entidad considera importante o fundamental para sus procesos, puede ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.
Aplicaciones o aplicativos: Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares.

Cableado estructurado: Cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc.

Cifrado de datos: Proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes.

Configuración Lógica: conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o Para poder ejecutar dicho programa correctamente.

Copia de respaldo o backup: se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

Contenido: Todos los tipos de información o datos que se divulguen a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, video, diseños, software, animaciones, etc.

Contraseñas: Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

Correo electrónico institucional: Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos, que se encuentra alojado en un hosting de propiedad de la Entidad.

Cuenta de acceso: Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema, administración de recursos, etc.

Dispositivos/Periféricos: Aparatos auxiliares e independientes conectados al computador o la red.

Dominio: Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.

Espacio en disco duro: Capacidad de almacenamiento de datos en la unidad de disco duro.

Herramientas ofimáticas: Conjunto de aplicaciones informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas. En la PYME se hace uso de la Herramienta Microsoft Office.

Información confidencial: Se trata de una propiedad de la información que pretende garantizar el acceso sólo a personas autorizadas.

Información/Documento electrónico: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se pueden clasificar por su forma y formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Licencia de uso: Contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas, es decir, es un conjunto de permisos que un desarrollador le puede otorgar a un usuario en los que tiene la posibilidad de distribuir, usar y/o modificar el producto bajo una licencia determinada.

Mantenimiento lógico preventivo: Es el trabajo realizado en el disco duro del equipo de cómputo, con la finalidad de mejorar el rendimiento general del sistema operativo.

Mantenimiento físico preventivo: Actividad de limpieza de elementos como polvo, residuos de alimentos y otro tipo de partículas que debe realizarse sobre el equipo de cómputo, con el propósito de posibilitar que su correcto funcionamiento sea más prolongado en el tiempo.

Medios de almacenamiento extraíble: Son aquellos soportes de almacenamiento diseñados para ser extraídos del computador sin tener que apagarlo. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, CompactFlash, Memory Stick).

Plataforma web: Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.

Propiedad intelectual: Se relaciona con las creaciones de la mente como invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. Es el conjunto de derechos que corresponden a los autores y a otros titulares.

Recurso informático: Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento de un computador o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

Red de datos: Es un conjunto de ordenadores que están conectados entre sí, y comparten recursos, información, y servicios.

Riesgo: Posibilidad de que se produzca un contratiempo o una desgracia, las vulnerabilidades y amenazas a que se encuentran expuestos los activos de información.

Servicio informático: Conjunto de actividades asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios.

Servidor: Se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red, pero también pueden acceder a él a través de la computadora donde está funcionando.

Sistema de información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Software antivirus: Son programas que buscan prevenir, detectar y eliminar virus informáticos. En los últimos años, y debido a la expansión de Internet, los nuevos navegadores y el uso de ingeniería social, los antivirus han evolucionado para detectar varios tipos de software fraudulento, también conocidos como malware.

Software de gestión: Son todos aquellos programas utilizados a nivel empresarial, que por su definición genera acción de emprender algo y por su aplicación persigue fines lucrativo y no lucrativo. También es un software que permite gestionar todos los procesos de un negocio o de una empresa en forma integrada. Por lo general está compuesto por modulo cruzado del proceso del negocio.
Software malicioso: Es aquel que se ha diseñado específicamente para dañar un computador, este tipo de software realiza acciones maliciosas como instalar software sin el consentimiento del usuario o virus.

Tráfico de red: Es la cantidad de datos enviados y recibidos por los usuarios de la red.
UPS: Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

DOCUMENTOS DE REFERENCIA

Documentos de fundamentación Legal:

Ley 87 de 1993: “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones”.

Ley 527 de 1999: “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.

Ley 1273 de 2009: “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Ley 594 de 2000: “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.
Ley 599 de 2000: “Por la cual se expide el Código Penal”.

Ley 1437 de 2011: “Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo”.

Decreto 2609 de 2012: “Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado”.

Decreto 2573 de 2014 “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”.

POLÍTICAS GENERALES DE SEGURIDAD FÍSICA

Se destinará un área en la entidad que servirá como centro de telecomunicaciones en el cual se ubicarán los sistemas de telecomunicaciones y servidores, debidamente protegidos con la infraestructura apropiada, de manera que se restrinja el acceso directo a usuarios no autorizados.

El centro de Telecomunicaciones deberá contar con sistema de protección contra incendios (Extintor Co2), control de temperatura (aire acondicionado) permanente a una temperatura no superior a 22 grados centígrados, así como sistema eléctrico de respaldo (UPS).

Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

Los equipos que hacen parte de la infraestructura tecnológica de la PYME, tales como servidores, estaciones de trabajo, centro de cableado, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

POLÍTICAS ORIENTADAS A LOS USUARIOS INTERNOS

Gestión de la Información:

Todo empleado de planta o contratista que inicie labores en la empresa, relacionadas con el uso de equipos de cómputo, software de gestión, aplicativos, plataformas web y servicios informáticos, debe aceptar las condiciones de confidencialidad y de uso adecuado de los recursos informáticos, así como

cumplir y respetar las directrices impartidas en el Manual de Políticas de Seguridad Informática.
Los empleados que se desvinculen y los contratistas que culminen su vínculo contractual con la Organización, deberán hacer entrega formal de los equipos asignados, así como de la totalidad de la información electrónica que se produjo y se recibió con motivo de sus funciones y actividades.

Toda la información recibida y producida en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentre almacenada en los equipos de cómputo, pertenece a la Organización, por lo tanto, no se hará divulgación ni extracción de la misma sin previa autorización de las directivas de la Entidad.

No se realizará por parte de los empleados o contratistas copia no autorizada de información electrónica confidencial y software de propiedad de la empresa. El retiro de información electrónica perteneciente a la Organización y clasificada como confidencial, se hará única y exclusivamente con la autorización del Directivo competente.

Ningún empleado o contratista podrá visualizar, copiar, alterar o destruir información que no se encuentre bajo su custodia.

Todo contrato o convenio relacionado con servicios de tecnología y/o acceso a información, debe contener una obligación o cláusula donde el contratista o tercero acepte el conocimiento de las políticas de seguridad y acuerde mantener confidencialidad de la información con la suscripción de un acuerdo o compromiso de confidencialidad de la información, el cual se hará extensivo a todos sus colaboradores.

Hardware y Software:

La instalación y desinstalación de software, la configuración lógica, conexión a red, instalación y desinstalación de dispositivos, la manipulación interna y reubicación de equipos de cómputo y periféricos, será realizada únicamente por personal del área de Sistemas.

El espacio en disco duro de los equipos de cómputo pertenecientes a la Organización será ocupado únicamente con información institucional, no se hará uso de ellos para almacenar información de tipo personal (documentos, imágenes, música, video).

Ningún empleado o contratista podrá acceder a equipos de cómputo diferentes al suyo sin el consentimiento explícito de la persona responsable.
Ningún empleado o contratista podrá interceptar datos informáticos en su origen, destino o en el interior de un sistema informático protegido o no con una medida de seguridad, sin autorización.

Ningún empleado o contratista podrá impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, salvo el personal autorizado del área de TIC´S en aplicación de las políticas o medidas de seguridad.

No se permite el uso de la plataforma y servicios informáticos (equipos de cómputo, periféricos, dispositivos, internet, red de datos, correo electrónico institucional) de la Organización, para actividades que no estén relacionadas con las labores propias de La Entidad.

Los empleados y contratistas serán responsables de contar con conocimientos actualizados en informática básica y el uso de herramientas ofimáticas.

Correo Electrónico:

El correo electrónico institucional es exclusivo para envío y recepción de mensajes de datos relacionados con las actividades de la empresa, no se hará uso de él para fines personales como registros en redes sociales, registros en sitios web con actividades particulares o comerciales o en general entablar comunicaciones en asuntos no relacionados con las funciones y actividades en la Entidad.

La información transmitida a través de las cuentas de correo electrónico institucional no se considera correspondencia privada, ya que estas tienen como

fin primordial la transmisión de información relacionada con las actividades ordinarias de la empresa.

Es prohibido utilizar el correo electrónico institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

Internet:

No se harán descargas de archivos por internet que no provengan de páginas conocidas o relacionadas con las funciones y actividades en la Entidad.

El Servicio de internet de la empresa no podrá ser usado para fines diferentes a los requeridos en el desarrollo de las actividades propias de la Entidad. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la Organización o de las personas.

La Organización se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la Entidad.

Cuentas de Acceso:

Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, cada empleado y contratista es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen. Se permite su uso única y exclusivamente durante el tiempo que tenga vínculo laboral o contractual con la Organización.

Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios.

La contraseña inicial de acceso a la red que le sea asignada debe ser cambiada la primera vez que acceda al sistema, además, debe ser cambiada mínimo cada 4 meses, o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

Todo empleado o contratista que se retire de la Entidad de forma definitiva o temporal (superior a 1 semana), deberá hacer entrega formal a quien lo reemplace en sus funciones o a su superior inmediato de las claves de acceso de las cuentas asignadas, con el fin de garantizar la continuidad de las operaciones a su cargo.

Seguridad Física:

Es responsabilidad de los empleados y contratistas velar por la conservación física de los equipos a ellos asignados, haciendo uso adecuado de ellos y en el caso de los equipos portátiles, estos podrán ser retirados de las instalaciones de la Entidad única y exclusivamente por el usuario a cargo y estrictamente para ejercer labores que estén relacionadas con la Organización. En caso de daño, pérdida o robo, se establecerá su responsabilidad a través de los procedimientos definidos por la normatividad para tal fin.

Los empleados y contratistas deberán reportar de forma inmediata a los directivos la detección de riesgos reales o potenciales sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, peligro de incendio, peligro de robo, entre otros. Así como reportar de algún problema o violación de la seguridad de la información, del cual fueren testigos.

Mientras se operan equipos de cómputo, no se deberá consumir alimentos ni ingerir bebidas.

Se debe evitar colocar objetos encima de los equipos de cómputo que obstruyan las salidas de ventilación del monitor o de la CPU.

Derechos de Autor:

Ningún usuario, debe descargar y/o utilizar información, archivos, imagen, sonido, software u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de estos.

Uso de Unidades de Almacenamiento Extraíbles:

Los empleados y contratistas que tengan información de propiedad de la empresa en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

Toda información que provenga de un archivo externo de la Entidad o que deba ser restaurado tiene que ser analizado con el antivirus institucional vigente.

Clasificación de la información:

Los documentos electrónicos resultantes de los procesos misionales y de apoyo de la Organización, se tratarán conforme a los lineamientos y parámetros establecidos en el Sistema de Gestión Documental de la entidad. Los activos de información asociados a cada sistema de información serán identificados y clasificados por su tipo y uso siguiendo lo establecido en las tablas de retención documental vigentes.

Personal de sistemas:

El control de los equipos tecnológicos deberá estar bajo la responsabilidad del área de Sistemas, así como la asignación de usuarios y la ubicación física.

En el área de Sistemas se deberá llevar un control total y sistematizado de los recursos tecnológicos tanto de hardware como de software.

El área Sistemas será la encargada de velar por que se cumpla con la normatividad vigente sobre propiedad intelectual de soporte lógico (software).

Las licencias de uso de software estarán bajo custodia del área de Sistemas. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas u otros medios) que acompañen a las versiones originales de software.

El área de Sistemas es la única dependencia autorizada para realizar copia de seguridad del software original, aplicando los respectivos controles. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

El acceso a los sistemas de información y red de datos será controlado por medio de nombres de usuario personales y contraseña. El área de Sistemas será la encargada de crear y asignar las cuentas de acceso y sus permisos a dominio de red, sistemas de información y correo electrónico, previo cumplimiento del procedimiento establecido para tal fin.

Se deben asignar usuarios unificados para todos y cada uno de los sistemas, servicios y aplicaciones, garantizando la estandarización por cada usuario; es decir, que cada usuario debe tener el mismo nombre de usuario para todos los sistemas y aplicaciones de la Entidad. La estandarización de los nombres de usuario estará compuesta de la siguiente forma: (Primer letra del nombre + apellido, en caso de existir duplicidad, Primeras dos letras del primer nombre + punto (.) + apellido).

Las cuentas de acceso a sistemas, servicios y aplicaciones no podrán ser eliminadas al retiro de los empleados o contratistas, debe aplicarse la inactivación del usuario.

Se realizará Backup a la información institucional y bases de datos, conforme a lo establecido en la política de Backup y cronograma, así como en los casos

extraordinarios: desvinculación de empleado o contratista, envío de equipo para garantía, mantenimiento correctivo de equipo.

Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de información de la Entidad deberán ser salvaguardadas por el área de Sistemas en un archivo protegido ante el acceso a terceros no autorizados.

La red interna de la Organización deberá estar protegida de amenazas externas, a través de sistemas que permitan implementar reglas de control de tráfico desde y hacia la red.

Todos los equipos de la entidad deben tener instalado un antivirus, en funcionamiento, actualizado y debidamente licenciado.

Se realizará mantenimiento lógico preventivo a los equipos de cómputo mínimo cada 6 meses y mantenimiento físico preventivo mínimo una vez por año, que incluya el cableado estructurado. El área de TIC´S deberá elaborar el plan y cronograma de mantenimientos, el cual será notificado a los usuarios, adicionalmente, deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de hurto y/o pérdida de equipos e información.

Directivos:

La Entidad debe garantizar capacitación a los empleados y contratistas en el manejo del software de gestión, plataformas y aplicativos implementados en la Organización.

Deberá notificarse al área de Sistemas las novedades de vinculación y desvinculación de personal de la empresa, con el fin de crear o cancelar, según sea el caso, los accesos a los sistemas de información, correo electrónico y red de datos.

electrónico y red de datos.

POLÍTICAS ORIENTADAS A LOS USUARIOS EXTERNOS

a. El acceso de terceras personas a la Entidad debe ser controlado y su ingreso a las diferentes dependencias debe ser autorizado por los empleados a cargo.

POLÍTICA DE ADMINISTRACIÓN DE BACKUP

Objetivo

Establecer las directrices para la ejecución y control de las copias de seguridad de la información digital perteneciente a la Organización.

Alcance

Estas directrices son aplicables a la información institucional, bases de datos y archivos de restauración de los equipos pertenecientes a la Organización.

Clasificación de la Información

Información Institucional:

Entiéndase como información institucional aquella relativa a las operaciones realizadas por cada una de las dependencias de la Organización, su producción, almacenamiento y gestión está a cargo de cada uno de los empleados y contratistas. Información que se encuentra alojada en los equipos de cómputo.

Bases de Datos:

Las bases de datos son el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, la Organización cuenta con la base de datos Oracle en su versión 11g.

Archivos de Restauración del Sistema:

Los archivos de restauración son la copia de las unidades necesarias para que se ejecute el Sistema Operativo, son la herramienta para recuperar el Sistema Operativo de un error grave o restaurar el equipo si la unidad de disco duro o el equipo dejan de funcionar.

Esquema de Backups

Las copias de seguridad de la empresa se realizan de la siguiente manera:

Copias de seguridad de equipos en LAN

Cada empleado de la Organización cuenta con un correo empresarial adquirido en la Suite de Google, cada uno de estos cuenta con 30GB de espacio de almacenamiento en Drive. La política de la empresa es hacer uso de este recurso para que cada empleado ubique los archivos considerados como críticos para la labor que desarrolla en la Organización dentro de este drive. De esta manera se protegen la información ante posibles desastres que puedan afectarla, esta labor es responsabilidad de cada persona, siendo el área de Sistemas de la empresa la encargada de brindar la capacitación y los mecanismos técnicos correspondientes para que el trabajador realice esta tarea.

Copias de seguridad de Servidores

De manera diaria y en horario especial en donde no hay usuarios conectados a los mismos, los servidores realizan una copia de seguridad de su configuración y datos de manera automática, estos backups son almacenados en un disco externo compartido desde un servidor NAS. Existe un documento adicional que describe este proceso detalladamente llamado PROCEDIMIENTO DE BACKUPS.

Copia de seguridad de la página web de la empresa

La página web de la empresa se maneja en un servidor dedicado contratado para su almacenamiento, a su vez, cuenta con un servidor espejo que respalda en tiempo real toda la información. Adicional a este esquema un tercero especializado, encargado del manejo de la página ha programado backups completos de manera diaria y se almacenan en dichos servidores. Para contar con una copia local el Analista de sistemas se encargará de descargar el backup correspondiente con una periodicidad de 8 días y de almacenarlo en los discos externos pertenecientes a la Organización para su respaldo.

Backup de la Base de datos ORACLE

La base de datos Oracle almacenada en el servidor será respaldada de manera diaria, de manera manual por parte del Analista de sistemas utilizando el software ORACLE SQL DEVELOPER para exportar los diferentes esquemas, tablas, vistas y configuraciones que hagan parte de la misma y que son necesarias para su correcto funcionamiento. El archivo .SQL generado será etiquetado con la fecha del respaldo para su identificación y será almacenado en los discos duros externos correspondientes. El proceso se detalla de manera completa en el PROCEDIMIENTO DE BACKUPS.

Respaldo de las copias de seguridad

Existe un disco duro de 8TB adicional, el cual se almacena en la caja fuerte de la oficina del Director Administrativo y financiero y está bajo su responsabilidad, éste recurso será conectado cada dos (2) días al equipo del Analista de Sistemas y su funcionalidad es la de respaldar las copias de seguridad que se generan diariamente en el disco principal conectado al servidor NAS, para esta labor su contenido se actualizará para crear un disco idéntico que pueda servir como soporte en caso de que daño o pérdida del disco principal.
Igualmente se cuenta con un espacio de almacenamiento en Nube de 8TB para respaldar los discos correspondientes en una tercera opción.

Periodicidad

Lo servidores ejecutan su respaldo a las 07:00 p.m. de manera diaria y automática.
El Servidor correspondiente a la aplicación CGUNO, contabilidad usada anteriormente en la empresa, realiza sus copias de seguridad a las 12:40 p.m. de manera automática.
La actualización entre discos duros externos se realiza de manera manual, cada dos días, los lunes, miércoles y viernes en horas de la tarde. Esta labor es responsabilidad única del Analista de Sistemas.

Control de versiones

Todas las copias de seguridad poseen etiquetas que permiten definir el tipo de respaldo realizado y la fecha y hora del proceso.

Control de los Backups

Los Backups permanecen en los discos duros externos durante un periodo de 2 meses, después de este tiempo serán eliminados para poder contar con el espacio en disco que ocupan.

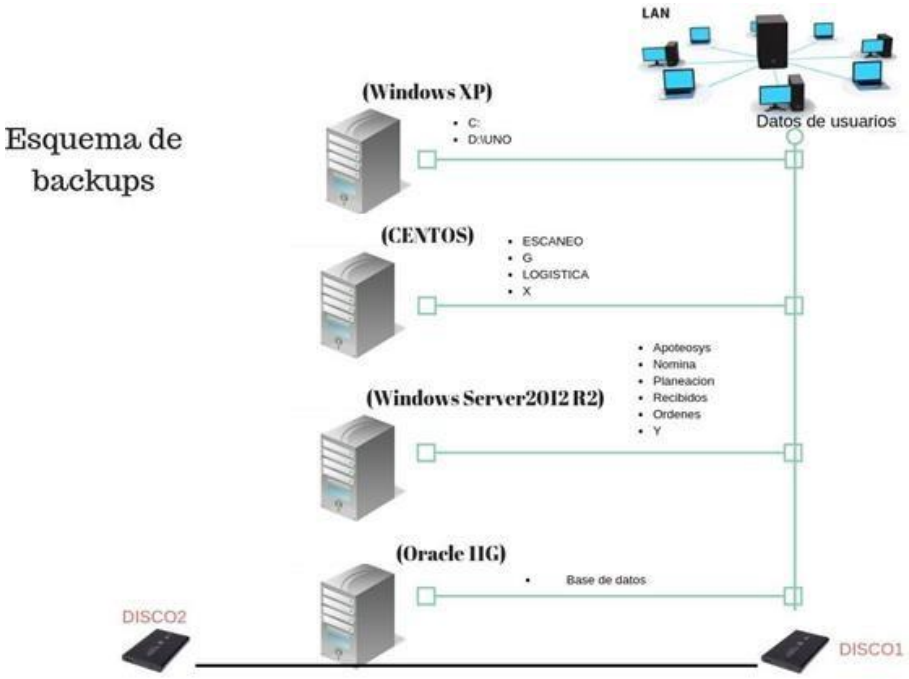
- Tipos de Backup

Las copias de seguridad se realizarán bajo el método de backup completo y backup diferencial.

Backup completo: se hace un respaldo completo de todos archivos del equipo. Este abarca el 100% de los datos.

Backup diferencial: La copia diferencial únicamente copia los archivos y directorios que han sido creados y/o modificados desde la última copia completa

Esquema de Backups



Integridad de los Backups

Cada Backup de cada servidor es un grupo de archivos comprimido en formato ZIP, protegido por contraseña. Para determinar la integridad de cada uno de ellos se procederá a abrirlos y verificar si contienen información, si ésta es correcta y si es posible abrir algunos archivos contenidos (la muestra depende de la cantidad total de archivos del Backup), los cuales se escogerán aleatoriamente.

Cifrado de los Backups

Los respaldos contarán con un cifrado AES256 bits que es uno de los algoritmos de cifrado más utilizados y seguros actualmente disponibles, protegidos ante accesos no autorizados mediante una contraseña fuerte que cumpla con los estándares de manejo de passwords seguros existentes en el momento, como manejo de mayúsculas, minúsculas, números y alfanuméricos.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SITIO WEB

El sitio web de la empresa es manejado mediante un tercero contratado, quien se encarga del manejo de los contenidos aprobados por la Gerencia.

Aceptación de Términos

Se presume que cuando un usuario accede al sitio web de la Organización lo hace bajo su total responsabilidad y que, por tanto, acepta plenamente y sin reservas el contenido de los siguientes términos y condiciones de uso del sitio web de la entidad.

Esta declaración de uso adecuado de la información está sujeta a los términos y condiciones de la página web de la empresa, con lo cual constituye un acuerdo legal entre el usuario y la página.

Si el usuario utiliza los servicios de la página web, significa que ha leído, entendido y aceptado los términos expuestos. Si no está de acuerdo con ellos, tiene la opción de no proporcionar ninguna información personal, o no utilizar el servicio de la página.

Condiciones generales respecto al contenido del sitio web

La Organización se reserva, en todos los sentidos, el derecho de actualizar y modificar en cualquier momento y, de cualquier forma, de manera unilateral y sin previo aviso, las presentes condiciones de uso y los contenidos de la página web.

El sitio web tiene por finalidad brindar al usuario todo tipo de información relacionada con la empresa, sus eventos y el desarrollo de las actividades relacionadas con su razón social. La información contenida en esta página web, está redactada de forma breve, sencilla y clara, en formato de contenidos para web. La organización procurará que la información satisfaga las necesidades de los usuarios.

El sitio web puede tener enlaces a otros sitios de interés o a documentos localizados en otras páginas web de propiedad de otras entidades, personas u organizaciones diferentes a la Organización. En estos casos el usuario deberá someterse a las condiciones de uso y a la política de privacidad de las respectivas páginas web.

La Organización no se hace responsable respecto a la información que se halle fuera de este sitio web y no sea gestionada directamente por el administrador del sitio.

Los vínculos (links) que aparecen en el sitio web tienen como propósito informar al usuario sobre la existencia de otras fuentes susceptibles de ampliar los contenidos que ofrece la página web o que guardan relación con ellos.

El establecimiento de un vínculo (link) con el sitio web de otra empresa, entidad o programa no implica necesariamente la existencia de relaciones entre la Organización y el propietario del sitio o página web vinculada, ni la aceptación o aprobación por parte de ella y de sus contenidos o servicios.

POLITICA DE REDES SOCIALES Y MENSAJERIA

La información que se publique o divulgue por cualquier medio de Internet, de cualquier empleado, contratista o colaborador de la Organización que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instagram, etc, se considera fuera del alcance de este manual y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado. Toda información distribuida en las redes sociales que sea originada por la entidad debe ser autorizada por los jefes de área para ser socializadas y con un vocabulario institucional.

11. CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

Todo el personal de la Organización es responsable de conocer y asegurar la implementación de las políticas de seguridad informática dentro de sus áreas de responsabilidad, así como del cumplimiento de las políticas por parte de su equipo de trabajo.
El presente documento se aprueba y autoriza por las partes involucradas.

Elaborado por: Revisado por:

FERNANDO MUÑOZ BOJORGE	**ELIECER MARTINEZ**
Analista de Sistemas.	Director Administrativo y Financiero.