DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE TECNOLOGÍA DE LA EMPRESA BAKER TILLY COLOMBIA LTDA DE LA CIUDAD DE BOGOTÁ, BAJO LA NORMA ISO 27001:2013

RONALD ALEJANDRO GONZÁLEZ GARÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA
2016

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE TECNOLOGÍA DE LA EMPRESA BAKER TILLY COLOMBIA LTDA DE LA CIUDAD DE BOGOTÁ, BAJO LA NORMA ISO 27001:2013

RONALD ALEJANDRO GONZÁLEZ GARÍA

Monografía para optar el título de
Especialista en Seguridad Informática

Asesor
Esp. Ing. Freddy Enrique Acosta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TUNJA
2016

Nota De Aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Tunja, 28 de noviembre de 2016

DEDICATORIA

A Dios, que es mi guía en todo momento, siempre está a mi lado guiándome por el camino de la vida, fortaleciendo cada uno de mis pasos día a día para salir adelante.

A mi Mamá Dora María, por brindarme en todo momento el apoyo que necesito para salir adelante y esos valores que me hacen único en mi forma de ser.

A mi Hermana Alexandra María González García, que siempre me apoya y ayuda en todo los momentos de mi vida.

A mi esposa Yendy Katherine que inspira mi vida con solo mirarla a sus hermosos ojos y a la bebe más hermosa, dulce y tierna que con su sonrisa irradia felicidad Angell Salomé.

Ronald Alejandro

AGRADECIMIENTOS

Ronald Alejandro expresa sus agradecimientos a:

Esp. Ing. Arturo Erazo, tutor de los cursos Proyecto de Grado I y II por enseñanzas y orientación en la ejecución del Anteproyecto Diseño Del Sistema De Gestión De Seguridad De La Información (S.G.S.I) Para El Área De Tecnología De La Empresa Baker Tilly Colombia Ltda. de la ciudad de Bogotá - Bajo La Norma ISO 27001:2013.

Al Esp. Ing. Freddy Enrique Acosta, asesor del proyecto de grado por su apoyo y confianza en mi trabajo y su capacidad para guiar mis ideas ha sido un aporte invaluable, las ideas propias, siempre enmarcadas en su orientación y rigurosidad, han sido la clave del buen trabajo que hemos realizado juntos, el cual no se puede concebir sin su siempre oportuna participación. Le agradezco también el haberme facilitado siempre los medios suficientes para llevar a cabo todas las actividades propuestas durante el desarrollo de este trabajo de grado.

Al Ingeniero Carlos Vázquez – Gerente de Tecnología de la Empresa Baker Tilly Colombia por permitirme llevar a cabo el diseño de un SGSI para dicha empresa y brindarme la información suficiente para realizar este trabajo.

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

AMENAZA: Es el potencial que un intruso o evento explote una vulnerabilidad específica. Es cualquier probabilidad que pueda ocasionar un resultado indeseable para la organización o para un activo en específico. Son acciones que puedan causar daño, destrucción, alteración, pérdida o relevancia de activos que podrían impedir su acceso o prevenir su mantenimiento[1].

ACCIÓN CORRECTIVA: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección[2].

ACCIÓN PREVENTIVA: La organización debe mejorar de forma continua la eficacia del SGSI a través del uso de la Política de Seguridad de la Información, Objetivos de Seguridad de la Información, resultados de auditorías, análisis de eventos monitorizados, acciones correctivas y preventivas y la revisión por la dirección[3].

ACEPTACIÓN DEL RIESGO: Decisión informada de asumir un riesgo concreto[4].

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización[5].

AUDITORÍA: proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría[6].

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados[7].

---

[1] DORIA, Andrés. Riesgos y Control Informático. [online]. Marzo 2014. Disponible en Internet: <http://itriesgosycontrol.blogspot.com.co/>.

[2] NEIRA, Agustín y SPOHR, Javier. ISO27000.es. "International Organization For Standardization Iso27000". [online] [citado 28 de febrero 2012]. Glosario Disponible en internet: < http://www.iso27000.es/glosario.html>

[3] BORGHELLO, Cristian, Mejora continua de un SGSI según ISO 27001. 19 de noviembre de 2006. [online]. Disponible en Internet: http://blog.segu-info.com.ar/2006/11/mejora-continua-de-un-sgsi-segun-iso.html.

[4] Ministerio de Trabajo, Proceso Administración del SIG Procedimiento Gestión de Riesgos. Versión 3. 02 de diciembre de 2014 [online]. Disponible en internet:< archivo.ucr.ac.cr/docum/ISOEIC27000.pdf>. Pág. 1.

[5] PACHECO, J.C. Especialización en Auditoria de Sistemas y Seguridad de la Información ISO/IEC-27001 ISO/IEC – 27002. 26 de agosto de 2011. [online]. Disponible en Internet:< https://www.academia.edu/5868574/Seguridad_de_la_informaci%C3%B3n-sesion_1-v1>.Pág. 10.

[6] INCONTEC. NORMA TÉCNICA COLOMBIANA NTC-ISO 19011. Directrices para la auditoria de los Sistemas de gestión de la calidad y/o Ambiental. [online]. Disponible en Internet:< http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO19011.pdf> Pág. 2.

[7] INCOTEC. Norma Técnica NTC-ISO/IEC Colombiana 27001. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS. [online]. Disponible en Internet:< http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf>. Pág. 2.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo[8].

CONTROL CORRECTIVO: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige[9]**.**

CONTROL PREVENTIVO: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse[10].

CORRECCIÓN: Acción para eliminar una no conformidad detectada[11].

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[12]**.**

GESTIÓN DE RIESGOS: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos[13].

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información[14]**.**

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.[15]

---

[8] CEEI. Centro Europeo de Empresas e Innovación. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA SEGURIDAD DE LA INFORMACIÓN, ISO 27001. [online]. Disponible en Internet: < http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf> Pág. 36.

[9] Ibíd. Pág. 37

[10] Ibíd. Pág. 37

[11] Norma Internacional ISO 9000:2015. Sistemas de gestión de la calidad —Fundamentos y vocabulario. [online]. Disponible en internet:< www.aj.gob.bo/sitios/SitioWebAJ/.../Norma%20ISO%209000%20(2015).pdf>. Pág. 31.

[12] INCOTEC. Norma Técnica NTC-ISO/IEC Colombiana 27001, Ibíd. Pág.2

[13] GONZALEZ, Hugo, ISO 9001:2015. ENFOQUE BASADO EN RIESGOS, 10 de agosto de 2015. [online]. Disponible en Internet: < https://calidadgestion.wordpress.com/2015/08/10/iso-90012015-enfoque-basado-en-riesgos/>.

[14] INCOTEC. Norma Técnica NTC-ISO/IEC Colombiana 27001, Ibíd. Pág.11

[15] NEIRA, Agustín y SPOHR, Javier. Ibíd.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares[16].

NO REPUDIO: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente[17].

PDCA (Plan-Do-Check-Act): Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI)[18].

PLAN DE CONTINUIDAD DEL NEGOCIO: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro[19].

PLAN DE TRATAMIENTO DE RIESGOS: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.[20]

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.[21].

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas.[22]

---

[16] PRESIDENCIA DE LA REPUBLICA, Manual de la Política de Seguridad para las Tecnologías de la Información y las Comunicaciones – TICS. Versión 5. Diciembre 2014. [online]. Disponible en Internet:< http://wp.presidencia.gov.co/sitios/dapre/sigepre/manuales/M-TI-01%20Manual%20general%20Sistema%20de%20Seguridad%20de%20la%20Informacion.pdf>. Pág. 9.

[17] Ibíd. Pág. 9.

[18] Ibíd. Pág. 10.

[19] MINTIC, Modelo de Seguridad y Privacidad de la Información. [online]. Disponible en Internet: < http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf>. Pág. 11.

[20] NEIRA, Agustín y SPOHR, Javier .Ibíd.

[21] INCOTEC. Norma Técnica NTC-ISO/IEC Colombiana 27001, Ibíd. Pág.3

[22] NEIRA, Agustín y SPOHR, Javier. Ibíd.

RESUMEN

En la actualidad el uso de la tecnología en todos los aspectos ha hecho que la seguridad de la información no sea sólo un problema de las grandes empresas, sino que ahora esta problemática también acoge a las pequeñas y medianas empresas, ya que muchas de estas empresas inconscientemente quedan vulnerables ante la falta de controles que les permita proteger de intrusiones o ataques no deseados su más valioso activo que es la información.

Aquí se propone el diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de tecnología de la empresa Baker Tilly Colombia Ltda. de la ciudad de Bogotá, bajo la norma ISO 27001:2013, donde se provee prácticas apropiadas para el desarrollo e implementación de cada uno de sus componentes, estableciendo las fases, documentación y procedimientos requeridos y exigidos en el estándar para continuar con el diseño del SGSI de una manera adecuada.

Por lo tanto, se debe realizar un análisis de los riesgos, vulnerabilidades y amenazas de manera cualitativa y cuantitativo de la empresas, puesto que muchas de las compañías posee recursos económicos muy limitados para llevar a cabo un sistema de seguridad robusto, por esta razón se debe implementar un mecanismo que satisfaga las necesidades de las pequeñas y medianas empresas (Pyme), donde cada uno de los componentes informáticos juegue un papel importante a la hora de permanecer en el mercado de estas compañías.

Por consiguiente, se podrá proteger el recurso más importante de la empresa que es, sus datos y/o información, donde el diseño de un Sistema de Gestión de Seguridad de la información (SGSI) proporcione una metodología sencilla y completa que permita proteger los activos que posee, donde se establezcan procesos de restauración y mitigación de riesgos entre otros y adoptando las medidas correctivas y preventivas que sean necesarias.

Finalmente, al momento de establecer un SGSI, se debe detallar cada uno de los componentes que se encuentran asociados permitiendo tener un control sobre los activos tecnológicos que la empresa posee, permitiendo así al ciclo Deming detallar el proceso de mejora continua proporcionando una realimentación constate de cada uno de los procesos y que estos perduren en el tiempo.

Palabras Claves

ISO 27001:2013, PYME, Sistema de Gestión de Seguridad de la Información, vulnerabilidades, amenazas.

ABSTRACT

Currently the use of technology in all aspects has made information security is not just a problem of big business, but now this problem is also home to small and medium-sized enterprises, as many of these companies unconsciously they remain vulnerable to the lack of controls that allow them to protect unwanted intrusions or attacks your most valuable asset is information.

Here the design of a management system of information security (ISMS) for the area technology company Baker Tilly Colombia Ltda is proposed for the city of Bogotá, under ISO 27001. 2013, where practices is provided appropriate development and implementation of each of its components, setting the stage, and required documentation and procedures required by the standard to proceed with the design of the ISMS in an appropriate manner.

Therefore, you must perform an analysis of risks, threats and vulnerabilities qualitative and quantitative fashion companies, since many of the companies has very limited financial resources to carry out a security system robust, for this reason should implement a mechanism that meets the needs of small and medium enterprises (SMEs), where each of the computer components play an important role to stay in the market for these companies.

Therefore, it can protect the most important asset of the company that is, data and / or information, where the design of a Management System Information Security (ISMS) provides a simple and comprehensive methodology to protect assets it has, where restoration processes and risk mitigation including establishing and adopting corrective and preventive measures necessary.

Finally, when establishing an ISMS, should detail each of the components that are associated allowing you to have control over the technology assets that the company owns, allowing the cycle Deming detail the process of continuous improvement by providing a feedback constant of each of the processes and these last in time.

Keywords

ISO 27001: 2013, SME Management System Information Security, vulnerabilities, threats.

INTRODUCCIÓN

Desde hace ya algunos años la información está definida como el activo más valioso de una compañía (los costos derivados de pérdida de seguridad no son sólo costos económicos directos, sino que también afectan a la imagen de la empresa), por lo que, cada vez más, la seguridad de la información forma parte de los objetivos de las organizaciones y; sin embargo, y a pesar de esa concienciación generalizada, muchas compañías no se enfrentan a este aspecto con la globalidad con la que debiera tratarse[23].

No obstante, es un hecho indiscutible que los procesos de negocio son soportados y/o gestionados por sistemas de información en todas las organizaciones apoyando la toma de decisiones, además muchas veces la misma información y el acceso a ella, hace que el producto o servicio se intercambia como objeto del negocio.

Por lo tanto, la Seguridad de la Información en la actualidad no puede ser establecida como el resultado de un accionar defensivo o reactivo que permita salvaguardar los activos de una organización; por ende, toda empresa que gestione adecuadamente la seguridad de la información, estará dando cumplimiento a sus obligaciones y generando confianza entre sus clientes y posibles inversionistas.

Por consiguiente, la parte más importante siempre tiene que ver con la capacitación que se brinde a nuestros funcionarios, porque así yo tenga una gran seguridad informática, la seguridad de la información depende más de las personas que de las máquinas[24].

Finalmente, la información es uno de los principales activos para todas las organizaciones bien sea privada o públicas que deben protegerse a través de una implementación de un Sistema de Seguridad de la Información (SGSI), permitiendo mitigar muchos de los problemas que se enfrentan las organizaciones cuando posee alguna vulnerabilidad en su sistema de información.

[23] RECIO, Mª Jesús. De la seguridad informática a la seguridad de la información [online], Julio-Septiembre 2012. Disponible en Internet:<http://www.aec.es/c/document_library/get_file?uuid=e25028ca-cb3b-4ffd-ada0-4ce2efa86f80&groupId=10128>

[24] Sitio Web Ministerio de Tecnologías de la Información y las Comunicaciones.[online], Disponible en internet: <http://www.mintic.gov.co/gestionti/615/w3-article-5482.html>

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización. En la actualidad dado el incremento de la utilización del internet, la evolución de la tecnología y la falta de conocimiento para mitigar riesgos de ataques, ha generado innumerables amenazas que aprovechan vulnerabilidades de las empresas para materializar riesgos y generar un impacto negativo en las organizaciones, ocasionando que se pierdan alguna o todas las características que debe preservar la información: disponibilidad, integridad, confidencialidad[25].

Debido a lo anterior, se nota la necesidad de analizar qué grado de vulnerabilidad pueden llegar a tener las empresas que usan el internet dentro de sus procesos organizacionales, con el propósito de identificar que falencias se tienen a la hora de protegerse contra posibles ataques e infiltraciones en sus sistemas de información[26].

Cuando se habla de seguridad de la información, la mayoría de las organizaciones cometen errores que suelen ser la causa de la mayoría de los incidentes informáticos, pensando que la información que tienen no es importante para ningún individuo o tercero, por lo tanto dejan a un lado la gestión de los datos, y siempre tienen la mentalidad de reparar y no mantener, es por esto que en la mayorías de las compañías la cultura de seguridad de la información es poca.

Por lo tanto, el área de Tecnología de la empresa Baker Tilly Colombia Ltda, entre sus objetivos tiene el de garantizar la continua del negocio en cualquier evento que se presente, así como el de proporcionar soporte y apoyo a todas las diferentes áreas con que cuenta la empresa.

---

[25] LADINO, Marta; VILLA Paula; y LOPEZ Ana Mª. Fundamentos de ISO 27001 y su aplicación en las empresas [online]. Vol. 1, Nº. 47, 2011, págs. 334-339, ISSN 0122-1701. Disponible en Internet:< http://dialnet.unirioja.es/servlet/articulo;jsessionid=9C775AB95C346646A580B4D771E9B3DB.dialnet02?codigo=4527565> Pág. 334

[26] RODAS, Alexa. Análisis Y Especificaciones de requerimientos de Seguridad Informática en las Empresas. [online][citado en abril de 2012]Disponible en Internet:< http://bibliotecadigital.usbcali.edu.co/jspui/bitstream/10819/1565/1/Analisis_Especificaciones_Requerimientos_Rodas_2013.pdf>. Pág. 3

No obstante, la infraestructura tecnológica que tiene Baker Tilly Colombia Ltda, se encuentra desactualizada debido a que muchos de los equipos no se encuentran en el Directorio Activo (DA), por tal motivo existe la posibilidad de incumplimiento de políticas de seguridad de acceso, como por ejemplo el cambio de clave periódico, la utilización de contraseñas inseguras, la ejecución de actividades no autorizadas, la duplicidad de usuarios, entre otras, a esto se le puede adicionar que los usuarios puedan romper la seguridad y acceder a datos confidenciales, lo que implicaría el robo de información, o su la alteración.

Asimismo, al no contar con políticas para el manejo de dispositivos de almacenamiento externo, restricciones de navegación en internet, controles de acceso de usuarios y en general una infraestructura de tecnología actualizada dificulta establecer responsabilidades en caso de requerirse por cometimiento de errores graves, accidentales o intencionales.

1.2 FORMULACIÓN DEL PROBLEMA

¿Al diseñar un sistema de seguridad de la información basado en la norma ISO 27001:2013, se pueden identificar los riesgos que actualmente se tienen dentro de la Empresa BAKER TILLY COLOMBIA LTDA, lo que permitirá gestionar y tratar el riesgo asociado al uso de la información?

1.3 OBJETIVOS

1.3.1 Objetivo General

Diseñar un sistema de gestión de seguridad de la información (SGSI) para el área de tecnología de la empresa BAKER TILLY COLOMBIA Ltda de la ciudad de Bogotá, bajo la norma ISO 27001:2013.

1.3.2 Objetivos Específicos

- Revisar la situación actual de la empresa Baker Tilly Colombia Ltda, que permita conocer los procesos y procedimientos que allí se utilizan.

- Clasificar los activos de la información de la empresa Baker Tilly Colombia Ltda, utilizando la metodología MAGERIT.

- Plantear controles con base a la norma ISO 27001:2013, que permitan administrar el funcionamiento de un sistema de detección de intrusos dentro de un Sistema de gestión de seguridad de la información.

- Formular las medidas necesarias y selección de controles para conocer, prevenir, impedir, reducir o controlar los riesgos estudiados.

1.4 JUSTIFICACIÓN

En la actualidad toda organización tiene objetivos, por lo general relacionados con el mercado y los negocios, y requiere que desde los procesos de operaciones hasta las políticas de uso de recursos, sean definidos a un nivel general, de manera confiable. Si bien gran parte de la información se vincula con computadoras y redes, hay otra parte que no se representa en forma de bits, sino por ejemplo en papeles, en la memoria de las personas, en el conocimiento y experiencia de la organización misma, en la madurez de sus procesos, etc. En ambos casos, la información debe ser protegida de manera diferente, y aquí entra en juego un Sistema de Gestión de Seguridad de la Información (SGSI)[27].

En muchas organizaciones creen que implementar un Sistema de Gestión de Seguridad de la Información (SGSI) es demasiado esfuerzo, y está solo destinado a grandes corporaciones, lo que a veces termina derivando en un manejo caótico o muy minimalista de la administración de la seguridad. Sin embargo es posible en algunos casos aplicar unos pocos principios, en lugar de un SGSI completo, para conseguir mejoras significativas. Para esto será necesario olvidar las formalidades del cumplimiento de una norma, pero sin dejar de seguir sus lineamientos principales[28].

Por consiguiente, un SGSI permite obtener una visión global del estado de los sistemas de información sin caer en detalles técnicos, además de poder observar las medidas de seguridad aplicadas y los resultados obtenidos, para poder con todos estos elementos tomar mejores decisiones estratégicas. Otro punto

[27] PACHECO, Federico, La importancia de un SGSI [online]. 10 de septiembre de 2010, Disponible en internet< http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/>

[28] PACHECO, Federico, La importancia de un SGSI. Ibíd.

importante es que un SGSI debe estar documentado y ser conocido a distintos niveles por todo el personal, y estar incluido en un proceso global que permita la mejora continua[29].

Al implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) en la organización se deben tener en cuenta algunas recomendaciones como son:

- Conocimiento de los altos directivos de lo que puede suceder si no se implementa el sistema de gestión de seguridad de la información. A la alta dirección debe hablársele en términos del negocio, es decir, demostrar las pérdidas económicas, que pueden tenerse en caso de no contar con un SGSI. De esta tarea puede encargarse el jefe del área de sistemas de la organización.

- Se debe realizar una identificación de los activos relacionados con la información, desde los equipos que la soportan hasta las aplicaciones para su uso y la información misma. Después identificar los más críticos para la compañía y con base en estos empezar la tarea de diseño e implementación del SGSI.

- Cuando las directivas de la organización tiene claro la necesidad de implantar un SGSI y han identificado los componentes críticos entre los activos, debe fomentarse una cultura de seguridad con todos los miembros de la organización para minimizar los riesgos por desconocimiento. Se debe tener en cuenta que plasmar en un papel algunas normas de seguridad no crean una cultura, es un proceso que debe realizarse de manera constante, ya que para generar cultura es necesario crear conciencia del cambio[30].

El diseño de un Sistema de Gestión de Seguridad Informática (SGSI) trae como resultado un gran beneficio para la organización, donde la implementación de elementos para la seguridad de la información en la empresa genera una gran confianza entre los usuarios tanto internos como externos, permitiendo ser más competitivos en el mercado hoy en día, además debemos considerar que la información es el activo valioso de la empresa, y que se debe propender porque esta mantenga a los largo del tiempo su integridad, confidencialidad y disponibilidad.

[29] PACHECO, Federico, La importancia de un SGSI. Ibíd.

[30] LADINO, Marta; VILLA Paula; y LOPEZ Ana Mª. Fundamentos de ISO 27001 y su aplicación en las empresas [online]. Vol. 1, Nº. 47, 2011, págs. 334-339, ISSN 0122-1701. Disponible en Internet:< http://dialnet.unirioja.es/servlet/articulo;jsessionid=9C775AB95C346646A580B4D771E9B3DB.dialnet02?codigo=4527565>

Por lo anterior es importante tener en claro que para proteger la organización de los distintos riesgos y amenazas que tienen que afrontar día a día, es necesario tener una visión clara con lo que cuenta la empresa, conocer los distintos procedimientos que son aplicados para la mitigación de los riesgos y las amenazas, lo que conlleva a generar nuevos procedimiento o mejorar los actuales e implementar controles de seguridad basados en la evaluación de riegos que nos permita tener una medición de la eficacia.

Por lo tanto la seguridad de la información dejará de ser una acción común dentro de la organización y pasara a ser un trabajo apoyado por la alta gerencia, lo que conformara un conjunto de actividades sistemáticas y controladas, con el objeto de crear una cultura organizacional en la seguridad, siendo todos los empleados los protagonistas y responsables de estas acciones.

1.5 ALCANCES Y LIMITACIONES

1.5.1 Alcance

El proyecto es enmarcado en la línea Sistema de Gestión de Seguridad de la Información (SGSI) y lo que pretende es el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para el área de tecnología de la empresa Baker Tilly Colombia Ltda, de la ciudad de Bogotá, bajo la norma ISO 27001:2013.

1.5.2 Limitaciones

Es de resaltar que el desarrollo de la presente monografía, no enmarca temas como los que se definen a continuación:

- La implementación, revisión, mantenimiento y mejora del sistema de gestión de seguridad de la Información (SGSI).

- Elaboración de políticas de seguridad.

1.6 DISEÑO METODOLÓGICO

1.6.1 Tipo de investigación descriptiva.

Consiste en identificar las características del evento en estudio. Los perfiles, las taxonomías, los estudios historiográficos, los estudios anatómicos en medicina, los estudios topográficos, por ejemplo, son investigaciones descriptivas[31].

1.6.2 Tipo de investigación explicativa

Es aquella que busca comprender las relaciones entre distintos eventos, se interesa fundamentalmente por el "por qué" y el "cómo" de los fenómenos. Es este tipo de investigación el que genera las teorías y los modelos que a la larga conducen a las revoluciones científicas. La teoría de la relatividad de Einstein, la teoría psicoanalítica de Freud, la teoría de la evolución de Darwin, la teoría de la gravedad de Newton, son algunos ejemplos del producto de la investigación explicativa[32].

1.6.3 Tipo de investigación proyectiva.

Tiene como objetivo diseñar o crear propuestas dirigidas a resolver determinadas situaciones. Los proyectos de arquitectura e ingeniería, el diseño de maquinarias, la creación de programas de intervención social, el diseño de programas de estudio, los inventos, la elaboración de programas informáticos, etc., son ejemplos de investigación proyectiva. Este tipo de investigación potencia el desarrollo tecnológico[33].

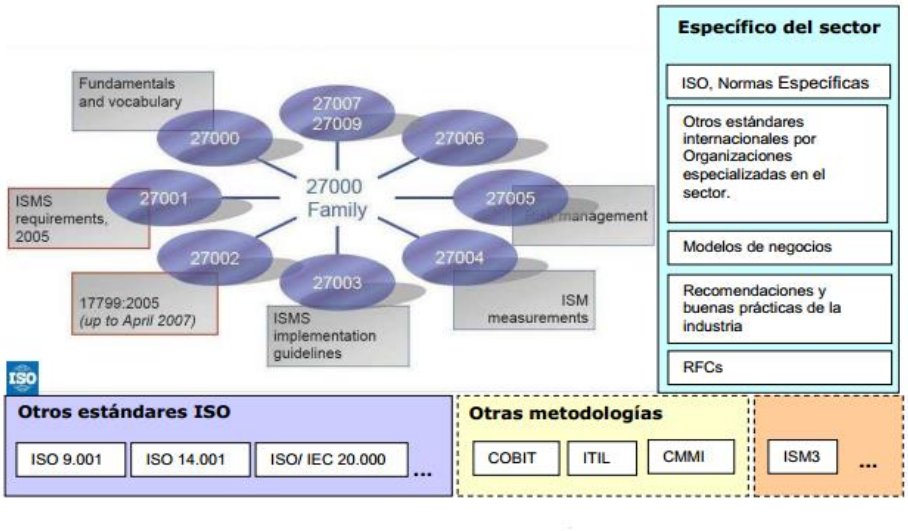
[31] HURTADO DE BECERRA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000. Pág. 48.
[32] Ibíd., Pág. 48, 49.
[33] Ibíd., Pág. 59.

2. MARCO DE REFERENCIA

2.1 MARCO TEORICO

En la Figura 1 se ilustra el marco normativo de los diferentes estándares que, de una u otra manera, están vinculados a un Sistema de Gestión de la Seguridad de la Información, en este se ven representados estándares internacionales de diferente naturaleza y con diferente alcance. Algunos de ellos, como por ejemplo la serie ISO/IEC 27.000 e ISM3, son específicos de la gestión de seguridad de la información, generales y aplicables a cualquier sector de actividad. Pero también deben tenerse en cuenta otros estándares y recomendaciones que son específicas del sector[34].

Figura 1. Contexto Normativo de un SGSI



Fuente: Alan Bryden, COPANT Seminar on Security Standards, La Paz, 25 de abril de 2006. Pág. 33. Disponible en internet <http://www.iso.org/iso/livelinkgetfile?llNodeId=21657&llVolId=-2000> (marzo de 2012).

Un SGSI, como sistema de gestión que es, de una disciplina específica como lo es la seguridad de la información, debe relacionarse con otros sistemas de gestión, por ejemplo de Gestión de Calidad entre otros. Es así que también deben considerarse en el contexto, estos otros sistemas y los respectivos estándares

[34] PALLAS, Gustavo M. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. [online][citado en marzo de 2012]. Disponible en internet: <https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf> Pág 6.

metodológicos en los que se apoyan[35].

2.1.1 Serie ISO/IEC 27.000[36]

Las normas de la familia ISO 27.000, destacando fundamentalmente la ISO/IEC 27.001 e ISO/IEC 27.002, tienen como principales objetivos:

- Establecer un marco metodológico para un SGSI.
- La adopción de controles proporcionales a los riesgos percibidos.
- La documentación de políticas, procedimientos, controles y tratamiento de riegos.
- Identificación y asignación de responsabilidades al nivel adecuado.
- Formalización, seguimiento y revisión de los controles y riesgos, de forma sistemática (periódica) y metodológica.
- Generación y preservación de evidencias.
- Tratamiento de los incidentes de seguridad.
- Revisión y mejora continúa del SGSI.
- Gestión de Riesgos
- Uso de métricas para evaluar efectividad y eficiencia de los controles y del propio SGSI.

Los lineamientos metodológicos y los requerimientos de la norma ISO/IEC 27.001 son propuestos bajo el enfoque metodológico del Ciclo de Deming: Planificar – Hacer – Verificar – Actuar (PHVA)[37].

Entre ellas existen normas que son básicamente una especificación de Requerimientos como la ISO/IEC 27.001 e ISO/IEC 27006. Otras son guías de implementación o lineamientos guía que son soporte del ciclo PHVA para los sistemas de gestión de la seguridad de la información, como la ISO/IEC 27003 o ISO/IEC 27.005.

A continuación, se describen brevemente los más relevantes para este trabajo[38]:

- "***ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary"***, provee información introductoria a seguridad de la información y a la gestión de la seguridad de la información, el estado y la relación de las normas de la familia de estándares para un SGSI.

---

[35] Ibíd,. Pág. 7.
[36] NEIRA, Agustín y SPOHR, Javier. ISO27000.es. "Sistema de Gestión de la Seguridad de la Información". [online] [citado febrero 2012].Disponible en internet: http://www.iso27000.es/doc_sgsi_all.htm
[37] O la correspondiente sigla en inglés PDCA (Plan, Do, Check, Act)
[38] SO/IEC 27000, «Information technology -Security techniques -Information security management systems - Overview and vocabulary" International Organization for Standarization (ISO),» de Information security management systems, p. [online], Disponible en internet <http://www.iso.org>.

- ***"ISO/IEC 27001:2005 - Information technology - Security techniques - Information Security Management Systems - Requirements***", es una norma que admite certificación y especifica los requerimientos para la definición, implementación, implantación, mantenimiento y mejora de un SGSI.

- ***"ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management"*** - provee una guía de implementación de los controles aplicables a la seguridad de la información. Presenta once (11) cláusulas de control de la seguridad que contienen un total de treinta y nueve (39) categorías de seguridad y por lo tanto igual número de indicaciones de Objetivos de Control, con varios Controles por cada uno de ellos. Estas cláusulas, objetivos de control y controles, son incorporados en el Anexo A de la norma ISO/IEC 27.001.

- ***"ISO/IEC 27003 - Information technology - Security techniques - Information security management system implementation guidance"*** - provee información práctica y una guía de implementación de la norma ISO/IEC 27001.

- ***"ISO/IEC 27004 - Information technology - Security techniques - Information security management measurements"*** provee una guía y consejos para el desarrollo y uso de métricas para evaluar la efectividad de un SGSI, los objetivos de control y controles utilizados para implementar y gestionar la Seguridad de la Información, de acuerdo con la norma ISO/IEC 27001.

- ***"ISO/IEC 27005:2008 - Information technology - Security techniques - Information security risk management"*** – provee una guía metodológica para la Gestión de Riesgos de una Organización, alineada con los requerimientos de la norma ISO/IEC 27001.

- ***"ISO/IEC 27006:2007 - Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems"*** – establece los requerimientos para Organismos que prestan servicios de auditoría y certificación.

- ***"ISO/IEC 27007 Information technology - Security techniques - Information security management systems - Auditor guidelines"*** - provee una guía para la realización de las auditorías de un SGSI y la competencia de los auditores, de acuerdo a la norma ISO/IEC 27001.

2.1.2 Norma ISO/IEC 27.001 y el ciclo de Deming.

La norma ISO/IEC 27.001 es un estándar que especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Especifica además los requerimientos para la implementación de controles de seguridad para las necesidades de una organización, un sector de la misma, o un proceso, según el alcance del SGSI. Establece entre otras cosas, la documentación exigida para su certificación en el caso del cumplimiento de todos los requisitos.

Sin embargo, si bien sugiere un enfoque para su cumplimiento, no establece una metodología concreta para lograr los productos y esa documentación requerida, ni especifica un flujo de trabajo (workflow) con procesos bien definidos.

Se establece un mapeo de las etapas del ciclo de Deming y los productos o entregables exigidos por la norma.

En la tabla 1, se especifican los principales procesos que indica la referida norma, mapeados con las etapas del ciclo PHVA[39].

Tabla 1 – Ciclo de Deming (PHVA) aplicado a la norma ISO/IEC 27001

Ciclo PHVA	Procesos
Planificar (***P****lan***)	• Establecer el contexto. • Alcance y Limites. • Definir Política del SGSI. • Definir Enfoque de Evaluación de Riesgos. • Identificación de riesgos. • Análisis y Evaluación de riesgos. • Evaluar alternativas para el Plan de tratamiento de riesgos. • Aceptación de riesgos. • Declaración de Aplicabilidad.
Hacer (***D****o***)	• Implementar plan de tratamiento de riesgos. • Implementar los controles seleccionados. • Definir las métricas. • Implementar programas de formación y sensibilización. • Gestionar la operación del SGSI. • Gestionar recursos. • Implementar procedimientos y controles para la gestión de incidentes de seguridad.

[39] PALLAS, Gustavo M. Op. Cit., Pág. 19

Verificar (***C**heck*)	• Ejecutar procedimientos de seguimiento y revisión de controles. • Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. • Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. • Revisión de la evaluación de riesgos periódicamente. Realizar auditorías internas. • Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad. • Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI del SGSI. • Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. • Revisión de la evaluación de riesgos periódicamente. • Realizar auditorías internas. • Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad. • Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI.
Actuar ***(Act)***	• Implementar las mejoras identificadas para el SGSI. • Implementar las acciones correctivas y preventivas pertinentes. • Comunicar acciones y mejoras a todas las partes involucradas

Fuente: PALLAS, Gustavo M. Tesis de Maestría "Metodología de Implantación de un SGSI en un grupo empresarial jerárquico". Pág. 19, [online] [citado febrero 2012].Disponible en internet: http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

Para el caso de la implantación de Sistemas de Gestión de la Seguridad informática, el ciclo PDCA es una estrategia efectiva para la organización y documentación que se requiere en este proceso. La figura 2 enseña el modelo basado en los procedimientos esenciales para un SGSI[40] (Ver figura 2).

[40] Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I. Capítulo 1 Seguridad Informática. Lección 1.5.1 Ciclo PDCA (Edward Deming). [Online] [Citado en abril 2012]. Disponible en Internet en < http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

Figura 2. Ciclo PDCA (PHVA) para la implantación de SGSI

Fuente: Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I. Capítulo 1 Seguridad Informática. Lección 1.5.1 Ciclo PDCA (Edward Deming). [Online] [Citado en abril 2012]. Disponible en Internet en < http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

2.1.2.1 Planear

En esta etapa se enmarca todo el proceso de análisis de la situación en que actualmente se encuentra la empresa respecto a los mecanismos de seguridad implementados y la normativa ISO/IEC 17799:2005, la cual se pretende implantar para evaluación y certificación. Así mismo en la etapa de planeación se organizan fases relevantes como son:

- Establecer el compromiso con los directivos de la empresa para el inicio, proceso y ejecución
- Fase de análisis de información de la organización, En esta fase se comprueba cuáles son los sistemas informáticos de hardware y los sistemas de información que actualmente utiliza la empresa para el cumplimiento de su misión u objeto social.

- Fase de evaluación del riesgo; En esta fase se evalúa los riesgos, se tratan y se seleccionan los controles a implementar[41].

2.1.2.2 Hacer

En esta etapa se implementan todos los controles necesarios de acuerdo a una previa selección en la etapa de planeación, teniendo en cuenta el tipo de empresa. También se formula y se implementa un plan de riesgo[42].

2.1.2.3 Verificar

Consiste en efectuar el control de todos los procedimientos implementados en el SGSI. En este sentido, se realizan exámenes periódicos para asegurar la eficacia del SGSI implementado, se revisan los niveles de riesgos aceptables y residuales y se realicen periódicamente auditorías internas para el SGSI[43].

2.1.2.4 Actuar

Desarrollar mejoras a los hallazgos identificadas al SGSI y validarlas, realizar las acciones correctivas y preventivas, mantener comunicación con el personal de la organización relevante[44].

El estándar ISO/IEC 27001:2013 especifica los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos empresariales generales de la organización. Es decir, explica cómo diseñar un SGSI y establecer los controles de seguridad, de acuerdo con las necesidades de una organización o de partes de la misma, pero no aclara mediante qué procedimientos se ponen en práctica. Como todo sistema de gestión, el estándar ISO/IEC 27001:2013 emplea el ciclo PDCA para el mejoramiento continuo[45].

El estándar reclama es que exista un sistema documentado (política, análisis de riesgos, procedimientos, etc.), donde la dirección colabore activamente y se

---

[41] Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I. Capítulo 1 Seguridad Informática. Lección 1.5.1 Ciclo PDCA (Edward Deming). [Online] [Citado abril 2012]. Disponible en Internet en < http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

[42] Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I Ibíd.

[43] Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I Ibíd.

[44] Universidad Nacional Abierta y A Distancia. Op. Cit.

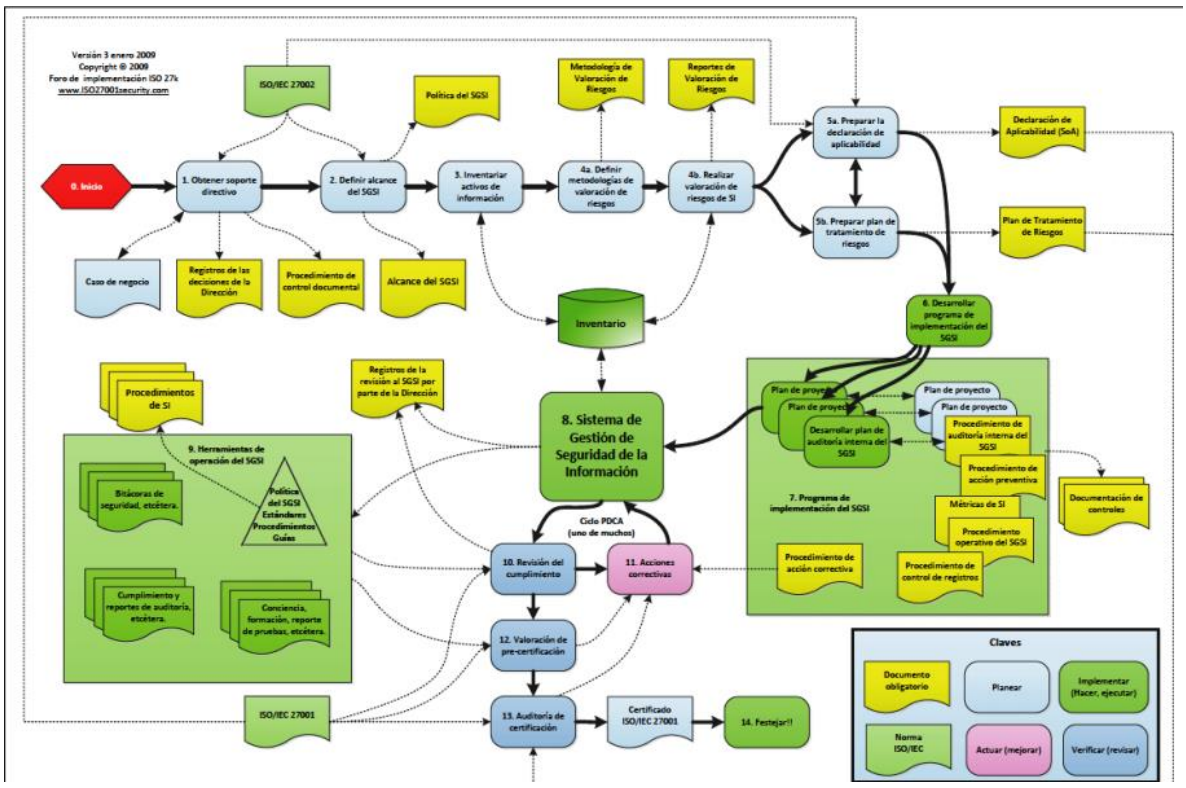
[45] GÓMEZ, L., ANDRÉS, A. Guía de Aplicación de la Norma UNE-ISO/IEC 27001 Sobre Seguridad en Sistemas de Información para PYMES. España: Asociación Española de Normalización y Certificación. 2012. p. 17

implique en el desarrollo y gestión del sistema. Se controlará el funcionamiento del sistema para que marche correctamente y la mejora sea continua, practicándose auditorías internas y revisiones del sistema para verificar que se están obteniendo los resultados esperados. Igualmente se activarán acciones encaminadas a solucionar los problemas detectados en las actividades de comprobación (auditorías y revisiones), a prevenir problemas y a mejorar aquellos asuntos que sean susceptibles de ello. El sistema documentado comprende lo siguiente:

- Políticas: Proporcionan las guías generales de actuación en cada caso.
- Procedimientos: Proporcionan las instrucciones a generar en base a una tarea o actividad.
- Registros: Son las evidencias que se generan de los actividades realizadas[46].

En la figura 3 se muestra el modelo de implementación de un SGSI bajo el estándar ISO/IEC 27001.

Figura 3. Modelo de implementación de un SGSI bajo el estándar ISO/IEC 27001.



Fuente: NEIRA, Agustín y SPOHR, Javier. ISO27000.es. "International Organization For Standardization Iso27000". [Online] Disponible en internet: < http://www.iso27001security.com/ISO27k_ISMS_implementation_and_certification_process_v3_Spanish.pdf> p. 1.

[46] GÓMEZ, L., ANDRÉS Op. Cit. Pág. 24

En Colombia, el Instituto Colombiano de Normas Técnicas (ICONTEC) adopta la norma ISO/IEC 27001:2013 por traducción bajo la referencia NTC-ISO-IEC 27001, y contiene una serie de requisitos que son indispensables para ser conformes a ella. Estos requisitos indispensables son los numerales 4, 5, 6, 7, 8, 9 y 10 que se detallan a continuación en la tabla 2[47]:

Tabla 2. Requisitos de la Norma ISO-IEC 27001:2013

NUMERAL NORMA ISO-IEC 27001:2013	DESCRIPCIÓN GENERAL
4. CONTEXTO DE LA ORGANIZACIÓN	La organización debe estar consciente de las cuestiones internas y externas que podrían influir en los resultados deseados de la seguridad de la información, así como determinar su alcance, límites y capacidad, garantizando que el SGSI cumpla los requerimientos de la norma.
5. LIDERAZGO	La alta gerencia de la organización debe liderar el proceso del SGSI verificando que se cumplan los requerimientos de la norma, garantizando los recursos, documentando las políticas y objetivos de seguridad propuestos, asignando las responsabilidades para cada una de las actividades y promoviendo el mejoramiento continuo.
6. PLANIFICACIÓN	La organización debe escoger una metodología de clasificación, análisis y evaluación de riesgos, formando criterios para establecer los controles de seguridad y así mantener los niveles de riesgo a un nivel aceptable de acuerdo a las políticas y objetivos de seguridad.
7. SOPORTE	La organización debe velar por comunicar las políticas de seguridad de la información a sus empleados y que éstos se comprometan al mejoramiento continuo del SGSI. A su vez, también se deben garantizar los recursos y la cualificación de las personas para llevar a cabo cada actividad. También se deben generar los documentos que exige la norma y que éstos tengan su nivel de clasificación.
8. OPERACIÓN	La organización debe documentar y planear los procesos para llevar a cabo las actividades, incluyendo las valoraciones de riesgos de la seguridad de la información y el plan de tratamiento de riesgos.
9. EVALUACIÓN DEL DESEMPEÑO	La organización debe velar el desempeño de la seguridad de la información y medir la eficacia del SGSI, mediante auditorías internas a intervalos planificados, con el fin de verificar si se están cumpliendo con los objetivos y políticas de seguridad así como con la norma.
10. MEJORA	La organización debe aplicar las acciones correctivas y promover un mejoramiento continuo.

[47] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: ICONTEC. 2013. p. 9.

Fuente: INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: ICONTEC. 2013. p. 9.

El estándar ISO/IEC 27001 es certificable, las organizaciones auditoras requieren una serie de documentos y registros obligatorios, los cuales se muestran en la tabla 3 que a continuación se enseña[48]:

Tabla 3. Documentos obligatorios para el estándar ISO/IEC 27001:2013.

DOCUMENTO	DESCRIPCIÓN GENERAL (Capítulo de ISO 27001:2013)
Alcance del SGSI	Se redacta al inicio de la implementación y contiene el alcance y limitaciones del SGSI. (4.3).
Políticas y Objetivos de Seguridad de la Información	Documento de alto nivel que detalla el principal objetivo del SGSI y las directrices generales relativas a la seguridad de la información. (5.2, 6.2).
Metodología de Evaluación y Tratamiento de Riesgos	Detalla la selección de la metodología de evaluación y tratamiento de riesgos a aplicar. (6.1.2).
Declaración de Aplicabilidad	Se redacta en base a los resultados del tratamiento del riesgo y describe qué controles del Anexo A son aplicables, cómo se implementarían y su estado actual. (6.1.3 d).
Plan de Tratamiento del Riesgo, Informe sobre Evaluación y Tratamiento de Riesgos	Redacta un plan de acción sobre cómo implementar los diversos controles definidos por la Declaración de Aplicabilidad. (6.1.3e, 6.2), (8.2, 8.3).
Definición de Funciones y Responsabilidades de Seguridad	Detalla las funciones y responsabilidades relativas a la seguridad de la información. (A.7.1.2, A.13.2.4).
Inventario de Activos	Detalla todos los activos informáticos de la organización. (A.8.1.1).
Uso Aceptable de los Activos	Define el tratamiento que reciben los activos que no han sido involucrados en otro proceso. (A.8.1.3).
Política de Control de Acceso	Detalla las políticas para el control del acceso lógico y físico. (A.9.1.1).
Procedimientos Operativos para Gestión de TI	Describe todas las operaciones de carácter técnico (copias de seguridad, transmisión de la información, códigos maliciosos, etc.) (A.12.1.1).
Principios de Ingeniería para Sistema Seguro	Contiene los principios de ingeniería de seguridad bajo la forma de un procedimiento o norma y que se defina cómo incorporar técnicas de seguridad en todas las capas de

[48] KOSUTIC, D. "Lista de documentación obligatoria requerida por ISO/IEC 27001". [En línea]. 2 de Septiembre de 2014 Disponible en ISO 27001 Academy<http://www.iso27001standard.com/es/descargas-gratuitas/scrollTo-11725>.

DOCUMENTO	DESCRIPCIÓN GENERAL (Capítulo de ISO 27001:2013)
	arquitectura: negocio, datos, aplicaciones y tecnología. (A.14.2.5).
Política de Seguridad para Proveedores	Detalla el procedimiento para la selección de contratistas. (A.15.1.1)
Procedimiento para Gestión de Incidentes	Define cómo se informan, clasifican y manejan las debilidades, eventos e incidentes de seguridad. (A.16.1.5).
Procedimientos de la Continuidad del Negocio	Describe los planes de continuidad del negocio, planes de respuesta ante incidentes, planes de recuperación para el sector comercial de la organización y planes de recuperación ante desastres. (A.17.1.2).
Requisitos Legales, Normativos y Contractuales	Documento que contiene toda la normatividad que la organización debe cumplir. (A.18.1.1).

Fuente: KOSUTIC, D. Lista de documentación obligatoria requerida por ISO/IEC 27001. [En línea].[Citado marzo 2012] Disponible en ISO 27001 Academy: http://www.iso27001standard.com/es/descargasgratuitas/scrollTo-11725.

2.1.3 COblT[49]

COblT define una metodología y un marco de trabajo adecuado para la gestión de Tecnología de la Información (IT), orientado en el negocio y en procesos, y basado en controles. Para ello considera tres dimensiones:

a) Los dominios, procesos y actividades de IT;
b) Los requerimientos de la información del negocio;
c) Los recursos de IT.

Define cuatro dominios, con sus procesos (34) que a su vez describen actividades concretas y especifican una serie de objetivos de control. Estos dominios son: Planificación y Organización (PO), Adquisición e Implementación (AI), Entrega y Soporte (ES), y Monitoreo y Evaluación (ME).

En particular, en el dominio PO, se centra la atención en la alineación de IT con los objetivos y estrategia del negocio, y en la gestión de riesgos. Así como en *ES*, se especifica un proceso de "Aseguramiento de Continuidad del Servicio / Operaciones".

A los efectos de satisfacer los objetivos de negocio se definen siete criterios en términos de requerimientos de la información, ellos son: efectividad, eficiencia,

[49] Ross R., Katzke S., Johnson A., Swanson M., Stoneburner G., "Managing Risk from Information Systems - An Organizational Perspective (second public draft)", NIST SP 800-39, National Institute of Standards and Technology, U.S. Department of Commerce. [online]. Disponible en internet: <http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf> (marzo de 2009).

confidencialidad, integridad, disponibilidad, cumplimiento (Marco legal y reglamentario, normas, contratos, etc.), y confiabilidad.

2.1.4 Metodología MAGERIT.

MAGERIT es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información elaborado por el CSAE (Consejo Superior de Administración Electrónica) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios[50], donde actualmente está en su versión 3.

El objetivo principal de MAGERIT es proteger los activos informáticos en pro de ayudar al alcance de la misión de una organización de acuerdo a las Dimensiones de Seguridad[51] propuestas que se encuentran en la tabla número 4.

Tabla 4. Dimensiones de Seguridad para la Identificación y Valoración de Amenazas en MAGERIT.

Dimensión de Seguridad	Nomenclatura	Definición
Disponibilidad	D	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].
Integridad	I	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].
Confidencialidad	C	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007].
Autenticidad	A	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008].
Trazabilidad	T	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 15-16.

[50] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 6.

[51] Ibíd., p. 15-16.

Para el proceso de Gestión de Riesgo, MAGERIT contempla dos (2) grandes tareas a realizar: el Análisis de Riesgos y el Tratamiento de Riesgos. El ***Análisis de Riesgos*** busca calificar los riesgos identificados, bien cuantificando sus consecuencias (análisis cuantitativo), bien ordenando su importancia relativa (análisis cualitativo). De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante.

Este proceso de análisis conlleva la identificación de los activos, sus amenazas y los controles de seguridad propuestos, estimando así el impacto y el riesgo al que están expuestos cada uno de los activos y su repercusión en el nivel de seguridad de la información en una organización. Por su parte, el ***Tratamiento de Riesgos*** recopila las actividades encaminadas a modificar la situación de riesgo. Es una actividad que presenta numerosas opciones como veremos más adelante[52].

Como MAGERIT es una metodología sistemática, sigue una serie de pasos para realizar la Gestión del Riesgo, los cuales son los siguientes:

2.1.4.1 *Inventario de Activos*

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización [53].

Son también los elementos que una organización posee para el tratamiento de la información[54]. En la tabla 5 MAGERIT clasifica los activos en los siguientes tipos:

Tabla 5. Clasificación de los tipos de activos informáticos en MAGERIT.

Tipo de activo	Nomenclatura	Definición
Activos Esenciales	[Essential]	Son aquellos que son esenciales para la supervivencia de la organización y que su carencia o daño afectaría directamente su existencia. Generalmente desarrollan misiones críticas.
Arquitectura del Sistema	[Arch]	Son aquellos que permiten estructurar el sistema, su arquitectura interna y sus relaciones con el exterior.
Datos/Información	[D]	Es aquella información que le permite a una organización prestar sus servicios.
Claves Criptográficas	[K]	Son aquellos que permiten cifrar la

[52] AMUTIO, M. A., CANDAU, J., & MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 20.
[53] Ibíd., Pág. 22.
[54] SUÁREZ, L., AMAYA, C. A. Sistema de Gestión de la Seguridad de la Información. Bogotá: UNAD. 2013. p. 45.

		información. Incluye los algoritmos de encriptación.
Servicios	[S]	Son aquellos que satisfacen las necesidades de los usuarios.
Software/Aplicaciones Informáticas	[SW]	Son aquellos que procesan los datos y permiten brindar información para la prestación de servicios.
Hardware/Equipamiento Informático	[HW]	Son los medios físicos donde se depositan los datos y prestan directa o indirectamente un servicio.
Redes de Comunicaciones	[COM]	Son los medios de transporte por donde viajan los datos.
Soportes de Información	[Media]	Son los dispositivos físicos que permiten el almacenamiento temporal o permanente de la información.
Equipamiento Auxiliar	[AUX]	Son aquellos equipos que brindan soporte a los sistemas de información sin estar relacionado con los datos.
Instalaciones	[L]	Son los lugares donde se hospedan los sistemas de Información y comunicaciones.
Personal	[P]	Son las personas relacionadas con los sistemas de información.

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 7-13.

2.1.4.2 *Valoración de los Activos*[55]

Cada activo de información tiene una valoración distinta en la empresa, puesto que cada uno cumple una función diferente en la generación, almacenaje o procesamiento de la información. Pero a la hora de valorarlos no sólo debemos tener en cuenta cuanto le costó a la empresa adquirirlo o desarrollarlo, sino que además debemos contemplar el costo por la función que ella desempeña y el costo que genera ponerlo nuevamente en marcha en caso de que éste llegase a dañarse o deteriorarse. Es por ello que se hace necesario tener en cuenta diferentes variables a la hora de darle valor a un activo.

MAGERIT establece dos (2) tipos de valoraciones: ***Cualitativa*** que es aquella que permite calcular el valor de un activo en base al impacto que pueda tener en la organización y la ***Cuantitativa*** que estima el costo del activo (*incluyendo costo de compra, de reparación, configuración, mantenimiento, etc.*). Mientras que la ***Cualitativa*** permite establecer órdenes de magnitud (***MA*** [*Muy Alto*], ***A*** [*Alto*], ***M***

[55] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD, 233003 Sistema de Gestión de la Seguridad de la Información SGSI, Capitulo 3 Análisis de Riesgos,. Valoración de los activos. [online][citado en abril 2012]. Disponible en Internet: < http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/322__paso_2_valoracin_de_los_activos.html>

[*Medio*], ***B*** [*Bajo*] y ***MB*** [*Muy Bajo*]) y no genera valores numéricos, la ***Cuantitativa*** sí permite calcular el costo y/o valor monetario.

2.1.4.3 *Identificación y Valoración de Amenazas*

MAGERIT establece cinco (5) ***Dimensiones de Seguridad*** (***D*** [*Disponibilidad*], ***I*** [*Integridad*], ***C*** [*Confidencialidad*], ***A*** [*Autenticidad*] y ***T*** [*Trazabilidad*]) donde es necesario determinar los criterios de valoración en cada dimensión. Estos valores y/o criterios son similares a los establecidos en la ***tabla 21 de Valoración cualitativa de los activos informáticos en MAGERIT[56].***

2.1.4.4 *Identificación de Amenazas*

Las amenazas son los eventos que ocurren sobre un activo que podría causarle daño a una organización. MAGERIT emplea un catálogo de amenazas posibles sobre los activos de un sistema de información88, los cuales en la tabla 6 se ven clasificados[57]:

Tabla 6. Catálogo de Amenazas sobre los activos informáticos en MAGERIT

Tipo de amenaza	Nomenclatura	Definición
Desastres Naturales	[N]	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
De Origen Industrial	[I]	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada
Errores y Fallos No Intencionados	[E]	Fallos no intencionales causados por las personas
Ataques Intencionados	[A]	Fallos deliberados causados por las personas.

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 25-47.

[56] AMUTIO, M. A., CANDAU, J., & MAÑAS, J. A. MAGERIT. Libro I. Op. Cit. Pág. 24-25.

[57] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 25-47.

2.1.4.5 Valoración de Amenazas

Para establecer la valoración de las amenazas es necesario determinarla frecuencia o probabilidad de ocurrencia. En MAGERIT, las frecuencias o probabilidades se muestran en la tabla 7 que se enseña a continuación[58]:

Tabla 7. Probabilidad o Frecuencia de ocurrencia de las amenazas en MAGERIT

Probabilidad o frecuencia	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semanas	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: SUÁREZ, L., AMAYA, C. A. Sistema de Gestión de la Seguridad de la Información. Bogotá: UNAD. 2013. p. 52.

2.1.4.6 *Impacto Potencial*

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema[59].

2.1.4.7 *Riesgo Potencial*

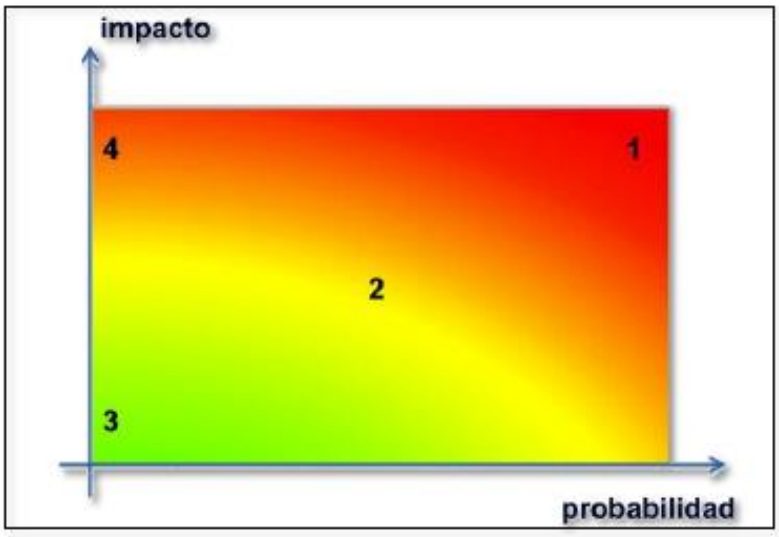
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia[60]. Por ende, el riesgo es calculado como:

Riesgo = Probabilidad x Impacto.

El riesgo crece con el impacto y con la probabilidad como se muestra en la figura número 4 que a continuación se muestra (Ver figura 4):

[58] SUÁREZ, L., AMAYA, C. A. Sistema de Gestión de la Seguridad de la Información. Bogotá: UNAD. 2013. p. 52.
[59] AMUTIO, M. A., CANDAU, J., & MAÑAS, J. A. MAGERIT. Libro I. Op. Cit. Pág. 28.
[60] Ibíd, Pág. 28.

Figura 4. Zonas de riesgos.



Fuente: AMUTIO, M. A., CANDAU, J., & MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 30.

Donde las zonas identifican lo siguiente[61]:

- ***Zona 1***: Riesgos muy probables y de muy alto impacto (***MA: Críticos***).
- ***Zona 2***: Riesgos que varían desde situaciones improbables y con impacto medio hasta situaciones muy probables pero de impacto bajo o muy bajo (***M: Apreciables***).
- ***Zona 3***: Riesgos improbables y de bajo impacto (***MB, B: Despreciables o Bajos***).
- ***Zona 4***: Riesgos improbables pero de muy alto impacto (***A: Importantes***).

La relación de la probabilidad e impacto para determinar el riesgo de forma cualitativa se muestra en la tabla 8.

[61] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 30.

Tabla 8: Estimación cualitativa del riesgo.

RIESGO		PROBABILIDAD				
		MB	B	M	A	MA
IMPACTO	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de Técnicas. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 7

2.1.4.8 *Controles de Seguridad (Salvaguardas)*:

Los ***Controles de Seguridad*** o ***Salvaguardas*** son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, donde se deben establecer los controles para cada amenaza de cada activo. En la tabla número 9 se puede observar las salvaguardas propuestas en MAGERIT[62]:

Tabla 9. Salvaguardas sobre los activos informáticos en MAGERIT

Salvaguarda	Nomenclatura
Protecciones generales u horizontales	H
Protección de los datos / información	D
Protección de las claves criptográficas	K
Protección de los servicios	S
Protección de las aplicaciones (software)	SW
Protección de los equipos (hardware)	HW
Protección de las comunicaciones	COM
Protección en los puntos de interconexión con otros sistemas	IP
Protección de los soportes de información	MP
Protección de los elementos auxiliares	AUX
Seguridad física – Protección de las instalaciones	L
Salvaguardas relativas al personal	PS
Salvaguardas de tipo organizativo	G
Continuidad de operaciones	BC
Externalización	E
Adquisición y desarrollo	NEW

[62] Ibíd. P. 53 – 57.

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 53-57.

2.1.5 Generalidades.

La Tecnología Informática (TI) ha penetrado todos los sectores del mundo actual, desde el punto de vista personal hasta los negocios.

Hoy en día las empresas almacenan información de sus clientes, usuarios y proveedores en bases de datos, se comunican con ellos a través del correo electrónico, videoconferencias en vivo, etc. La TI ha cumplido un rol determinante en el éxito de las organizaciones, ya que ha pasado de ser un área ignorada por los accionistas a ser un componente clave en los procesos de negocio, así como en la creación de nuevas oportunidades como un factor diferencial para obtener una ventaja competitiva. Teniendo esto en mente, la TI no solamente soporta las estrategias de negocio existentes de una compañía, sino que genera nuevas estrategias, agregando valor a los productos y servicios que la organización ofrece.

Debido a lo anterior, la mayoría de las organizaciones hoy en día ejecutan sus procesos críticos de negocios soportados por tecnología informática y éstos se realizan de forma automática; de ésta manera los directivos confían en los datos e información suministrada por el personal del área de sistemas y telecomunicaciones para la toma de decisiones. Es por esto que se debe reconocer que la TI juega un papel muy importante en las estrategias corporativas de las organizaciones, fundamentalmente porque en la actualidad las empresas mantienen una estrecha relación con sus usuarios, clientes y proveedores y es notoria la necesidad de poseer una infraestructura tecnológica e informática que soporte esta área crítica de negocio, con el fin de generar valor a la estrategia del negocio y por ende beneficio económico.

La dependencia actual de las organizaciones en TI se hace más notoria debido a que nuestra economía se basa en la generación de conocimiento[63], donde el uso de la tecnología en administrar, desarrollar y transmitir activos intangibles como la información y el conocimiento son esenciales para las estrategias de negocio.

Pero a su vez, depender en gran medida de la TI en los procesos de negocio conlleva a considerar ciertos factores y riesgos que son inherentes al uso de ellas, como lo son las amenazas humanas (cibercrimen, fraude, malware, etc.),

[63] PETERSON, R. Integration Strategies and Tactics for Information Technology Governance. En W. VAN GREMBERGEN, Strategies for Information Technology Governance (p. 37-80). IDEA Group Publishing. 2004. p. 3.

tecnológicas (caídas de las redes, hardware/software obsoleto, etc.) y naturales (incendios, inundaciones, terremotos, etc.).

Es por esto que los datos e información de las organizaciones se deben mantener en un entorno seguro donde se mantengan los niveles de riesgos informáticos en un nivel aceptable, y la seguridad informática se manifiesta en tres (3) principios básicos: confidencialidad, integridad y disponibilidad[64].

- **Confidencialidad**: Conservar las restricciones autorizadas en el acceso y divulgación de la información, incluyendo los medios para proteger la privacidad personal e información del propietario. Propiedad que establece que la información no es disponible o divulgada a individuos no autorizados, entidades o procesos[65].

- **Integridad:** Proteger el acceso contra la indebida modificación o destrucción de la información, e incluye el aseguramiento del no-repudio y autenticidad de la información.

- **Disponibilidad:** Garantizar el funcionamiento y usabilidad del servicio cuando sea solicitado por las personas autorizadas[66].

Independientemente del tamaño o actividad de una organización, generalmente se identifican siete (7) dominios de una infraestructura de TI, donde se deben garantizar los principios anteriormente mencionados en cada uno de ellos. Dentro de la tabla 10 se muestran estos dominios[67].

Tabla 10. Dominios de una típica infraestructura TI en una organización.

DOMINIO	DESCRIPCIÓN
USUARIO	Personas que acceden a los sistemas de información de la organización. Es el ente más débil de la infraestructura TI.
ESTACIÓN DE TRABAJO	Es cualquier dispositivo (PC, Laptop, Tabletas, Teléfonos Inteligentes, etc.) que se conecta a la red de la organización.
RED LOCAL (LAN)	Colección de computadoras que se conectan a través de un medio y

[64] Se le conoce como la Tríada CIA, por sus siglas en inglés Confidentiality, Integrity, Availability. KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 10.

[65] HODEGHATTA, U., & NAYAK, U. The InfoSec Handbook: An Introduction to Information Security. New York: Apress Media. 2014. p. 52.

[66] RHODES-OUSLEY, M. Information Security: The Complete Reference (Segunda ed.). McGrawHill. 2013. p. 86.

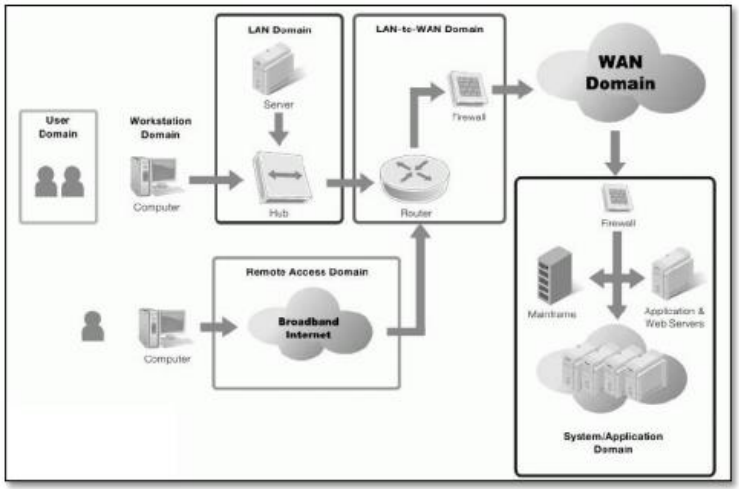
[67] KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 15-36.

	generalmente comparte información. Permite conectar computadoras y obtener acceso a sistemas, aplicaciones, información e Internet.
RED LOCAL A RED AMPLIA	Permite la conexión al mundo exterior de la organización e Internet. Generalmente permite el acceso a información públicamente accesible.
RED AMPLIA (WAN)	Permite la conexión de oficinas remotas de una misma organización.
ACCESO REMOTO	Permite conectar usuarios remotos a la infraestructura TI de la organización.
SISTEMAS/APLICACIONES	Contiene todos los sistemas, aplicaciones y datos que son fundamentales para el funcionamiento de la organización.

Fuente: KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 15-36.

En la figura 5 se muestra los dominios que maneja una organización.

Figura 5. Dominios de una típica infraestructura TI en una organización.



Fuente: KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 32.

2.1.6 Amenazas a la Seguridad de la Información.

La infraestructura de TI de una organización está compuesta por activos. Un Activo o Recurso Informático, se define como todo aquello pueda generar valor para la empresa u organización y que éstas sientan la necesidad de proteger. Un

activo está representado por los objetos físicos (hardware, routers, switches, hubs, firewalls, antenas, computadoras), objetos abstractos (software, sistemas de información, bases de datos, sistemas operativos) e incluso el personal de trabajo y las localidades físicas.

Estos activos están propensos a amenazas, las cuales son aquellas que representan un peligro para los activos o a la seguridad de la información en general., las cuales pueden ser perpetuadas internamente o externamente[68].

A continuación en la tabla 11 se enseña algunas de las amenazas sobre seguridad de la información.

Tabla 11. Amenazas a la seguridad de la información.

AMENAZA	FACTOR
Adquisición de contraseñas	Ataques de Fuerza Bruta, Ataques de Diccionario, Ingeniería Social, entre otras.
Aplicación	Desbordamientos de Búfer (Buffer Overflow), Privilegios de Administrador (Rootkits), TOCTTU (Time to Check, Time to Use).
Código Malicioso	Virus, Gusanos, Troyanos, Spyware, Adware, Bombas Lógicas.
Denegación de Servicios (DoS, Denial of Service)	Inundamiento de SYN (SYN Flooding), Smurf, Teardrop, Ping de la Muerte, Envenenamiento DNS (DNS Poisoning).
Husmeo	Sniffing.
Reconocimiento	Escaneo de Puertos, Escaneos de Vulnerabilidades.
Seguridad de Aplicaciones Web / Bases de Datos.	Secuencias de Comandos en Sitios Cruzados (XSS, Cross-Site Scripting), Inyección SQL (SQL Injection).
Suplantación de Identidades.	Suplantación IP (IP Spoofing), Secuestro de Sesión (Session Hijacking), Hombre en el Medio (Man in the Middle)

Fuente: KIM, D., SALOMON, M. G. Fundamentals of Information System Security. Estados Unidos de América: Jones & Bartlett Learning International. 2012. p. 32.

2.2 MARCO CONCEPTUAL

2.2.1 Información

[68] HODEGHATTA, U., & NAYAK, U. Op. Cit. o. 31

Múltiples trabajos se han dedicado a disertar sobre el término información y su importancia como recurso indispensable para la sociedad y cuyo desarrollo ha rebasado cualquier pronóstico realizado años atrás. El sector de la información y su industria se han convertido en un factor esencial para el accionar humano en la sociedad moderna. La investigación sobre el concepto de información se remite a la Edad Media, donde se decía que la información y, más específicamente la palabra, daban forma e impregnaba de carácter a la materia y a la mente.[69]

2.2.2 Riesgo

La posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se lo mide en términos de consecuencias y probabilidades.[70].

2.2.3 Administración De Riesgos.

Se llama así al proceso de identificación, análisis y evaluación de riesgos[71].

2.2.4 Seguridad De La Información

Es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.[72]

2.2.5 Sistema De Gestión De Seguridad De La Información (SGSI)

Un SGSI o ISMS, de sus siglas en inglés (Information Security Management System), es la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información [73.]

2.2.6 La Seguridad Informática[74]

---

[69] Goñi Camejo, Ivis, "Contribuciones Breves, Algunas reflexiones sobre el concepto de información y sus implicaciones para el desarrollo de las ciencias de la información. [online] [citado febrero]. Disponible en internet: http://www.bvs.sld.cu/revistas/aci/vol8_3_00/aci05300.htm

[70] Administración De Riesgos. AS/NZS 4360:2004: Risk Management [online]. Disponible en Internet: http://www.bcu.gub.uy/Acerca-de-BCU/Marzo2012/Bibliograf%C3%ADa%20PGE/Administracion_de_riesgo_Estandar_Australiano.pdf. Pág. 5

[71] Ibíd. Pág. 3.

[72] NEIRA, Agustín y SPOHR, Javier. ISO27000.es. "International Organization For Standardization Iso27000". [online] [citado febrero 2012]. Disponible en internet: http://www.iso27000.es.

[73] NEIRA, Agustín y SPOHR, Javier. Ibíd.

[74] Jeimy J. Cano, Ph.D., CFE. "La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes".[online][citado marzo 2012]. Disponible en internet en: <http://www.isaca.org/Journal/archives/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx>

Es la disciplina que se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías, antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información, establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.

Considerando lo revisado por Tim Kayworth y Dwayne Whitten, una adecuada estrategia de seguridad de la información deberá articular tres elementos claves (Cano, 2011):

• Balance de necesidades: protección de la información y desarrollo de negocios.
• Aseguramiento del cumplimiento normativo.
• Desarrollo y afianzamiento de la cultura corporativa

En la figura 6 se enseña las diferencias que existen entre *Information Security* vs *IT Security*.

Figura 6. IT Security vs Information Security.

Fuente: GONZÁLEZ, Julián. ¿SEGURIDAD INFORMÁTICA O SEGURIDAD DE LA INFORMACIÓN? [Online][Citado marzo 2012]. Disponible en Internet: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html.

2.2.7 Pilares de la seguridad Informática[75]

Existen múltiples definiciones sobre la seguridad informática orientadas a la norma, a la disciplina, a su característica, etc., pero para lograr que abarque variables importantes se puede afirmar que la seguridad informática es la que

[75] Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I. Capítulo 1 Seguridad Informática. Lección 1 Pilares de la seguridad informática. [online]. Disponible en Internet en < http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/11_leccin_1_pilares_de_la_seguridad_informtica.html>

permite lograr que todos los sistemas informáticos utilizados en cualquier contexto, se encuentren seguro de cualquier daño o riesgos, ya sea por parte de personas ajenas que en forma voluntaria o involuntaria lo pueda hacer o de cualquier desastre natural. En este sentido, la protección de la información requiere de un conjunto de software o aplicativos diseñados, documentos estándares y metodologías existentes que permitan aplicar las normativas certificables internacionalmente y técnicas apropiadas para llevar un control en la seguridad. Se expresa control en la seguridad, porque se considera un tanto difícil garantizar la seguridad de la información en forma completa o llevada a un 100%, por cuanto intervienen diferentes amenazas a las que las organizaciones y/o personas se encuentran continuamente expuestas.

Lo que se persigue proteger en la información, son los cuatro pilares importantes que conlleva a que la información sea protegida a gran escala. A continuación se especifican en su orden:

Confidencialidad: La información sólo puede ser accedida y utilizada por el personal de la empresa que tiene la autorización para hacerlo. En este sentido se considera que este tipo de información no puede ser revelada a terceros, ni puede ser pública, por lo tanto debe ser protegida y es la que tiende a ser más amenazada por su característica.

Integridad: Se refiere al momento en que la información no ha sido borrada, copiada o modificada, es decir, cuando se conserva tal como fue creada o enviada desde cualquier medio desde su origen hacia su destino.

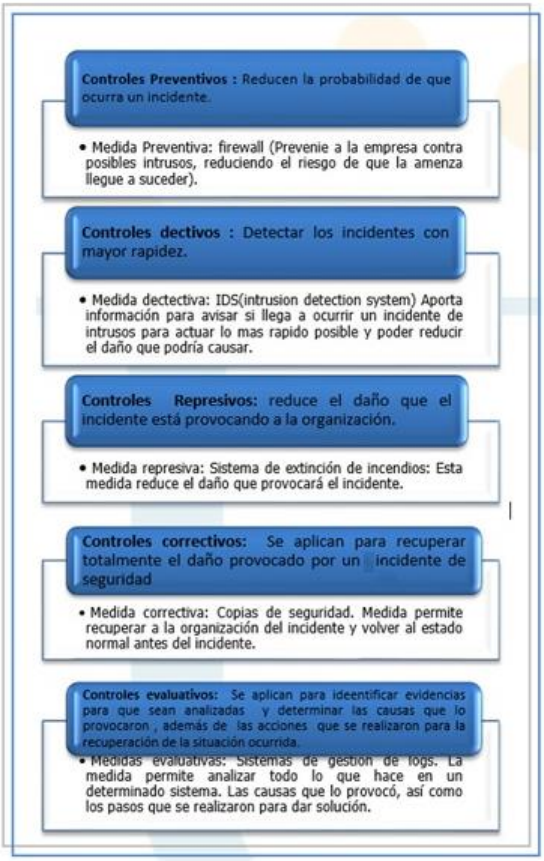
Disponibilidad: Se refiere a que la información facilitada en cualquier medio digital o software se encuentre disponible para el procesamiento de la información, para el correcto funcionamiento de una organización, así como de sus clientes o personal requerido sin que estos sean interrumpidos.

Autenticidad: Este pilar se define aquella información legítima, que al ser interceptada, puede ser copiada de su formato original a pesar de que la información sea idéntica. Un ejemplo comparativo a la autenticidad de algo, se presenta muchas veces en la copia de una pintura original de una obra de arte que ha sido copiada idéntica a la obra original del autor, es decir, que a pesar de que la información es igual, no es auténtica.

Ahora bien, antes de que exista un indecente de seguridad que afecte cualquiera de sus pilares, tuvo que haber un riesgo de seguridad que en su momento no fue detectado, esto quiere decir; que el significado de un riesgo es cuando existe una amenaza a la seguridad que no ha llegado a afectar a la organización y un incidente, es cuando se materializa el riesgo. Es por ello, la necesidad de la aplicación de controles de seguridad que protege contra todo aquello que pueda

causar un incidente de seguridad. En la figura 7 se muestran los controles de seguridad (Ver figura 7).

Figura 7. Controles de Seguridad.



Fuente: Universidad Nacional Abierta y A Distancia. Sistema de Gestión de la Seguridad de la Información SGSI. Unidad I. Capítulo 1 Seguridad Informática. Lección 1 Pilares de la seguridad informática. [Online]. Disponible en Internet en < http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/11_leccin_1_pilares_de_la_seguridad_informtica.html>.

2.3 MARCO LEGAL

A la hora de implementar un SGSI, es necesario tener en cuenta desde el diseño se cumplan todas las normas y/o decretos que apliquen durante el desarrollo de las actividades, estableciendo la manera adecuada de proteger a los activos de las organizaciones de cualquier delito.

Durante el diseño de un SGSI para las organizaciones es necesario conocer algunas leyes, decretos y normas que buscan la protección del bien individual o colectivo, que a continuación se describen:

2.3.1 Ley 1266[76]

"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

2.3.2 Ley 1273 [77]

"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".

2.3.3 Decreto 2573[78]

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.

2.3.4 Decreto 1360[79]

"Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor".

---

[76] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1266. (Diciembre 31 de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15

[77] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (Enero 5 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. Diario Oficial 47.223 de enero 5 de 2009. p. 1-4

[78] COLOMBIA. CONGRESO DE LA REPUBLICA. Decreto 2573. (Diciembre 12 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. Diario Oficial 49363 de diciembre 12 de 2014. p. 1-5

[79] COLOMBIA. CONGRESO DE LA REPUBLICA. Decreto 1368. (Junio 23 de 1989). Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor. Diario Oficial 38871 de junio 23 de 1989. p. 1-2

2.3.5 Ley 527[80]

"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".

2.3.6 Decreto 1747[81]

"Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales".

2.3.7 Ley estatutaria 1266[82]

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

[80] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527. (Agosto 21 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. Diario Oficial No. 43.673, de 21 de agosto de 1999. p. 1-10

[81] COLOMBIA. CONGRESO DE LA REPUBLICA. Decreto 1747. (Septiembre 11 de 2000). Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. Diario Oficial No. 44.160, Bogotá, jueves 14 de septiembre de 2000. p. 1-11

[82] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatutaria 1266. (Diciembre 31 de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial No. 47.219 de 31 de diciembre de 2008. p. 1-14

3. SITUACIÓN ACTUAL DE LA EMPRESA BAKER TILLY COLOMBIA LTDA.

3.1 INTRODUCCIÓN.

En este capítulo se dará a conocer los procedimientos que BAKER TILLY COLOMBIA LTDA maneja, además de su historia y servicios que presta.

3.2 DESCRIPCIÓN DE LA EMPRESA

3.2.1 Historia

Baker Tilly, en Colombia, fue fundada en 1994 ofreciendo servicios propios del ejercicio de la profesión contable y afines a un grupo de empresas locales.

En el año de 2004 la firma ingresa como firma-miembro de la red Baker Tilly International, después de un riguroso proceso de selección y verificación del cumplimiento de los estándares de calidad requeridos por la red a nivel mundial, otorgándosele a la firma la licencia para usar el nombre “Baker Tilly Colombia”.

En el año 2012, la firma es autorizada a cambiar su nombre por el prefijo Baker Tilly, con el fin de trabajar por el posicionamiento de la marca a nivel mundial.

3.2.2 Misión

BAKER TILLY COLOMBIA LTDA es una empresa independiente dedicada a Prestar soluciones legales integrales que brinden respaldo, confianza y seguridad a las necesidades de los clientes, bajo resultados que superen sus expectativas. Estamos conformados por un equipo comprometido con la más alta calidad de trabajo legal, colaboración mutua y altos niveles de conducta profesional.

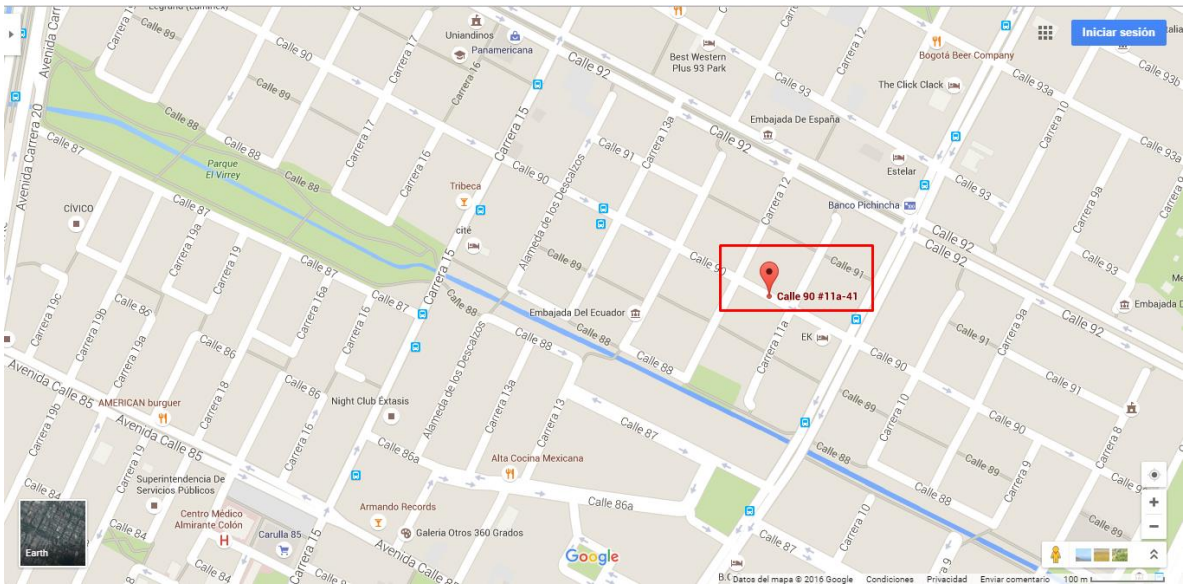
3.2.3 Visión (AL AÑO 2020)

BAKER TILLY COLOMBIA LTDA, será una firma líder por su prestigio y reconocimiento nacional e internacional, que construye estructuras legales de excelencia y proyectos innovadores y sostenibles, bajo el entendimiento profundo de las necesidades de negocios de nuestros clientes.

3.2.4 Ubicación Geográfica

BAKER TILLY COLOMBIA LTDA, se encuentra ubicada en la Cll. 90 No. 11ª – 41 barrio la cabrera, donde se puede detallar en la figura 8.

Figura 8. Ubicación Geográfica.

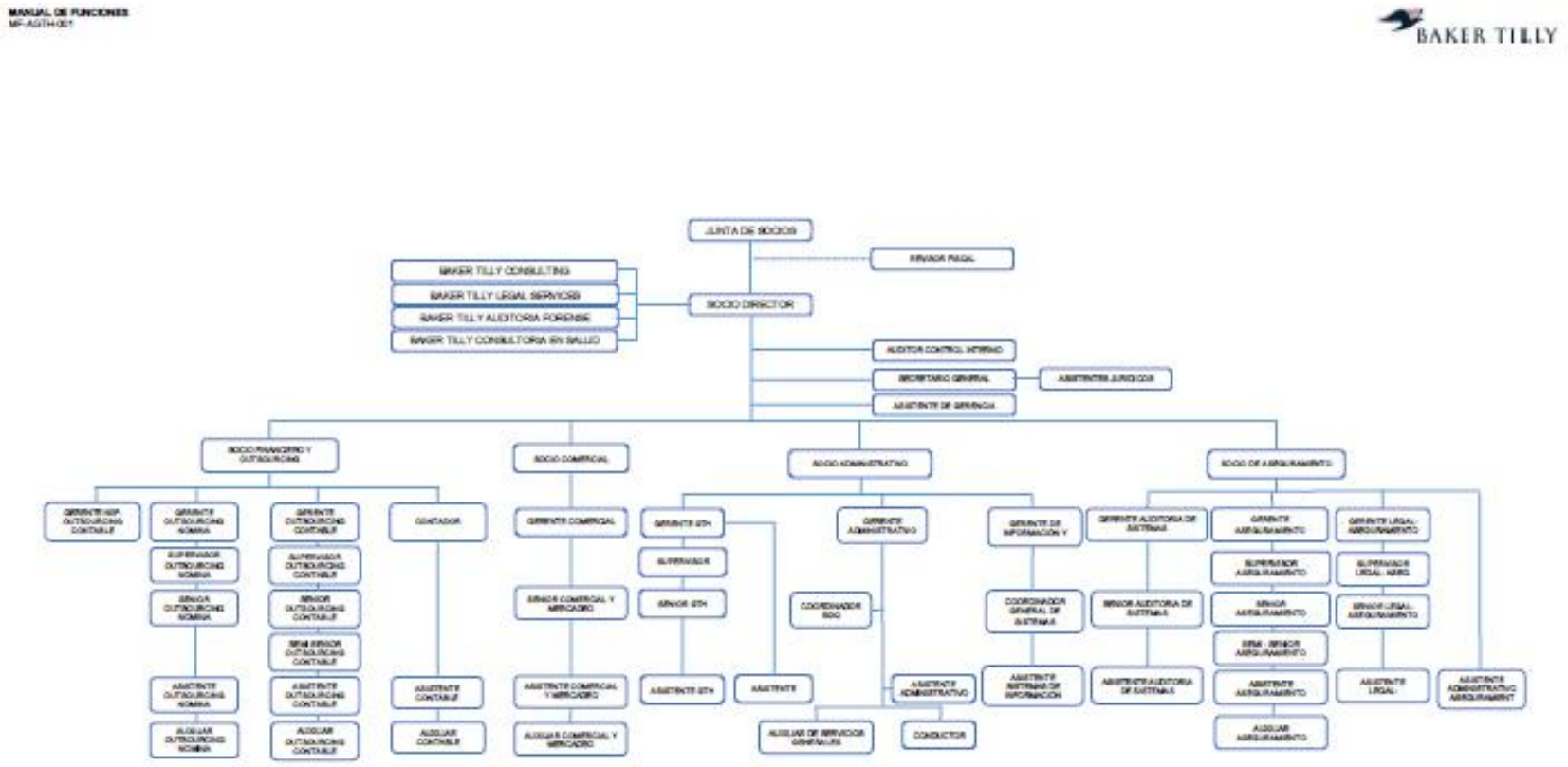


Fuente: Propiedad del Autor

3.3 ESTRUCTURA ORGANIZACIONAL

En la figura 9 se puede detallar la estructura organizacional de la empresa BAKER TILLY COLOMBIA LTDA.

Figura 9. Estructura Organizacional Baker Tilly Colombia Ltda.



Fuente: http://www.bakertilly.co/nosotros/estructura-organizacional/

3.4 AREA DE SISTEMAS

3.4.1. Caracterización del Área de Sistemas

3.4.1.1. Misión

El área de sistemas tiene como misión apoyar cada una de las iniciativas existentes y generar nuevas que conlleven al crecimiento de BAKER TILLY COLOMBIA LTDA mediante la utilización de las tecnologías de la información TIC y herramientas tecnológicas apropiadas que permitan optimizar de manera segura y eficiente los procesos que se llevan a cabo en cada departamento de la empresa

3.4.1.2. Objetivos

- Elaborar, desarrollar y proponer la implementación de nuevas tecnologías y sistemas informáticos dentro de Baker Tilly Colombia Ltda.
- Elaborar planes de mantenimiento preventivo y brindar soporte técnico solicitado por las distintas áreas que conforman la empresa.

3.4.1.3. Estructura Organizacional del área de sistemas

En las figuras 10 y 11 se puede observar la dependencia Jerárquica de la Gerencia de Tecnología.

Figura 10. Estructura Organizacional Gerencia de Tecnología.

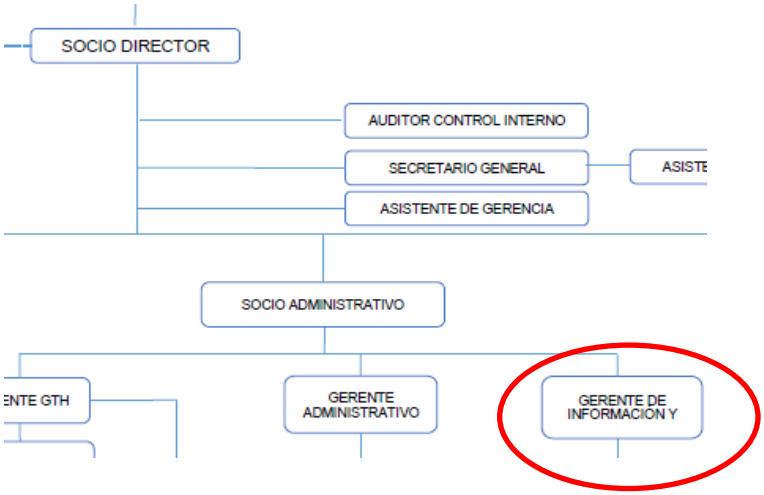
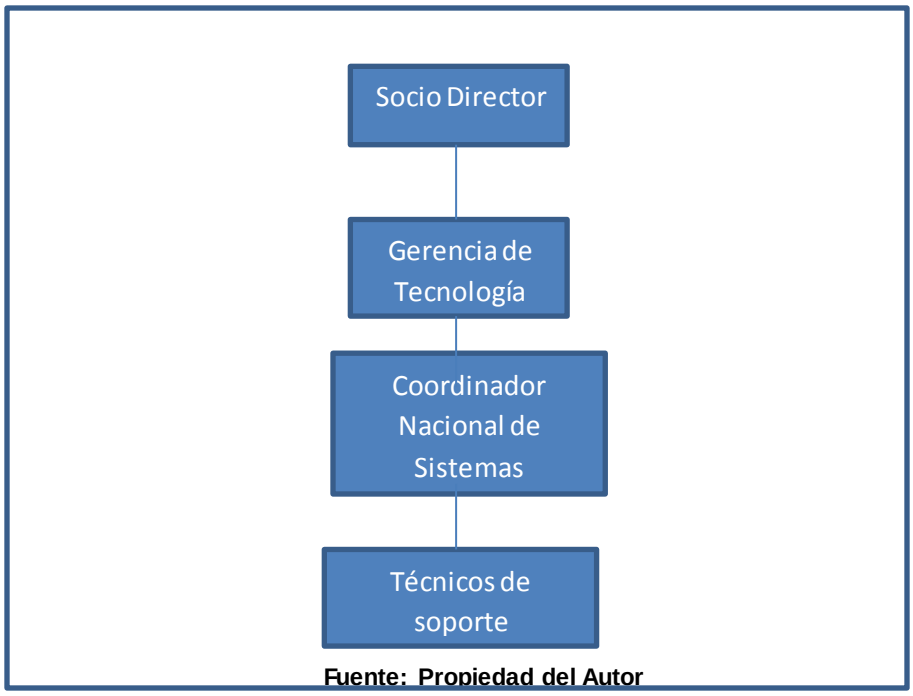


Figura 11. Detalle de Estructura Organizacional Gerencia de Tecnología



Fuente: Propiedad del Autor

3.4.1.4. Descripción de cargos y funciones

La oficina de Sistemas de Información está actualmente liderada y dirigida por la Gerencia de Tecnología. Los cargos y funciones principales se describen a continuación (Ver Tablas 12, 13 y 14):

Tabla 12. Cargo y funciones principales de la oficina de Sistemas.

Cargo	Gerente de Información y Tecnología
Funciones del Cargo	
• Dirigir y planificar la estrategia de tecnologías de información de la Firma alineadas a los objetivos del negocio. • Estructuración de planes de contingencia. • Comunicar los planes, objetivos, metas, políticas, normas y procedimientos al personal a su cargo. • Dirigir procesos de evaluación y cambios tecnológicos. • Promover el desarrollo de proyectos de tecnología de información y/o comunicación. • Poner en práctica sistemas de respaldo en caso de fallo. • Definir los planes y políticas del proceso, así como los planes de contingencia, disponibilidad y seguridad de la información, con el fin de asegurar un alto nivel de servicio, investigación y nuevas tendencias y posicionamiento acorde con las mejores prácticas del mercado.	

Fuente: Propiedad del Autor

Tabla 13. Cargo y funciones principales de la oficina de Sistemas.

Cargo	Coordinador General de Sistemas
Funciones del Cargo	
• Garantizar diariamente el correcto funcionamiento de los equipos de la firma, los servidores, aplicaciones, red interna e internet de la firma. • Administrar y solucionar problemas del entorno de red y sistemas operativos. • Revisar los Backup de la información contenida en el servidor de la firma y aquella que se considere importante y confidencial para el desarrollo de las actividades, antes de su entrega al Gerente Administrativo y de Operaciones. • Administrar las cuentas de correo y chat corporativo de los usuarios de la Firma. • Administrar las cuentas de acceso a la red y demás aplicaciones que requieran autenticación de usuario.	

Fuente: Propiedad del Autor

Tabla 14. Cargo y funciones principales de la oficina de Sistemas.

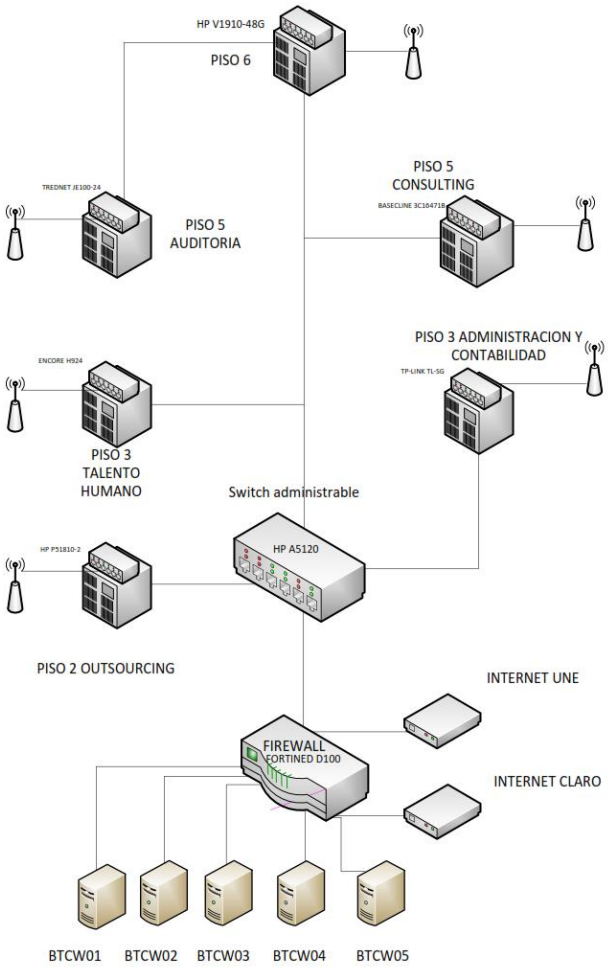
Cargo	Auxiliar de Sistemas
Funciones del Cargo	
• Realizar el mantenimiento preventivo de los equipos de cómputo de la Firma de acuerdo al procedimiento establecido. • Realizar la asignación de equipos y accesorios tecnológicos a los funcionarios de la Firma de acuerdo al procedimiento establecido. • Realizar el mantenimiento en redes de telecomunicaciones. • Realizar y controlar el Backup de todos los equipos de la Firma.	

Fuente: Propiedad del Autor

3.4.1.5. Infraestructura tecnológica

En la figura 12 se enseña la infraestructura tecnológica que dispone la empresa Baker Tilly Colombia.

Figura 12. Infraestructura tecnológica



Fuente: Área de Sistemas Baker Tilly Colombia

3.4.1.6. Políticas de uso para la utilización de INTERNET

La empresa Baker Tilly Colombia Ltda, tiene establecida algunas políticas para el uso de internet las cuales se enuncian a continuación:

SOBRE USO DE INTERNET

Los privilegios de uso de Internet estarán de acuerdo a la necesidad de acceso que requiera el desarrollo de la función de cada usuario.

SOBRE USO ADECUADO DE INTERNET

Debe entenderse que el acceso a Internet en Baker Tilly Colombia responde a la utilización de una herramienta de uso estrictamente laboral. Pare estos efectos, cualquier propósito ajeno a las funciones estrictamente laborales serán restringidas.

SOBRE MAL USO DEL INTERNET

- Está estrictamente prohibido el ingreso a Páginas Web con contenido pornográfico.
- Solo se permitirá el uso del "CHAT" en las aplicaciones permitidas como Skype Corporativo y Hangouts del correo corporativo, cualquier chat de red social como Facebook, Whatsapp etc. no están permitidas.
- El usuario no debe descargar ningún programa o software, sin la debida autorización, tales como: Shareware, software de evaluación, etc. Archivos de música (MP3, WAV, etc.) ya que estos no poseen licencia para su uso.
- El usuario no debe instalar ningún programa para reproducir MP3, RA, WAV, o emisoras de radio vía Internet.
- El usuario no debe instalar ningún programa para reproducir videos o emisoras de televisión vía Internet. (REAL AUDIO, BWV, etc.), dado que estos no poseen licencia para su uso.
- El usuario no debe abrir, ni revisar correos electrónicos considerados inseguros, debido al riesgo de contener mensajes de dudosa procedencia o archivos contaminados con virus que perjudique el equipo en uso, propiedad de Baker Tilly Colombia y que puedan afectar a la red institucional.
- No se debe usar Internet para realizar llamadas internacionales personales. Sólo los usuarios autorizados podrán realizar video conferencias de acuerdo a la descripción de sus funciones y necesidades del Servicio para el que responde.
- Se prohíbe cualquier tipo de transmisión vía Internet que no se autorizada (escuchar música y ver vídeo)

SANCIONES POR MAL USO DE INTERNET

- Los equipos que cuenten con Internet, podrán ser sometidos a auditoría con el fin de verificar el buen uso del mismo.
- El Director o Jefe será informado sobre el mal uso que se le está otorgando a Internet en su área.
- El Jefe inmediato recibirá un reporte sobre el comportamiento del usuario, para que evalué el tiempo que el Funcionario utiliza la herramienta.

3.5 SISTEMAS DE INFORMACIÓN

3.5.1 SIIGO – Provee los módulos de sistema de información contable y módulo de sistema de información de Nómina.

Principales módulos de SIIGO / FINANCIERO.

- Documentos
- Contabilidad
- Cuentas por cobrar
- Cuentas por pagar
- Ventas (modulo informativo)

Principales módulos del SIIGO / NÓMINA.

- Procesos de Nómina
- Pago de Nómina.
- Parafiscales.
- Cálculos de provisiones de Nómina.
- Planilla integrada de autoliquidación de aportes.
- Pagos en Medios magnéticos.
- Pago electrónico de Nómina.
- Incrementos de sueldo
- Informes de Nomina.

3.6 SERVICIOS QUE PRESTAN

3.6.1 Aseguramiento

Baker Tilly brinda confiabilidad y seguridad en la información suministrada para la toma de decisiones y el cumplimiento de los objetivos empresariales. Nuestra labor se efectúa de acuerdo a normas de auditoría, con los más rigurosos procedimientos de control y estándares de calidad que brindan confiabilidad en las operaciones desarrolladas y en la información suministrada por la compañía.

Servicios:

- Auditoría Externa
- Revisoría Fiscal
- Auditoría Interna
- Auditorías Especiales
- Auditoría en Tecnología de la Información[83].

3.6.2 Outsourcing

Por medio de los servicios de Outsourcing, permitimos a las empresas administrar todas las funciones del "Back Office", para lograr incrementar la eficiencia en las operaciones y la rentabilidad del negocio.

Servicios:

- Outsourcing Contable
- Outsourcing de Nómina
- Outsourcing Administrativo[84].

3.6.3 Auditoría Forense

Baker Tilly – Auditoría Forense, reúne un equipo de profesionales de amplia experiencia y trayectoria nacional e internacional en prevención, detección y

[83] Baker Tilly Colombia. Aseguramiento [online]. Disponible <http://www.bakertilly.co/servicios/aseguramiento/>
[84] Baker Tilly Colombia. Outsourcing [online]. Disponible <http://www.bakertilly.co/servicios/outsourcing/>

control de lavado de activos y del financiamiento del terrorismo – LA / FT. Presta sus servicios a empresas a nivel nacional e internacional del sector real y financiero y a organismos públicos que requieren fortalecer sus mecanismos de control en estas áreas, dando cumplimiento a la normativa nacional e internacional.

Servicios:

- Implementación de sistemas integrados de prevención de lavado de activos y financiación del terrorismo SIPLAFT para empresas del sector real y el SARLAFT para el sector financiero
- Consultoría en prevención de fraude para empresas del sector real y financiero
- Auditoría forense, determinación de causas, efectos y recomendaciones
- Debida Diligencia de Conocimiento – DDC – Check List
- Sensibilización y capacitación en prevención y detección de operaciones asociadas con el LA / FT[85].

3.7 PROCESOS ACTUALES

La empresa posee un procedimiento interno el cual a continuación se describe:

OBJETIVO: Garantizar que los procesos de Baker Tilly que sirven como habilitadores tecnológicos de la operación se encuentren disponibles cumpliendo con las normativas y políticas vigentes.

3.8.1 Descripción de Procedimiento

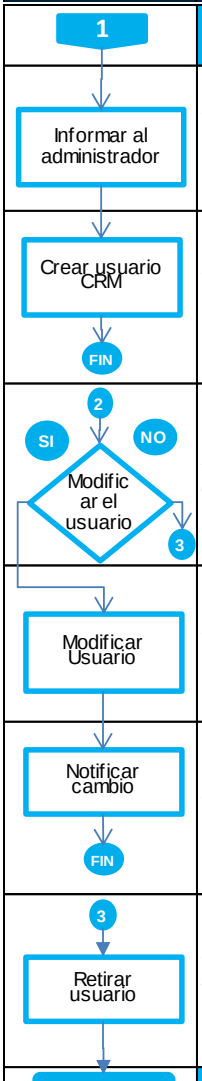
En las tablas 15, 16, 17, 18 y 19 se describen los diferentes procedimientos que la empresa tiene (Ver tablas 15, 16, 17, 18 y 19).

En la tabla 15 se describe el proceso de como el área de sistemas lleva a cabo la creación, modificación y retiro de usuarios de los sistemas de información.

[85] Baker Tilly Colombia. Auditoria Forense [online]. Disponible<http://www.bakertilly.co/servicios/auditoria-forense/>

Tabla 15. Flujograma del Proceso Interno, Gestión de Usuarios.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO	DOCUMENTO ASOCIADO
INICIO				
Solicitar la creación, modificación o retiro de usuario	5.1.1. Realizar la solicitud al área de sistemas para la creación, modificación o retiro de los usuarios. *Nota: Para el caso de incorporación de nuevos colaboradores el proceso de RRHH debe informar como mínimo un día hábil de anticipación.*	Lideres de proceso	Correo Electrónico	N/A
Analizar solicitud	5.1.2. Realizar revisión de la solicitud	Coordinador General de Sistemas	N/A	
NO / SI — El usuario existe? — 2	5.1.3 Verificar que el usuario solicitado no exista	Coordinador General de Sistemas	N/A	N/A
Crear correo electrónico y cuenta en huddle	5.1.4 Crear la cuenta de correo electrónico, para la creación de esta se debe utilizar la inicial del primer nombre + el primer apellido completo del usuario a registrar. Ejemplo. Para el usuario Carlos Andrés Gómez la cuenta de correo es cgomez *Nota: Cuando se presente el caso de coincidencia en inicial y en apellido, se utilizará la inicial del primer nombre + la inicial del segundo nombre + el primer apellido completo*	Coordinador General de Sistemas	F-AGAO-015 Acceso básico y capacitación	N/A
SI / NO — Requier e cuenta Skype — FIN	5.1.5. Verificar si la solicitud requiere creación de usuario en Skype se debe utilizar el usuario de la cuenta de correo agregando el sufijo ".baker" Ejemplo cgomez.baker	Coordinador General de Sistemas	N/A	N/A
Crear usuario de Skype	5.1.6.Crear la cuenta en el servicio de mensajería Skype para lo cual se debe agregar el sufijo ".baker" al usuario de correo electrónico. Ejemplo cgomez.baker	Coordinador General de Sistemas	F-AGAO-015 Acceso básico y capacitación	N/A
SI / NO — Requiere cuenta CRM? — FIN	5.1.7 Verificar si requiere cuenta de CRM	Coordinador General de Sistemas	N/A	N/A
1				

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO	DOCUMENTO ASOCIADO
				
	5.1.8. informar al administrador de la plataforma del requerimiento de creación de usuario. Ejemplo cgomez	Coordinador General de Sistemas	Correo Electrónico	N/A
	5.1.9 Creación del usuario de CRM, con el mismo usuario de correo de electrónico Ejemplo: cgomez	Administrador de aplicación	F-AGAO-015 Acceso básico y capacitación	N/A
	5.1.10 Verificar el sistema de información donde se debe realizar el cambio	Coordinador General de Sistemas	N/A	N/A
	5.1.11 Realizar el cambio requerido sobre el usuario.	Coordinador General de Sistemas	N/A	N/A
	5.1.12. Enviar correo electrónico al usuario notificando los cambios realizados.	Coordinador General de Sistemas	Correo Electrónico	N/A
	5.1.13 Identificar el usuario a retirar en los sistemas de información y procedes a realizar el retiro o inactivación de la cuenta	Coordinador General de Sistemas	N/A	N/A

Fuente: Proceso de calidad Baker Tilly Colombia, Mayo 2012

La tabla 16 se encuentra el proceso de incidencia que la empresa Baker Tilly Colombia Ltda maneja para atender los incidentes que se puedan presentar (Ver tabla 16).

Tabla 16. Flujograma del Proceso Interno, Gestión de Incidencias.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO	DOCUMENTO ASOCIADO
INICIO				
Informar la incidencia	5.2.1 Informar al proceso de sistemas de la incidencia	Cliente interno	Correo electrónico, llamada telefónica y verbalmente	N/A
Registrar incidencia	5.2.3 Registrar la incidencia reportada	Asistente de sistemas	Correo electrónico, llamada telefónica	N/A
1				
1				
Analizar la incidencia	5.2.2. Realizar el análisis y priorización de la incidencia reportada	Asistente de sistemas	F-AGAO-018 Registro de Incidentes	N/A
Diagnosticar Incidencia	5.2.4. Realizar el diagnostico inicial de la incidencia.	Asistente de sistemas	N/A	N/A
NO / SI / Requiere escalar? / 1	5.2.5. Identificar si el daño debe ser escalado al superior inmediato	Asistente de sistemas	N/A	N/A
Solucionar incidencia	5.2.6. Aplicar la solución identificada.	Asistente de sistemas	N/A	N/A
SI / NO / Incidente resuelto? / 1	5.2.7. Verificar si la solución propuesta resuelve el incidencia	Asistente de sistemas	N/A	N/A
Cerrar incidencia / FIN	5.2.8 Constatar con el usuario que la incidencia esta resuelta	Asistente de sistemas	F-AGAO-018 Registro de Incidentes	N/A

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO	DOCUMENTO ASOCIADO
1 → Escalar Solución	5.2.9. Escalar incidencia con el jefe inmediato	Asistente de sistemas	N/A	N/A
Analizar incidencia	5.2.10. Analizar la incidencia y las soluciones aplicadas.	Coordinador General de Sistemas / Gerente de Sistemas e información	N/A	N/A
Solucionar incidencia	5.2.11. Aplicar la soluciones alternas identificadas	Coordinador General de Sistemas	N/A	N/A
Cerrar incidencia	5.2.12. Constatar con el usuario que la incidencia esta resuelta	Coordinador General de Sistemas	F-AGAO-018 Registro de Incidentes	N/A
FIN				

Fuente: Proceso de calidad Baker Tilly Colombia, Mayo 2012

La gestión de disponibilidad, se encarga de realizar un cronograma de mantenimiento de los equipos de cómputo que la empresa tiene, puesto que la empresa posee una política de llevar a cabo el mantenimiento como mínimo dos veces al año, el proceso se puede observar en la tabla 17.

Tabla 17. Flujograma del Proceso Interno, Gestión de la Disponibilidad

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO	DOCUMENTO ASOCIADO
INICIO				
Elaborar cronograma de mantenimientos	5.3.1. Elaborar el cronograma de mantenimiento para los equipo de computo, la política es como mínimo realizar dos mantenimientos al año. *Nota: Para los equipos servidores se realizaran tres mantenimiento al año.*	Coordinador General de Sistemas / Gerente de Sistemas e información	Excel	Cronograma de mantenimientos
Programar mantenimiento	5.3.2. Realizar la programación de los mantenimientos a través de correo electrónico informando la fecha del mantenimiento	Coordinador General de Sistemas	Correo electrónico	N/A

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO	DOCUMENTO ASOCIADO
Ejecutar mantenimiento	5.3.3. Realizar el mantenimiento preventivo y correctivo de acuerdo con el cronograma	Asistente de sistemas	N/A	N/A
Diligenciasr formato de mantenimiento	5.3.4. Registrar en el formato los resultados del mantemiento realizado	Asistente de sistemas	Mantenimiento preventivo	N/A
FIN				

Fuente: Proceso de calidad Baker Tilly Colombia, Mayo 2012

La Gestión de la Configuración y Activos del Servicio permite a la organización realizar cambio de equipos de cómputo a los funcionario, bien sea por deterioro, daño en algún componente y realizar un buen proceso, es por eso que en la tabla 18 enseña el procedimiento.

Tabla 18. Flujograma del Proceso Interno, Gestión de la Configuración y Activos del Servicio

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO	DOCUMENTO ASOCIADO
INICIO				
Solicitar la asignación o cambio de equipo	5.4.1. Realizar la solicitud al área de sistemas para la asignación a cambio de equipo.	Lideres de proceso	N/A	N/A
SI / NO / Existe disponi bilidad? / FIN	5.4.2. Verificar la disponibilidad de equipos de computo, de no existir disponibilidad se debe realizar requision de compra de cuardo con el procedimiento XXX	Coordinador General de Sistemas	N/A	N/A
Asignar equipo	5.4.3 Realizar el alistamiento y asignación del equipo de computo.	Asistente de sistemas	F-AGAO-017 Asignación de equipo	N/A
FIN				

Fuente: Proceso de calidad Baker Tilly Colombia, Mayo 2012

En la Tabla 19 Flujograma del Proceso Interno, Gestión de Operaciones da a conocer el proceso que se realiza para llevar a cabo el respaldo de información de los sistemas de información de los equipos de cómputo que la empresa posee,

para conocer más a detalle este proceso se observar en la tabla dicha anteriormente.

Tabla 19. Flujograma del Proceso Interno, Gestión de Operaciones

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO	DOCUMENTO ASOCIADO
INICIO				
Determinar la información a respaldar	5.5.1. Establecer la información que debe ser respaldada	Lideres de proceso / Gerente de tecnología e información	N/A	N/A
Estimar los recursos requeridos	5.5.2. Determinar la capacidad requerida para respaldar la información así como el esquema a utilizar.	Gerente de tecnología e información / Coordinador General de Sistemas	N/A	N/A
Configurar la herramienta de toma de respaldos	5.5.3. Realizar la configuración de las rutinas de backup en el herramienta para toma de respaldos.	Gerente de tecnología e información / Coordinador General de Sistemas	N/A	Documento de configuración herramienta de toma de respaldos
Realizar monitoreo	5.5.4. Realizar diariamente la revisión de los correos que de forma automática envía la aplicación con el resultado del proceso de toma de backup.	Coordinador General de Sistemas	F-AGAO-016 Control de copias	N/A
Realizar pruebas sobre respaldos	5.5.5 Realizar mensualmente una prueba de restauración del sistema de información SIIGO.	Coordinador General de Sistemas / Líder de proceso	F-AGAO-016 Control de copias	N/A
NO / SI / Prueba satisfac toria? / FIN	5.5.6. Verificar que el respaldo de información sea funcional.	Líder de proceso	F-AGAO-016 Control de copias	N/A
Revisar la configuración de la herramienta de backup	Revisar la configuración de los esquemas de backup que fallaron.			
FIN				

Fuente: Proceso de calidad Baker Tilly Colombia, Mayo 2012

4. CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN Y RECURSOS QUE SE DEBEN PROTEGER EN LA EMPRESA BAKER TILLY COLOMBIA LTDA UTILIZANDO LA METODOLOGÍA MARGERIT

4.1 INTRODUCCIÓN

En el siguiente capítulo se realizará la clasificación de los activos y recursos que se deben proteger en la empresa Baker Tilly Colombia Ltda, teniendo como base la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MARGERIT).

4.2. CLASIFICACIÓN DE LA INFORMACIÓN[86]

La siguiente lista de clasificación de la información puede ser tomada como referencia para que la empresa Baker Tilly la use:

- **Sensitiva**, los datos deben ser protegidos al más alto nivel de seguridad. La publicación o acceso no autorizado a ésta información debería causar el máximo nivel de alerta en la organización.

- **Confidencial**, los datos aquí clasificados son menos restrictivos que los sensitivos pero su publicación podría ocasionar un daño importante en la organización.

- **Privada**, es la información que debe ser protegida contra una publicación deliberada a nivel de departamento, por ejemplo: recursos humanos.

- **Propietaria**, información que generalmente no está disponible a terceros fuera de la organización.

- **Pública**, los datos que están disponibles a terceros y al público en general fuera y dentro de la organización.

4.3. ACTIVOS INFORMATICOS

Los activos informáticos son todos aquellos elementos que la empresa posee para el tratamiento de la información (hardware, software, recurso humano, etc.), el cual se deben diferenciar los activos en varios tipos de acuerdo a la función que ejercen.

[86] RIOS, Julián. Cómo clasificar la información corporativa en términos de seguridad. [online][citando en abril de 2012]. Disponible en internet:< http://www.auditool.org/blog/control-interno/4250-como-clasificar-la-informacion-corporativa-en-terminos-de-seguridad>

4.3.1. Activos de la información área de sistemas

Dentro de los activos o recursos informáticos encontrados en la oficina de Sistemas de Baker Tilly Colombia se encuentran los que están enmarcados en la tabla 20 que a continuación se enseña.

Tabla 20. Activos informáticos en la oficina de Sistemas de Baker Tilly Colombia Ltda.

Recurso	Descripción	Medio
Copias de Seguridad	Copias de seguridad de los diferentes Sistemas de Información de la empresa (SIIGO,Huddle y correo institucional), servidor, base de datos y los equipos de cómputo.	Syncback
Gestión de Identidades	Gestión de las identidades, usuarios, contraseñas y privilegios de las cuentas administrativas para el uso de las computadoras de la compañía y sistemas de información (SIIGO, Huddle, correo institucional).	
Registros de Actividad	Archivos de registros de actividad de los diferentes Sistemas de Información que la empresa contiene.	
Páginas web	Página web para el acceso al público	www.bakertilly.com
Correo Electrónico	Software utilizado para el correo electrónico empresarial.	
Gestores de Bases de Datos	Administran y gestionan las bases de datos que se utilizan para soportar los procesos de la empresa.	SQL Server 2012 R2
Software de Antivirus	Software para prevenir y eliminar el malware.	AVAST versión free
Sistemas Operativos	Software que administra los recursos de los equipos de cómputo de uso empresarial.	Windows 7 Professional Windows 8.1 Pro Windows 10
Firewall	Controla el tráfico entrante/saliente de la red de datos aplicando reglas de seguridad.	**FORTINET** con los servicios: DHCP ANTIVIRUS VPN FIREWALL GESTIÓN DE USO
Servidores	Computadoras especializadas en proveer los recursos, almacenar datos y ejecutar el software y diferentes aplicaciones a través de la red.	Windows 2003 Windows 2008 Server Windows 2012 R2 Server

Recurso	Descripción	Medio
Dispositivos de respaldo.	Dispositivos que almacenan la información y son útiles para la recuperación de desastres.	Cd´s Discos Duros (500 GB y 1TB)
Computadoras Portátiles	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.	
Computadoras de Escritorio	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.	
Escáner	Dispositivos para transformar la información en formato digital.	
Impresoras	Dispositivos para la impresión en papel.	
Router	Redirige el tráfico de datos de la red interna con el exterior. Permite la conexión a internet a través del ISP (Proveedor de Servicios de Internet).	No hay
Switches	Administra las VLANS el permite realizar la segmentación de la red de datos y gestionar y optimizar el ancho de banda, así como expandir la conexión de las computadoras de uso institucional.	
Acces Point	Amplían la cobertura de la red por medio de conexiones inalámbricas.	
Red de Área Local	Permite la interconexión de las computadoras que posee la empresa así como el acceso a los diferentes servicios.	
Rack	Aloja los servidores, router, switches y firewall protegiéndolos de la humedad, golpes o uso malintencionado.	
Fuente de Alimentación	Provee y regula la energía a los Servidores.	
Cableado Eléctrico	Provee energía eléctrica a las instalaciones y dispositivos.	
Sistema de alimentación interrumpida.	Provee energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas (Servidores).	Únicamente para servidores con autonomía de 30 min.

Fuente: Propiedad del Autor

4.3.2. CLASIFICACION DE LOS ACTIVOS DE LA INFOMACIÒN

La clasificación de los activos de la información permite determinar la sensibilidad y criticidad de los activos, con el objetivo de brindar una base para llevar a cabo la protección de los mismos

A continuación se clasificaran los activos según el **Tipo de Activo,** teniendo como guía la metodología MARGERIT**.**

[D] DATOS/INFORMACIÓN

En la tabla 21 muestra los activos (copias de respaldo [backup], registro de actividad [log]) que serán almacenados en equipos de información que dispone la empresa.

Tabla 21. Datos/Información

Código	Subtipo	Descripción	Contenido	Medio
D_BCK	[backup]	Copias de Seguridad de los Sistemas de Información y equipos de cómputo de la empresa.	Copias de seguridad de los diferentes Sistemas de Información de la empresa (SIIGO, Huddle y correo institucional), servidor, base de datos y los equipos de cómputo.	Syncback
D_LOG	[log]	Registros de Actividad.	Archivos de registros de actividad de los diferentes Sistemas de Información.	Logs de los diferentes sistemas de información, servidores, dase de datos de la empresa.

Fuente: Propiedad del autor

[S] SERVICIOS

En la tabla 22 se contemplan los servicios prestados por los sistemas de información que dispone la empresa.

Tabla 22. Servicios

Código	Subtipo	Descripción	Contenido	Medio
S_MAI	[email]	Correo Electrónico	Administran y gestionan las bases de datos que se utilizan para soportar los procesos de la empresa.	Correo institucional que cada funcionario posee. (nombre@bakertillycolombia.com)

Código	Subtipo	Descripción	Contenido	Medio
S_WWW	[www]	Página Web.	Página web para el acceso al público.	www.bakertilly.com
S_GID	[int]	Gestión de Identidades	Gestión de las identidades, usuarios, contraseñas y privilegios de las cuentas administrativas para el uso de las computadoras de la compañía.	Existencia de un proceso para la creación, modificación y eliminación de usuarios y que es realizado por el personal del área de sistemas de la empresa.

Fuente: Propiedad del autor

[SW] SOFTWARE

En la tabla 23 se muestran las aplicaciones que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios que presta la compañía.

Tabla 23. Software

Código	Subtipo	Descripción	Contenido	Medio
SW_DBS	[dbms]	Gestores de Bases de Datos	Software utilizado para el correo electrónico empresarial.	Se dispone de un motor de base de datos. (SQL server 2012 r2)
SW_OFM	[office]	Ofimática	Software necesario para la realización de las actividades de los funcionarios de la empresa.	Microsoft Office Professional Plus 2013
SW_AVS	[antivirus]	Software de Antivirus	Software para prevenir y eliminar el malware.	Avast Free Antivirus
SW_OPS	[os]	Sistemas Operativos	Software que administra los recursos de las computadoras de uso institucional.	Microsoft Windows Professional 7. Windows 8.1 pro. Windows 10.

Fuente: Propiedad del autor

[HW] HARDWARE

La tabla 24 enseña los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.

Tabla 24. Hardware

Código	Subtipo	Descripción	Contenido	Medio
HW_BCK	[backup]	Dispositivos de Respaldo	Dispositivos que almacenan la información y son útiles para la recuperación de desastres.	Cd´s Discos Duros (500 GB y 1TB)
HW_FRW	[firewall]	Firewall	Controla el tráfico entrante/saliente	FORTINET

Código	Subtipo	Descripción	Contenido	Medio
			de la red de datos aplicando reglas de seguridad.	
HW_HOS	[host]	Servidores	Equipos especializados en proveer los recursos, almacenar datos y ejecutar el software y diferentes aplicaciones a través de la red.	**-BTCW01 –** Windows 2003, SIN SOPORTE **-BTCW03** Windows 2008 SERVER SIN LICENCIA **-BTCW04 -** WINDOWS 2003 sin Soporte **-BTCW05 –** Windows 2012 R2 server con Soporte y licencia.
HW_PCM	[mobile]	Computadoras Portátiles.	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.	
HW_PCP	[pc]	Computadoras de Escritorio.	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.	
HW_PRT	[print]	Impresoras	Dispositivos para la impresión en papel.	
HW_ROU	[router]	Router	Redirige el tráfico de datos de la red interna con el exterior. Permite la conexión a internet a través del ISP (Proveedor de Servicios de Internet).	
HW_SCN	[scaner]	Escáner	Dispositivos para transformar la información en formato digital.	
HW_SWH	[switch]	Switch	Administra las VLAN el permite realizar la segmentación de la red de datos y gestionar y optimizar el ancho de banda, así como expandir la conexión de las computadoras de uso institucional.	2 SWITCH HP
HW_WAP	[wap]	Acces Point	Amplían la cobertura de la red por medio de conexiones inalámbricas.	

Fuente: Propiedad del autor

[COM] COMUNICACIONES

La tabla 25 incluye los medios de transporte que llevan datos de un sitio a otro, incluyendo los servicios de comunicaciones contratados (Ver tabla 25).

Tabla 25. Comunicaciones

Código	Subtipo	Descripción	Contenido	Medio
COM_INT	[internet]	Internet	Permite el acceso a recursos de la web.	Canal principal 20 Megas de UNE Canal secundario 12 Megas de CLARO.
COM_LAN	[LAN]	Red de Área Local	Permite la interconexión de las computadoras que posee la empresa así como acceso a los diferentes servicios.	
COM_WIF	[wifi]	Conectividad Inalámbrica	Permite la conectividad inalámbrica de las computadoras, así como amplía la cobertura.	

Fuente: Propiedad del autor

[AUX] EQUIPO AUXILIAR

La tabla 26 se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

Tabla 26. Equipo Auxiliar.

Código	Subtipo	Descripción	Contenido	Medio
AUX_RCK	[furniture]	Rack	Aloja los servidores, router, switches y firewall protegiéndoles de la humedad, golpes o uso malintencionado.	
AUX_PWR	[power]	Fuente de Alimentación	Provee y regula la energía a los Servidores.	
AUX_UPS	[ups]	Sistema de Alimentación Ininterrumpida.	Provee energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas.	UPS que tienen una autonomía de 30 minutos.
AUX_WIR	[wire]	Cableado Eléctrico	Provee energía eléctrica a las instalaciones y dispositivos.	

Fuente: Propiedad del autor

[L] INSTALACIONES

En la tabla 27 se encuentra el lugar donde se hospedan los sistemas de información y comunicaciones que dispone la empresa.

Tabla 27. Instalaciones

Código	Subtipo	Descripción	Contenido	Medio
L_SIT	[site]	Oficina de Sistemas	Estructura física que alberga la Oficina de Sistemas de Información de la empresa.	Edificio de 6 plantas.

Fuente: Propiedad del autor

[P] PERSONAL

La tabla 28 enseña el personal encargado de manejar los sistemas de información de la compañía.

Tabla 28. Personal

Código	Subtipo	Descripción	Contenido	Responsable
P_GTE	[gte]	Gerente de información y tecnología	Persona encargada de planificar la estrategia de tecnologías de información de la Firma alineadas a los objetivos del negocio	Gerente de información y tecnología.
P_CGS	[cgs]	Coordinador General de Sistemas	Persona encargada de garantizar diariamente el correcto funcionamiento de los equipos de la firma, los servidores, aplicaciones, red interna e internet de la firma.	Coordinador General de Sistemas.
P_AUX	[aux]	Auxiliar de Sistemas	Persona encargada de realizar el mantenimiento preventivo de los equipos de cómputo de la Firma de acuerdo al procedimiento establecido.	Coordinador General de Sistemas.

Fuente: Propiedad del autor

4.4. DIMENSIONES DE VALORACIÓN

Las dimensiones de valoración son aquellas características que hacen que un activo sea valioso para la organización y se utilizan para valorar las consecuencias de la materialización de una amenaza.

4.4.1 DE ACUERDO AL IMPACTO

La valoración de los activos de la oficina de Sistemas de Baker Tilly Colombia Ltda se determina de acuerdo al tipo ***Cualitativo*** que establece MAGERIT y el impacto que tiene en la empresa, de acuerdo a la siguiente escala que enseña la tabla 29.

Tabla 29. Valoración cualitativa de los activos informáticos en MAGERIT.

Impacto	Nomenclatura	Valor	Descripción
MUY ALTO	**MA**	**10**	El daño tiene consecuencias muy graves para la organización y podrían ser irreversibles.
ALTO	**A**	**7 – 9**	El daño tiene consecuencias muy graves para la organización.
MEDIO	**M**	**4 – 6**	El daño contiene consecuencias relevantes para la organización y

Impacto	Nomenclatura	Valor	Descripción
			su operación.
BAJO	B	1 – 3|	El daño contiene consecuencias relevantes, pero no afecta a una gran parte de la organización.
MUY BAJO	MB	0	El daño no contiene consecuencias relevantes para la organización.

Fuente: SUÁREZ, L., AMAYA, C. A. Sistema de Gestión de la Seguridad de la Información. Bogotá: UNAD. 2013. p. 52.

[D] DATOS/INFORMACIÓN

La tabla 30 enseña el impacto que tiene el activo de Datos/Información en la organización si estos tuvieran algún incidente.

Tabla 30. Impacto Datos/Información

Código	Descripción	Impacto	Razón
D_BCK	Copias de Seguridad de los Sistemas de Información.	MA	Los archivos de copias de seguridad son determinantes para la recuperación de información si existe algún evento de desastres.
D_LOG	Registros de Actividad.	MA	Los archivos de registros son esenciales para realizar seguimiento a fallos en los Sistemas de información para determinar posibles causas de malfuncionamiento o acceso no autorizado.

Fuente: Propiedad del autor

[S] SERVICIOS

En la tabla 31 se muestra el impacto que tiene cada uno de los servicios que posee la empresa.

Tabla 31. Impacto de los Servicios

Código	Descripción	Impacto	Razón
S_MAI	Correo Electrónico	A	El correo electrónico se utiliza para la comunicación interna de los funcionarios.
S_WWW	Página Web.	M	Acceso a la página web de la compañía que oferecen servicios al público interesado.
S_GID	Gestión de Identidades	MA	Acceso del personal administrativo a sus cuentas de usuario en el dominio de la organización.

Fuente: Propiedad del autor

[SW] SOFTWARE

La tabla 32 da a conocer el impacto que tiene los activos de software si sufriera algún incidente en la empresa.

Tabla 32. Impacto del Software

Código	Descripción	Impacto	Razón
SW_DBS	Gestores de Bases de Datos	MA	Almacena toda la información de los diferentes Sistemas de Información, así como el soporte para el desarrollo normal de los procesos y tomas de decisiones. Dentro de ellos se encuentran…
SW_OFM	Ofimática	B	Utilizado para la ejecución de tareas.
SW_AVS	Software de Antivirus	M	Utilizado para la prevención y eliminación de software malintencionado, así como evitar la propagación de malware por la red.
SW_OPS	Sistemas Operativos	M	Administra los recursos de software y hardware de las diferentes computadoras que se utiliza en la empresa.

Fuente: Propiedad del autor

[HW] HARDWARE

En la tabla 33 (Impacto del Hardware), muestra el impacto que tendría en la organización en caso de un incidente.

Tabla 33. Impacto del Hardware

Código	Descripción	Impacto	Razón
HW_BCK	Dispositivos de Respaldo	MA	Dispositivos que almacenan los archivos de las copias de seguridad necesarios para la recuperación en caso de desastres.
HW_FRW	Firewall	MA	Dispositivo que filtra los paquetes. Esencial para la configuración de seguridad de la red de datos.
HW_HOS	Servidores	MA	Dispositivos esenciales para el correcto funcionamiento de los diferentes Sistemas de Información que soportan los procesos institucionales. Dentro de ellos se encuentran los Servidores de Aplicaciones, DNS, Bases de Datos, Mail y Web.
HW_PCM	Computadoras Portátiles.	B	Dispositivos para la ejecución de tareas.
HW_PCP	Computadoras de Escritorio.	B	Dispositivos para la ejecución de tareas.
HW_PRT	Impresoras	MB	Dispositivo para realizar impresiones en papel.
HW_ROU	Router	A	Esencial para direccionar el tráfico de datos interno y externo. A su vez, hace el papel de Gateway para dar salida a Internet.
HW_SCN	Escáner	MB	Dispositivo para digitalizar documentos.
HW_SWH	Switch	A	Esencial para direccionar el tráfico de datos

Código	Descripción	Impacto	Razón
			interno, administración y segmentar el ancho de banda con el fin de optimizarla.
HW_WAP	Acces Point	B	Dispositivos que amplían la cobertura de la red para dar acceso inalámbrico.

Fuente: Propiedad del autor

[COM] COMUNICACIONES

La tabla 34 enseña el impacto que tendría la empresa donde le activo de las comunicaciones sufriera fallas.

Tabla 34. Impacto de la Comunicaciones

Código	Descripción	Impacto	Razón
COM_INT	Internet	A	Esencial para tener acceso a redes externas.
COM_LAN	Red de Área Local	MA	Esencial para la transmisión de datos y dar soporte al normal funcionamiento de los servicios internos. Incluye todo el cableado estructurado.
COM_WIF	Conectividad Inalámbrica	B	Amplía la cobertura y otorga acceso inalámbrico a estos tipos de dispositivos.

Fuente: Propiedad del autor

[AUX] EQUIPO AUXILIAR

El activo de equipo auxiliar posee una serie de impactos que la tabla 35 da a conocer.

Tabla 35. Impacto del Equipo Auxiliar

Código	Descripción	Impacto	Razón
AUX_RCK	Rack	A	Otorga alta velocidad de transmisión en el tráfico de datos interno. Da soporte de conectividad a toda la institución.
AUX_PWR	Fuente de Alimentación	MA	Esencial para el funcionamiento normal de todos los dispositivos que soportan los Sistemas de Información y procesos de la compañía.
AUX_UPS	Sistema de Alimentación Ininterrumpida.	A	Esencial para mantener funcionando a los dispositivos en caso de una eventual falla en el suministro eléctrico, así como también evita el daño parcial o total del hardware.
AUX_WIR	Cableado Eléctrico	MA	Cableado esencial para mantener en funcionamiento los dispositivos y el normal desarrollo de los procesos institucionales.

Fuente: Propiedad del autor

[L] INSTALACIONES

El activo Instalaciones es uno de los más importantes en la valoración, es por esto que la tabla 36 enseña el impacto que tiene este activo.

Tabla 36. Impacto en la Instalaciones

Código	Descripción	Impacto	Razón
L_SIT	Oficina de Sistemas	MA	Esencial para el normal funcionamiento de todos los Sistemas de Información que soportan los procesos institucionales.

Fuente: Propiedad del autor

[P] PERSONAL

La tabla 37 muestra el impacto que tiene el personal en la organización.

Tabla 37. Impacto del Personal

Código	Descripción	Impacto	Razón
P_GTE	Gerente de información y tecnología	MA	
P_CGS	Coordinador General de Sistemas	A	Personas encargadas de administrar los diferentes Sistemas de Información que dan soporte a los procesos institucionales y sus servicios.
P_AUX	Auxiliar de Sistemas	B	Personas encargadas de dar soporte a los diferentes equipos que dispone la organización.

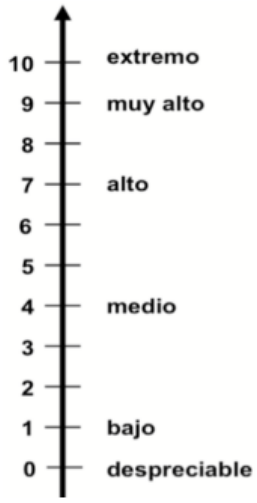
Fuente: Propiedad del autor

4.4.1.1. Criterios de valoración

La metodología MARGERIT, da a conocer una escala de valoración, cuyo objetivo es realizar una valoración cualitativa dando respuesta a valoraciones subjetivas por parte del personal de la empresa.

En la figura 12 enseña los criterios de valoración que maneja la metodología MARGERIT (Ver figura 12).

Figura 12. Criterios de Valoración



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 19

4.4.1.2. Valoración de los activos

Las tablas siguientes pretenden guiar con más detalle a los usuarios valorando de forma homogénea activos cuyo valor es importante por diferentes motivos[87].

Tabla 38. Escala Estándar Información de carácter personal

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo

[87] AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II. Óp. Cit. P.19-23.

Tabla 39. Escala Estándar Obligaciones legales

[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación

Tabla 40. Escala Estándar Seguridad

[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Tabla 41. Escala Estándar Intereses comerciales o económicos

[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	Causa de muy significativas ganancias o ventajas para individuos u organizaciones.
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales

[cei] Intereses comerciales o económicos		
		relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas

Tabla 42. Escala Estándar Interrupción del servicio

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

Tabla 43. Escala Estándar Orden Público

[po] Orden público		
9	9.po	alteración sería del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

Tabla 44. Escala Estándar Operaciones

[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

Tabla 45. Escala Estándar Administración y Gestión

[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.adm	Probablemente impediría la operación efectiva de una parte de la Organización.
1	1.adm	Pudiera impedir la operación efectiva de una parte de la Organización.

Tabla 46. Escala Estándar Pérdida de confianza (reputación)

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar

[lg] Pérdida de confianza (reputación)		
		negativamente a las relaciones con otras organizaciones.
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

Tabla 47. Escala Estándar Persecución de delitos

[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

Tabla 48. Escala Estándar tiempo de recuperación del servicio

[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

Tabla 49. Escala Estándar Información Clasificada (Nacional)

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

4.2.2 DE ACUERDO A LAS DIMENSIONES DE SEGURIDAD

4.4.2.1. Criterios de valoración

El objetivo de las dimensiones de seguridad es valorar la información en los siguientes aspectos [D] Disponibilidad, [I] Integridad, [C] Confidencialidad [A] Autenticidad y [T] Trazabilidad para determinar que tan relevante es ese activo y cómo afectaría a la empresa se llegara a materializar el daño.

4.4.2.2. Valoración de activos

La metodología MARGERIT tiene de una escala estándar, esta se puede observar en el apartado **4.4.1.2. Valoración de los activos,** a continuación se va a realizar la valoración de los activos que dispone la empresa.

[D] DATOS/INFORMACIÓN

En la tabla 50 enseña los diferentes valores referentes a la dimensión de seguridad del activo datos/información

Tabla 50. Dimensión de Seguridad – Datos/Información

Código	Descripción	Dimensión de Seguridad				
		[D]	[I]	[C]	[A]	[T]
D_BCK	Copias de Seguridad de los Sistemas de Información.	**3**		**2**		
D_LOG	Registros de Actividad.			**2**		**3**

Código	Dimensión de Seguridad	Descripción
D_BCK	**[D]**	**3. adm:** Probablemente impediría la operación efectiva de una parte de la Organización.
	[C]	**2. lg:** Probablemente cause una pérdida menor de la confianza dentro de la Organización.
D_LOG	**[C]**	**2. lg:** Probablemente cause una pérdida menor de la confianza dentro de la Organización.
	[T]	**3.si:** Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.

Fuente: Propiedad del Autor

[S] SERVICIOS

La tabla 51 da a conocer los diferentes valores referentes a la dimensión de seguridad del activo servicios

Tabla 51. Dimensión de Seguridad – Servicios

Código	Descripción	Dimensión de Seguridad				
		[D]	[I]	[C]	[A]	[T]
S_MAI	Administran y gestionan las bases de datos que se utilizan para soportar los procesos de la empresa.	3		2		
S_WWW	Página web para el acceso al público.	3				
S_GID	Gestión de las identidades, usuarios, contraseñas y privilegios de las cuentas administrativas para el uso de las computadoras de la compañía.	5	2	2		4

Código	Dimensión de Seguridad	Descripción
S_MAI	**[D]**	**3. adm:** Probablemente impediría la operación efectiva de una parte de la Organización.
	[C]	**2. lg:** Probablemente cause una pérdida menor de la confianza dentro de la Organización.
S_WWW	**[D]**	**3. adm:** Probablemente impediría la operación efectiva de una parte de la Organización.
S_GID	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización.
	[I]	**2.pi1:** Pudiera causar molestias a un individuo.
	[C]	**2.lg:** Probablemente cause una pérdida menor de la confianza dentro de la Organización.
	[T]	**4.crm:** Dificulte la investigación o facilite la comisión de delitos.

Fuente: Propiedad del Autor

[SW] SOFTWARE

En la tabla 52 enseña los diferentes valores referentes a la dimensión de seguridad del activo Software.

Tabla 52. Dimensión de Seguridad – Software

Código	Descripción	Dimensión de Seguridad				
		[D]	[I]	[C]	[A]	[T]
SW_DBS	Gestores de Bases de Datos	7	7	7	7	

SW_OFM	Ofimática	**1**				
SW_AVS	Software de Antivirus			**7**		
SW_OPS	Sistemas Operativos	**5**	**7**			

Código	Dimensión de Seguridad	Descripción
SW_DBS	**[D][I][A]**	**7.adm:** Probablemente impediría la operación efectiva de la Organización
	[C]	**7.lro:** Probablemente cause un incumplimiento grave de una ley o regulación
SW_OFM	**[D]**	**1.adm:** Pudiera impedir la operación efectiva de una parte de la Organización
SW_AVS	**[C]**	**7.si:** Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
SW_OPS	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización
	[I]	**7.si:** Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

Fuente: Propiedad del Autor

[HW] HARDWARE

La tabla 53 enseña los diferentes valores referentes a la dimensión de seguridad del activo Hardware.

Tabla 53. Dimensión de Seguridad – Hardware

Código	Descripción	Dimensión de Seguridad				
		[D]	[I]	[C]	[A]	[T]
HW_BCK	Dispositivos de Respaldo			**2**		**3**
HW_FRW	Firewall	**7**				
HW_HOS	Servidores	**5**		**7**	**7**	
HW_PCM	Computadoras Portátiles.	**1**				
HW_PCP	Computadoras de Escritorio.	**1**				
HW_PRT	Impresoras	**1**				
HW_ROU	Router	**5**			**7**	
HW_SCN	Escáner	**1**				
HW_SWH	Switch	**5**			**7**	
HW_WAP	Acces Point	**1**				

Código	Dimensión de Seguridad	Descripción
HW_BCK	**[C]**	**2.lg:** Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[T]	**3.si:** Probablemente sea causa de

		una merma en la seguridad o dificulte la investigación de un incidente
HW_FRW	**[D]**	**7.si:** Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_HOS	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización
	[C][A]	**7.si:** Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_PCM	**[D]**	**1.adm:** Pudiera impedir la operación efectiva de una parte de la Organización
HW_PCP	**[D]**	**1.adm:** Pudiera impedir la operación efectiva de una parte de la Organización.
HW_PRT	**[D]**	**1.adm:** Pudiera impedir la operación efectiva de una parte de la Organización.
HW_ROU	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización
	[T]	**7.si:** Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_SCN	**[D]**	**1.adm:** Pudiera impedir la operación efectiva de una parte de la Organización.
HW_SWH	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización
	[T]	**7.si:** Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_WAP	**[D]**	**1.adm:** Pudiera impedir la operación efectiva de una parte de la Organización

Fuente: Propiedad del Autor

[COM] COMUNICACIONES

La tabla 54 da a conocer la calificación que se le proporcionó al activo de comunicaciones de acuerdo a la dimensión de seguridad.

Tabla 54. Dimensión de Seguridad – Comunicaciones

Código	Descripción	Dimensión de Seguridad				
		[D]	[I]	[C]	[A]	[T]
COM_INT	Internet	**3**				
COM_LAN	Red de Área Local	**5**				
COM_WIF	Conectividad Inalámbrica	**1**				

Código	Dimensión de Seguridad	Descripción
COM_INT	**[D]**	**3.adm:** Probablemente impediría la operación efectiva de una parte de la Organización
COM_LAN	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización
COM_WIF	**[D]**	**1.adm:** Pudiera impedir la operación efectiva de una parte de la Organización

Fuente: Propiedad del Autor.

[AUX] EQUIPO AUXILIAR

La tabla 55 enseña los diferentes valores referentes a la dimensión de seguridad del activo Equipo Auxiliar.

Tabla 55. Dimensión de Seguridad – Equipo Auxiliar

Código	Descripción	Dimensión de Seguridad				
		[D]	[I]	[C]	[A]	[T]
AUX_RCK	Rack	**5**				
AUX_PWR	Fuente de Alimentación	**5**				
AUX_UPS	Sistema de Alimentación Ininterrumpida.	**5**				
AUX_WIR	Cableado Eléctrico	**5**				

Código	Dimensión de Seguridad	Descripción
AUX_RCK	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_PWR	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_UPS	**[D]**	**5.adm:** Probablemente impediría la

		operación efectiva de más de una parte de la Organización
AUX_WIR	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización

Fuente: Propiedad del Autor

[L] INSTALACIONES

La tabla 56 enseña los diferentes valores referentes a la dimensión de seguridad del activo Instalaciones.

Tabla 56. Dimensión de Seguridad – Instalaciones

Código	Descripción	Dimensión de Seguridad				
		[D]	[I]	[C]	[A]	[T]
L_SIT	Oficina de Sistemas	**7**				

Código	Dimensión de Seguridad	Descripción
L_SIT	**[D]**	**7.adm:** Probablemente impediría la operación efectiva de la Organización

Fuente: Propiedad del Autor

[P] PERSONAL

La tabla 57 enseña los diferentes valores referentes a la dimensión de seguridad del activo Personal.

Tabla 57. Dimensión de Seguridad – Personal

Código	Descripción	Dimensión de Seguridad				
		[D]	[I]	[C]	[A]	[T]
P_GTE	Gerente de información y tecnología	5				
P_CGS	Coordinador General de Sistemas	5				
P_AUX	Auxiliar de Sistemas	1				

Código	Dimensión de Seguridad	Descripción
P_GTE	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización
P_CGS	**[D]**	**5.adm:** Probablemente impediría la operación efectiva de más de una parte de la Organización
P_AUX	**[D]**	**1.adm:** Pudiera impedir la operación efectiva de una parte de la Organización

Fuente: Propiedad del Autor

4.5 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS.

De acuerdo a las amenazas que se identifican en MAGERIT, éstas se establecen para cada activo determinando su probabilidad o frecuencia de ocurrencia y el impacto que tiene en cada una de las dimensiones de seguridad**.**

4.5.1. Criterios de Evaluación

De acuerdo al impacto potencial se determinó los diferentes niveles de impacto dando unos porcentajes que se muestran en la tabla 58 los cuales serán aplicados a los diferentes activos que dispone la empresa.

Tabla 58. Impacto

IMPACTO	VALOR CUANTITATIVO
Muy Alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy Bajo	5%

FUENTE: GYSSELL, Carem, Memoria. PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001: 2005.[online][citado en abril de 2012]. Disponible en Internet: <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23088/12/cnietogTFM0613memoria.pdf>. Pág. 22.

4.5.2. Evaluación de las amenazas a los activos

Tomando como base la tabla 58 Impacto, se dispone a realizar la evaluación de las amenazas de los diferentes activos que tiene la empresa Baker Tilly Colombia Ltda, cabe resaltar que en caso materializarse una amenaza el impacto podría ser del 5% al 100% de pérdida del valor del activo.

Así mismo, teniendo en cuenta la dimensión de seguridad de cada activo se asignará un porcentaje (%) de impacto.

Por otro lado la frecuencia es tomada con base a la tabla 7 Probabilidad o Frecuencia de ocurrencia de las amenazas en MAGERIT (ver tabla 7).

[D] DATOS/INFORMACIÓN – COPIAS DE SEGURIDAD

En la tabla 59 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo copias de seguridad (Ver tabla 59).

Tabla 59. Evaluación de Amenazas – Copia de Seguridad

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
D-DATOS/INFORMACIÓN						
Copia de Seguridad de los Sistemas de Información						
5.3.1. [E.1] Errores de los usuarios	5	5%	50%	75%	0%	0%
5.3.10. [E.15] Alteración accidental de la información	5	0%	100%	20%	0%	0%
5.3.11. [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12. [E.19] Fugas de información	5	0%	0%	100%	0%	0%
5.3.9. [E.14] Escapes de información	5	50%	50%	75%	0%	0%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	0%	100%	0%	0%
5.4.14. [A.18] Destrucción de información	5	0%	100%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	5	0%	0%	100%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	75%	75%	0%	0%

Fuente: Propiedad del Autor

[D] DATOS/INFORMACIÓN – REGISTRO DE ACTIVIDAD

En la tabla 60 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Registro de Actividad.

Tabla 60. Evaluación de Amenazas – Registro de Actividad

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
D-DATOS/INFORMACIÓN						
Registro de Actividad						
5.3.11. [E.18] Destrucción de información	5	20%	0%	0%	0%	0%
5.3.12. [E.19] Fugas de información	5	0%	0%	100%	0%	0%
5.3.3. [E.3] Errores de monitorización (log)	5	100%	0%	0%	0%	100%
5.4.1. [A.3] Manipulación de los registros de actividad (log)	5	0%	100%	0%	0%	100%
5.4.13. [A.15] Modificación deliberada de la información	5	100%	100%	0%	0%	0%
5.4.14. [A.18] Destrucción de información	5	100%	100%	0%	0%	0%

Fuente: Propiedad del Autor

[S] SERVICIOS – CORREO ELECTRÓNICO

En la tabla 61 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo correo electrónico (Ver tabla 61).

Tabla 61. Evaluación de Amenazas – Correo Electrónico

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
S-SERVICIOS						
Correo Electrónico						
5.3.1. [E.1] Errores de los usuarios	50	0%	0%	0%	0%	0%
5.3.10. [E.15] Alteración accidental de la información	10	0%	75%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.3.9. [E.14] Escapes de información	50	0%	0%	100%	0%	0%
5.4.11. [A.13] Repudio	5	0%	0%	0%	100%	20%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	100%	0%	0%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	10	0%	0%	100%	0%	0%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.3. [A.5] Suplantación de la identidad del usuario	5	0%	0%	75%	75%	20%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	100%	75%	0%	0%
5.4.8. [A.10] Alteración de secuencia	5	0%	100%	0%	100%	0%
5.4.9. [A.11] Acceso no autorizado	10	0%	0%	100%	0%	0%

Fuente: Propiedad del Autor

[S] SERVICIOS – GESTIÓN DE ENTIDADES

En la tabla 62 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Gestión de identidades.

Tabla 62. Evaluación de Amenazas – Gestión de Identidades

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
S-SERVICIOS						
Gestión de Identidades						
5.3.10. [E.15] Alteración accidental de la información	5	0%	100%	0%	100%	20%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.3.9. [E.14] Escapes de información	50	0%	0%	50%	0%	0%
5.4.11. [A.13] Repudio	5	0%	0%	0%	50%	0%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	100%	100%	0%	0%
5.4.14. [A.18] Destrucción de	5	100%	0%	0%	0%	0%

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
información						
5.4.15. [A.19] Divulgación de información	5	0%	0%	100%	0%	0%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.3. [A.5] Suplantación de la identidad del usuario	5	0%	0%	100%	75%	20%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	100%	75%	100%	20%
5.4.9. [A.11] Acceso no autorizado	5	0%	0%	100%	0%	0%

Fuente: Propiedad del Autor

[S] SERVICIOS – PAGINA WEB

En la tabla 63 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Página Web.

Tabla 63. Evaluación de Amenazas – Página Web

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
S-SERVICIOS						
Página Web						
5.3.10. [E.15] Alteración accidental de la información	10	0%	0%	50%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[SW] SOFTWARE – GESTIÓN BASE DE DATOS

En la tabla 64 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo gestores de base de datos en cada uno de sus ítems.

Tabla 64. Evaluación de Amenazas – Gestores de Base de Datos

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
SW-SOTFWARE						
Gestores de Base de Datos						
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	75%	75%	0%	75%
5.3.1. [E.1] Errores de los usuarios	10	5%	5%	5%	0%	0%
5.3.10. [E.15] Alteración accidental de la información	5	75%	75%	0%	75%	0%
5.3.11. [E.18] Destrucción de	5	100%	0%	0%	0%	0%

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
información						
5.3.12. [E.19] Fugas de información	5	0%	100%	100%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	10	50%	75%	75%	0%	0%
5.3.2. [E.2] Errores del administrador	10	50%	50%	50%	0%	0%
5.3.6. [E.8] Difusión de software dañino	5	5%	5%	5%	0%	0%
5.3.9. [E.14] Escapes de información	5	0%	0%	75%	0%	0%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	100%	100%	100%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	5	0%	75%	100%	0%	0%
5.4.16. [A.22] Manipulación de programas	5	0%	50%	50%	0%	0%
5.4.3. [A.5] Suplantación de la identidad del usuario	10	0%	0%	50%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	100%	0%
5.4.5. [A.7] Uso no previsto	5	75%	75%	75%	75%	0%
5.4.6. [A.8] Difusión de software dañino	5	5%	5%	5%	0%	0%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	0%	20%	0%	0%	0%
5.4.8. [A.10] Alteración de secuencia	5	50%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	100%	100%	100%	100%	0%

Fuente: Propiedad del Autor

[SW] SOFTWARE – OFIMÁTICA

En la tabla 65 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Ofimática.

Tabla 65. Evaluación de Amenazas – Ofimática

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
SW-SOTFWARE						
Ofimática						
5.2.6. [I.5] Avería de origen físico o lógico	10	20%	0%	0%	0%	0%
5.3.1. [E.1] Errores de los usuarios	50	5%	0%	0%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	50	50%	0%	0%	0%	0%
5.3.6. [E.8] Difusión de software dañino	10	50%	0%	0%	75%	0%
5.4.5. [A.7] Uso no previsto	50	0%	0%	0%	0%	0%
5.4.6. [A.8] Difusión de software dañino	5	50%	0%	50%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	50%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[SW] SOFTWARE – SISTEMAS OPERATIVOS

En la tabla 66 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo sistemas operativos.

Tabla 66. Evaluación de Amenazas – Sistemas Operativos

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
SW-SOTFWARE						
Sistemas Operativos						
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.3.1. [E.1] Errores de los usuarios	10	75%	0%	0%	0%	20%
5.3.10. [E.15] Alteración accidental de la información	10	50%	20%	20%	0%	0%
5.3.11. [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12. [E.19] Fugas de información	5	0%	0%	75%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	5	50%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	75%	0%	0%	0%	20%
5.3.6. [E.8] Difusión de software dañino	10	75%	50%	0%	0%	0%
5.3.9. [E.14] Escapes de información	5	0%	0%	5%	0%	0%
5.4.13. [A.15] Modificación deliberada de la información	5	75%	100%	100%	0%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	5	0%	0%	100%	0%	0%
5.4.16. [A.22] Manipulación de programas	5	0%	0%	50%	0%	50%
5.4.3. [A.5] Suplantación de la identidad del usuario	5	100%	100%	100%	0%	20%
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	0%	20%
5.4.5. [A.7] Uso no previsto	5	50%	0%	0%	0%	0%
5.4.6. [A.8] Difusión de software dañino	5	75%	0%	0%	0%	0%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	50%	0%	0%	0%	0%
5.4.8. [A.10] Alteración de secuencia	5	50%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	75%	75%	0%	20%

Fuente: Propiedad del Autor

[SW] SOFTWARE – ANTIVIRUS

En la tabla 67 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo antivirus.

Tabla 67. Evaluación de Amenazas – Antivirus

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
SW-SOTFWARE						
Antivirus						
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.3.1. [E.1] Errores de los usuarios	50	50%	0%	0%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	10	50%	0%	0%	0%	0%
5.3.6. [E.8] Difusión de software dañino	10	75%	0%	0%	75%	0%
5.4.5. [A.7] Uso no previsto	5	20%	0%	0%	0%	0%
5.4.6. [A.8] Difusión de software dañino	5	50%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	100%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[HW] HARDWARE - COMPUTADORAS DE ESCRITORIO

En la tabla 68 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo computadoras de escritorio.

Tabla 68. Evaluación de Amenazas – Computadoras de Escritorio

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Computadoras de Escritorio						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	10	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	50%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%

5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Fuente: Propiedad del Autor

[HW] HARDWARE - COMPUTADORAS PORTÁTILES

En la tabla 69 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo portátil.

Tabla 69. Evaluación de Amenazas – Computadoras Portátiles

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Computadoras Portátiles						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	20%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	10	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	50%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Fuente: Propiedad del Autor

[HW] HARDWARE - DISPOSITIVOS DE RESPALDO

En la tabla 70 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo dispositivos de respaldo.

Tabla 70. Evaluación de Amenazas – Dispositivos de Respaldo

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Dispositivos de Respaldo						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	5	50%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	75%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	5	50%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	50%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Fuente: Propiedad del Autor

[HW] HARDWARE - ESCÁNER

En la tabla 71 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo escáner.

Tabla 71. Evaluación de Amenazas – Escáner

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Escáner						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%

5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	10	75%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[HW] HARDWARE - FIREWALL

En la tabla 72 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo firewall.

Tabla 72. Evaluación de Amenazas – Firewall

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Firewall						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	5	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	75%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	0%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Fuente: Propiedad del Autor

[HW] HARDWARE - IMPRESORA

En la tabla 73 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo copias de seguridad.

Tabla 73. Evaluación de Amenazas – Impresora

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Impresora						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	10	75%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[HW] HARDWARE – ACCESS POINT

En la tabla 74 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Access Point.

Tabla 74. Evaluación de Amenazas – Access Point

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Access Point						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	5	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%

5.3.2. [E.2] Errores del administrador	10	75%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Fuente: Propiedad del Autor

[HW] HARDWARE - ROUTER

En la tabla 75 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo router.

Tabla 75. Evaluación de Amenazas – Router

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Router						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	5	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	75%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Fuente: Propiedad del Autor

[HW] HARDWARE - SERVIDORES

En la tabla 76 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo servidores.

Tabla 76. Evaluación de Amenazas – Servidores

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Servidores						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	5	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	75%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Fuente: Propiedad del Autor

[HW] HARDWARE - SWITCH

En la tabla 77 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Switch.

Tabla 77. Evaluación de Amenazas – Switch

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Switch						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%

5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	5	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	75%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Fuente: Propiedad del Autor

[COM] COMUNICACIONES - CONECTIVIDAD INALÁMBRICA

En la tabla 78 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo conectividad inalámbrica.

Tabla 78. Evaluación de Amenazas – Conectividad Inalámbrica

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
COM-COMUNICACIONES						
Conectividad Inalámbrica						
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	10	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	20%	0%	0%	0%	0%
5.3.7. [E.9] Errores de [re-]encaminamiento	5	0%	20%	0%	0%	0%
5.4.10. [A.12] Análisis de tráfico	5	0%	50%	50%	0%	0%
5.4.12. [A.14] Interceptación de información (escucha)	5	0%	0%	100%	0%	0%
5.4.18. [A.24] Denegación de servicio	70	100%	0%	0%	0%	0%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	0%	0%	75%	75%	20%
5.4.8. [A.10] Alteración de secuencia	5	0%	0%	75%	75%	20%
5.4.9. [A.11] Acceso no autorizado	50	50%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[COM] COMUNICACIONES - INTERNET

En la tabla 79 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo internet.

Tabla 79. Evaluación de Amenazas – Internet

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
COM-COMUNICACIONES						
Internet						
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	10	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	5	20%	0%	0%	0%	0%
5.3.7. [E.9] Errores de [re-]encaminamiento	5	0%	20%	0%	0%	0%
5.4.10. [A.12] Análisis de tráfico	5	0%	50%	50%	0%	0%
5.4.12. [A.14] Interceptación de información (escucha)	5	0%	0%	100%	0%	0%
5.4.18. [A.24] Denegación de servicio	10	100%	0%	0%	0%	0%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	0%	0%	75%	75%	20%
5.4.8. [A.10] Alteración de secuencia	5	0%	0%	75%	75%	20%
5.4.9. [A.11] Acceso no autorizado	10	50%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[COM] COMUNICACIONES – RED ÁREA LOCAL

En la tabla 80 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo red área local.

Tabla 80. Evaluación de Amenazas – Red Área Local

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
COM-COMUNICACIONES						
Red Área Local						
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	70	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	20%	0%	0%	0%	0%
5.3.7. [E.9] Errores de [re-]encaminamiento	5	0%	20%	0%	0%	0%
5.4.10. [A.12] Análisis de tráfico	5	0%	50%	50%	0%	0%
5.4.12. [A.14] Interceptación de información (escucha)	5	0%	0%	100%	0%	0%
5.4.18. [A.24] Denegación de servicio	70	100%	0%	0%	0%	0%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	0%	0%	75%	75%	20%
5.4.8. [A.10] Alteración de secuencia	5	0%	0%	75%	75%	20%

5.4.9. [A.11] Acceso no autorizado	50	50%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[AUX] EQUIPO AUXILIAR – CABLEADO ELÉCTRICO

En la tabla 81 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo cableado eléctrico.

Tabla 81. Evaluación de Amenazas – Cableado Eléctrico

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
AUX-AUXILIAR						
Cableado Eléctrico						
5.2.1. [I.1] Fuego	5	100%	100%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	100%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	75%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	100%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	5	75%	5%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	5	75%	20%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	100%	0%	0%	0%
5.4.20. [A.26] Ataque destructivo	5	0%	100%	75%	0%	0%

Fuente: Propiedad del Autor

[AUX] EQUIPO AUXILIAR – FUENTE DE ALIMENTACIÓN

En la tabla 82 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo fuente de alimentación.

Tabla 82. Evaluación de Amenazas – Fuente de Alimentación

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
AUX-AUXILIAR						
Fuente de Alimentación						
5.2.1. [I.1] Fuego	5	100%	100%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	100%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	75%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	5%	100%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	5%	5%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	5	20%	20%	0%	0%	0%

5.4.19. [A.25] Robo	5	100%	100%	0%	0%	0%
5.4.20. [A.26] Ataque destructivo	5	100%	100%	0%	0%	0%

Fuente: Propiedad del Autor

[AUX] EQUIPO AUXILIAR – RACK

En la tabla 83 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Rack.

Tabla 83. Evaluación de Amenazas – Rack

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
AUX-AUXILIAR						
Rack						
5.2.1. [I.1] Fuego	5	100%	100%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	100%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	75%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	5%	100%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	5%	5%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	5	20%	20%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	100%	0%	0%	0%
5.4.20. [A.26] Ataque destructivo	5	100%	100%	0%	0%	0%

Fuente: Propiedad del Autor

[AUX] EQUIPO AUXILIAR – SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

En la tabla 84 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Sistema de alimentación ininterrumpida.

Tabla 84. Evaluación de Amenazas – Sistema de Alimentación Ininterrumpida

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
AUX-AUXILIAR						
Sistema de Alimentación Ininterrumpida						
5.2.1. [I.1] Fuego	5	100%	100%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	100%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	75%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	5%	100%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	5%	5%	0%	0%	0%

5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (Hardware)	5	20%	20%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	100%	0%	0%	0%
5.4.20. [A.26] Ataque destructivo	5	100%	100%	0%	0%	0%

Fuente: Propiedad del Autor

[L] INSTALACIONES – OFICINA DE SISTEMAS

En la tabla 85 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo oficina de sistemas.

Tabla 85. Evaluación de Amenazas – Oficina de Sistemas

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
L-INSTALACIONES						
Oficina de Sistemas						
5.1.3. [N.*] Desastres Naturales	5	100%	0%	0%	0%	0%
5.2.12. [I.11] Emanaciones electromagnéticas	5	20%	0%	0%	0%	0%
5.3.10. [E.15] Alteración accidental de la información	5	0%	100%	0%	0%	0%
5.3.11. [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12. [E.19] Fugas de información	5	0%	0%	100%	0%	0%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	100%	100%	100%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	100%	0%	0%
5.4.15. [A.19] Divulgación de información	5	0%	100%	100%	0%	0%
5.4.20. [A.26] Ataque destructivo	5	100%	0%	0%	0%	0%
5.4.5. [A.7] Uso no previsto	5	50%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[P] PERSONAL - GERENTE DE INFORMACIÓN Y TECNOLOGÍA

En la tabla 86 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Gerente de Información y Tecnología.

Tabla 86. Evaluación de Amenazas – Gerente de Información y Tecnología

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
P-PERSONAL						
Gerente de Información y Tecnologia						
5.3.12. [E.19] Fugas de información	5	0%	0%	0%	75%	0%
5.3.18. [E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%

5.3.5. [E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%
5.4.22. [A.28] Indisponibilidad del personal	5	50%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[P] PERSONAL - COORDINADOR GENERAL DE SISTEMAS

En la tabla 87 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Coordinador General de Sistemas.

Tabla 87. Evaluación de Amenazas – Coordinador General de Sistemas

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
P-PERSONAL						
Coordinador General de Sistemas						
5.3.12. [E.19] Fugas de información	5	0%	0%	0%	75%	0%
5.3.18. [E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
5.3.5. [E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%
5.4.22. [A.28] Indisponibilidad del personal	5	50%	0%	0%	0%	0%

Fuente: Propiedad del Autor

[P] PERSONAL - AUXILIAR DE SISTEMAS

En la tabla 88 se puede observar la evaluación de amenaza y el porcentaje de impacto que se le proporcionó al activo Auxiliar de Sistemas.

Tabla 88. Evaluación de Amenazas – Auxiliar de Sistema

Activos	Frecuencia	[D]	[I]	[C]	[A]	[T]
P-PERSONAL						
Auxiliar de Sistemas						
5.3.12. [E.19] Fugas de información	5	0%	0%	0%	75%	0%
5.3.18. [E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
5.3.5. [E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%
5.4.22. [A.28] Indisponibilidad del personal	5	50%	0%	0%	0%	0%

Fuente: Propiedad del Autor

4.6 RIESGO POTENCIAL

4.6.1. Criterios de Evaluación

Determinar el nivel de riesgo potencial de cada uno de los activos en una valoración cualitativa de acuerdo a las zonas de riesgo que propone MAGERIT.

4.6.2. Evaluación del riesgo potencial a los activos

El riesgo es calculado en base al impacto que tiene cada activo y según el tipo de amenaza general (Naturales, Industriales, Errores No Intencionados, Ataques Intencionados); es decir, no se calcula en cada dimensión de seguridad (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad). Sólo se toma en cuenta que ocurra cualquier amenaza dentro de su respectiva categoría y se escoge el peor de los casos.

Para esto se tomará como referencia la tabla 89, donde se detalla la posible amenaza que puede afectar los activos de una empresa y son clasificados de la siguiente manera:

Tabla 89. Amenazas sobre los activos informáticos

Tipo de amenaza	Nomenclatura	Definición
Desastres Naturales	[N*]	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
De Origen Industrial	[I*]	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
Errores y Fallos No Intencionados	[E*]	Fallos no intencionales causados por las personas.
Ataques Intencionados	[A*]	Fallos deliberados causados por las personas.

Fuente: AMUTIO, M. A., CANDAU, J., MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 25-47.

Para hallar el riesgo potencial se toma como base la Tabla 8: Estimación cualitativa del riesgo (Ver tabla 8).

[D] DATOS/INFORMACIÓN

La tabla 90 muestra el riesgo potencial del tipo de activo Datos/información.

Tabla 90. Riesgo Potencial – Datos/Información

Código	Activo	Impacto	Probabilidad	Tipo de Amenaza	Riesgo_ID	Riesgo Potencial
D_BCK	Copia de seguridad de los Sistemas de Información.	MA	MB	E*, A*	R_D_BCK	A
D_LOG	Registro de Actividad.	MA	MB	E*, A*	R_D_LOG	A

Fuente: Propiedad del Autor

[S] SERVICIOS

La tabla 91 muestra el riesgo potencial del tipo de activo Servicios.

Tabla 91. Riesgo Potencial – Servicios

Código	Activo	Impacto	Probabilidad	Tipo de Amenaza	Riesgo_ID	Riesgo Potencial
S_MAI	Correo Electrónico	A	M	E*, A*	R_S_MAI	A
S_GID	Gestión de Identidades	MA	M	E*, A*	R_S_GID	MA
S_WWW	Página Web	A	M	E*, A*	R_S_WWW	A

Fuente: Propiedad del Autor

[SW] SOFTWARE

La tabla 92 muestra el riesgo potencial del tipo de activo software.

Tabla 92. Riesgo Potencial – Software

Código	Activo	Impacto	Probabilidad	Tipo de Amenaza	Riesgo_ID	Riesgo Potencial
SW_DBS	Gestores Base de Datos	MA	B	I*, E*, A*	R_SW_DBS	MA
SW_OFI	Ofimática	B	M	I*, E*, A*	R_SW_OFI	B
SW_AVS	Antivirus	M	M	I*, E*, A*	R_SW_AVS	M
SW_OPS	Sistemas Operativos	M	B	I*, E*, A*	R_SW_OPS	M

Fuente: Propiedad del Autor

[HW] HARDWARE

La tabla 93 muestra el riesgo potencial del tipo de activo hardware.

Tabla 93. Riesgo Potencial – Hardware

Código	Activo	Impacto	Probabilidad	Tipo de Amenaza	Riesgo_ID	Riesgo Potencial
HW_BCK	Dispositivos de Respaldo	MA	M	I*, E*, A*	R_HW_BCK	MA
HW_FRW	Firewall	MA	M	I*, E*, A*	R_HW_FRW	MA
HW_HOS	Servidores	MA	M	I*, E*, A*	R_HW_HOS	MA
HW_PCM	Computadoras Portátiles	B	M	I*, E*, A*	R_HW_PCM	B
HW_PCP	Computadoras de Escritorio	B	M	I*, E*, A*	R_HW_PCP	B
HW_PRT	Impresoras	MB	M	I*, E*, A*	R_HW_PRT	MB
HW_ROU	Router	A	M	I*, E*, A*	R_HW_ROU	A
HW_SCN	Escáner	MB	M	I*, E*, A*	R_HW_SCN	MB
HW_SWH	Switch	A	M	I*, E*, A*	R_HW_SWH	A
HW_WAP	Access Point	B	M	I*, E*, A*	R_HW_WAP	B

Fuente: Propiedad del Autor

[COM] COMUNICACIONES

La tabla 94 muestra el riesgo potencial del tipo de activo Comunicaciones.

Tabla 94. Riesgo Potencial – Comunicaciones

Código	Activo	Impacto	Probabilidad	Tipo de Amenaza	Riesgo_ID	Riesgo Potencial
COM_INT	Internet	A	A	E*, A*	R_COM_INT	MA
COM_LAN	Red Área Local	MA	A	E*, A*	R_COM_LAN	MA
COM_WIF	Conectividad Inalámbrica	B	A	E*, A*	R_COM_WIF	M

Fuente: Propiedad del Autor

[AUX] EQUIPO AUXILIAR

La tabla 95 muestra el riesgo potencial del tipo de activo equipo auxiliar.

Tabla 95. Riesgo Potencial – Equipo Auxiliar

Código	Activo	Impacto	Probabilidad	Tipo de Amenaza	Riesgo_ID	Riesgo Potencial
AUX_RCK	Rack	A	M	I*, E*, A*	R_AUX_RCK	A
AUX_PWR	Fuente de Alimentación	MA	M	I*, E*, A*	R_AUX_PWR	MA
AUX_UPS	Sistema de Alimentación	A	M	I*, E*, A*	R_AUX_UPS	A

	Ininterrumpida					
AUX_WIR	Cableado Eléctrico	MA	M	I*, E*, A*	R_AUX_WIR	MA

Fuente: Propiedad del Autor

[L] INSTALACIONES

La tabla 96 muestra el riesgo potencial del tipo de activo instalaciones.

Tabla 96. Riesgo Potencial – Instalaciones

Código	Activo	Impacto	Probabilidad	Tipo de Amenaza	Riesgo_ID	Riesgo Potencial
L_SIT	Oficina de Sistemas	MA	MB	N*,I*, E*, A*	R_L_SIT	A

[P] PERSONAL

La tabla 97 muestra el riesgo potencial del tipo de activo personal.

Tabla 97. Riesgo Potencial – Personal

Código	Activo	Impacto	Probabilidad	Tipo de Amenaza	Riesgo_ID	Riesgo Potencial
P_GTE	Gerente de información y tecnología	MA	B	E*, A*	R_P_GTE	MA
P_CGS	Coordinador General de Sistemas	A	B	E*, A*	R_P_CGS	A
P_AUX	Auxiliar de Sistemas	M	B	E*, A*	R_P_AUX	M

Fuente: Propiedad del Autor

5. DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD.

Se realiza un Análisis Diferencial referente al **Anexo A** del estándar ISO/IEC 27001:2013 con el fin de determinar el nivel de cumplimiento de los ***Dominios, Objetivos de Control y Controles de Seguridad*** conformes al estándar ISO/IEC 27002:2013. Estos corresponden a los numerales 5 al 18.

Tabla 98. Anexo A de la Norma ISO/IEC 27001:2013. Políticas de la Seguridad de la Información.

<table>
<tr><td>A.5</td><td colspan="3">POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.5.1</td><td colspan="3">Orientación de la dirección para la gestión de la seguridad de la información.</td></tr>
<tr><td colspan="4">Objetivo: Brindar orientación y soporte por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.</td></tr>
<tr><td>A.5.1.1</td><td colspan="2"><u>Políticas para la seguridad de la información</u></td><td>Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td>Las políticas de la seguridad de la información hoy en día proporcionan un direccionamiento estratégico acorde a los requerimientos que la compañía necesita.</td><td></td><td colspan="2">La empresa actualmente no tiene implementado un SGSI y no existe un documento que contemple políticas de seguridad de la información.</td></tr>
<tr><td>A.5.1.2</td><td colspan="2"><u>Revisión de las políticas para la seguridad de la información</u></td><td>Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
<tr><td>SI</td><td>NO</td><td>SI</td><td>NO</td></tr>
<tr><td>Las políticas de seguridad de la información deben ser evaluadas con el objetivo de dar respuesta a los cambios de la compañía que necesita.</td><td></td><td colspan="2">No existe una revisión de las políticas de seguridad de la información ya que actualmente no se tiene el documento relacionado (ver A.5.1.1).</td></tr>
</table>

Tabla 99. Anexo A de la Norma ISO/IEC 27001:2013. Organización de la Seguridad de la Información

<table>
<tr><td>A.6</td><td colspan="3">ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.6.1</td><td colspan="3">Organización Interna</td></tr>
<tr><td colspan="4">Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.</td></tr>
<tr><td>A.6.1.1</td><td colspan="2"><u>Roles y responsabilidades para la seguridad de la información</u></td><td>Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.</td></tr>
<tr><td colspan="2">APLICA</td><td colspan="2">CUMPLE</td></tr>
</table>

SI	NO	SI	NO
Los roles y responsabilidades son vitales para la protección de los activos informáticos de la organización, así como los procesos específicos para la seguridad de la información.		No están definidos los roles y responsabilidades relativas a la seguridad de la información, puesto que no se tiene implementado un SGSI en la empresa.	
A.6.1.2	**Separación de deberes**	**Control:** Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Los funcionarios no deben tener acceso ni modificar información sin autorización previa.		Los funcionarios se encuentran separado por áreas y solo tienen acceso a los activos y/o información necesaria para llevar a cabo su trabajo. Manuales y cargos.	
A.6.1.3	**Contacto con las autoridades**	**Control:** Se deben mantener contactos apropiados con las autoridades pertinentes.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Para reportar las incidencias relacionadas con la seguridad de la información, debe existir un procedimiento para contactar a las autoridades pertinentes.		Los incidentes relacionados con seguridad de la información son resueltos internamente.	
A.6.1.4	**Contacto con grupos de interés especial**	**Control:** Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Los grupos de interés especial mejoran el conocimiento y las prácticas relativas a la seguridad de la información, así como las actualizaciones de los equipos y/o dispositivos que la empresa posee.		No se tiene contacto con autoridades nacionales para los incidentes de seguridad que la empresa presentar.	
A.6.1.5	**Seguridad de la información en la gestión de proyectos**	**Control:** La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyectos.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Toda empresa debe implementar una metodología de **análisis de riesgos** y esta debe ser parte del proceso de implementación de un proyecto de TI con el objetivo de llevar un control y poderlos		Los proyectos de TI desde sus inicios no contemplan los riegos referentes a la seguridad de la información.	

direccionarlos.	
A.6.2	**Dispositivos móviles y teletrabajo**
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	
A.6.2.1	**Políticas para dispositivos móviles**
Control: Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	
APLICA	**CUMPLE**
SI / **NO**	**SI** / **NO**
Los dispositivos móviles son un riesgo potencial para la seguridad de la información.	No existe una política de seguridad sobre dispositivos móviles.
A.6.2.2	**Teletrabajo**
Control: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	
APLICA	**CUMPLE**
SI / **NO**	**SI** / **NO**
El teletrabajo debería tener una política de seguridad sobre las condiciones y restricciones.	Aunque se permite el acceso a algunos dispositivos de forma remota, no se implementa el teletrabajo.

Tabla 100. Anexo A de la Norma ISO/IEC 27001:2013. Seguridad de los recursos humanos

A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**
A.7.1	**Antes de asumir el empleo**
Objetivo: Asegurar que los empleados y contratistas comprenden las responsabilidades y son idóneos en los roles para que los consideran.	
A.7.1.1	**Selección**
Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	
APLICA	**CUMPLE**
SI / **NO**	**SI** / **NO**
Aparte de las competencias técnicas, el personal contratado debería ser éticamente correcto y confiable especialmente si accede a información sensible de la organización.	El personal es seleccionado cuidadosamente en base a su perfil y la idoneidad del trabajo a realizar.
A.7.1.2	**Términos y condiciones del empleo**
Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información..	
APLICA	**CUMPLE**
SI / **NO**	**SI** / **NO**

Los acuerdos contractuales de los empleados deberían tener cláusulas relativas a la confidencialidad de la información y respecto a las leyes y derechos de propiedad intelectual.		Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.
A.7.2	**Durante la ejecución del empleo**	
Objetivo: Asegurarse de los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A.7.2.1	**Responsabilidades de la dirección**	**Control:** La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
La alta dirección debe asegurar que los roles y responsabilidades estén claramente definidos antes de brindar acceso confidencial a los funcionarios, además los empleados deben estar comprometidos con las políticas de seguridad de la información.		No existen políticas de la seguridad de la información.
A.7.2.2	**Toma de conciencia, educación y formación en la seguridad de la información**	**Control:** Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes a su cargo.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Llevar a cabo capacitaciones relacionada con la seguridad de la información, los empleados son deben tomar conciencia de la importancia que tiene implementar un SGSI en la organización.		No se tiene implementado un SGSI ni un plan de concientización formal relativo a la seguridad de la información.
A.7.2.3	**Proceso disciplinario**	**Control:** Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Los procesos disciplinarios son analizados en base al grado de responsabilidad del empleado y el impacto que tiene en la organización.		Teniendo en cuenta que la organización no tiene implementado un SGSI y no se tiene plan de concientización referente a la seguridad de la información, el funcionario está sujeto a un proceso disciplinario en caso de haber una incidencia.
A.7.3	**Terminación y cambio de empleo**	

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
A.7.3.1	**Terminación o cambio de responsabilidades de empleo**	**Control:** Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los acuerdos contractuales deberán plasmar el compromiso correspondiente a la confidencialidad de la información aún después de la terminación del contrato y/o cambio de empleo.		Existen cláusulas de confidencialidad de la información en el contrato que el funcionario firma al momento de ingresar a la empresa.

Tabla 101. Anexo A de la Norma ISO/IEC 27001:2013. Gestión de Activos

A.8	**GESTIÓN DE ACTIVOS**	
A.8.1	**Responsabilidad por los activos**	
Objetivo: Identificar los activos organizacionales y definir las responsabilidades apropiadas.		
A.8.1.1	**Inventario de activos**	**Control:** Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se deben elaborar y mantener un inventario de estos activos.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
El inventario y clasificación de activos permite identificar la importancia de cada uno de ellos y su impacto en la organización.		Actualmente no existe un documento que clasifique la criticidad de la información y de los activos.
A.8.1.2	**Propiedad de los activos**	**Control:** Los activos mantenidos en el inventario deben tener un propietario.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los propietarios de los activos que posee la empresa son responsables del uso durante todo su ciclo de vida.		No se especifican los propietarios de los activos informáticos inventariados.
A.8.1.3	**Uso aceptable de los activos**	**Control:** Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los empleados son los responsables del		En la actualidad no existe un documento que

uso que les dan a los activos informáticos de la empresa.	especifique las reglas que se deben tomara para el buen uso de los activos.
A.8.1.4	**Devolución de activos**
APLICA	**CUMPLE**
SI / **NO**	**SI** / **NO**
La devolución de cualquier activos debe ser formalizada y la información almacenada en dispositivos personales transferida a la organización.	Existen registros de devolución de los activos entregados por los empleados al momento de retirarse de la empresa (Terminación de contrato o Despido), necesarios para firmar paz y salvo con la empresa.
A.8.2	**Clasificación de la información**
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo a su importancia para la organización.	
A.8.2.1	**Clasificación de la información**
APLICA	**CUMPLE**
SI / **NO**	**SI** / **NO**
La clasificación de la información es vital importancia para determinar el grado y control de seguridad que debería tener la empresa.	Actualmente no existe un documento que clasifique la criticidad de la información y de los activos.
A.8.2.2	**Etiquetado de la información**
APLICA	**CUMPLE**
SI / **NO**	**SI** / **NO**
El etiquetado de la información debe reflejar el esquema de clasificación adoptador por la organización.	Actualmente no existe procedimiento alguno para el etiquetado y/o clasificación de la información.
A.8.2.3	**Manejo de activos**
APLICA	**CUMPLE**
SI / **NO**	**SI** / **NO**
El acceso a los activos debería restringirse de acuerdo a su esquema de clasificación.	Actualmente no existen procedimientos para el manejo de la información, ya que ésta no está clasificada

A.8.3	**Manejo de medios**

Objetivo: Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios..		
A.8.3.1	**Gestión de medios removibles**	**Control:** Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación de la organización.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los medios removibles pueden almacenar información confidencial y deberían tener el mismo tratamiento y esquema de clasificación que cualquier otro activo informático.		No se cuenta con un procedimiento para la gestión de los medios removibles que pueda manejar la empresa.
A.8.3.2	**Disposición de los medios**	**Control:** Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los medios removibles podrían almacenar información confidencial y deberían ser removidos, además almacenar las copias de seguridad en lugares seguros y garantizar que su información sea encriptado y no sea revocable o legible.		No se dispone de un procedimiento debidamente documentado para la disposición de medios.
A.8.3.3	**Transferencia de medios físicos**	**Control:** Los medios que contienen información se deben proteger contra acceso no autorizados, uso indebido o corrupción durante el transporte.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los medios transportados podrían tener información sensitiva.		No se transportan activos informáticos.

Tabla 102. Anexo A de la Norma ISO/IEC 27001:2013. Control de Acceso

A.9	**CONTROL DE ACCESO**	
A.9.1	**Requisitos del negocio para control de acceso**	
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información..		
A.9.1.1	**Política de control de acceso**	**Control:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
El control de acceso físico y lógico permite tener un control sobre los riesgos de divulgación de información o acceso físico a		No existe una política de seguridad de la información, pero se mantienen un control tanto físico como lógico.

los activos a personal no autorizado.		
A.9.1.2	**Acceso a redes y a servicios en red**	**Control:** Sólo se debe permitir acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Las redes y servicios en red proveen acceso a diferentes servicios dentro de la organización al personal autorizado.		El acceso a ella está protegido a personas no autorizadas.
A.9.2	**Gestión de acceso de usuarios**	
Objetivo: Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
A.9.2.1	**Registro y cancelación de registro de usuarios**	**Control:** Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
		Se realiza el proceso de asignación de usuarios, pero no existe un documento referente al tema, además cuando una persona se retira de la empresa no tiene el proceso para la cancelación del registro.
A.9.2.2	**Suministro de acceso de usuarios**	**Control:** Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los permisos y privilegios de los usuarios son asignados o revocados de forma automática mediante un proceso formal.		Los funcionarios tienen un identificador de usuario dentro de la empresa.
A.9.2.3	**Gestión de derechos de acceso privilegiado**	**Control:** Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los privilegios de acceso a cualquier sistema o información deberían ser otorgados de acuerdo a las políticas de acceso.		No se tiene definido.
A.9.2.4	**Gestión de información de autenticación secreta de usuarios**	**Control:** La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**

La autenticación de los funcionarios en los sistemas de información debe mantenerse confidencial y secreta para evitar alteración y/o modificación de la información por parte de personas no autorizadas.	No exite un mecanismos para llevar un control.

A.9.2.5	**Revisión de los derechos de acceso de usuarios**	**Control:** Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares

APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Los derechos de acceso verifican qué puede hacer un usuario sobre la información o sistemas.		NO se encuentra documentado, pero se realiza regularmente sobre los sistemas de información de la compañía.	

A.9.2.6	**Retiro o ajuste de los derechos de acceso**	**Control:** Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
La remoción de los derechos de acceso permite que los empleados no sigan teniendo acceso a información o a los sistemas una vez terminado el contrato o cambio en el cargo.		No existe un proceso y/o documentación formal de remoción de los privilegios de acceso de los empleados que cambian el cargo o terminan contrato, pero cada vez que un usuario ya no trabaja en la compañía se le es retirado todos los permisos para ingresar a los diferentes sistemas de información.	

A.9.3	**Responsabilidades de los usuarios**

Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación

A.9.3.1	**Uso de información de autenticación secreta**	**Control:** Se debe exigir a los usuarios que cumplan con las prácticas de la organización para el uso de información de autenticación secreta.

APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
La información confidencial debería ser accedida sólo por las personas autorizadas y para fines de la organización.		La información de autenticación del empleado en los sistemas y acceso a información es confidencial.	

A.9.4	**Control de acceso a sistemas y aplicaciones**

Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.

A.9.4.1	**Restricción de acceso a la información**	**Control:** El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**

El acceso a la información debe ser granular en pro de evitar revelación o acceso a personas no autorizadas.		Los derechos de acceso a los sistemas de información son controlados de acuerdo a rol y responsabilidad del empleado en la organización.
A.9.4.2	**Procedimiento de ingreso seguro**	**Control:** Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
El inicio de sesión seguro permite que una persona no autorizada tenga acceso a información privilegiada.		Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro.
A.9.4.3	**Sistema de gestión de contraseñas**	**Control:** Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los privilegios de acceso a cualquier sistema o información deberían ser otorgados de acuerdo a las políticas de acceso.		Existen sistemas que la contraseña fue suministrada manualmente y este no posee el mecanismo de obligar al usuario a cambiarla.
A.9.4.4	**Uso de programas utilitarios privilegiados**	**Control:** Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y los controles de las aplicaciones.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los programas utilitarios deben ser instalados cuidadosamente para que no afecten a los sistemas o a la información existente.		Los sistemas se pueden instalar software, ya que a los funcionarios se les suministra la clave del administrador para llevar a cabo esta tarea.
A.9.4.5	**Control de acceso a códigos fuente de programas**	**Control:** Se debe restringir el acceso a los códigos fuentes de los programas.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Se utilizan los sistemas de información pero no se hacen implementaciones		Se utilizan los sistemas de información pero no se hacen implementaciones

Tabla 103. Anexo A de la Norma ISO/IEC 27001:2013. Criptografía

A.5	CRIPTOGRAFIA	
A.10.1	**Controles criptográficos**	
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o integridad de la información.		
A.10.1.1	**Política sobre el uso de controles criptográficos**	**Control:** Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
La criptografía cifra mediante algoritmos de encriptación los mensajes transmitidos garantizando la confidencialidad, integridad y autenticidad de los mensajes, impidiendo así que sea legible por personas no autorizadas.		No existe una política sobre el uso de algoritmos de encriptación para el cifrado de la información transmitida.
A.10.1.2	**Gestión de llaves**	**Control:** Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
La gestión de llaves criptográficas vela por su seguridad, mantenimiento, renovación, distribución y destrucción.		No existe una política sobre el uso y distribución de llaves criptográficas

Tabla 104. Anexo A de la Norma ISO/IEC 27001:2013. Seguridad física y del entorno

A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	
A.11.1	**Áreas seguras**	
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
A.11.1.1	**Perímetro de seguridad física**	**Control:** Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
El perímetro de seguridad física impide el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización.		Existe un perímetro físico controlado por personal de seguridad.
A.11.1.2	**Controles de acceso físicos**	**Control:** Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

APLICA		CUMPLE	
SI	**NO**	**SI**	**NO**
Los controles de accesos físicos impiden el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización		No existe un mecanismo digital (Tarjetas de aproximación), que permita el control del personal que ingresa, solo existe personal de seguridad.	
A.11.1.3	**Seguridad de oficinas, recintos e instalaciones**	**Control:** Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Las oficinas y lugares de trabajo claves deberían estar protegidas impidiendo el acceso físico a personas no autorizadas así como no ser públicamente visibles.		Las oficinas y lugares de trabajo no están protegidas por medios físicos para controlar el acceso.	
A.11.1.4	**Protección contra amenazas externas y ambientales**	**Control:** Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Protección física contra los desastres naturales y/o humanos.		No existe una protección física contra los desastres naturales y/o humanos.	
A.11.1.5	**Trabajo en áreas seguras**	**Control:** Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Las áreas seguras deben estar físicamente aseguradas y revisadas periódicamente.		No se posee áreas seguras para ser aseguradas físicamente.	
A.11.1.6	**Áreas de despacho y carga**	**Control:** Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Los lugares de entrega de equipos y otros dispositivos están controlados y se restringe el acceso a áreas externas de la organización.		La entrega de equipos y otros dispositivos ocurre al interior de la oficina de sistemas de la empresa.	
A.11.2	**Equipos**		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			
A.11.2.1	**Ubicación y protección de los equipos**	**Control:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de	

		acceso no autorizado.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Los equipos deben estar protegidos físicamente de amenazas ambientales (fuego, incendio, agua, humo) y humanas (robo) y evitar el acceso no autorizado a los mismos.		Los equipos que se encuentra en la empresa se encuentran protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, entre otras y para los equipos que manejan los funcionarios que se encuentran fuera de la organización se dispone de unos lineamientos para su uso.	
A.11.2.2	**Servicios de suministro**	**Control:** Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Los servicios de suministros como de energía, ventilación deben estar acordes a las características de los equipos.		Los servicios de suministros como de energía, ventilación están acordes a las características de los equipos.	
A.11.2.3	**Seguridad del cableado**	**Control:** El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se deben proteger contra interceptación, interferencias o daño.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
El cableado de energía eléctrica y de telecomunicaciones debe estar debidamente protegidos.		El cableado eléctrico que dispone el área de sistemas se encuentra separado del cableado de datos previniendo así interferencias, intercepciones o daños.	
A.11.2.4	**Mantenimiento de equipos**	**Control:** Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
El mantenimiento de los equipos es garantía de funcionamiento y rendimiento.		Se lleva a cabo el mantenimiento de los equipos de acuerdo al cronograma, la cual disponen realizarlo como mínimo dos (2) veces por año.	
A.11.2.5	**Retiro de activos**	**Control:** Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
La eliminación de software e información sólo debería ser realizada por el personal autorizado.		La información que maneja la empresa y sus funcionarios es alojada en la nube en una aplicación que se llama Huddle.	
A.11.2.6	**Seguridad de equipos y activos fuera de las**	**Control:** Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la	

	instalaciones	organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los equipos y/o dispositivos que pertenecen a la empresa y que están a disposición de los funcionarios externos deben aplicar las medidas mínimas de seguridad para los activos que manejan.		Los equipos que se utilizan afuera de las instalaciones de la empresa, cuando el funcionario se encuentra en un cliente este debe dejar su equipo bajo llave y le es prohibido transportarlo a su hogar.
A.11.2.7	**Disposición segura o reutilización de equipos**	**Control:** Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Para la disposición o reutilización de equipos se debería tener un procedimiento que garantice la destrucción total de la información contenida con el fin de evitar de ser leída por personas no autorizadas.		No posee un proceso para llevar a cabo esta tarea.
A.11.2.8	**Equipos de usuario desatendido**	**Control:** Los usuarios deben asegurarse de que los equipos desatendidos se les de la protección apropiada.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los usuarios deben cerrar sesiones y proteger el equipo con contraseñas robustas cuando no estén utilizando ya que podría estar expuesto a acceso no autorizado.		No existe una política documentada en la empresa, y los usuarios no son conscientes y no aplican la seguridad apropiada cuando el equipo no lo están utilizando.
A.11.2.9	**Políticas de escritorio limpio y pantalla limpia**	**Control:** Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
El almacenamiento de información confidencial y sensible no debe estar expuesta al público.		No existe una política debidamente documenta y muchos de los funcionarios posee información confidencial de los clientes que la empresa maneja.

Tabla 105. Anexo A de la Norma ISO/IEC 27001:2013. Seguridad de las operaciones

A.12	**SEGURIDAD DE LAS OPERACIONES**	
A.12.1	**Procedimientos operacionales y responsabilidades**	
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
A.12.1.1	**Procedimientos de Operación documentados**	**Control:** Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Esta documentación es de carácter obligatorio en la norma ISO 27001:2013. Los procedimientos operacionales deben estar documentados y disponibles para todos los usuarios. Estos procedimientos incluyen las copias de seguridad, almacenamiento, manejo de errores, encendido/apagado de equipos, instalación/configuración de sistemas, etc.		La empresa dispone de procedimientos operacionales.
A.12.1.2	**Gestión de cambios**	**Control:** Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Los cambios en los equipos que afectan la seguridad de la información deberían ser controlados y debidamente planeados y probados.		No existe procedimiento de control de cambios.
A.12.1.3	**Gestión de capacidad**	**Control:** Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido por el sistema.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Los recursos deberían ser monitoreados con el fin de gestionar su capacidad y rendimiento, así como proyectar que responda a las necesidades de la organización a largo plazo.		No se realiza monitoreo de los recursos de los sistemas de información.
A.12.1.4	**Separación de los ambientes de desarrollo, pruebas y operación**	**Control:** Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**

La empresa no desarrolla ningún tipo de aplicaciones	La empresa no realiza ningún tipo de desarrollo.

A.12.2	**Protección contra códigos maliciosos**

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

A.12.2.1	**Controles contra códigos maliciosos**	**Control:** Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
El software malicioso es un riesgo potencial para los sistemas y equipos que está latente en la mayoría de empresas, ya que pueden hacer que los sistemas operen de forma inadecuada, captura ilegal de información, entre otros.		Aunque no existe una política definida contra el malware, los usuarios son conscientes de los efectos que éstos podrían tener sobre el sistema de información. De igual forma, los equipos poseen software antimalware.	

A.12.3	**Copias de respaldo**

Objetivo: Proteger contra la pérdida de datos.

A.12.3.1	**Respaldo de la Información**	**Control:** Se debe hacer copias de respaldo de información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Las copias de seguridad (backups) e imágenes de los sistemas garantizan que la información esencial e instalación de software podría ser recuperada después de fallas o desastres.		Aunque la empresa no disponga de políticas, pero existe un procedimiento para llevar a cabo las copias de seguridad, realizan procesos de respaldo de la información de los diferentes sistemas de información.	

A.12.4	**Registro y seguimiento**

Objetivo: Registrar eventos y generar evidencia.

A.12.4.1	**Registro de eventos**	**Control:** Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Los registros (logs) almacenan información relevante sobre los eventos ocurridos en la operación de un sistema.		Lleva a cabo un control de los cambios ocurridos en los equipos de los funcionarios.	

A.12.4.2	**Protección de la información**	**Control:** Las instalaciones y la información de

	de registro	registro se deben proteger contra alteración y acceso no autorizado.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los registros de eventos deberían ser custodiados para prevenir modificación no autorizada.		Los registros de eventos no están protegidos contra el acceso no autorizado.
A.12.4.3	**Registros del administrador y del operador**	**Control:** Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los administradores de los sistemas de información tienen accesos privilegiados y podrían modificar información de los registros de eventos.		Las acciones y registros de los administradores de los sistemas de información de la empresa son almacenados y protegidos de cualquier modificación.
A.12.4.4	**Sincronización de relojes**	**Control:** Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
La sincronización de los relojes de los sistemas permite mantener una referencia única de tiempo y zona horaria.		Aunque no se tiene una política documentada sobre la sincronización de los relojes, todos los sistemas están sincronizados bajo un único formato de tiempo y zona horaria.
A.12.5	**Control de software operacional**	
Objetivo: Asegurarse de la integridad de los sistemas operacionales.		
A.12.5.1	**Instalación de software en los sistemas operativos**	**Control:** Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Se debe controlar las instalaciones de software en los sistemas operativos		Aunque no existe una política documentada o procedimientos sobre la instalación de software en los sistemas operativos, en los equipos no se puede instalar software sin la autorización del administrador del sistema operativo.
A.12.6	**Gestión de la vulnerabilidad técnica**	
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
A.12.6.1	**Gestión de las vulnerabilidades técnicas**	**Control:** Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a

		estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
El inventario de los activos se debería mantener actualizado con el fin de identificar a tiempo los riesgos asociados a las vulnerabilidades y amenazas técnicas.		Aunque existe un inventario de los activos físicos y del software operacional, no se tiene una metodología de riesgos que los evalúe.	
A.12.6.2	**Restricciones sobre la instalación de software**	**Control:** Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Cualquier persona con elevados privilegios de acceso podría instalar cualquier software en un equipo y/o dispositivo. El no control podría liderar a la instalación de software malicioso o no permitido.		Aunque no exista una política debidamente documentada sobre este proceso, la instalación de cualquier software es realizada sólo por el personal autorizado y con software probado y licenciado, además de otorgar el principio del menor privilegio.	
A.12.7	**Consideraciones sobre auditorías de sistemas de información**		
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.			
A.12.7.1	**Controles de auditorías de sistemas de información**	**Control:** Los requisitos y actividades que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio.	
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Las auditorías de los sistemas deberían ser acordadas, planeadas y controladas sin interferir en el desarrollo normal de los procesos.		No se dispone un plan de auditoría para la verificación de los sistemas operativos.	

Tabla 106. Anexo A de la Norma ISO/IEC 27001:2013. Seguridad de las comunicaciones

A.13	**SEGURIDAD DE LAS COMUNICACIONES**	
A.13.1	**Gestión de la seguridad de las redes**	
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
A.13.1.1	**Controles de redes**	**Control:** Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
APLICA		**CUMPLE**
SI	**NO**	**SI**	**NO**
Las redes deberían proteger la transmisión de la información garantizando su		No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la	

confidencialidad e integridad y en algunos casos su disponibilidad.		información transmitida en las redes sea segura.
A.13.1.2	**Seguridad de los servicios de red**	**Control:** Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o contraten externamente.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
El acceso a la red de los proveedores de servicios de red debería ser controlado y monitoreado.		El acceso a la red de los proveedores de servicio de red es monitoreado y controlado.
A.13.1.3	**Separación en las redes**	**Control:** Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los usuarios y servicios deberían estar separados lógicamente en unidades organizacionales o dominios, o a través de VLANS.		Se encuentra segmentada 3 Vlan (Equipos de comunicaciones, Servidores y usuarios)
A.13.2	**Transferencia de información**	
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	**Políticas y procedimientos de transferencia de información**	**Control:** Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los procedimientos y controles ayudan a mantener la seguridad de la información cuando es transferida a otra entidad.		No existe una política o documentación sobre los procedimientos y controles para la transferencia segura de la información.
A.13.2.2	**Acuerdos sobre transferencia de información**	**Control:** Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Se debe disponer de acuerdos sobre los procedimientos para la transferencia segura de la información.		No se han implementado controles criptográficos que garanticen la seguridad en la transmisión de la información.
A.13.2.3	**Mensajería Electrónica**	**Control:** Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**

Se deberían proteger los mensajes enviados internamente de los empleados de la organización.		No se han implementado controles criptográficos que garanticen la seguridad en la transmisión de la información.
A.13.2.4	**Acuerdos de confidencialidad o de no divulgación**	**Control**: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de una organización para la protección de la información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los acuerdos con los empleados o con entes externos deberían tener acuerdos de confidencialidad de la información.		En los contratos de los empleados se estipula el compromiso con la confidencialidad de la información.

Tabla 107. Anexo A de la Norma ISO/IEC 27001:2013. Adquisición, desarrollo y mantenimiento de sistemas

A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	
A.14.1	**Transferencia de información**	
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que presten servicios sobre redes públicas.		
A.14.1.1	**Análisis y especificación de requisitos de seguridad de la información**	**Control:** Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los requerimientos de la seguridad de la información deberían ser identificados utilizando varios métodos en concordancia con las políticas y regulaciones.		No existe una política o documentación sobre los procedimientos mencionado.
A.14.1.2	**Seguridad de servicios de las aplicaciones en redes públicas**	**Control:** La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad.		No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida en las redes sea segura.
A.14.1.3	**Protección de las transacciones de los servicios de las aplicaciones**	**Control:** La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión

		incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad.		No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida en las redes sea segura.
A.14.2	**Seguridad en los procesos de desarrollo y soporte**	
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	**Política de desarrollo seguro**	**Control:** Se deben establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Las políticas y controles de seguridad deberían ser aplicados en el desarrollo de software.		La empresa no realiza desarrollo de software.
A.14.2.2	**Procedimientos de control de cambios en sistemas**	**Control:** Los cambios de sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
El procedimiento formal de los cambios en el desarrollo de software debería ser documentado para garantizar la integridad del sistema o aplicación.		La empresa no realiza desarrollo de software.
A.14.2.3	**Revisión técnica de las aplicaciones después de cambios en la plataforma de operación**	**Control:** Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones de seguridad de la organización.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los cambios en las aplicaciones deberían ser revisados y probados antes de implementarlas de manera que se garantice que no comprometa la seguridad.		No dispone un procedimiento establecido para realizar esta tarea.
A.14.2.4	**Restricciones en los cambios a los paquetes de software**	**Control:** Se deben desalentar las modificaciones de los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
APLICA		**CUMPLE**

SI	NO	SI	NO
Limitar las modificaciones de software sólo a lo estrictamente necesario.		La empresa no realiza desarrollo de software y las actualizaciones y modificaciones de software son desarrolladas por la empresa encargada.	

A.14.2.5	**Principios de construcción de los sistemas seguros**	**Control:** Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

APLICA		CUMPLE	
SI	**NO**	**SI**	**NO**
Se deberían establecer y documentar los principios de desarrollo de software seguro.		La empresa no realiza desarrollo de software.	

A.14.2.6	**Ambiente de desarrollo seguro**	**Control:** Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.

APLICA		CUMPLE	
SI	**NO**	**SI**	**NO**
Los ambientes de desarrollo de software también deberían estar protegidos de acceso no autorizado o de ejecución de software malicioso.		La empresa no realiza desarrollo de software.	

A.14.2.7	**Desarrollo contratado externamente**	**Control:** La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

APLICA		CUMPLE	
SI	**NO**	**SI**	**NO**
El software desarrollado externamente debería tener licencia, acuerdos y prácticas de desarrollo y pruebas seguros.		Se asegura que el software desarrollado externamente contiene las prácticas de desarrollo y pruebas seguros.	

A.14.2.8	**Pruebas de seguridad de sistemas**	**Control:** Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de seguridad.

APLICA		CUMPLE	
SI	**NO**	**SI**	**NO**
Se deben realizar visitas y pruebas de seguridad al software que se está desarrollando.		NO se realizan pruebas de seguridad	

A.14.2.9	**Pruebas de aceptación de sistemas**	**Control:** Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados

APLICA		CUMPLE	
SI	NO	SI	NO
Se deberían realizar pruebas de seguridad en base a los requerimientos de seguridad de la organización		No se realizan las pruebas de seguridad debido a que aún no existen los lineamientos o políticas de la seguridad de la información.	

A.14.3	Datos de prueba
Objetivo: Asegurar la protección de los datos usados para pruebas.	
A.14.3.1	**Protección de datos de prueba** — **Control:** Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.

APLICA		CUMPLE	
SI	NO	SI	NO
Los datos de prueba deberían ser seleccionados cuidadosamente y que no contengan ninguna información confidencial.		La empresa no desarrolla software.	

Tabla 108. Anexo A de la Norma ISO/IEC 27001:2013. Relación con los proveedores

A.15	RELACIONES CON LOS PROVEEDORES
A.15.1	Seguridad de la información en las relaciones con los proveedores
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	
A.15.1.1	**Política de seguridad de la información para las relaciones con proveedores** — **Control:** Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar y se deben documentar.

APLICA		CUMPLE	
SI	NO	SI	NO
La organización debería emplear los controles y procedimientos de seguridad para el acceso a los activos por parte de los proveedores.		No se tiene una política de seguridad definida.	

A.15.1.2	**Tratamiento de la seguridad dentro de los acuerdos con proveedores** — **Control:** Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

APLICA		CUMPLE	
SI	NO	SI	NO
Se deberían establecer acuerdos de seguridad documentados entre la organización y los proveedores para el acceso a los activos.		No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos	

A.15.1.3	**Cadena de suministro de tecnología de información y comunicación**	**Control:** Los acuerdos con los proveedores deben incluir requisitos para tratar los riesgos de seguridad de información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Los suministros de los proveedores deberían estar acordes a las políticas de seguridad de la información de la organización.		No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos.
A.15.2	**Gestión de la prestación de servicios de proveedores**	
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.		
A.15.2.1	**Seguimiento y revisión de los servicios de los proveedores**	**Control:** Las organizaciones deben hacer seguimiento, revisar y auditar con la regularidad la prestación de servicios de los proveedores.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
El monitoreo y acceso de los proveedores debería ser acorde las políticas de seguridad de la organización.		No existe una política de seguridad de la información y procedimientos.
A.15.2.2	**Gestión de cambios en los servicios de los proveedores**	**Control:** Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de riesgos
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Se deberían establecer acuerdos de seguridad documentados entre la organización y los proveedores para el acceso a los activos.		No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos
A.15.1.3	**Cadena de suministro de tecnología de información y comunicación**	**Control:** Los acuerdos con los proveedores deben incluir requisitos para tratar los riesgos de seguridad de información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Los cambios de los proveedores deberían estar acordes a los requerimientos de seguridad de la información de la organización.		Solo se tiene servicio con proveedores de internet.

Tabla 109. Anexo A de la Norma ISO/IEC 27001:2013. Gestión de incidentes de seguridad de la información

A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
A.16.1	**Gestión de incidentes y mejoras de la seguridad de la información**	
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	**Responsabilidades y procedimientos**	**Control:** Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Los planes y procedimientos para gestionar los incidentes relacionados a la seguridad de la información deberían estar documentados.		No existen los procedimientos documentados para gestionar los incidentes relativos a la seguridad de la información.
A.16.1.2	**Reporte de eventos de seguridad de la información**	**Control:** Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Todos los empleados deben estar pendientes de los eventos y reportes de seguridad de la información.		Los empleados están no alertados de los eventos e incidentes correspondientes relativos a la seguridad de la información.
A.16.1.3	**Reporte de debilidades de seguridad de la información**	**Control:** Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Se deberían implementar mecanismos de reportes de incidentes de seguridad de la información en donde todos los empleados deberían reportar las brechas de seguridad con el fin de prevenir incidentes.		Los empleados no están comprometidos en reportar las brechas lo antes posible.
A.16.1.4	**Evaluación de eventos de seguridad de la información y decisiones sobre ellos**	**Control:** Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**

La clasificación y priorización de los incidentes de seguridad ayudan a identificar el impacto en la organización.	Los activos no están clasificados y no existe una metodología de análisis y evaluación de riesgos informáticos
A.16.1.5	**Respuesta a incidentes de seguridad de la información**	**Control:** Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Deberían existir procedimientos documentados para dar respuesta a los incidentes restableciendo la operación al nivel de seguridad aceptable lo más pronto posible.		Aunque las respuestas son inmediatas, los procedimientos de respuesta no están documentados, así como tampoco existe un Plan de Continuidad del Negocio.	
A.16.1.6	**Aprendizaje obtenido de los incidentes de seguridad de la información**	**Control:** El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto sobre incidentes futuros.
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Se debería recolectar información de los incidentes ocurridos con el fin de prevenirlos en el futuro.		Se aplican los controles necesarios para prevenirlos, pero no existe documentación referente a los incidentes.	
A.16.1.7	**Recolección de evidencia**	**Control:** La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**
Se deberían recolectar las evidencias y registros para tomar acciones legales		No se dispone de un procedimiento debidamente documentado.	

Tabla 110. Anexo A de la Norma ISO/IEC 27001:2013. Aspectos de seguridad de la información de la gestión de la continuidad de negocio

A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	
A.17.1	**Continuidad de seguridad de la información**	
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización		
A.17.1.1	**Planificación de la continuidad de la seguridad de la información**	**Control:** La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
APLICA		**CUMPLE**	
SI	**NO**	**SI**	**NO**

Los Planes de Continuidad del Negocio (BCP) y los Planes de Recuperación de Desastres (DRP) deberían estar planificados y documentados para restablecer la operación normal dado un evento. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013		No existe la documentación o los procedimientos para los BCP y DRP.
A.17.1.2	**Implementación de la continuidad de la seguridad de la información**	**Control:** La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los Planes de Continuidad del Negocio (BCP) y los Planes de Recuperación de Desastres (DRP) deberían estar planificados y documentados para restablecer la operación normal dado un evento. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013		No existe la documentación o los procedimientos para los BCP y DRP.
A.17.1.3	**Verificación, revisión y evaluación de la continuidad de la seguridad de la información**	**Control:** La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los procedimientos y controles para la restablecer los servicios se deberían revisar en intervalos regulares con cada uno de los responsables para verificar su efectividad.		No existe la documentación o los procedimientos para los BCP y DRP.
A.17.2	**Redundancias**	
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.		
A.17.2.1	**Disponibilidad de instalaciones de procesamiento de información**	**Control:** Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
La información debería ser redundante con el fin de mantener la disponibilidad de los servicios y ser probadas en intervalos regulares.		La organización no dispone de redundancia de la información.

Tabla 111. Anexo A de la Norma ISO/IEC 27001:2013. Cumplimiento

A.18	CUMPLIMIENTO	
A.18.1	Cumplimiento de los requisitos legales y contractuales	
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatuarias, de reglamentación o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad.		
A.18.1.1	**Identificación de la legislación aplicable a los requisitos contractuales**	**Control:** Todos los requisitos estatuarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Los administradores deberían identificar toda la información legislativa aplicable a la organización con el fin de cumplir con los requerimientos del negocio.		Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley.
A.18.1.2	**Derechos de propiedad intelectual**	**Control:** Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Se deberían definir las políticas y procedimientos para controlar la propiedad intelectual.		La empresa no desarrolla software.
A.18.1.3	**Protección de registros**	**Control:** Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**
Los registros deberían estar clasificados de acuerdo al esquema adoptado por la organización de acuerdo al nivel de confidencialidad.		No existe un nivel de clasificación formal de confidencialidad de los registros.
A.18.1.4	**Privacidad y protección de información de datos personales**	**Control:** Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.
APLICA		**CUMPLE**
SI / **NO**		**SI** / **NO**

Se debería documentar y definir políticas relativas a la protección de datos personales de acuerdo a las reglamentaciones que la ley exige.		No existe una política o documento debidamente documentado.
A.18.1.5	**Reglamentación de controles criptográficos**	**Control:** Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los controles criptográficos permiten garantizar la confidencialidad, integridad y autenticidad de la información.		No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida y/o almacenada sea segura.
A.18.2	**Revisiones de seguridad de la información**	
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales		
A.18.2.1	**Revisión independiente de la seguridad de la información**	**Control:** El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Se debe realizar auditorías de los procesos, procedimientos y sistemas por medio de entidades externas.		No se realizan auditorías con entidades externas, la misma empresa es la encargada de realizar las auditorias pero no hay un plan estipulado.
A.18.2.2	**Cumplimiento con las políticas y normas de seguridad**	**Control:** Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Se deberían realizar revisiones de las políticas de seguridad con el fin de verificar su cumplimiento.		La empresa no dispone de políticas de seguridad de la información.
A.18.2.3	**Revisión del cumplimiento técnico**	**Control:** Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de información.
APLICA		**CUMPLE**
SI	**NO**	**SI** / **NO**
Los test de penetración deben ser realizados por con herramientas		La empresa no dispone de política de seguridad.

automáticas, con personal calificado y en intervalos programados y acordados con el fin de verificar las políticas de seguridad así como los requerimientos.	

6. PROCEDIMIENTO PARA LA IMPLEMENTACIÓN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI

A continuación se describe el manual de procedimientos para implementar el Sistema de Gestión de Seguridad de la Información - SGSI en el área de sistemas de la empresa Baker Tilly Colombia Ltda, de acuerdo a los controles seleccionados anteriormente los que no se mencionan en el manual se encuentran detallados en la implementación de los mismos.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Generalidades

La información es un recurso que como el resto de los activos, tiene un valor significativo para la empresa, por lo tanto debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la empresa de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos organizacionales.

Es importante que los principios de la Política de Seguridad sean parte de la cultura de la empresa. Para esto, se debe asegurar un alto compromiso por parte de la alta dirigencia y de los líderes de cada proceso de la organización que permita la difusión, consolidación y cumplimiento de la Política de Seguridad de la Información.

Objetivo

Proteger los recursos de información que dispone la organización y la tecnología utilizada para su procesamiento, frente a las diferentes amenazas tanto internas como externas, bien sea deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en las Política de Seguridad de la información y mantenerlas actualizadas, para efectos de asegurar su vigencia y nivel de eficacia.

Establecer las directrices, procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos de cómputo de Baker Tilly Colombia Ltda y el uso adecuado de los mismos.

Alcance

Esta política se aplica inicialmente al área de sistemas de Baker Tilly en todo el ámbito de sus recursos y a la totalidad de los procesos, ya sean internos o externos que se encuentren vinculados a la entidad a través de contratos o acuerdos con terceros.

La finalidad de las políticas de seguridad, es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los equipos de cómputo de la empresa, bien sea que se encuentren conectados o no a la red, como la información guardada en ellos, por lo tanto, la violación de dichas políticas puede acarrear medidas disciplinarias.

Para el desarrollo de las políticas, es necesario considerar las diferentes fuentes de información, que permiten el desempeño diario de las funciones del área de sistemas de la organización.

El propósito de este manual es establecer las directrices, procedimientos y los requisitos necesarios para asegurar la protección de la información de Baker Tilly Colombia Ltda al encontrase conectada a red de computadoras.

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

Generalidades

Es importante tener bien definido un marco de gestión para efectuar diferentes tareas como la aprobación de Políticas, la coordinación de su implementación y la asignación de funciones y responsabilidades, para tener una eficiente administración de la seguridad de información.

Objetivo

- Administrar la seguridad de la información dentro de Baker Tilly Colombia Ltda y establecer un marco gerencial para dar inicio y controlar su implementación, además establecer funciones y responsabilidades.
- Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de la información en la empresa.
- Monitorear cambios significativos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento, supervisar y/o monitorear los incidentes relativos a la seguridad.

- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas.
- Aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas y/o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro de Baker Tilly Colombia Ltda.

Crear un comité de seguridad donde estén definidas las funciones de cada miembro y puedan desempeñar sus actividades y ayudar a mejorar la seguridad en la empresa, asimismo se debe proponer a la Gerencia para su aprobación, definición y asignación de las responsabilidades que surjan de sus funciones.

GESTIÓN DE LOS ACTIVOS DE RED

Generalidades

Baker Tilly Colombia debe tener conocimiento sobre los activos que posee como parte importante de la administración de riesgos.

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Objetivo

- Garantizar que los activos de información reciban un apropiado nivel de protección, además de clasificar la información para señalar su sensibilidad y criticidad.

- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Responsabilidad sobre los activos

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada.

El responsable de la seguridad de la información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada propietario de la información debe llevar la supervisión de clasificación y rotulación de la información de su área de competencia de acuerdo a lo establecido en las políticas.

Se debe identificar los activos más importantes asociados a cada sistema de información y elaborar un inventario con dicha información, el cual será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad mínimo de 4 meses.

Una vez realizado el inventario, se debe clasificar el activo, en base a tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad

SEGURIDAD DE LOS RECURSOS HUMANOS

Generalidades

La seguridad de la información se basa en la capacidad para conservar la integridad, confidencialidad y disponibilidad de los activos.

Para lograr lo anterior es fundamental educar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad. Así mismo, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

Objetivo

Reducir los riesgos de error humano, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Indicar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la firma en el transcurso de sus tareas normales.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Seguridad en los recursos

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo, estas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de las políticas de seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

Términos y condiciones de la relación laboral

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la empresa y del horario normal de trabajo.

Los derechos y obligaciones del empleado relacionados con la seguridad de la información, por ejemplo con las leyes de Propiedad Intelectual o la legislación de protección de datos, estas deberán estar aclaradas e incluidas en los términos y condiciones del contrato.

Conocimiento y capacitación de la seguridad de información

Todos los empleados de Baker Tilly deberán recibir una adecuada capacitación y actualización periódica en materia de la política de seguridad de la información, normas y procedimientos para la seguridad. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la Política. Cada 6 meses se deberá revisar el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

El personal que ingrese a Baker Tilly recibirá el material, indicándosele el procedimiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan,

además se otorgará una guía de usuario para que tengan un mejor conocimiento con respecto a las amenazas informáticas y sus posibles consecuencias dentro de la empresa de tal manera que se llegue a concienciar y crear una cultura de seguridad de la información.

SEGURIDAD FÍSICA Y DEL ENTORNO

Generalidades

La seguridad física y ambiental minimiza los riesgos de daños e interferencias a la información y a las operaciones de la empresa. Además, trata de evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las instalaciones e información de la compañía.

Proteger el equipamiento de procesamiento de información crítica de la empresa ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la organización.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

Generalidades

Debido a los peligros existentes como software malicioso, virus, troyanos, etc. es importante que se adopten controles para prevenir cualquier tipo de amenazas.

Las comunicaciones establecidas permiten el intercambio de información, se deberá establecer controles para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Es necesario establecer controles que impidan el acceso no autorizado a los sistemas de información por parte de personal diferente a los que tienen permisos, para lo cual es necesario se implementen procedimientos para controlar la asignación de privilegios de acceso a los diferentes sistemas y aplicativos de la empresas.

Es importante para la seguridad de la información controlar el acceso a los recursos, y protegerlos contra el acceso no autorizado, modificación o robo.

Objetivo

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones. Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas.
- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Mantener un registro de eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Alcance

En el procedimiento para implementar este control, se define una política de control de acceso que se aplica a todos los usuarios internos y externos que tienen diferentes permisos para acceder a los sistemas de información, red y bases de datos.

Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran la seguridad.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Generalidades

En este control se deben revisar las aplicaciones como puntos críticos de vulnerabilidades, es necesaria una adecuada administración de la infraestructura, Sistemas Operativos y Software Base, en las distintas plataformas, para asegurar

una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Con este control se pretende cubrir varios puntos de seguridad, entre los principales objetivos se tienen:

• Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
• Definir los métodos de protección de la información crítica o sensible.

Alcance

Los controles se aplican a los sistemas informáticos, y a los sistemas operativos que integran.

Se debe entender como información confidencial a toda información que se refiere a planes de negocio, tecnología no anunciada, información financiera no pública; e información personal.

Revisión técnica de los cambios en el sistema operativo

Cada vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, el administrador de la red debe tener un procedimiento en el cual incluya:

- Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
- Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación. Para lo cual el administrador debe planificar el día en el cual se llevará a cabo el cambio e informarlo a los usuarios y coordinar con los responsables de cada área en caso de que ellos deban realizar algún trabajo por el cual no pueden suspender sus actividades. Estos cambios deben programarse para fines de semana donde no haya impacto en los usuarios.
- Asegurar la actualización del Plan de Continuidad de las Actividades de la empresa.

Restricción del cambio de paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del responsable del Área sistemas, deberá:

- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

Este es un punto que debe ser analizado con todos los responsables de las áreas y el administrador de la red, deben realmente aprobar los cambios que implica varios procedimientos como son en el ámbito legal, financiero, recursos, etc.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Divulgación de eventos y de debilidades de la seguridad de la información

Es importante que el área de sistema de Baker Tilly tenga un procedimiento a seguir cuando se presente un incidente de seguridad en la red, pues es necesario que pueda aprender de los errores y evitar que un ataque ocurra. Por lo cual es importante que luego de cada incidente siga un procedimiento, técnicas, configuraciones necesarias para reforzar lo modificado y mejorar la seguridad.

Es necesario que se tenga un mejor control del uso apropiado de los recursos de la red, en otros términos, todos los recursos de la informática deben usarse de una manera ética y responsable. El uso de recursos de tecnología de información puede categorizarse ampliamente como aceptable, tolerable, o prohibió:

- El uso aceptable de recursos de tecnología de información es el uso legal consistente con los requerimientos de la organización, en base a las políticas de la misma que permitan solventar los problemas de la empresa.
- El uso tolerable es el uso legal para otros propósitos que no chocan con la política del uso aceptable de la organización.
- El uso prohibido, es el uso ilegal y todo el uso que no son aceptables ni tolerables.

Administración de incidentes y mejoras de la seguridad de la información

Después que el incidente ha sido resuelto, es necesario realizar una documentación del mismo para poder determinar las experiencias aprendidas del mismo.

Como resultado de un análisis posterior al reporte de incidentes, el personal de seguridad puede necesitar emitir alarmas o advertencias a todos los empleados de la empresa sobre las acciones tomar para reducir vulnerabilidades que se explotaron durante el incidente.

GESTION DE CONTINUIDAD DEL NEGOCIO

Generalidades

Un punto importante para toda organización, es administrar de forma ordenada las actividades necesarias para la continuidad del negocio, en este procedimiento se deben involucrar a todos los empleados de Baker Tilly.

El plan de continuidad debe mantenerse actualizado y ser una parte integrada en los diversos procesos de las diferentes áreas de la empresa.

Objetivo

Este control es importante para cubrir los puntos críticos de la empresa en caso de algún desastre, a continuación se detallan los principales objetivos:

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
- Maximizar la efectividad de las operaciones de contingencia de la empresa con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) Detección y determinación del daño y la activación del plan.
b) Restauración temporal de las operaciones y recuperación del daño producido al sistema original.
c) Restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

- Asignar funciones para cada actividad definida.

Alcance

Al desarrollar el plan de continuidad del negocio para la empresa, se debe considerar los parámetros sobre los cuales se va a desarrollar el mismo para poder los desastres. Para este caso cuando se realizó en análisis de riesgos y vulnerabilidades se consideraron diferentes tipos de desastres como son:

Desastres naturales:

- Terremotos
- Fuego

Desastres artificiales, es decir aquellos relacionados con la computación:

- Sabotaje de los sistemas informáticos, y de la información.
- Ataque de Negación de Servicio en los servidores de la red.
- Virus, gusanos, y otros ataques informáticos.
- Faltas de la infraestructura (interrupciones para uso general, interrupciones de la energía, etc.).
- Fallas de comunicaciones (hardware interno y externo, así como software y redes).

Una vez identificados los tipos de desastres la empresa debe seguir y desarrollar un plan para asegurar la viabilidad a largo plazo, es necesario que la gerencia se involucre en la elaboración del plan, pero es el Comité de Seguridad de la Información que determina que tipos de planes son aplicables pues se requiere de financiamiento de los mismos.

Las pruebas son útiles si reflejan también condiciones reales y si los resultados de la prueba se utilizan para mejorar el plan.

Es importante comenzar con un plan simple para probar y después aumentar el alcance de la prueba gradualmente. Para cada caso es importante:

- Identifique el alcance y las metas para la prueba.
- Documente el plan de prueba y los resultados.
- Repase los resultados con los participantes y prepare las lecciones aprendidas de la prueba.
- Ponga al día el plan basado en los resultados de la prueba.

Proceso de gestión de la continuidad del negocio

Para sobrevivir, la organización debe asegurar el funcionamiento de aplicaciones críticas en un tiempo razonable, frente a un desastre. Las organizaciones necesitan entrenar a sus empleados para ejecutar los planes de contingencia, para lo cual se requiere:

- Que los empleados sean conscientes de la necesidad del plan
- Informar a todos los empleados de la existencia del plan y proporcionar los procedimientos para seguir en caso de una emergencia.
- Entrenar al personal con las responsabilidades identificadas para cada uno de ellos, para realizar la recuperación del desastre y procedimientos de continuidad de negocio

- Dar la oportunidad para que se pueda llevar a cabo el plan de contingencia, para poder realizar un simulacro de la forma en la que se ejecuta el mismo.

Desarrollo e implantación de planes de contingencia

Al desarrollar el plan se debe tener bien definido y especificado las responsabilidades ha asignarse a cada persona responsable de un proceso determinado, se debe considerar los siguientes responsables:

Personal encargado de la administración de la recuperación: Debe actuar al momento que se presente el desastre, y cuyo trabajo consiste en ejecutar el plan de recuperación de desastre y restaurar los procesos críticos en el menor tiempo, para este caso es el Comité de Seguridad.

Personal operacional: Son aquellos que están encargados de la operación del negocio hasta que las cosas vuelvan a la normalidad, estas personas tienen responsabilidades cotidianas y desarrollan las mismas funciones bajo circunstancias normales.

Personal de las comunicaciones: Personal que diseña los medios de comunicar la información a los empleados, a los clientes, y al público en general. Son los encargados de considerar qué información puede darse y por quién. Esto es crítico en los primeros días de una interrupción pues habrá una mayor demanda para la información, y ocurre en un momento en que los canales normales son interrumpidos por daños en los mismos.

Una vez que se encuentra definido el personal necesario para los diferentes procesos del plan, es necesario que se realicen pruebas del mismo. Pues un plan que no ha sido probado puede presentar fallas en el momento de su ejecución. Las pruebas no deben ser costosas ni interrumpir la operación diaria del negocio. Entre las pruebas que se pueden considerar son:

Prueba de papel. Esto puede ser tan simple como discutir el plan en una reunión del personal considerando sucesos actuales. Es importante documentar la discusión y utilizar cualquier lección aprendida como parte del proceso para mejorar el plan.

Camino Estructurado. Aquí es donde el personal define diversos panoramas para supervisar el plan en equipo.

Prueba de componentes. En esta prueba, cada parte del plan total se puede probar independientemente. Los resultados entonces se miran para considerar cómo el plan total pudo haber trabajado si todos los componentes fueron probados simultáneamente.

Simulación. No incluye realmente la mudanza a una localización alterna sino puede incluir la simulación de interrupciones para uso general como manera de ver que tan completo es un plan.

Ejercicio de la recuperación del desastre. En esta prueba, se activa el plan y los sistemas informáticos se cambian a sus sistemas de reserva, que pueden incluir el funcionamiento en los sitios alternativos. Esto a veces se llama una prueba "paralela" pues los sistemas de producción seguirán siendo funcionales mientras que los sistemas de la recuperación se ponen en producción para probar su funcionalidad.

CUMPLIMIENTO

Generalidades

Los controles implementados en puntos anteriores deben ser complementados con regulaciones de disposiciones legales y contractuales que están actualmente rigiendo en el país. Pero es necesario definir internamente de forma clara los requisitos normativos y contractuales pertinentes a cada sistema de información de la empresa.

Objetivos

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la empresa y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad.

Alcance

Este control se aplica a todo el personal de la empresa.

Derechos de propiedad intelectual

Es necesario para toda organización conocer las leyes para no tener problemas futuros debido a incumplimiento de las mismas. La infracción a estos derechos

podría dar como resultado acciones legales que derivarían en demandas penales.

Salvaguarda de los registros de la organización

Los registros críticos de Baker Tilly se deben proteger contra pérdida, destrucción y posibles falsificaciones.

Para un mejor control los registros van a clasificarse dependiendo del área y el uso; además de detallar la forma de almacenamiento, el responsable de cada registro y el período de retención, es decir el tiempo que debe transcurrir antes de que sean destruidos.

Protección de los datos y de la privacidad de la información personal

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

Se debe redactar Compromiso de Confidencialidad, el cual deberá ser suscrito por todos los empleados.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate.

Evitar el mal uso de los recursos de tratamiento de la información

Los recursos de procesamiento de información se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

7. CONCLUSIONES

- La falta de políticas, controles y normativas de seguridad pueden ocasionar consecuencias graves en el cumplimiento de los objetivos de la empresa.

- Para asegurar el éxito del Sistema de Gestión de Seguridad e la Información - SGSI es de vital importancia contar con el apoyo incondicional de la alta gerencia para la aprobación, la divulgación y su aplicación en la organización.

- La implementación de un Sistema de Gestión de Seguridad de la Información - SGSI en la empresa Baker Tilly Colombia Ltda, brindará seguridad en los sistemas de información e incrementará la confianza tanto de sus funcionarios como de sus clientes mejorando su imagen ante ellos generando solidez de la misma.

- Se requiere establecer un plan anual de capacitación, formación y sensibilización en seguridad de la información, con el objetivo de crear una cultura de seguridad en los funcionarios de la entidad.

- Aplicar la metodología Magerit para el análisis de riesgo es el primer paso para garantizar la seguridad de los activos de información y el normal funcionamiento interno de la entidad.

8. RECOMENDACIONES

- Con el objetivo de beneficiar y mejorar el proyecto, se recomienda un compromiso de la Alta Gerencia de la empresa Baker Tilly Colombia Ltda, donde el diseño o implementación de un Sistema de Gestión de Seguridad de la información (SGSI) no solamente sea un proyecto de la oficina de sistema y del Gerente de Sistemas de la organización, si no que se dé a conocer a toda la empresa con el fin de optimizar los procesos y tener el apoyo que permita el cumplimiento de los objetivos estratégicos y permitiendo los objetivos de TI alinearse a estos.
- Determinar las amenazas de los activos con mayor exactitud y permitir detallar las especificaciones técnicas de los mismos, asimismo, llevar a cabo la capacitación a los funcionarios en temas relacionados a la seguridad de la información y la creación de políticas de seguridad.

- Identificar de forma clara cuales son los activos y asignarles un grado de protección según su criticidad, indicando como debe ser tratado y protegido; para de esta forma mantener una adecuada protección de los activos.

- Realizar análisis periódicos de los riesgos y monitorear continuamente la situación, pues la seguridad que se requiere proporcionar con un SGSI es permanente para lo cual es necesario de un proceso continuo.

- Adquirir un software de gestión de riesgos para la metodología MAGERIT, con el propósito de obtener resultados más precisos y permita en tiempo real calcular los niveles de riesgo potencial y residual para compararlos con los niveles de riesgos aceptables.

9. BIBLIOGRAFIA

AMUTIO, M. A., CANDAU, J., & MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. p. 127.

AMUTIO, M. A., CANDAU, J., & MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. p. 75.

AMUTIO, M. A., CANDAU, J., & MAÑAS, J. A. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de Técnicas. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. p. 42.

COLOMBIA. CONGRESO DE LA REPÚBLICA. "Ley 1273 de 2009". Online. 10 de Mayo de 2015. Disponible en Ministerio de Tecnologías de la Información y las Comunicaciones: (http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf).

DEBARATI, H., & JAISHANKAR, K. Cyber Crime and the Victimization of Women: Laws, Rights, and Regulations.IGI Global, 2011.

GÓMEZ, L., & ANDRÉS, A. Guía de Aplicación de la Norma UNE-ISO/IEC 27001 Sobre Seguridad en Sistemas de Información para PYMES. España: Asociación Española de Normalización y Certificación, 2012. p. 214.

HODEGHATTA, U., & NAYAK, U. The InfoSec Handbook: An Introduction to Information Security.New York: Apress Media, 2014. p. 376.

ICONTEC. Norma Técnica Colombiana: NTC-ISO-IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación, 2013.

KIM, D., & SALOMON, M. G. Fundamentals of Information System Security. United States of America: Jones & Bartlett Learning International, 2012. p 544.

KOSUTIC, D. 9 Steps to Cibersecurity: The Manager's Information Security Manual (Primera ed.). Zagreb: EPPS Services Ltd, 2012. p. 80.

LITTLEJOHN SHINDER, D., & TITTEL, E. Scene of the Cybercrime: Computer Forensics Handbook. Syngress Publishing, 2002. p. 754.

OFFICE GOVERNMENT OF COMMERCE. ITIL V3 Foundation Complete Certification Kit. Londres: The Art of Service, 2009.

PETERSON, R. Integration Strategies and Tactics for Information Technology Governance. En W. VAN GREMBERGEN, Strategies for Information Technology Governance (págs. 37-80). IDEA Group Publishing, 2004.

RHODES-OUSLEY, M. Information Security: The Complete Reference (Segunda ed.). McGraw-Hill, 2013. p. 897.

SUÁREZ, L., & AMAYA, C. A. Sistema de Gestión de la Seguridad de la Información. Bogotá: Universidad Nacional Abierta y a Distancia, 2013. p. 97.

UNAD (2014). Módulo de la asignatura de Proyecto de Seguridad Informática I, capitulo 1 – generalidades.

UNAD (2014). Módulo de la asignatura de Proyecto de Seguridad Informática I, capitulo 2 – Investigación en seguridad informática.

UNAD (2014). Módulo de la asignatura de Proyecto de Seguridad Informática I, capitulo 3 – Proyectos de seguridad informática.

VAN GREMBERGEN, W. Strategies for Information Technology Governance. IDEA Group Publishing, 2004.

10. WEBGRAFÍA

Alan Bryden, COPANT Seminar on Security Standards, Disponible: http://www.iso.org/iso/livelinkgetfile?llNodeId=21657&llVolId=-2000
International Organization for Standarization (ISO), Disponible: http://www.iso.org/

Erazo, Arturo. Video titulado componentes de un anteproyecto para la especialización en seguridad informática de la UNAD (2014). Disponible en: http://conferencia2.unad.edu.co/p7d56iscjb1/.

Guía Metodológica para Implantación de un Sistema de Gestión de Seguridad Informática, Disponible en: http://www.agesic.gub.uy/innovaportal/file/3696/1/res_005_anexo_sgsi.pdf

KOSUTIC, D. *¿Cómo obtener la certificación ISO 27001?* En Línea. 2 de Abril de 2010. Disponible en ISO 27001 & ISO 22301: (*http://blog.iso27001standard.com/es/tag/sgsi/*)

Metodologías para la implantación de SGSI, Disponible en: http://agesic.gub.uy/innovaportal/file/1065/1/primera.pdf