Análisis de los riesgos y vulnerabilidades de un data center en Colombia para crear una matriz de riesgo acorde lo establecido en la norma ISO 27001: 2013

Camilo Andrés Ñustes Bermúdez
Esteban Camilo Orjuela Supelano

Universitaria Agustiniana
Facultad de Ingenierías
Ingeniería en Telecomunicaciones
Bogotá D.C.
2021

Análisis de los riesgos y vulnerabilidades de un data center en Colombia para crear una matriz de riesgo acorde lo establecido en la norma ISO 27001: 2013

Camilo Andrés Ñustes Bermúdez
Esteban Camilo Orjuela Supelano

Director
Francisco Clemente Valle Diaz

Trabajo de grado para optar al título de ingeniero en Telecomunicaciones

Universitaria Agustiniana
Facultad de Ingeniería
Ingeniería en Telecomunicaciones
Bogotá D.C.
2021

Resumen

Un data center almacena, protege y distribuye la información a través del uso de herramientas para analizar datos que permiten tomar mejores decisiones al interior de las organizaciones. El entorno actual, exige a las empresas contar con políticas encaminadas a la seguridad de la información, la cual representa un rol determinante para su correcto funcionamiento, garantizando los tres pilares fundamentales de la información; confidencialidad, integridad y disponibilidad. Para la presente investigación se realizó el análisis de los riesgos y vulnerabilidades de un data center en Colombia a través de la elaboración de una matriz de riesgos bajo los parámetros establecidos en la norma ISO 27001:2013, mediante la cual se listaron controles para el desempeño de riesgos, monitoreo, funcionamiento y efectividad de un data Center, teniendo en cuenta el mejoramiento constante de la seguridad de la información.

Previo a la realización de la matriz de riesgos, fue necesario la recolección de datos bajo los parámetros de la investigación cuantitativa, iniciando por el estudio teórico de la noma en referencia. Posteriormente, se conoció la infraestructura física y lógica de un data center, lo que permitió el establecimiento de medidas capaces de mitigar los riesgos que puedan afectar la información de un data center en Colombia, las cuales se detallan en la siguiente investigación.

Palabras claves: riesgo, ISO 27001:2013, matriz de riesgo, data center

Abstract

A data center stores, protects and distributes information through the use of tools to analyze data that allow better decisions to be made within organizations. The current environment requires companies to have policies aimed at information security, which represents a decisive role for its correct operation, guaranteeing the three fundamental pillars of information; confidentiality, integrity and availability. For this research, the analysis of the risks and vulnerabilities of a data center in Colombia was carried out through the elaboration of a risk matrix under the parameters established in the ISO 27001: 2013 standard, through which controls were listed for the risk performance, monitoring, operation and effectiveness of a data center, taking into account the constant improvement of information security.

Prior to the realization of the risk matrix, it was necessary to collect data under the parameters of the quant research, starting with the theoretical study of the standard in reference. Subsequently, the physical and logical infrastructure of a data center was known, which will achieve the establishment of measures capable of mitigating the risks that can affect the information of a data center in Colombia, which are detailed in the following investigation.

Keywords: risk, ISO 27001:2013, risk matrix, data center

Tabla de contenido

Lista de figuras

Introducción

Las organizaciones actualmente, están inmersas en continuos cambios tecnológicos que se viven día a día, donde se reconoce el protagonismo y el valor de la información en sus procesos productivos, por lo mismo es importante tener su información correctamente identificada y protegida, como además la disponibilidad de la misma por las partes interesadas y autorizadas, enmarcada bajo las interacciones de cumplimiento, normatividad y comercial, garantizando convenios de confidencialidad y demás compromisos a los que se comprometen colaboradores de la empresas así como sus terceros, quienes se obligan a ofrecer un uso, procedimiento, funcionamiento y categorización a la información bajo una adecuada gestión y protección.

La información al ser un recurso que es considerado como un activo más de la organización, el cual tiene costo para la misma y por lo tanto debería ser debidamente protegida. Es por ello por lo que las políticas de seguridad de la información salvaguardan a la misma de una vasta gama de amenazas existentes y futuras que estén asechando este activo, para hacer de él uso no deseado por la organización, por lo que se hace importante que la gestión de la seguridad de la información asegure la continuidad de los sistemas de información, reducir los peligros de mal y afirmar el eficiente cumplimiento de las metas de las organizaciones.

La gestión de la seguridad de la información tiene como fin la custodia de los activos de la información en cualquier de sus estados frente a algunas amenazas o brechas que atenten contra sus principios primordiales de disponibilidad, integridad y confidencialidad, lo cual se logra por medio de la implementación de medidas de control y estabilidad de la información, que permitan gestionar y minimizar los peligros e impactos a que está expuesta y se pueda conseguir el mayor retorno de las inversiones en las oportunidades de negocio.

Es viable reducir el grado de riesgo de manera significativa, con ello la materialización de las amenazas y el impacto de estos sin necesidad de hacer altas inversiones ni disponer de una enorme composición de personal. Para ello se hace primordial conocer y gestionar de forma ordenada los peligros a los que está sometido el sistema informático, tener en cuenta métodos adecuados y planear e implantar los controles de estabilidad que correspondan.

Problemática

Actualmente, las organizaciones tanto del sector privado como público, se enfrentan a un gran reto ya que al contar con tecnologías informáticas que facilitan la administración de la información deben optar por adquirir dentro de cada institución, normas o leyes que permanezcan en el marco de las tecnologías de información capaces de encarar peligros que atenten contra la información sensible, minimizando el impacto en cada amenaza, actualmente teniendo en cuenta que la información es soportada por hardware y software, es fundamental tener una visión holística en cuanto a las normal a implementar para descubrir falencias en la seguridad y medidas correctivas que se pueden implementar en cada caso, alineadas con el cumplimiento de las leyes y mejorando la imagen de la institución (Barrios, 2014).

A lo largo de los últimos años se han presentado sucesos de ciberseguridad que evidenciaron que ningún sector es inmune a los ataques y que es fundamental continuar los métodos de estabilidad, y reducción del riesgo. Actualmente las empresas requieren de un sistema de gestión de seguridad de la información por lo que se hace necesario realizar inicialmente un análisis de las principales causas de perdida de información, es por esto que es de gran importancia las normas y estándares internacionales de seguridad de la información con el fin de que sean implementadas dentro de las organizaciones, teniendo en cuenta que la información es considerada como un activo de alto valor según la clasificación de la información determinada por cada entidad (Díaz, 2020).

Es por esto que la norma ISO 27001 cumple con un papel muy importante al momento de establecer las normas de seguridad de la información dentro de las instituciones ya que su objetivo principal es la defensa, protección y gestión de la información logrando preservar la confidencialidad, integridad y disponibilidad de la información lo que trae múltiples beneficios para la organización que la implemente como aprobar auditorias orientadas a la seguridad de los datos, evitar incumplimientos legales, cumplir con el reglamento general de protección de datos, aplicar mejores prácticas, ventajas comerciales entre otras. Al ser un estándar internacional para la seguridad de la información compuesto de un conjunto de normas entre ellas una nueva que se debe empezar a implementar dirigida al cloud computing para así cubrir un conjunto amplio de procesos dirigidos a la seguridad de la información (ISO N. , 2013).

Justificación

La privacidad y la seguridad de la información para las compañías es parte fundamental, por lo que es importante garantizar la seguridad informática en los diferentes centros de cómputo donde se alberga dicha información.

Es importante reconocer las falencias de seguridad que tienen los diferentes tipos de data center en Colombia para así poder establecer estrategias o soluciones orientadas a minimizar el impacto negativo al interior de las compañías.

Es por esta razón, que las compañías en la actualidad se han interesado en implementar dentro de sus políticas, el sistema de gestión de la seguridad de la información, alineadas con la norma ISO 27001, mediante la cual se busca obtener la certificación para ser altamente competitivos en el sector, generando valor agregado en diversos campos. Contar con las herramientas adecuadas encaminadas al análisis del sistema de seguridad de la información, permitirá monitorear que el entorno de la organización cuente con los estándares de confiabilidad deseados.

Lo anterior se convierte en una necesidad de suma importancia ya que actualmente se evidencia que el principal objetivo de los ciber criminales son los data center, al ser una infraestructura crítica y de alto valor por el tipo de operaciones que realizan y por la información que alojan de diferentes compañías nacionales e internacionales (Sánchez, 2020).

La investigación realizada durante este trabajo, permite dar una óptica global sobre un fenómeno que está latente en la sociedad, debido a la falta de conocimiento sobre el manejo de los datos personales a los cuales las entidades tienen acceso. Con la realización de este proyecto se pretende sentar un antecedente para futuras investigaciones centradas en la seguridad informática.

Objetivos

Objetivo general

Analizar los riesgos y vulnerabilidades de un data center en Colombia para crear una matriz de riesgo acorde a lo establecido en la norma ISO 27001: 2013

Objetivos específicos

- Identificar la parte teórica de la norma ISO 27001: 2013 la cual se compone de políticas de seguridad, planes de contingencia, directrices enfocadas a la seguridad de la información.
- Reconocer la infraestructura física y lógica que requiere un data center en Colombia para gestionar la seguridad de la información.
- Analizar la información recolectada para establecer el diseño de la matriz de riesgo para un data center en Colombia.
- Establecer medidas con la cuales se puedan mitigar los riesgos, desde los más simples hasta los más complejos que puedan afecten la gestión de la seguridad de la información en un data center en Colombia

Marco referencial

Estado del arte

El presente plan explica el proceso de preparación de un modelo de administración de estabilidad de la información con base en la regla ISO/IEC 27001 para el Data-Center de la facultad de ingeniería y ciencias aplicadas, así como estructurar políticas y controles basados en los lineamientos, controles y parte lógica de la arquitectura de red. Se puede constatar mediante la aplicación de la metodología MAGERIT que los límites iniciales de peligro para amenazas humanas accidentales y deliberadas se encontraban entre 8,6 y 9,3 respectivamente. Al llevar a cabo las políticas seleccionadas se puede obtener que el peligro redujo a rangos de 4,6 y 41 tanto en origen humano accidental y deliberado, lo cual involucra una optimización, sin embargo, no desecha que se elabore una idealización constante para conservar los niveles de peligro bajos (ESPINOSA, 2017).

La implementación del sistema de gestión ISO 27001:2013 contribuye a la protección de la información de los procesos de TI (Tecnología de la Información), por medio de la utilización de lineamientos y controles que la resguarde. En este trabajo se detallan las ocupaciones para una adecuada utilización del sistema de administración de seguridad de la información, asimismo recalca la trascendencia de concienciar al personal en el valor de proteger la dimensiones: confidencialidad, integridad y disponibilidad por medio de la utilización de una metodología que posibilite detectar las amenazas que atenten contra la estabilidad de la información en los procesos de TI de la organización GMD® que administra la plataforma tecnológica. Las técnicas que se usaron fueron las siguientes: Encuestas, estudio documentario y auditorías Como conclusión la premisa general nos muestra que el sistema de administración de seguridad de la información ISO 27001:2013 posibilita proteger la información de distintas amenazas por medio del cumplimiento de las metas de estabilidad y el no disponer de multas o penalidades por perdida de la información (VÁSQUEZ, 2018).

El siguiente proyecto es realizado por la universidad de ciencias informáticas de cuba la cual da a conocer una metodología para la implementación e integración de modelos , herramientas y modelos para la optimización , monitorización y revisión para la seguridad de la información de cualquier empresa basando en una de la norma más importante en la actualidad la cual es ISO/IEC 27002 esto con el fin de que el proceso sea menos complejo, efectivo y con una adaptación al

usuario mucho más confortable con un 90% de eficiencia ante los anteriores métodos (Informáticas, 2018)

Marco teórico

Sistema de Gestión de seguridad de información SGSI.

> Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. (CONSULTING, 2018).

Matriz de riesgos consolidada.

Es una herramienta de gestión que permite identificar y observar los riesgos a los cuales está expuesta cualquier organización, su finalidad es analizar, comparar por niveles de riesgo para poder proponer estrategias o acciones para poder mitigar este riesgo y para realizar una evaluación en caso de que este riesgo se materialice para la organización (Rimac, 2021).

Data center.

Un Data Center, es una instalación, construcción o inmueble de gran tamaño donde se albergan y mantienen numerosos equipos electrónicos como servidores, ventiladores, conexiones y otros recursos necesarios que se utilizan para mantener una red o un sistema de computadores, información, conexiones y datos de una o varias empresas. Dichas instalaciones necesitan contar con la suficiente energía para operar todo ese sistema, así como una ventilación adecuada para su funcionamiento óptimo y sistemas de seguridad avanzados para evitar fugas de datos u otros riesgos. A pesar de que una empresa puede contar con su propio Data Center, lo más recomendable es que la encargada de tener dicho centro de datos y resguardar esa gran cantidad de información, sea una empresa dedicada a este rubro; así podrá mantener la seguridad y continuidad del negocio (Networks, 2019).

Modelo de seguridad y privacidad de la información.

Contempla un periodo de operación conformado por 5 etapas, las cuales permiten que las entidades logren gestionar correctamente la privacidad y seguridad de sus activos de información (MINTIC, 2016).

Redes.

Es un conjunto de dispositivos tanto físicos como lógicos los cuales nos permiten compartir los recursos entre diferentes hosts, y tiene una infraestructura física la cual nos permite transportar la información desde una fuente hacia el destino y viceversa además las redes informáticas se pueden clasificar según su tamaño , importancia, cantidad de equipos , velocidad, alcance lo cual da una infinidad de diferentes opciones para la creación o transportación de la información (Alegsa, 2016) .

Wifi.

Es un mecanismo que nos permite conectarnos a internet de forma inalámbrica mediante cualquier dispositivo móvil es posible la conexión mediante el uso de radiofrecuencias e infla rojos empleado principalmente para la transmisión de información normalmente su alcance es de 5 a 150 metros mediante el emisor (SoftwareLab.org, 2017) .

Cloud computing.

La computación en la nube ofrece a los individuos y a las empresas de todos los tamaños la capacidad de un pool de recursos de computación con buen mantenimiento, seguro, de fácil acceso y bajo demanda, como servidores, almacenamiento de datos y solución de aplicaciones Eso proporciona a las empresas mayor flexibilidad en relación a sus datos e informaciones, que se pueden acceder en cualquier lugar y hora, siendo esencial para empresas con sedes alrededor del mundo o en distintos ambientes de trabajo (Salesforce, 2020).

Riesgo informático.

La exploración de peligro informático es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se hallan expuestos, con el fin de decidir los controles adecuados para acetar, reducir, transcurrir o eludir la ocurrencia del peligro (Lagorio, 2016).

VPN Virtual Prívate Network.

Es una tecnología de red que se usa para conectar una o más computadoras a una red privada usando Internet. Como describimos en el artículo sobre para qué sirve una VPN, las organizaciones acostumbran usar estas redes para que sus empleados, a partir de sus viviendas, hoteles, etcétera., logren entrar a recursos corporativos que, de otro modo, no podrían. No obstante, conectar la PC de un empleado a los recursos corporativos es tan solo una de las funcionalidades de una VPN (Goujon, 2012).

Consecuencia de un riesgo.

Son los efectos ocasionados por la ocurrencia de un riesgo que afecta o favorece las metas y procesos de las entidades, primordialmente se otorgan sobre las personas, bienes materiales o inmateriales. Con incidencias importantes tales como riegos físicos, fallecimiento, sanciones, pérdidas económicas, perdida de información, bienes, imagen, credibilidad, confianza, interrupción del servicio e infortunio ambiental. (William, 2021)

Marco Legal

La realización del proyecto debe contemplar los diferentes parámetros que se tienen en la actualidad para el uso de la información informática y parámetros para una buena seguridad de la información de cualquier empresa de cualquier ámbito laboral.

La norma ISO 27 001 es una de las principales normas que rigen a nivel mundial para el derecho y la gestión de la seguridad informática la cual permite el buen aseguramiento, la confidencialidad e integridad de la información informática así mismo describe la como poder gestionar la seguridad de la información de cualquier empresa (NORMA TÉCNICA NTC-ISO/IEC, 2006).

Ley 527 de 1999 Por tal razón y para tener buenas prácticas se determinan y se establecen medidas para el acceso uso de mensaje de datos para el comercio electrónico y firmas electrónicas y se crean las entidades de certificación (colombia, LEY 527 DE 1999, 1999).

La ley 34/2002 se basa en los servicios de la información y el comercio electrónico el cual regula el buen uso de los datos personales de los usuarios y a su vez establece la validez de los contratos que se realizan por vía electrónica actualmente está vigente en España y en los miembros de la Unión Europea. (BOE, 2002).

Ley Estatutaria 15 81 de 2012 En la presenta ley principalmente dictan las disposiciones pautas y factores a la hora de la recolección de datos privados o personales de una persona natural por parte de cualquier empresa o entidad financiera. (Colombia, 2013).

Ley 1341 DE 2009 Es la ley la cual define los principios y conceptos sobre la seguridad y la organización de la información y el uso eficiente de la infraestructura tecnológica por parte del estado colombiano y se crea la agencia nacional del espectro. (colombia, 2009).

Decreto 2609 de 2012 Lineamientos en general de la táctica de régimen online de la república de Colombia que dirige el ministerio de las tecnologías de información y las comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones. (colombia, Decreto 2693 de 2012, 2012).

Como puede evidenciarse en la norma vigente, organizaciones internacionales y el gobierno ha promovido a través de leyes, decretos o sentencias, el correcto uso de información personal lo cual es indispensable a la hora del uso de datos personales o privados por cualquier organización o compañía.

Metodología

> La aplicación de un método ordena y orienta la ejecución de cualquier actividad. Así mismo, implica una planificación que impide obrar de manera azarosa e improvisada. En consecuencia, los métodos se aplican en diversas esferas de la vida humana: existen métodos de trabajo, de enseñanza, métodos terapéuticos y los métodos de investigación. (Arias, 2016)

Años de investigación y recolección de datos dan evidencias de los diferentes métodos y formas de investigar dependiendo los objetivos y criterios básicos, siendo los más destacados:

- Investigación pura o teórica
- Investigación cualitativa y cuantitativa
- Investigación aplicada (castillero, 2020).

De esta manera y con el propósito de responder a la problemática planteada, la investigación que se empleará durante el desarrollo del proyecto será sobre el método cuantitativa con referencia a lo anterior se realizará una matriz de riegos y vulnerabilidades para un data center en Colombia basados sobre la norma internacional ISO 27001.

Para el desarrollo de este proyecto fue necesario la recolección de información y de datos sobre el funcionamiento de varios centros de cómputo tanto en su parte física como en su apartado lógico para poder abarcar más vulnerabilidades y riesgos a los que se encuentra la información almacenada por estos mismos.

Una vez desarrollado el proyecto se podrá establecer medidas de seguridad de la información la cual se podrá utilizar en la mayoría de los data center existentes o para la creación de estos mismos si es necesario.

Desarrollo Objetivo N 1

Norma ISO 27001

El uso de la información es un aspecto importante para la buena operación y funcionamiento de cualquier compañía en el país es por esta razón que es importante velar por su integridad y fiabilidad por se crea la norma ISO 27001.

> Esta regla específica los requisitos para implantar, llevar a cabo, conservar y mejorar constantemente un sistema de administración de la estabilidad de la información dentro del entorno de la organización. La regla incluye los requisitos para la valoración y el procedimiento de peligros de estabilidad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en la regla son genéricos y permanecen previstos para ser aplicables a cada una de las empresas, independientemente de su tipo, tamaño o naturaleza (INCONTEC, 2013).

Esta norma es recomendada para ser usada en la evaluación de los procesos de una compañía tanto internos como externos, en la cual se requiera el uso de los datos del usuario, aunque sea mínimo.

La norma ISO 27001, se complementa con las normas ISO 31000: 2009 e ISO 27005: 2011, las cuales brindan un soporte a los conceptos generales que se especifican en la ISO 27001.

Características.

Dentro de las principales características de la norma ISO 27001, se encuentran:

- Realización de análisis de riesgos de forma periódica, mediante el cual sea posible determinar su probabilidad de ocurrencia. Así mismo la norma exige que este análisis sea medido y evaluado en niveles de tiempo establecidos para tal fin.
- La norma establece que todos los niveles organizacionales de la empresa deben estar involucrados y alineados con las políticas de seguridad de la información iniciando con la alta gerencia.
- Establecimiento de políticas y objetivos específicos los cuales deben estar orientados en las necesidades específicas de la organización.
- La organización debe disponer de los recursos necesarios para cumplir con las fases que exige la norma, incluso después de su implementación.
- La información del sistema debe actualizarse periódicamente o cuando se presenten modificaciones. Cabe aclarar que todo cambio que se realice debe ser aprobado previamente antes de su correcta divulgación dentro de la compañía.

- La norma demanda que toda la información referente al sistema se encuentre debidamente soportada en el formato, documentos y recursos dispuestos para tal fin.
- Elaboración de indicadores que permitan el diagnóstico y toma de decisiones en la ejecución del sistema.

Ventajas.

Teniendo en cuenta que la ISO 27001 es una norma con carácter internacional que permite el aseguramiento y confidencialidad de la información, sus principales ventajas son:

- Permite tomar acciones preventivas para mitigar y eliminar el riesgo en el sistema de gestión de la seguridad de la información.
- Ser certificado en la norma demuestra que la organización cumple con altos estándares de seguridad lo que brinda confiabilidad a los clientes.
- Genera una ventaja competitiva en el mercado al ser una certificación internacional.

Fundamentos de la norma ISO 27001

Si bien la norma es certificable para cualquier compañía que lo solicite, se debe cumplir ciertos requisitos antes de solicitar la certificación ante una autoridad acreditada. La organización debe realizar una estructuración ajustable a las exigencias de la norma. Los requisitos principales para solicitar la certificación ISO 27001 son:

- La compañía debe contar con un sistema de la gestión de seguridad de la información.
- La empresa debe disponer de personal capacitado para dirigir la implementación del sistema.
- El sistema de seguridad de la información debe estar implementado por un tiempo mayor de tres meses.

Una vez la compañía cumpla con los requisitos, los principales temas que abarca la norma ISO 27001 para su certificación continua con el siguiente modelo.

Figura 1 Modelo de la norma ISO 27001. Gobierno (2021)

Las Fases y características de este modelo son las siguientes:

Planificación.

En la fase de planificación, se establecen políticas, objetivos y procesos para mejorar la seguridad de la información de acuerdo a las políticas de la compañía. Dentro de esta fase se encuentran las siguientes tareas:

- ✓ Definir el alcance acordado para el SGSI
- ✓ Definir políticas para el SGSI
- ✓ Identificar los riegos sobre el uso o almacenamiento de datos del SGSI
- ✓ Identificar los controles para el mejor uso de la información

Ejecución.

En la fase de ejecución, se implementan y gestionan los controles anteriormente estudiados en la fase de planificación. Se sugiere realizar pruebas o crear un entorno en el cual no se vea afectada la disponibilidad o fiabilidad de la información hasta tener certeza de su buen funcionamiento. Dentro de la fase de ejecución se encuentran las siguientes tareas:

- ✓ Implementar un plan para el tratamiento de riesgos
- ✓ Implementar las políticas, medidas, controles etc.
- ✓ Crear programas para la formación y concienciación de la seguridad de la información

Seguimiento.

En la fase de seguimiento, se verifican y miden los procesos del SGSI realizadas en la fase de ejecución. Dentro de la fase de seguimiento se encuentran las siguientes tareas:

- ✓ Implementar procedimientos para el control y la revisión del SGSI

- ✓ Revisiones regulares para conocer la eficiencia de SGSI a partir de las auditoria
- ✓ Tomar medidas correctivas y preventivas

Mejora.

En esta fase se adoptan acciones correctivas dictaminadas por el comité de SGSI. En caso de observar un fallo en cualquier fase, se tendrá que repetir el ciclo para dar continuidad con el proceso.

Puntos o aspectos más importantes para la norma ISO 27001

Políticas de Seguridad

Es el conjunto de normas o protocolos que toda compañía debe adoptar dentro de su esquema organizacional. Estas, deben estar alineadas a una gestión de riegos en general y estar aprobada por las directrices de la empresa.

Asignación de responsabilidades

Cada tarea o proceso debe asignarse de acuerdo al organigrama de la compañía. De esta manera se detallará las personas responsables de ejecutar cada tarea al interior de la organización.

Salvaguardar los registros de la organización

La información, considerada como un valioso activo dentro de la organización, requiere especial cuidado por lo que debe cumplir con las obligaciones de resguardar la confidencialidad, integridad y disponibilidad de la misma.

Estructura de la norma ISO 27001

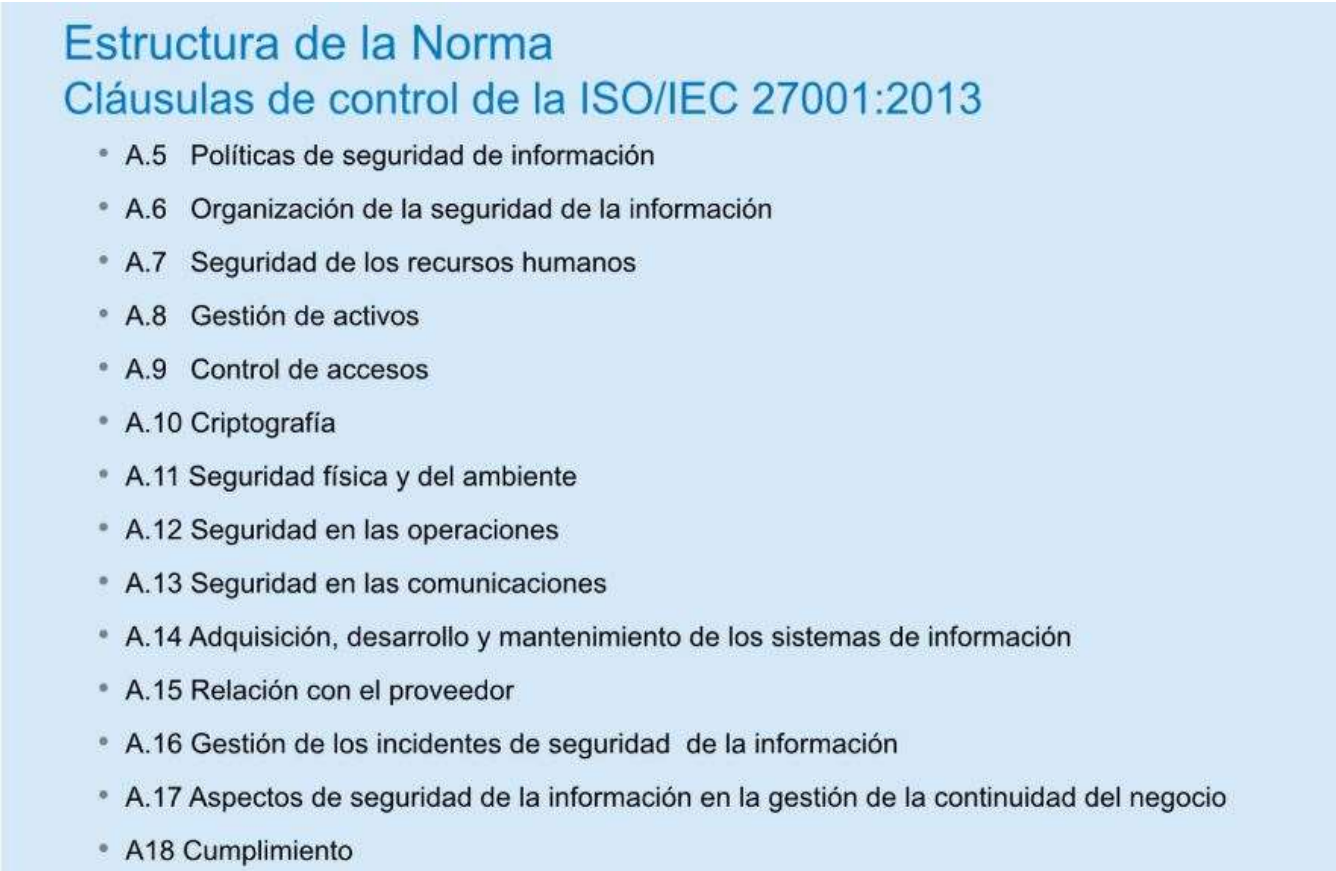


Figura 2 Estructura y cláusulas del control de la ISO 27001. Tools (2017)

La estructura de la norma ISO es uno de las más desarrolladas, pero a su vez una de las más fáciles de entender para cualquier persona en cualquier ámbito profesional conformándose por 14 Dominios, 35 objetivos de control y 114 controles disponibles en su totalidad como se muestran en la siguiente figura

Es importante aclarar que la norma ISO 27002 es un complemento de la norma anterior expuesta donde se encuentra el anexo A sus cláusulas, objetivos y controles más detallados y clasificados para el sistema de la gestión de la seguridad de la información

Desarrollo objetivo N 2

Es importante el conocimiento de la norma ISO 27001 ya que describe los dominios controles y objetivos para el buen desarrollo de una matriz de riesgos , esto ayudara a las empresas a mejorar la seguridad de la información, cumpliendo con las regularidades y adoptando procedimientos establecidos para salvaguardar la información digital como un activo de alto valor, es por esto que se hace fundamental la identificación del hardware del data center para realizar el proceso de aseguramiento y cumplimiento de la norma.

Se justificará porque es importante cada Dominio, Subdominio y controles para el buen funcionamiento de la seguridad de la información del data center en Colombia realizando una matriz de dominio la cual se encuentra anexo en la presente investigación

Elementos básicos de un data center

Todos estos equipos se montan en racks que maximizan el uso del espacio en la instalación. Los racks típicamente se instalan en vertical y se elevan un par de metros dejando suficiente espacio para los sistemas de cables, refrigeración y flujo de aire. El diseño de la red y los servicios de internet son vitales en un Centro de Datos. Existen kilómetros de cableado estructurado de distintas categorías y múltiples capas de comunicación como Smith, que actúan en capa 2 o capa 3 según sea el caso, y los routers o enrutadores componen la arquitectura de red para la comunicación interna y para administrar a los proveedores de servicios de internet conocidos como ISP.

Servidores.

El propósito principal de un data center es alojar los servidores necesarios para soportar los servicios ofrecidos a los clientes. El personal cualificado se encarga de que todos los servidores estén actualizados. Para que tengan un perfecto funcionamiento tanto software como hardware. Estos servidores se colocan en grandes armarios denominados rack. El proveedor del alojamiento proporciona el ancho de banda, la seguridad, refrigeración e instalaciones. Conectividad de red: Mediante suiches todos los servidores reciben y entregan información desde la red y hacia la red según la demanda y el trabajo al que estén destinados.

Energía.

Se necesita una fuente de alimentación para mantener todo este conjunto en marcha. Normalmente se usan fuentes redundantes y electro-generadores diésel para abastecer a todo el sistema en caso de fallo eléctrico. Los sistemas eléctricos deben de mantenerse constantes y sin fluctuaciones de voltaje o intensidad los cuales pueden perjudicar a todo el conjunto

Climatización.

La carga de trabajo a la que se someten los sistemas de un data center generan unas condiciones de calor muy elevadas. También se tiene en cuenta la disposición de los servidores para que la evacuación natural del aire sea la mejor posible.

Monitorización.

La información y procesos que alberga un data center es en la mayoría de los casos crítica, un fallo en el servidor. Por ejemplo, se dedique al procesamiento de los datos de tarjetas de crédito puede dejar en jaque a miles o millones de personas. Ir siempre un paso por delante de estos fallos o atajarlos inmediatamente es la labor de personal altamente cualificado. Que se dedica segundo a segundo a velar porque todo funcione correctamente.

Seguridad física.

existen controles de acceso biométricos como el reconocimiento de huellas y el reconocimiento facial. También existen componentes contra incendios y de detección de derrame de líquidos. (101, 2021)

Clasificación de un data center

El concepto de Tier indica el nivel de fiabilidad de un centro de datos definidos por cuatro niveles de disponibilidad. Mientras más grande sea el número o clase del Tier, mayor disponibilidad del servicio y en consecuencia mayores costos asociados en su construcción además de mayor disponibilidad de tiempo para su ejecución. En la actualidad se han definido cuatro tipos de Tier. El servicio puede sufrir interrupciones planificadas o no planificadas.

Data center Tier 1.

Es el nivel más bajo a la hora de hablar de un centro de cómputo. Generalmente estos Data center se localizan en empresas pequeñas las cuales no necesitan albergar su información en un gran sistema de almacenamiento. Estos tipos de data center son ideales para empresas que no poseen un gran tráfico web. Su estructura se evidencia en la figura 3.

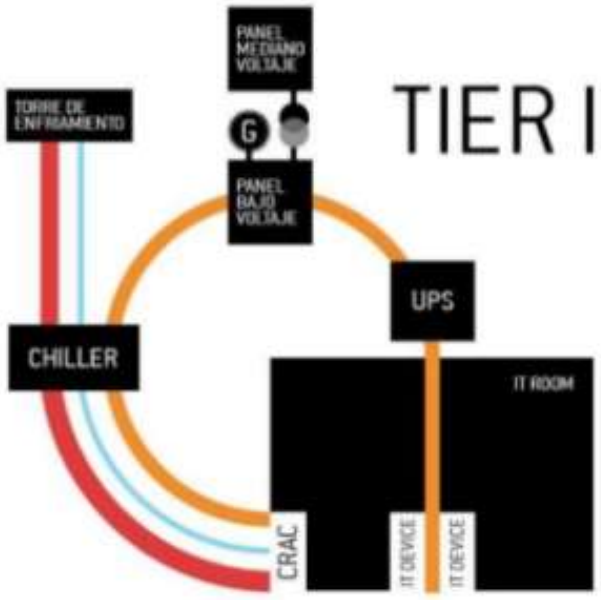


Figura 3 Modelo de la estructura física de un data center tier I. Novoa (2013)

Para poder ser certificados como un Tier 1, el data center deberá cumplir con los siguientes requerimientos.

- No podrá tener más de 28.8 horas de inactividad al año
- Su infraestructura constara de un solo enlace ascendente.
- Su infraestructura solo tendrá una única ruta de alimentación de energía
- Sus servidores no serán redundantes.

Data center Tier 2.

Este nivel de data center deberá contar con algunos componentes redundantes los cuales son menos susceptibles a interrupciones de la información en la parte física y lógica. Adicional, es de los centros de cómputo comúnmente utilizados por las empresas denominadas PYMES puesto que abarcan más información y tráfico de datos. Su estructura se evidencia en la figura 4.

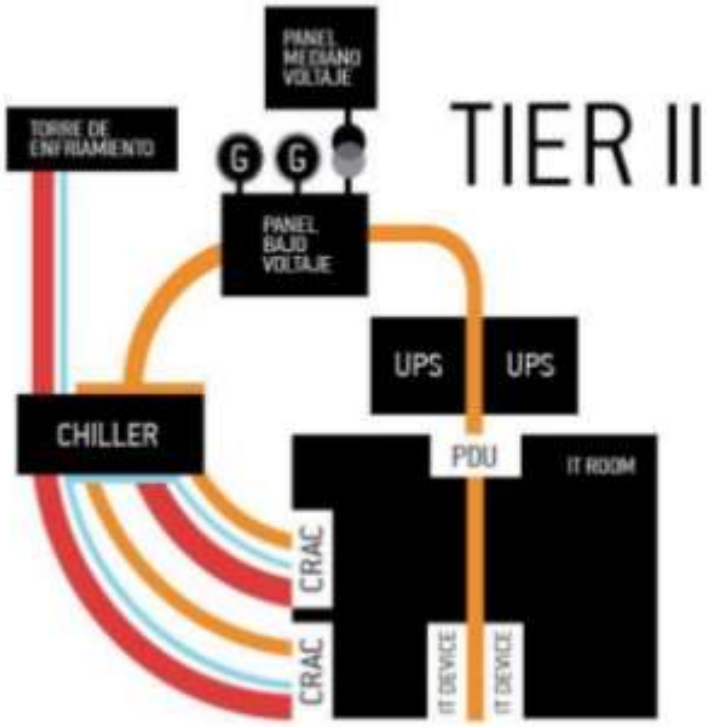


Figura 4 Modelo de la estructura física de un data center tier II. Novoa (2013)

Para poder ser certificados como un Tier 2 el data center deberá cumplir con los siguientes requerimientos.

- No podrá tener más de 22 horas de inactividad al año
- Contar con un generador de energía independiente
- Componentes de redundantes en la sección de energía y de enfriamiento desde una vía única
- Tendrá que poseer un piso elevado

Data center Tier 3.

Este tipo de data center está enfocado en las empresas medianas y grandes tales como aseguradoras, centros médicos, o tiendas virtuales del país, para las cuales los aspectos de eficiencia, seguridad y disponibilidad de la información es primordial para su adecuado funcionamiento. Su estructura se evidencia en la figura 5

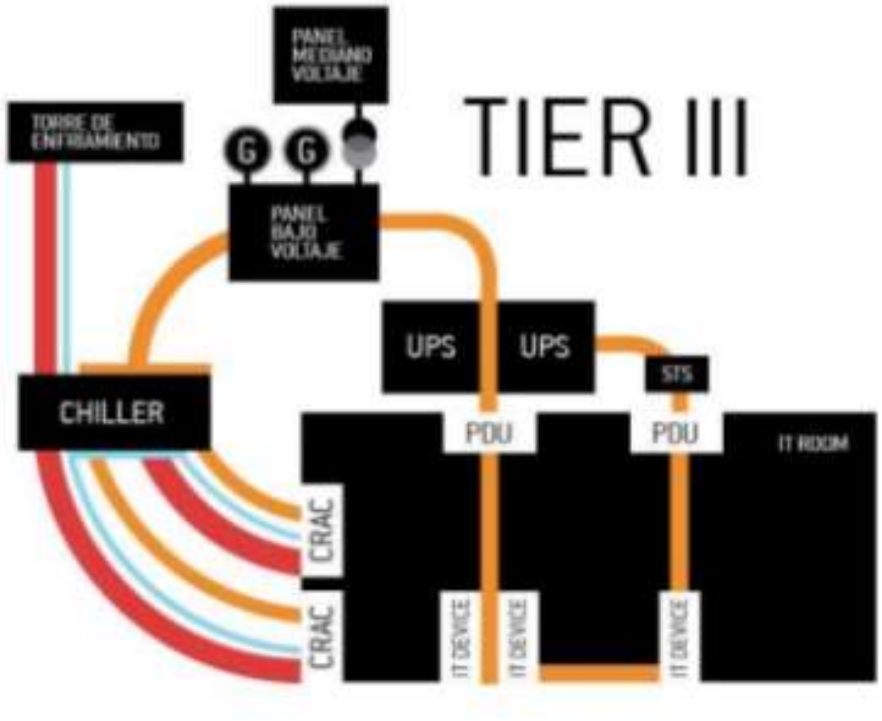


Figura 5 Modelo de la estructura física de un data center tier III. Novoa (2013)

Para poder ser certificados como un Tier 3, el data center deberá cumplir con los siguientes requerimientos

- Tendrá que poseer múltiples accesos de energía y refrigeración, por una sola vía y tendrá que Incluir componentes redundantes (N+1) en el apartado de la energía
- No podrá tener más de 1.6 horas de inactividad al año, como se puede evidenciar es uno de los aspectos más importantes a la data center Tier 2
- Este data center tendrá que contar con una protección de energía de 72 de horas contra cortes de energías y tendrá que ser un sistema exclusivo y con el requerimiento de no conectarse a ninguna fuente externa.

Data center Tier 4 (Tolerante a Fallas).

Este tipo de data center está enfocado en las compañías grandes e internacionales tales como entidades bancarias, compañías internacionales, operadores telefónicos y especialmente para entidades gubernamentales donde la disponibilidad, fiabilidad y seguridad de la información es permanente, debe ser las 24 horas del día los 7 días de la semana. Su estructura se evidencia en la figura 6.

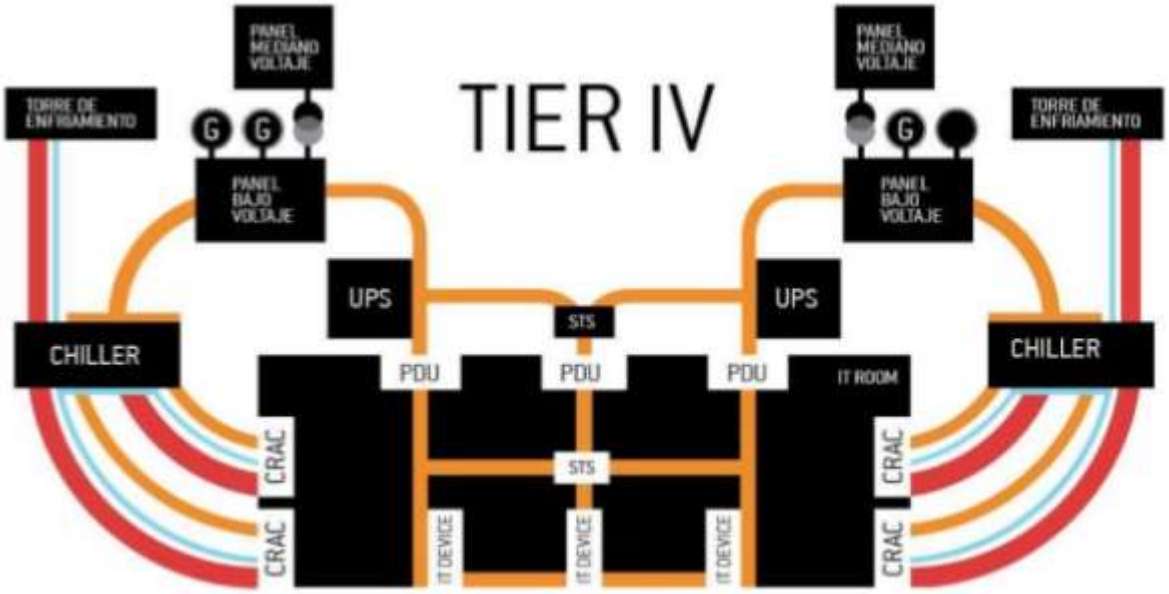


Figura 6 Modelo de la estructura física de un data center tier IV. Novoa (2013)

Para poder ser certificados como un Tier 4, el Data center deberá cumplir con los siguientes requerimientos

- Tendrá que poseer componentes de redundancia para cada proceso y flujo para la protección de datos lo cual ningún corte o falle puede detener el sistema
- No podrá más de 26 minutos de tiempo de inactividad al año
- Su infraestructura será de dos veces de la cantidad necesaria más un respaldo independiente (2N+1)
- Este data center tendrá que contar con una protección de energía de 72 de horas contra cortes de energías y tendrá que ser un sistema exclusivo y con el requerimiento de no conectarse a ninguna fuente externa

Tabla 1.

Disponibilidad para cada nivel de data center.

Nivel	Disponibilidad Garantizada
Tier 1	99,67%
Tier 2	99,74%
Tier 3	99,98%
Tier 4	99,99%

Nota. Autoría Propia, 2020.

Equipos y marcas utilizados por un data center en Colombia.

A continuación, mostraremos ilustraciones de los equipos más utilizados en un centro de cómputo.

Racks: los racks son un espacio fabricado en metal a modo de armario en el cual se introducen una serie de dispositivos informáticos o de comunicaciones, así como electrónico. Estos armarios rack están fabricados con el objetivo de permitir la introducción de equipamiento de diversos estilos y marcas. (Tectel, 2015)

Figura 7 Rack marca panduit. Panduit (2021)

Switch : son un elemento fundamental en la red doméstica y también en la red profesional, no solamente sirven para tener más puertos cableados para proporcionar más conexiones a los dispositivos, sino que también nos permiten proporcionar alimentación a través de sus puertos RJ-45 utilizando los estándares PoE (PoE, PoE+ y PoE++), también nos permiten segmentar la red local en VLANs, e incluso realizar agregación de enlaces para tener un mayor ancho de banda y mucho más. (Zone, 2020)

Figura 8 Switch Cisco SG220. 360 (2021)

Figura 9 Switch cisco Aruba 6200. Aruba (2021)

Firewall: Además denominado cortafuegos, es un sistema cuya funcionalidad es prevenir y defender a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole la entrada. Posibilita el tráfico entrante y saliente que hay entre redes de una misma red. (Grup, 2020)

Figura 10 Firewall Fortinet FortiGate 80. Fortinet (2021)

JUNIPER NETWORKS

Figura 11 Firewall Juniper. DBMG (2021)

Servidores de almacenamiento (NAS): Un sistema NAS es un dispositivo de almacenamiento conectado a una red que posibilita guardar y recobrar los datos en un punto centralizado para usuarios autorizados de la red y multiplicidad de consumidores (Seagate, 2021)

Figura 12 Servidor Nas IBM V3700. IBM (2021)

Cloud computing de un Data center

Los servicios de un centro computo van más allá del apartado del hardware ofreciendo a los clientes el servicio Cloud, un mecanismo de almacenamiento para la manipulación de información sin la necesidad de estar físicamente en los equipos, las cuales están conectadas generalmente por una VPN desde el centro de cómputo al cliente.

Modelos de Cloud

Cada modelo de Cloud se adecua rápidamente a los cambios que requieran las organizaciones. Uno de los factores más importantes es si los recursos de la información son de acceso exclusivo o compartido.

Nube privada.

Los recursos y accesos son de uso exclusivo de una organización y sus colaboradores.

Nube Comunitaria.

Los recursos son compartidos por una sociedad de empresas concretas, que tienen alguna característica particular que la realizan conformar parte de dicha sociedad. Estas obligan al distribuidor a compartir políticas concretas entre los usuarios de la nube comunitaria.

Nube Pública.

Los servicios se hallan alocados en los servidores del distribuidor o de terceras piezas. La infraestructura de la nube es compartida por diversos consumidores independientes y se debería garantiza la libertad entre los ámbitos de dichos consumidores.

Nube Híbrida.

Es una combinación entre nube publica, nube privada o nube comunitaria. (salazar, 2014)

Servicios de Cloud Computing

Principalmente son 3 servicios de cloud computing ofrecidos por los principales proveedores empresariales en Colombia los cuales son:

- IaaS Infraestructura como servicio: Es uno de los servicios más complejos ya que está enfocado a usuarios expertos otorgándoles un control absoluto al cliente, en este servicio el proveedor suministra los componentes de hardware al cliente.

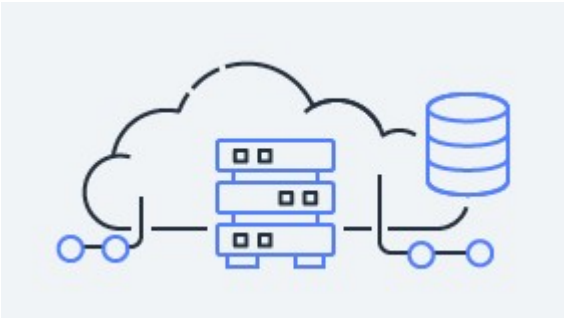


Figura 13 Modelo del servicio IaaS. Services (2021)

- PaaS Plataforma de servicio: Es uno de los servicios el cual el usuario solo tiene acceso a la plataforma la cual le da el proveedor el usuario nunca tendrá control ni permisos a utilizar la infraestructura de este mismo.

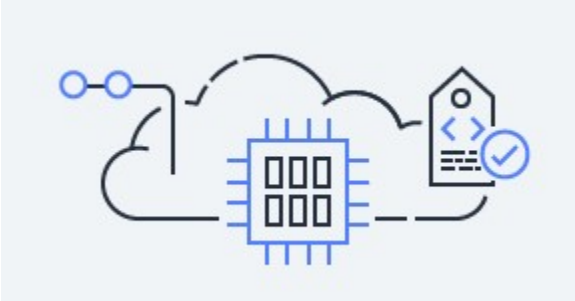


Figura 14 Modelo del servicio PaaS. Services (2021)

- SaaS Software como servicio: Es el servicio más común y enfocado para el usuario del día al día los ejemplos más claros de este servicio son los ofrecidos como Google Drive o One Drive

Figura 15 Modelo del servicio SaaS. Services (2021)

Principales Proveedores de Cloud Servicie en Colombia para un data center

Microsoft.

Microsoft es el principal proveedor ser servicios de almacenamiento ofreciendo los 3 servicios de cloud computing a nivel mundial.

Amazon.

Amazon, aunque es un proveedor nuevo en el mercado es uno de los más eficientes y aunque otorga precios altamente competitivos no cuenta con el servicio de software.

IBM.

IBM es uno de los proveedores más innovadores a lo largo de los últimos años tras haber superado a Salesforce.com tanto en los apartados de infraestructura como en la Cloud.

Salesforce.

Salesforce es una de las compañías con mayor enfoque en innovación digital y la estrategia disruptiva ofreciendo por el momento en el servicio de SaaS, pero siendo uno de los proveedores con más crecimiento en los últimos dos años

Costos promedio de un servicio de Cloud de un data center en Colombia

A continuación, se muestra una propuesta del servicio de cloud (IaaS) ofrecidos por la empresa Host dime Colombia desde su página web

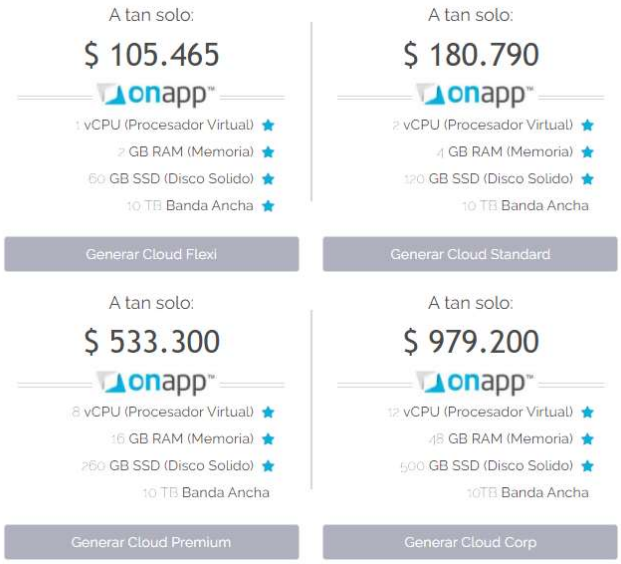


Figura 16 Servicio de cloud de un data center en Colombia. Host (2020)

Como se observa en la imagen la empresa Host dime ofrece unos paquetes de servicios de cloud, aunque el cliente puede reestructurar este paquete de servicios de acuerdo a su necesidad.

Arquitectura Cloud computing

A continuación, se presenta en la imagen el proceso y la arquitectura que posee un data center estándar para el servicio del proveedor de cloud computing con el cliente final

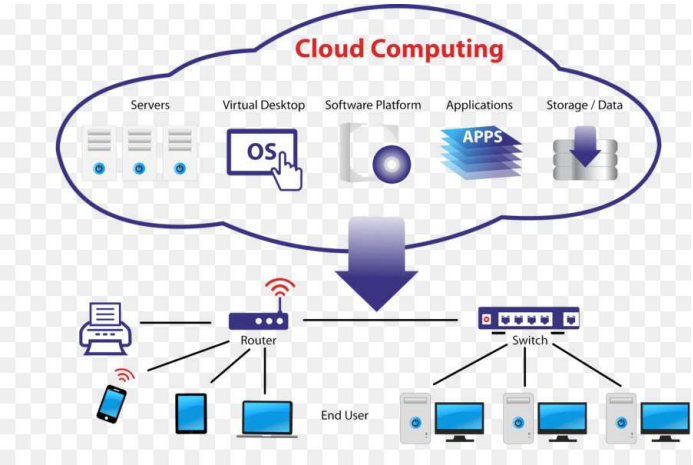


Figura 17 Arquitectura de Cloud computing. Services (2021)

Seguridad Lógica en un data center

Es la implantación de barreras, controles o procedimientos que resguarden el acceso a la información, garantizando que los usuarios que estén autorizadas para hacer uso de ella, accedan para los fines otorgados por las organizaciones, o dueño del activo de la información.

La seguridad lógica involucra todas aquellas medidas establecidas por la administración minimizando los riesgos de vulnerabilidad en la seguridad asociados con el desarrollo de sus actividades diarias.

Objetivo.

- Restringir el acceso a los programas y archivos de la organización a personal no autorizado.
- Asegurar que las personas puedan desarrollar sus actividades sin necesidad de un monitoreo constante, garantizando la integración de los archivos y programas.
- Asegurar el uso de programas, archivos e información correctos en los procedimientos establecidos por la organización.
- Garantizar que la información transmitida llegue al destinatario correcto evitando fuga de esta.

De que se encarga la seguridad lógica.

- Controles de acceso salvaguardando la integridad de la información.
- Identificar Individualmente a cada usuario y sus actividades en el sistema
- Controlar y asegurar la información generada.

Otra medida de estabilidad lógica fundamental es consumar con la Ley Orgánica de Defensa de Datos, proporcionando a los consumidores una gigantesca privacidad y estabilidad de sus datos, evitando que la información viaje por otros territorios sin control.

En la actualidad, varios centros de datos usan tecnología de virtualización, que posibilita desvincular el almacenamiento, la red y los servidores del centro de datos. Esta desvinculación posibilita a los administradores de TI gestionar los servicios del centro de datos de manera remota, y utilizar programa para realizar operaciones del centro de datos y para repartir cargas de trabajo de inmediato en diversos servidores según las necesidades. Ciertos centros de datos usan la tecnología de virtualización para entrar a la cloud pública y como elemento de su infraestructura del centro de datos.

El programa de estabilidad del centro de datos no solo impide que los usuarios no autorizados visualicen o roben datos confidenciales, sino que además se puede usar para hacer una réplica de estabilidad de la información incluida en el interior de datos para protegerla frente a pérdidas.

Las redes deben estar correctamente organizadas y administradas para lograr defender el activo de la información de la organización. los administradores de la red debieran llevar a cabo controles para garantizar la estabilidad de la información en las redes, y proteger los servicios asociados. Se debe tener en cuenta los siguientes ítems:

a) se debieran implantar las responsabilidades y métodos para de la administración del equipo remoto.

b) se debieran implantar controles especiales para defender la confidencialidad y la integridad de la data que pasa mediante las redes públicas o mediante las redes inalámbricas; y proyectar los sistemas y aplicaciones conectados. además, pueden pedir controles especiales para mantener la disponibilidad de los servicios de la red y los pc conectados.

c) se debiera utilizar registros de ingreso y monitoreo apropiados para permitir el registro de las actividades de estabilidad importantes.

d) las ocupaciones de administración debieran estar asociadas a las directrices de la alta dirección para poder mejorar y garantizar los controles a la seguridad de la información.

Programas o software utilizados por un data center en Colombia

A continuación, describiremos algunos de los programas o aplicaciones los cuales se encuentran en un data center en Colombia

SharePoint.

Las organizaciones usan Microsoft SharePoint para crear sitios Web. Se puede usar como un lugar seguro donde almacenar, organizar y compartir información desde cualquier dispositivo, así como acceder a ella. Lo que necesita es un explorador web, como Microsoft Edge, Internet Explorer, Chrome o Firefox (Microsoft, 2019).

Kawak.

KAWAK es un programa para centralizar la información y para acomodar y focalizar su compañía en la calidad y en la optimización continua y sustentable.

Cuente con un Sistema Integral de Administración e indicadores alineados con la táctica organizacional. Atienda de forma simple la normatividad de Estabilidad y Salud en el trabajo y del Ingenio Humano, las PQRS de su compañía y sus Auditorías. KAWAK cubre las reglas ISO 9001, ISO 14001, ISO 27001, ISO 31000, OHSAS 18001, RSE, GP1000, MECI, entre otros (TIC, 2021).

Novasoft.

Herramienta para registrar, mantener el control de, examinar, interpretar y gestionar de forma óptima las operaciones financieras de su organización con las aplicaciones financieras del Sistema modular e incluido de Administración Empresarial NOVASOFT, 100% web.

El sistema posibilita a la gerencia y área financiera regir el flujo de caja, ser más efectivo en los recaudos, automatizar los pagos a proveedores y conciliar los bancos (Guia TIC , 2021).

CSM.

El concepto CMS procede del inglés Content Management System, que significa Sistema de Administración de Contenidos. Es un sistema en línea que nos posibilita llevar a cabo un website de manera práctica e inmediata. Pero, no es sólo aquello, sino que su gran virtud, como su nombre lo dice, es la probabilidad de regir contenidos dinámicos de forma fácil, o sea, conservar un blog, un eco-merce o cualquier otro tipo de página web que demande una actualización constante.

GOTO Webinar.

GoToWebinar es uno de los instrumentos para hacer un webinar más conocidas en el mercado. Su uso es sencillo y además tiene una versión de prueba gratuita, por lo cual no te costará bastante producir tu propio webinar gratis, tan solo siguiendo unos pocos pasos (manuez, 2018).

Suit de adobe.

Las Suites de Adobe una recopilación de bastante más de 20 aplicaciones y servicios para escritorio y dispositivos móviles de fotografía, diseño, clip de video, website, vivencia de cliente y más. Ya puedes llevar tus ideas a nuevos sitios con Photoshop en el iPad, hacer un dibujo y pintar

con Fresco, y diseñar para 3D y RA. Únete a nuestra sociedad innovadora universal y cread algo mejor todos unidos (Adobe, 2021).

Google AdWords .

Google AdWords es el programa de publicidad de Google que posibilita producir anuncios que se presentan a los usuarios que buscan información relacionada con una keywords (keywords) específicas.

El sistema Adwords se fundamenta en un sistema de subasta, que destaca tu postura cuanto más pagues por cada click, que se compensa con datos acerca del grado de calidad de la página web o la landing page que corresponde, algo que únicamente conoce Google (Antevenio, 2015).

Moodle.

La plataforma Moodle es un sistema de educación creado para producir y gestionar espacios de aprendizaje onlineadaptados a las necesidades de docentes, alumnos y administradores

En términos más técnicos, es un sistema web dinámico pensado para gestionar ámbitos de educación virtual, con base en tecnología PHP y bases de datos MySQL. Las plataformas de educación en línea como Moodle además reciben el nombre de LMS, el acrónimo de Learning Management System (sistema de administración de aprendizaje) (Merayo, s.f.).

Azure.

La plataforma Azure está compuesta por bastante más de 200 productos y servicios en la nube diseñados para ayudarle a ofrecer vida a novedosas resoluciones que permitan solucionar los esfuerzos recientes y producir el futuro. Piensa, ejecute y administre aplicaciones en algunas nubes, en el ámbito local y en el perímetro, con los instrumentos y los marcos que prefiera (Microsoft, s.f.).

H2DESK.

H2Desk da una plataforma flexible para la prestación de ayuda al comprador. En el corazón hay un robusto motor de emisión de boletos que es simple de utilizar y simplifica las comunicaciones con los consumidores. Las propiedades integran gestión de tickets, chat en vivo, gestión de labores, seguimiento de SLA e adhesión de correspondencia electrónico. Los widgets del lado del comprador le permiten añadir de forma sencilla artículos, tutoriales y bastante más de la base de conocimientos. Comience una prueba gratuita de 30 días sin compromiso y considera una mesa de ayuda en minutos (Capterra, s.f.).

One Drive.

OneDrive es el servicio en la nube de Microsoft que le conecta a todos los archivos. Te posibilita guardar y defender tus archivos, compartirlos con otros usuarios y entrar a ellos a partir de cualquier sitio en todos tus dispositivos. Una vez que usa OneDrive cuenta facilitada por su organización o escuela, algunas veces se llama "OneDrive para el trabajo o el colegio ". Previamente se denominaba "OneDrive para la Compañía", por lo cual es viable que aún lo vea denominado de esta forma en sitios (Microsoft, s.f.).

RD Station.

RD Station Marketing es un programa que le dejará a las compañías hacer superiores campañas, nutrir leads, crear oportunidades comerciales calificadas y conseguir más resultados. A partir de redes sociales, emails, Landing Pages y Pop-ups, hasta Automatizaciones y Estudio (STATION, 2021).

Desarrollo objetivo N 3

Analizada la infraestructura del data center se realizará el desarrollo de la matriz de riesgo donde se expondrán las vulnerabilidades encontradas, clasificando sus tipos de riesgo, posibles causas, posibilidad de materialización del riesgo, entre otros. Identificando a los riesgos que se está expuesto el data center estableciendo niveles aceptables de riesgos como los controles a implementar.

Identificación de un riego

A continuación, se detallan las etapas más importantes para el reconocimiento y la administración de un riesgo.

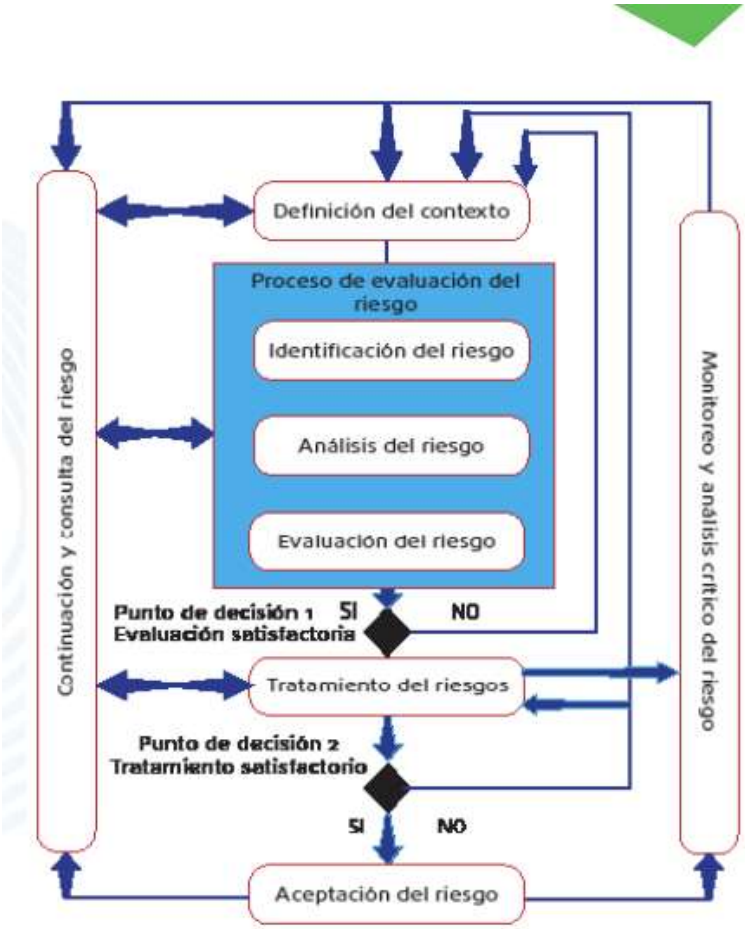


Figura 18 Proceso de gestión de un riesgo. 27005 (2018)

Contexto Estratégico.

El contexto Estratégico es poder identificar si los factores de un riesgo son externo o interno.

Los factores externos pueden ser oportunidades o amenazas y son características del entorno en el cual la entidad opera

Los factores internos pueden ser fortalezas o debilidades y son características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos.

El contexto estratégico es una base fundamental ya que su análisis suministrara la información sobre las causas de cada riesgo

Política para la administración de un riego.

La política de la administración de un riego tiene como objetivo que la alta dirección de la compañía pueda controlar o gestionar el riego con el propósito de poder salvaguardar los activos ante cualquier evento interno o externo el cual ocasione el incumplimiento de la compañía.

Identificación del riesgo.

Para la identificación de un riego es importante reconocer la causa por lo cual este puede suceder teniendo en cuenta los factores internos y externos con relación a: Infraestructura, Economía, Sociales, Culturales, Personas u organizaciones entre varios, una vez reconocida la identificación del riesgo se realizará una descripción breve de este para poder definir sus consecuencias.

En los riesgos de gestión es importante centrarse en los riesgos más impactantes para la entidad relacionados con los objetivos de los procesos y objetivos institucionales

Causas de un riesgo.

Se identifican por ser los medios o circunstancias y agentes generados por el riesgo, los agentes se entienden como todos los sujetos u objetos que tienen como capacidad la de originar un riesgo

A continuación, se presenta una tabla el cual es un ejemplo de los diferentes factores internos y externos de riego y sus causas.

EJEMPLO DE FACTORES INTERNOS Y EXTERNOS DE RIESGO	
FACTORES EXTERNOS	**FACTORES INTERNOS**
Económicos: Disponibilidad de capital, emisión de deuda o no pago de esta, liquidez, mercados financieros, desempleo, competencia.	Infraestructura: Disponibilidad de activos, capacidad de los activos, acceso al capital.
Medioambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.	Personal: Capacidad del personal, salud, seguridad.
Políticos: Cambios de Gobierno. Legislación, políticas públicas, regulación.	Procesos: Capacidad de diseño, ejecución proveedores, entradas, salidas, conocimiento.
Sociales: Demografía, responsabilidad social, terrorismo.	Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento.
Tecnológicos: interrupciones, comercio electrónico datos externos, tecnología emergente.	

Figura 19 Factores externos e internos de un riesgo. Educación (2013)

Descripción de un riesgo

Un riesgo se puede definir en 3 conceptos básicos

Riesgo de gestión: Identifica la posibilidad en la cual este riesgo puede llegar a ocurrir en los objetivos y metas de la organización (publica, 2021).

Riesgo de Corrupción: Posibilita que, por acción u omisión, se haga uso del poder para desviar la gestión de lo público hacia un beneficio privado (publica, 2021).

Oportunidad: Un riesgo también puede ser un efecto beneficioso.

Tipo de riesgo.

Una vez realizada la identificación del riego, se puede hacer una clasificación de este mismo, como se observa en la siguiente tabla.

Tabla 2.
Tipos de riesgo.

Tipos de riesgo	
Riesgo Estratégico	Se asocia con la manera en que se administra la entidad. El desempeño del peligro estratégico se enfoca a asuntos globales involucrados con la tarea y el cumplimiento de las metas estratégicas, la clara definición de políticas, diseño y conceptualización de la entidad de parte de la alta gerencia. (school, 2020)
Riesgo de imagen	Permanecen involucrados con la percepción y la confianza a causa de la ciudadanía hacia la organización (school, 2020)
Riesgo operativo	Entienden peligros provenientes del desempeño y operatividad de los sistemas de información institucional, de la definición de los procesos, de la composición de la entidad, de la articulación entre dependencias. (school, 2020)
Riesgo Financiero	Se relacionan con el desempeño de los recursos de la entidad que integran: la ejecución presupuestal, la preparación de los estados financieros, los pagos, manejos de excedentes de tesorería y el funcionamiento sobre los bienes. (school, 2020)
Riesgos de Cumplimiento	Se asocian con la función de la entidad para consumar con los requisitos legales, contractuales, de ética pública y generalmente con su compromiso frente a la sociedad. (school, 2020)
Riesgos de tecnología	Permanecen involucrados con la capacidad tecnológica de la Entidad para saciar sus necesidades recientes y futuras y el cumplimiento de la tarea. (school, 2020)
Riesgos ambientales	Riesgos para una organización debido a temas relacionados con el ambiente: Esto incluye el riesgo de no cumplir la legislación y criterios existentes, perdida de reputación, multas por no mantener permisos y licencias para el desarrollo y las actividades operativas (school, 2020)

Nota. Autoría Propia, 2020.

Tipos de impacto de un riesgo.

A continuación, se relaciona los tipos de impacto del riesgo el cual puede ocasionar.

- Confidencialidad de la información: Tiene relación con la pérdida o revelación de la misma. Una vez que se habla de información reservada institucional se hace referencia a aquella que por el motivo de ser de la entidad solo podría ser popular y divulgada al interior de la misma; de igual manera, la sensibilidad de la información es dependiente del valor que esta tenga para el desarrollo de la tarea de la entidad.
- Credibilidad o imagen: Tiene relación con la pérdida de la misma ante diferentes actores sociales o en la entidad.

- Legal: Se relaciona con las secuelas legales para una entidad, determinadas por los peligros involucrados con el incumplimiento en su funcionalidad administrativa, ejecución presupuestal y normatividad aplicable.
- Operativo: El efecto operativo aplica en la mayor parte de las entidades para los procesos clasificados como de apoyo, debido a que sus peligros tienen la posibilidad de influir el regular desarrollo de otros procesos.
- Ambiental: Cualquier cambio en el ambiente así sea adverso o productivo, que es el resultado total o parcial de las ocupaciones, productos o servicios de una organización.

Análisis de un Riesgo.

Es fundamental esta etapa ya que será aplicada a los riesgos, teniendo como objetivo principal la medición del riesgo inherente. Determinando la probabilidad en un riesgo se pueda materializar evaluando sus consecuencias e impactos, a razón de establecer el riesgo inicial.

Probabilidad: Posibilidad de ocurrencia de un peligro. Se mide conforme con la frecuencia (número de veces en que se ha presentado el peligro en un lapso determinado) o por la factibilidad (factores internos o externos que tienen la posibilidad de decidir que el peligro se presente) (santander, 2016).

Medición de probabilidad del riesgo.

A continuación, se ilustra el proceso para la medición de un riesgo teniendo en cuenta sus probabilidades y sus hechos pasados con un rango estimado de ocurrencia.

Nivel	Descriptor	Probabilidad	Hechos Pasados	Rango estimado de ocurrencia
1	Raro	Puede ocurrir en circunstancias excepcionales	No ha ocurrido en el ultimo año	<5%
2	Improbable	Insignificante posibilidad que el evento ocurra	Ha ocurrido entre 1 y 10 veces en el ultimo año	5%-10%
3	Posible	Alguna posibilidad que el evento ocurra	Ha ocurrido entre 10 y 59 veces en el último año.	10%-30%
4	Probable	Posibilidad ocurra varias veces	Ha ocurrido entre 60 y 119 veces en el último año.	30%-60%
5	Casi certeza	Ocurra la mayoría de las veces	Se ha presentado más de 120 veces en el ultimo año	>60%

Figura 20 Medición de probabilidad de riesgo. Sarlaft (2021)

Impacto: Son las secuelas o efectos que tienen la posibilidad de producir la materialización del peligro se corrupción de la entidad o compañía, este efecto se puede establecer por medio de la siguiente tabla de medición de efecto de peligros.

Nivel	Descriptor	Riesgo Legal	Riesgo Reputacional	Riesgo Operativo	Riesgo Contagio
1	Insignificante	Observaciones	Solo es de conocimiento de los directivos	Menos del 5% de las ganancias mensuales	No afecta a ningún segmento
2	Menor	Amonestación	De conocimiento de la empresa	Entre el 5% y el 15% de las ganancias mensuales promedio	Afecta uno o mas segmentos
3	Moderado	Multa	De conocimiento a nivel local	Entre el 15% y el 50% de las ganancias mensuales promedio	Afecta todo un producto
4	Mayor	Suspensión Institucional	De conocimiento a nivel nacional	Entre el 50% y el 100% de las ganancias mensuales promedio	Afecta mas de un producto
5	Catastrófico	Cancelación Institucional	De conocimiento a nivel internacional	Mas del 100% de las ganancias mensuales promedio	Afecta toda la operación

Figura 21 Medición de impacto de un riesgo. Sarlaft (2021)

Es necesario realizar la calificación del impacto para poder establecer la zona de riesgo y probabilidad, posterior a ello establecer la evaluación y la zona de nivel de riesgo. Realizándola a través del cruce de los resultados obtenidos del impacto y probabilidad por medio de una multiplicación como en el siguiente ejemplo:

Ejemplo de calificación:

Riesgo de gestión: probable (4) x moderado (3) = A: Zona de riesgo Alta

Resultados de calificación Zona del Riesgo de Gestión					
PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de Riesgo Baja: Asumir el Riesgo.
M: Zona de Riesgo Moderada: Reducir o Asumir el Riesgo.
A: Zona de Riesgo Alta: Evitar, Reducir, Compartir o Transferir el Riesgo.
E: Zona de Riesgo Extrema: Evitar, Reducir, Compartir o Transferir el Riesgo.

Figura 22 Resultados de calificación del riesgo de gestión. Mendoza (2014)

Para los riegos de gestión el resultado de la multiplicación entre la probabilidad y el impacto se ubica en una de las 4 zonas de riesgo que se describen a continuación

Ejemplo:

Riesgo de corrupción: probable (4) x catastrófico (20) = 80 Zona de Riesgo Extrema.

Resultado de calificación Zona del Riesgo de Corrupción				
Probabilidad	**Puntaje**	**Zona del riesgo de corrupción**		
Casi seguro	5	25 Moderada	50 Alta	100 Extrema
Probable	4	20 Moderada	40 Alta	80 Extrema
Posible	3	15 Moderada	30 Alta	60 Extrema
Improbable	2	10 Baja	20 Moderada	40 Alta
Rara Vez	1	5 Baja	10 Baja	20 Moderada
Impacto		Moderado	Mayor	Catastrófico
Puntaje		5	10	20
Baja: Se puede eliminar o reducir el riesgo con los controles establecidos en la entidad. **Moderada y Alta:** La entidad debe propender por eliminar el riesgo de corrupción o por lo menos llevarlo a zona baja. **Extrema:** Requiere de un tratamiento prioritario. Se deben implementar los controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos y tomar las medidas de protección. La entidad debe propender por eliminar el riesgo de corrupción o por lo menos llevarlo a zona baja.				

Figura 23 Resultados de calificación de riesgo de corrupción. Mendoza (2014)

Evaluación del Riesgo.

Su objetivo principal es comparar los resultados del análisis realizado al riesgo con los diversos controles establecidos, determinando la zona de riesgo final. En esta etapa se tiene dos objetivos adicionales:

Riesgo residual. Siendo este el riesgo resultante después de aplicados los controles.

Establecer las medidas adecuadas para reducir la probabilidad y el impacto causado por los eventos de riesgo que amenazan la organización.

En este momento la institución puede determinar y adoptar las medidas o controles que lleven a controlar el riesgo inherente.

Es importante tener claro la siguiente clasificación para determinar la naturaleza de los controles:

Controles correctivos: Son aquellos que permiten el retomar la actividad, después de un evento no deseado o la correcta modificación de esta falla para favorecer su ocurrencia.

Controles preventivos: orientados a suprimir las causas del riesgo, para prevenir la materialización u ocurrencia.

Se hace necesario establecer si el control es automático o manual:

Automático: Donde se requiere de herramientas tecnológicas como softwares o sistemas de información que admitan contraseñas de acceso, o controles de seguimiento, aprobaciones o ejecuciones que se realicen a través de ellos, sistemas de seguridad, grabación, entre otros. Es decir, el control automatizado guarda, procesa información de manera automática.

Manual: hace referencia a todas las políticas aplicables, para la autorización con el fin de dar confirmaciones a través de una plataforma de correo electrónico o archivos físicos , listas de chequeo, controles de seguridad incluyendo al personal designado y especializado para esta labor de la organización. Es decir, la información se guarda y se procesa por cada persona de la entidad mas no automático.

La evaluación de efectividad de controles de los riesgos de gestión y corrupción se puede realizar teniendo en cuenta los criterios que se encuentran en las siguientes tablas:

Criterios para la evaluación de los controles de riesgos de gestión	Evaluación
¿Posee una herramienta para ejercer el control?	15
¿Existen manuales, instructivos o procedimientos para el manejo del control?	15
¿En el tiempo que lleva el control ha demostrado ser efectivo?	30
¿Están definidos los responsables de la ejecución del control y del seguimiento?	15
¿La frecuencia de ejecución del control y seguimiento es adecuada?	25
Total	100

Figura 24 Criterios para la evaluación de los controles de riesgo de gestión. Mendoza (2014)

Criterios para la evaluación de los controles de riesgos de corrupción	Evaluación
¿Existen manuales, instructivos o procedimientos para el manejo del control?	15
¿Están definidos los responsables de la ejecución del control y del seguimiento?	5
¿El control es automático?	15
¿El control es manual?	10
¿La frecuencia de ejecución del control y seguimiento es adecuada?	15
¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10
¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30
Total	100

Figura 25 Criterios para la evaluación de los controles de riesgo de Corrupción. Mendoza (2014)

Acorde la calificación obtenida se realiza un análisis en la matriz, dependiendo si el control afecta el impacto o la probabilidad, determinando la zona de riesgo residual, la cual se obtiene multiplicando la probabilidad con el impacto después de aplicados los controles con el objetivo de reducir el nivel de riesgo al que está expuesto el proceso a analizar.

Descripción de la matriz de riesgo consolidada

A continuación, se detalla la estructura de la matriz de riesgos consolidada para el data center., la cual se encuentra plasmado en un archivo tipo Excel la cual se adjunta a la presente investigación.

La matriz de riesgo se encuentra conformada por 6 secciones de la siguiente forma:

Identificación de riesgos.

IDENTIFICACIÓN DE RIESGOS						
RIESGO	DESCRIPCION DEL RIESGO	PROCESO	TIPO DE RIESGO	FUENTE (INTERNA Y/O EXTERNA)	POSIBLES CAUSAS DE MATERIALIZACION DEL RIESGO	CONSECUENCIA DEL RIESGO

Figura 26 Identificación de riesgos de la matriz de riesgo. Autoría propia (2020)

Riesgo. Numero de riesgos en orden consecutivo encontrados en la totalidad de la investigación efectuada. Para este enfoque se detectaron 61 riesgos que podrían afectar la seguridad de la información.

Descripción del riesgo. En esta celda, se describe de manera detallada y concisa el riesgo identificado durante el desarrollo de la investigación.

Proceso. Se idéntica el proceso o el área al cual está relacionado el riesgo identificado de acuerdo a las siguientes opciones propuestas:

- Calidad,
- Compras y Subcontratación,
- Gestión de recursos, Implementación,
- Mantenimiento de Producto,
- Soporte
- Ventas

Tipo de riesgo. Se describe el tipo de riesgo al cual está relacionado. Para la presente investigación se realizó énfasis en los a riesgos asociados a la seguridad informática.

Fuente interna o externa. Se relaciona el riesgo a su fuente de origen; si es interno, externo o ambos.

Posibles causas de materialización del riesgo. Se describen la causa o las causas de la posible materialización del riesgo.

Consecuencias del riesgo. En esta celda***,*** se establecen las posibles consecuencias que puede generar el riesgo si este se materializa a la organización.

Evaluación de controles a implementar.

EVALUACIÓN DE CONTROLES A IMPLEMENTAR		
DESCRIPCION DE CONTROLES A IMPLEMENTAR	TIPO DE CONTROL (PREVENTIVO O DETECTIVO Y CORRECTIVO)	RESPONSABLE

Figura 27 Evaluación de controles a implementar de la matriz de riesgo. Autoría propia (2020)

Descripción de controles a implementar. Se sugieren controles de seguridad para mitigar el riesgo analizado.

Tipo de control: Se selecciona el tipo de control que puede ser correctivo o preventivo según el análisis del riesgo y de las implicaciones.

Responsable. Se identifica el responsable del área sobre el cual recae el riesgo analizado, bajo el siguiente listado.

- Área IT

- Dirección administrativo y financiero
- Líder de innovación
- Talento humano

Evaluación del riesgo.

Figura 28 Evaluación de riesgo de la matriz de riesgo. Autoría propia (2020)

Teniendo en cuenta la probabilidad y el impacto, si este riesgo se materializara, para dar una respuesta a este riesgo como se evidencia en la siguiente tabla.

Tabla 3.
Resultado del riesgo según su impacto y probabilidad.

impacto/ probabilidad	bajo	medio	alto
alta	moderado	importante	critico
media	bajo	moderado	importante
baja	bajo	bajo	moderado

Nota. Autoría propia, 2020.

Tratamiento del riesgo.

Figura 29 Tratamiento del riesgo de la matriz consolidada. Autoría propia (2020)

Es la forma como se tratará el riesgo de acuerdo al resultado de la tabla 4. Se sugieren unos tiempos para mitigar el riesgo analizado de acuerdo a la organización.

N acción. Se nombran las clausulas de la norma 27001: 2013 relacionado con el riesgo para generar los controles necesarios y mitigar el riesgo.

Plan de contingencia.

Figura 30 Plan de contingencia de la matriz consolidada. Autoría propia (2020)

Se proporciona un plan de contingencia con el fin de informar a los jefes de área, clientes, proveedores u otros que se vean afectados en un caso de la materialización del riesgo.

Relación al anexo A de la norma ISO 27001:2013.

Figura 31 Relación a la controles del anexo a de la norma. Autoría propia (2020)

Se describen los controles del anexo a de la norma ISO 27001:201 con el fin de profundizar en los parámetros del riesgo anteriormente analizado.

Explicación de los riesgos mas importantes hallados en la investigación

RSI-007.

Abuso de privilegios asignados o accesos no permitidos, en el caso de que un colaborador se retire y siga teniendo acceso al correo, plataformas y software de la empresa – Gestión de recursos.

Se realizó validación con el área de centralización de la organización donde se preguntó por las ultimas persona que se retiraron de ella, con este dato se obtuvieron el nombre de 3 personas.

Tabla 4.
Tabla de usuarios.

Funcionario	**Usuario**
Jaime Alejandro Romero Perez	jromerop
Maria Espitia Salazar	mespitias
Lucero Velandia Flores	lvelandiaf

Nota. Autoría propia, 2020.

La validación se realizó de la siguiente manera:

- Se solicitó a los integrantes del área ingreso a los equipos con su usuario respectivo entregado por el área de TI.

- Se evidenció que un funcionario nuevo que aún no tenía usuario asignado estaba trabajando con el usuario lvelandiaf
- Varios usuarios del área trabajaban con el usuario mespitias ya que era el único usuario que tenía ingreso a la aplicación de cash4u.
- El único usuario inactivo era el de jromerop ya que se intentó acceder con el usuario y clave e indicaba que la cuenta estaba deshabilitada.

Con esta validación se identificó que un área que está compuesta de 12 personas, 1 de ellas estaba usando un usuario que ya se había retirado de la organización para capacitarse y ejercer laborales a nombre de esa persona, 5 usaban el usuario de mespitia para el uso de la aplicación de cash4u para solicitudes con proveedores, justificando que ninguno de ellos tenía permisos para el uso de esta aplicación en el momento.

Estos 2 usuarios que usaban en esta área tenían los siguientes permisos.

- Uso de y licenciamiento de office 365
- Acceso a unidades compartidas
- Uso de correo
- Ingreso a aplicativos como cash4u, AWS, Filezilla entre otros

Se sugiere al área de TI elaborar el proceso de altas y bajas de usuario donde se debe establecer a cada jefe de área como responsable de informar a RRHH y TI el momento es que un colaborador de la organización se retire o ingrese al área, esto para deshabilitar todos los aplicativos en los que un colaborador tenga autorización de uso, o dar los permisos respectivos a aquellas persona que ingresen a las áreas para el uso de las herramientas informáticas para el desarrollo de sus actividades laborales.

RSI-013.

Robo de equipos de cómputo o dispositivos de almacenamiento a los ingenieros de desarrollo-Mantenimiento de producto.

Se evidencio que el mes de enero del presente año ocurrió un robo fuera de las instalaciones del data center a un ingeniero de desarrollo de la organización siendo hurtado el computador personal del ingeniero el cual se utilizaban para procesos de la compañía tales como soporte informático a demás integrantes y a proveedores de la organización así mismo este computador contenía una

carpeta encriptada acerca de los accesos remotos que disponía el ingeniero al data center y a diferentes equipos de la organización.

Cuando se le pregunto a la persona encargada de la gestión de los activos se evidencio que esta persona no tenia conocimiento de la informacion que poseía este equipo la cual es importante para la organización y que por esta razón no se había realizado un proceso interno ya que solo se puso la demanda ante las autoridades competentes por parte del afectado.

Por lo anterior se le recomiendo al área IT y administrativa lo siguiente.

- Se recomienda realizar respaldos de la informacion de los equipos personales de los ingenieros
- Respaldo de la Información en plataformas corporativas en la nube
- Realizar un inventario de los equipos personales de los ingenieros que se vean involucrados en los procesos de la organización y administrarlos como si fueran un activo del data center.
- Poseer un plan de contingencia ante estos incidentes fuera de las instalaciones.

RSI – 018.

Indisponibilidad del área Administrativa del data center – Soporte.

Se identifica que el área administrativa del data center consta de 5 equipos de cómputo, una impresora y están ubicados dos pisos arriba del mismo, en ella se cuenta con 3 persona quienes son las encargadas de registrar el ingreso del personal autorizado, gestión de insumos, documentación de mantenimientos y limpieza del data center donde se percibió que esta área se encuentra descuidada por la organización, pues se evidencia que su equipos de cómputo son marca HP con más de 8 años de uso y sin periodo de garantía vigente, su sistema operativo aún se encuentra en Windows 7 y están conectados a la energía directa, pues en esta área no hay tomas eléctricas reguladas.

Por lo anterior se recomienda a compras, TI y oficial de seguridad lo siguiente:

Realizar cambio de los equipos pues la mayoría de los equipos con los que cuenta la organización son marca Lenovo, ya que en cualquier momento los equipos que están actualmente pueden presentar fallas en hardware o en su sistema operativo, al realizar el cambio de equipo de ser posible nuevos de una vez se actualizaría el sistema operativo, el cual esta soportado por el fabricante y actualizado a posibles amenazas existentes en la red.

Adecuar energía regulada en esta área y que esté conectada a la UPS pues en caso de que se presenta corte de energía se pueda garantizar continuidad en labores.

Con estas recomendaciones se reduce el riesgo identificado referente a la indisponibilidad del área administrativa del data center.

RSI-021.

Pérdida de la disponibilidad y confidencialidad de la información de la unidad de calidad contenida en puestos de trabajo y/o archivos de gestión de la unidad de calidad.

Se identifico que los usuarios pueden realizar impresiones de documentos directamente sin inconveniente alguno, es decir cuando los usuarios en las estaciones envían documentos que están digitalizados a la impresora esta no tiene restricción alguna en ejecutar la labor, de igual manera se evidencio que en varias áreas dejan impresiones realizadas en la bandeja de impresión o cerca a la impresora, pues cuando hay un volumen alto de impresión los usuarios deben seleccionar entre toda la documentación impresa los documentos de su necesidad, donde pueden leer la documentación que está actualmente en el papel de otras terminales o áreas.

La validación se realizó de la siguiente manera:

- Se solicito a 5 usuarios que enviaran documentos a imprimir
- Cada usuario fue a la impresora a buscar el documento que habían enviado a imprimir
- Uno de los usuarios dentro de sus documentos trajo una hoja de otro usuario sin querer, pues las hojas estaban pegadas y no se percató en ello.
- En la bandeja de impresión aun así quedaron dos hojas que no se sabía quién las había enviado a imprimir

Evaluado esto, se le sugiere al área de TI ponerse en contacto con el proveedor de impresoras, pues estas están en arriendo y se evalué la forma en que cada funcionario tenga un usuario y contraseña para el uso de la impresora y así se pueda tener un control en el envío de impresiones.

Por lo que con esta propuesta en las áreas cada funcionario dentro de la matriz de acceso se le asignará un usuario de impresión y una clave, así cuando el funcionario requiera imprimir tendrá que realizar el siguiente procedimiento:

- Enviar la impresión desde su equipo de cómputo a la impresora
- Dirigirse a la impresora
- Digitar su usuario y contraseña entregado por el área de TI para liberar la cola de impresión.

- Recoger su impresión y disponer de ella a su necesidad.

Con esta sugerencia se mitiga el riesgo de documentación disponible en las impresoras y que cualquier otro funcionario tenga acceso a información que no es de su interés, o que este en ella por olvido de funcionarios cuando culminan sus jornadas laborales o los dejan por olvido en la bandeja de impresión.

RSI – 026.

Fuga o perdida de la información crítica del proceso de Implementación (carpeta de clientes), contenida en los equipos portátiles de los colaboradores de la Unidad de los miembros de la compañía del data center – Implementación

Los funcionarios que tienen equipo portátil asignado son aquellos que realizan visitas a clientes, trabajo en caso o miembros de la dirección y alta gerencia, donde se simulo que un equipo de estos se hubiera perdido, así se logra acceder a la información del mismo por medio de Hirens identificando que la información esta disponible para las personas que encuentren o roben el activo, por lo que se validó esta misma función en los dos modelos de equipos portátil que tienen en sus inventarios que son el Lenovo L440 y X1 carbón, con el mismo resultado.

Cuando se bootea una USB con hirens en estos equipos portátiles se puede tener acceso a la información, disco duro, y hasta modificar la clave de ingreso a administrador local y usuario de dominio.

Realizada esta actividad se sugiere al área de seguridad y TI dividir el disco duro de los portátiles, donde en la unidad C: se aloje únicamente el sistema operativo y en la unidad D: los perfiles de los usuarios de dominio echo esto, validar con el proveedor de antivirus la posibilidad de cifrar la unidad D: únicamente ya que por temas de rendimiento en las estaciones el cifrar C: generaría lentitud en el uso del equipo, de no ser esto posible evaluar si los equipos están en sistema operativo Windows 10 hacer uso de bitlocker que es una herramienta de cifrado nativo del sistema operativo, y adicional a ello establecer una clave de booteo en estos equipos para así dificultar la posibilidad de bootear unidades de almacenamiento en estos equipos.

RSI – 055.

Uso indebido de la información sensible como información solicitada por los proveedores para pruebas-Innovación.

Verificando uno de los procesos que tiene la entidad con la fábrica de software, se evidenció que cuando el proveedor requiere información importante del negocio esta es enviada por medio

de correo electrónico como archivo adjunto al destinatario, puntualmente la fábrica solicitó el envío de unas tablas de transacciones realizadas en una fecha específica de clientes jurídicos a los que la organización le presta sus servicios, allí el coordinador de software realizó la consulta en la base de datos, la comprimió y se la envió a fábrica sin problema alguno acorde solicitud del proveedor.

Teniendo evidencia de lo anterior se recomienda al oficial de seguridad de la información establecer una política en la cual este tipo de solicitudes donde hay información sensible contenida, pase por autorización de seguridad y no sea enviada por correo electrónico como actualmente se está realizando, para ello se puede establecer una conexión a un sitio SFTPS donde tanto proveedor como organización realicen la alimentación necesaria al sitio con la información requerida para el desarrollo de software requerido.

Con esta recomendación se suple la falencia encontrada referente al envío de información sensible por parte del coordinador de software a la fábrica de software que desarrolla para la organización, dejando la responsabilidad de autorización de envío de información solicitada a seguridad, y a TI la creación del sitio SFTPS para la socialización de documentación.

RSI – 059.

Difusión de software malicioso en el proceso de mercadeo en la red corporativa- ventas.

Se identifico que esta área la directora comercial al tener su equipo portátil y realizar visita a proveedores y clientes, constantemente hace uso de medios de almacenamiento extraíbles personales y corporativos, indagando expresa que hace uso de esto ya que los clientes y proveedores le pasan información para el ella o su equipo de trabajo, información que pasa a los equipos de su personal a cargo de la misma manera, por medio de USB o disco duro extraíble.

Por lo que se le sugiere al área de TI y seguridad establecer como política de información el bloqueo de puertos usb en los equipos por medio del antivirus o política de dominio, de igual manera si un funcionario requiera los puestos habilitados para el desempeño de sus funciones laborales, deberá contar con autoriza por parte de seguridad y estar registrado en matriz de acceso para llevar control y monitoreo del personal autorizado y los equipos que serán exentos de esta política.

De igual manera se recomienda que por política de dominio los usuarios estándar no puedan realizar instalación de software en las terminales, pues los únicos que puedan realizar esto sean colaboradores del área de TI, usuario local administrador o funcionarios que por matriz de acceso requieran de este permiso para la ejecución de software o macros.

Por lo anterior se reduce el riesgo con la recomendación dada ya que actualmente hay funcionarios que están haciendo uso de los puestos usb para intercambio de información, cargar el celular, conexión de periféricos no autorizados (ventiladores portátiles), e instalación de software siendo usuarios normales en directorio activo.

Desarrollo Objetivo N 4

Cuando los bienes informáticos que necesitan custodia son reconocidos y valorados según su criticidad se necesita detectar las amenazas sobre éstos y estimar el mal (impacto) que puede ocasionar su materialización. Para cada bien informático a defender las metas primordiales de estabilidad son la confidencialidad, la integridad y la disponibilidad, por lo cual se debe establecer cada amenaza sobre la base de como logre influir a estas propiedades de la información. El peso que todas estas propiedades tiene para los bienes informáticos cambia de una entidad a otra, en dependencia de la naturaleza de los procesos informáticos que se conducen a cabo en funcionalidad de su objeto social.

Varias de las amenazas más frecuentes son las que se muestran a continuación:

1) Pérdida de información.
2) Corrupción o modificación de información.
3) Sustracción, alteración o pérdida de equipos o componentes.
4) Divulgación de información.
5) Divulgación de información.
6) Interrupción de servicios.

Una amenaza puede incidir sobre diversos bienes informáticos con la misma posibilidad y no obstante sus secuelas no precisamente van a ser equivalentes, dependiendo en cada caso del valor del bien en cuestión. La interrelación entre la posibilidad de materialización de las amenazas que trabajan sobre un bien informático y la importancia para el mismo, determinando el peso del peligro.

Una vez se cuentan con los resultados logrados de las fases anteriores se debería hacer el desempeño del peligro enfocado a las ocupaciones a tomar, a conceptualizar, a mantener o mejorar los controles implementados con relación a los peligros. Así mismo, se necesita implantar los causantes de las ocupaciones y disponer de mecanismos de supervisión y monitoreo, para una correcta administración de dichos peligros con base a la valoración elaborada.

En las actividades de procedimiento del riesgo que debería contemplar la organización permanecen:

- Eludir el peligro: Tiene relación con evadir la actividad o la acción que da origen al peligro especial, es aplicable una vez que los peligros determinados son elevados, o si los precios para tratarlos.

- Admitir o incrementar el peligro: Admitir que no hay controles u ocupaciones de
- procedimientos conocidos, lo cual se convierte en un peligro residual, haciendo primordial la preparación de planes de contingencia para su funcionamiento.
- Remover la fuente de peligro: tomar las medidas encaminadas a prevenir su materialización.
- Cambiar la posibilidad
- Cambiar las secuelas
- Compartir el peligro: Mover, parcial o plenamente, las secuelas del peligro por medio de la tercerización.
- Retener el peligro (decisión informada): Si el grado del peligro sacia los criterios para su asentimiento, no se necesita llevar a cabo controles extras.

Las selecciones de las posibilidades para el procedimiento de los peligros tienen que desarrollarse de consenso con las metas de la organización, los criterios del peligro y los recursos accesibles, por lo cual es fundamental disponer de la colaboración de cada una de las piezas interesadas externas e internas en la toma de elecciones y en la preparación del proyecto de funcionamiento de peligros.

A continuación, se evidencia el primer riesgo de la matriz realizada para el data center para la correcta visualización de la totalidad los riesgos dirigirse a los anexos de la investigación.

IDENTIFICACIÓN DE RIESGOS						
RIESGO	DESCRIPCION DEL RIESGO	PROCESO	TIPO DE RIESGO	FUENTE (INTERNA Y/O EXTERNA)	POSIBLES CAUSAS DE MATERIALIZACION DEL RIESGO	CONSECUENCIA DEL RIESGO
RSI-001	Perdida de la disponibilidad y confidencialidad de la información almacenada en los servicios de almacenamiento exponiedo informacion confidencialidad de los diferentes clientes.	Gestión de Recursos	Seguridad de la información	Interna/ Externa	1. No verificación periódica de permisos y niveles de acceso por parte de los administradores de activos de información 2. Ausencia de lineamientos y sensibilización en el manejo de la información clasificada como secreta o confidencial	1. Fuga o perdida de información critica del proceso. 2. Afectación a terceros por la no confidencialidad de la información. 3. Pérdida financiera por acciones legales.

Figura 32 Riesgo N1 de la matriz parte 1. Autoría propia (2020)

EVALUACIÓN DE CONTROLES A IMPLEMENTAR		
DESCRIPCION DE CONTROLES A IMPLEMENTAR	**TIPO DE CONTROL (PREVENTIVO O DETECTIVO Y CORRECTIVO)**	**RESPONSABLE**
Respaldo de la Información en diferentes servidores de almacenamiento de informacion	Preventivo	Área IT
Control de acceso por usuario de dominio	Preventivo	Área IT
Realizar el proceso de Sincronización de respaldo de la informacion desde el datacenter con el cliente final	Preventivo	Talento Humano
Alta disponibilidad de la plataforma	Preventivo	Area IT

Figura 33 Riesgo N1 de la matriz parte 2. Autoría propia (2020)

EVALUACIÓN DEL RIESGO		
PROBABILIDAD	**IMPACTO**	**RESULTADO**
MEDIA	ALTO	IMPORTANTE

Figura 34 Riesgo N1 de la matriz parte 3. Autoría propia (2020)

TRATAMIENTO DEL RIESGO				
CRITICO	IMPORTANTE	MODERADO	BAJO	No. Acción (Ver reporte de acción)
	Mitigar 3M			1. AM01- Implementar buenas practicas de seguridad de la Información: (Politica de Activos de información, política especifica para usuario, Política de acceso lógico, Política de escritorio y pantalla limpia, política para transferencia de información) 2. AM02 - Implementar programa de sensibilización y capacitación a los implicados en la administracion de la informacion. 3. AM03 - Gestionar Matriz de Inventario de activos de información: 4. AM04 - Documentar controles operacionales: (Instructivo de Gestión de eventos para el monitoreo de los logs de las plataformas de nube, Instructivo de Gestión de Backup, Instructivo registro, administración y cancelación del registro de usuarios y Instructivo de uso de los diferentes serviioc como Amazon servicies , IBM CLOUD ,Microsft servicie). 5. AMO6 Seguimiento y medición (Auditoria, medición de indicadores, cumplimiento de politicas y controles por los usuarios de los procesos).

Figura 35 Riesgo N1 de la matriz parte 4. Autoría propia (2020)

PLAN DE CONTINGENCIA (SOLO SI EL RIESGO SE MATERIALIZA)	RELACION A LOS CONTROLES DEL ANEXO A LA NORMA ISO 2700.2013
1. Reportar el evento al área de IT, solicitar el ultimo Backup de la información del cliente por parte del datacenter o proovedor del servicio. 2. Revisar la ultima sincronización con respecto a la documentación que reposa en la carpeta compartida.	Plan de Tratamiento SGSI - Controles ISO 27002 AM01: A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN AM02: A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información AM03: A.8 GESTIÓN DE ACTIVOS AM04: A.12.3 Copias de respaldo, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7 Gestión de Log; A.9.2, A.9.2.1, A.9.2.2, A.9.2.3, Instructivo gestión de usuarios; A.18.1.3 Instructivo de uso de OneDrive) AM06:# 8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL; #9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN; # 9.2 AUDITORÍA INTERNA; 12,7 Controles de auditorias de sistemas de información; 18.2 Revisiones de seguridad de la información AM09: A.9.2.5 Revisión de los derechos de acceso de usuarios; A.9.2.6 Retiro o ajuste de los derechos de acceso.

Figura 36 Riesgo N1 de la matriz parte 5 y 6. Autoría propia (2020)

Con la información recolectada y los peligros reconocidos anteriormente, para entablar la posibilidad de que ocurra el peligro, su efecto y/o secuelas, los peligros se califican y evalúan para establecer el grado y las actividades a tomar. Este estudio le posibilita a la entidad decidir la capacidad para el desempeño del peligro. Como consecuencia del análisis llevado a cabo se produce el mapa de calor del peligro inherente de los peligros del proceso de administración documental.

Si bien es cierto el grado del peligro al que está expuesto una entidad en cada uno de sus procesos no se puede eliminar por completo, si es fundamental buscar el equilibrio y las medidas para su procedimiento que impidan que dichos peligros se materialicen y generen eventos que perjudiquen el común desarrollo de los procesos y el cumplimiento de las metas institucionales.

Posterior a la elaboración de la matriz de riesgo para un data center acorde a la norma ISO 27001-2013, se estudiaron en conjunto los resultados arrojados en la misma con el fin de aportar a la organización una clara perspectiva sobre los hallazgos encontrados en el transcurso de la investigación, para esta manera establecer políticas enfocadas en el consolidado que se evidencian a continuación

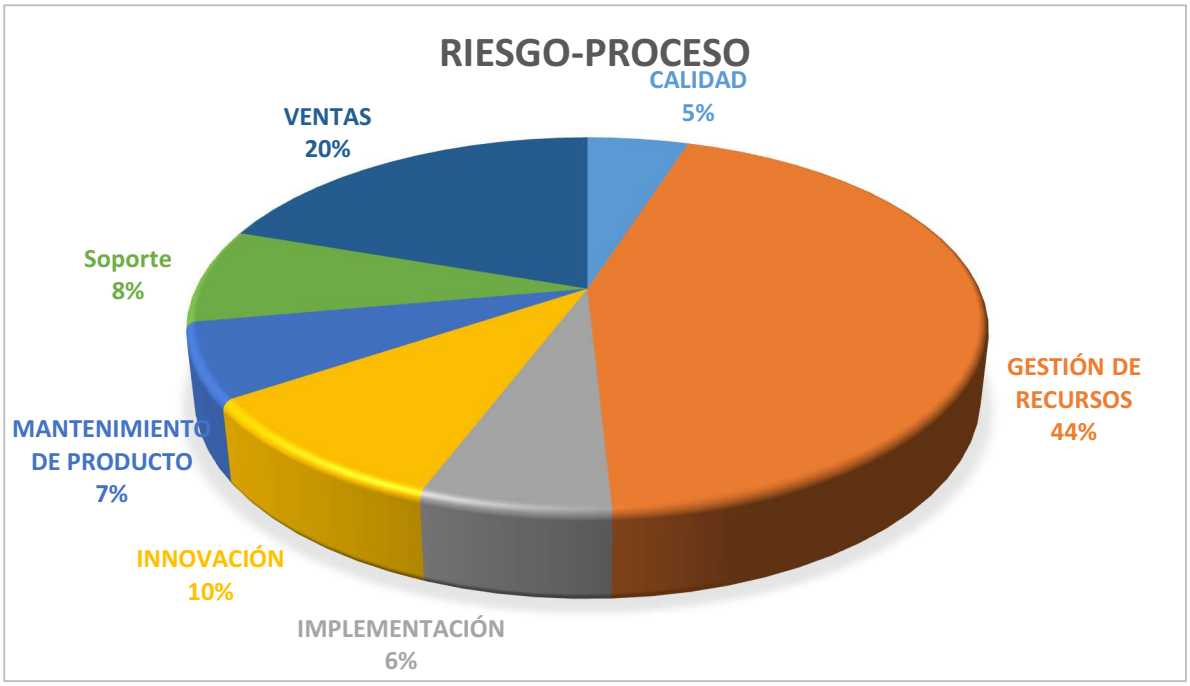
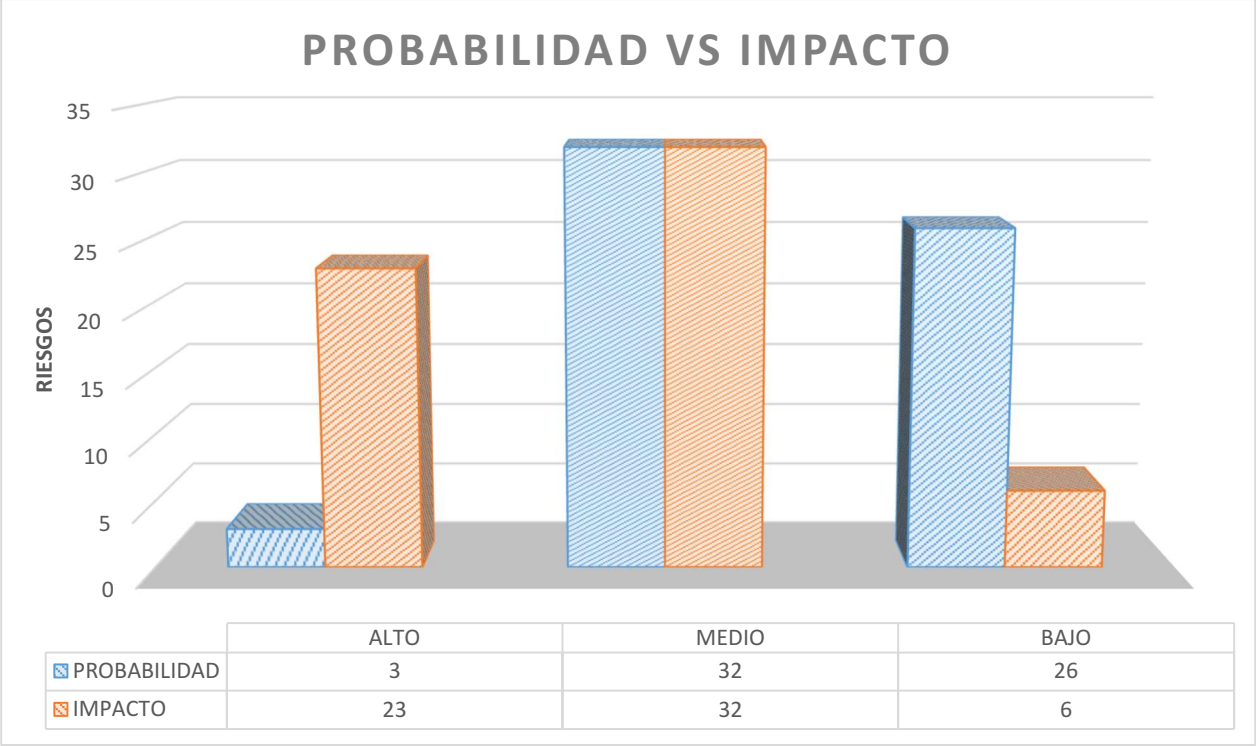


Figura 37 Grafico del riesgo vs proceso según los resultados de la matriz de riesgo. Autoría propia (2020)

En la figura 37 se evidencia que la gestión de recursos es el proceso en el cual se encuentra el mayor número de riesgos con un porcentaje de 44%.

Así mismo se evidencio que en el proceso de calidad se establecieron políticas adecuadas ya que represento el proceso con menor porcentaje en el cual se identificaron 3 riesgos.



	ALTO	MEDIO	BAJO
PROBABILIDAD	3	32	26
IMPACTO	23	32	6

Figura 38 Grafico de probabilidad vs riesgo según los resultados de la matriz. Autoría propia (2020)

En la figura 38 probabilidad vs impacto es posible realizar un comparativo entre estas dos variables. Se evidencio que del total de los 61 riesgos identificados ,32 arrojaron probabilidad e impacto medio lo que sitúa a la organización en un entorno medio de seguridad. De la misma manera se evidencia que la organización cuenta con una baja probabilidad de ocurrencia en la identificación de estos objetivos mientras que 23 riesgos pueden impactar negativamente al interior de la organización

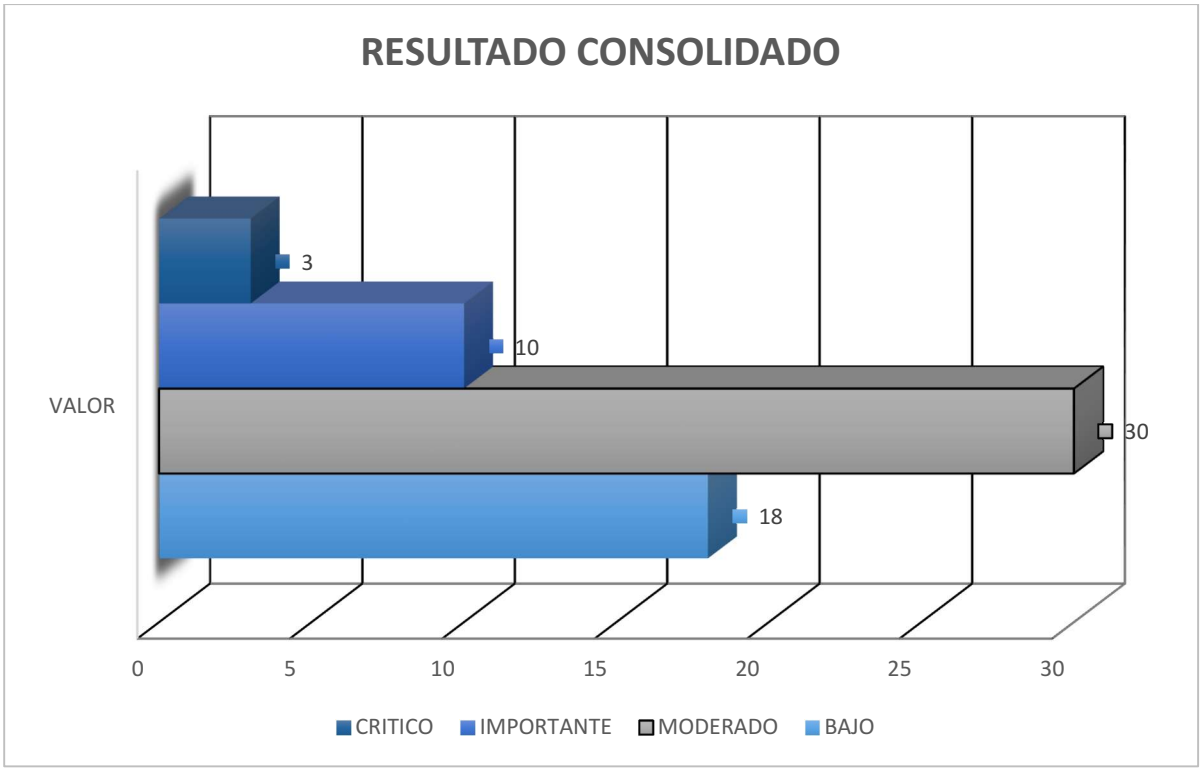


Figura 39 Resultado consolidado de la matriz de riesgo. Autoría propia (2020)

En la figura 39 de resultado consolidado es posible analizar el resultado de riesgos encontrados en la matriz de acuerdo a su clasificación; Critico, importante, moderado y bajo.

Dentro del resultado moderado se localizaron 30 riesgos representado el 49.18%.

3 riesgos evaluados se situaron en un resultado critico lo cual implica a la organización establecer políticas rigurosas, ya que este tipo de riesgos puede afectar significativamente el funcionamiento de la organización.

Es fundamental la colaboración de cada una de las piezas interesadas externas e internas de la entidad en la toma de elecciones para darles tratamiento a los peligros determinados y en la preparación del proyecto de funcionamiento de peligros que vaya de consenso con las metas de la entidad, los criterios del peligro y los recursos existentes. El funcionamiento de un estándar o buenas prácticas para asegurar la disponibilidad, totalidad y fiabilidad de la información en una entidad debería transformarse en una práctica indudable para reducir peligros

La gestión de la seguridad de la información va a ser implementada por medio del establecimiento de diversas barreras de custodia, seleccionando controles de diversos tipos de manera combinada y concéntrica, pudiendo con ello una cierta redundancia que garantice que, si una medida fracasa o resulta quebrantada, la siguiente medida entra en acción continuando la

defensa del activo o recurso. No es adecuado que el fallo de un solo mecanismo comprometa plenamente la estabilidad. La utilización de diversas medidas básicas puede en varios casos ser más seguro que el trabajo de una medida bastante sofisticada. Esto cobra más grande validez una vez que definida medida no podría ser aplicada por alguna limitación que existe, como tienen la posibilidad de ser, ejemplificando: las insuficiencias del equipamiento, que impiden la utilización de una medida técnica. En esta situación van a ser consideradas medidas o métodos complementarios de otro tipo que garanticen un grado de estabilidad correcto.

Conclusiones

En la actualidad, la información se ha convertido en parte fundamental de los data center en Colombia, por lo cual se han visto en la obligación de adoptar dentro de sus políticas un conjunto de medidas preventivas y reactivas bajo los estándares de la norma ISO 27001, las cuales permitan mitigar los riesgos a los que está expuesta la seguridad de la información. Bajo este concepto y como resultado de la presente investigación es posible concluir:

- Se identifico la parte teórica de la norma ISO 27001-2013, a través del estudio de su estructura, fases, características y fundamento, destacando sus cláusulas A.5 políticas de la información y A.6 organización de la seguridad de la información.
- Se analizo de manera satisfactoria los servicios y la infraestructura lógica y física de un data center en Colombia teniendo en cuenta directrices del estándar Tier Standard Uptime Institute el cual es reconocido globalmente por su confiabilidad y el desempeño general de los centros de datos.
- Con la realización de la matriz de riesgo, fue posible analizar 61 riesgos en una escala de: bajo, moderado, importante. Adicional, se sugirieron planes de contingencia para el data center si este riesgo se llegara a materializar en cualquier momento, bajo los parámetros de la norma ISO 27001 – 2013 en todo el proceso de la realización de la matriz de riesgo.
- Frente a la evidencia recaudada por la matriz de riesgos se propusieron estrategias capaces de mitigar desde un riesgo mínimo a uno complejo para la seguridad de la información del data center en Colombia.
- Se consolidaron los resultados de la matriz de riesgos a través de la elaboración de tres graficas en las cuales se logró analizar los datos identificados para el data center.

En conclusión, se integraron los conceptos de la norma ISO 27001-2013 con la infraestructura de un data center en Colombia para la creación de una matriz de riesgo dando la oportunidad que este documento ayude a todas la personas u organizaciones interesadas en adoptar medidas de seguridad de la información.

Referencias

101, D. (2021). *Datos 101*. Obtenido de https://www.datos101.com/blog/que-es-un-data-center/

27005, I. (2018).

360, D. (2021). Obtenido de https://datacenter360.net/switches-de-red/switches-cisco-catalyst/?gclid=EAIaIQobChMI4r38obuz8AIVhbzICh3K4gVEEAAYASAAEgJor_

Adobe. (2021). Obtenido de https://vilmanunez.com/webinar-gratis-online-con-gotowebinar/#:~:text=GoToWebinar%20es%20una%20de%20las,solo%20siguiendo%20unos%20pocos%20pasos

akami. (2016). LA BOTNET MIRAI. 2.

Alegsa, L. (2016). *Alegsa.com.ar*. Obtenido de http://www.alegsa.com.ar/Dic/red_de_telecomunicaciones.php

Antevenio. (2015). *Antevenio* . Obtenido de https://vilmanunez.com/webinar-gratis-online-con-gotowebinar/#:~:text=GoToWebinar%20es%20una%20de%20las,solo%20siguiendo%20unos%20pocos%20pasos

APC. (2021). *APC*. Obtenido de https://www.apc.com/shop/pa/es/products/Rack-PDU-2G-con-display-ZeroU-20-A-208-V-16-A-230-V-18-C13-2-C19/P-AP8858

APC. (2021). *Bechtle*. Obtenido de https://www.bechtle.com/be-es/shop/rack-apc-netshelter-sx-42u-750x1070-net--610707--p

Arias, F. G. (2016). *Otras voces en educacion* . Obtenido de http://otrasvoceseneducacion.org/archivos/77516

Aruba. (2021). *Aruba* . Obtenido de https://cdn.cnetcontent.com/syndication/feeds/hp-ent/inline-content/35/E/C/ECD8C61D5B6E1FBF72DA747D9B9D9A8797470D08_source.

Aruba. (2021). *Aruba networks* . Obtenido de https://www.arubanetworks.com/es/productos/switches/nucleo-y-centro-de-datos/

avast. (2020). *Avast*. Obtenido de https://www.avast.com/es-es/c-malware#:~:text=Malware%20es%20un%20t%C3%A9rmino%20general,su%20dispositivo%20sin%20su%20conocimiento.

Barrios, D. Á. (2014). *Scielo* . Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-00632014000100014

Bezz, G. P. (2016). *Análisis de botnets y ataques de.*

BOE. (2002). *BOE.* Obtenido de https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf

Capterra. (2020.). Obtenido de https://www.capterra.co/software/140124/h2desk

castillero, O. (2020). *Psicologia y mente* . Obtenido de https://psicologiaymente.com/miscelanea/tipos-de-investigacion

colombia, C. d. (1999). *LEY 527 DE 1999.* Bogota.

colombia, C. d. (2009). *MINCTIC.* Obtenido de https://mintic.gov.co/portal/604/articles-8580_PDF_Ley_1341.pdf

colombia, C. d. (2012). *Decreto 2693 de 2012.* Bogota.

Colombia, E. (2013). *MINTIC.* Obtenido de https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

CONSULTING, S. (2018). *SCS CONSULTING*. Obtenido de https://www.scsconsulting.es/seguridad-de-la-informacion/#:~:text=En%20el%20contexto%20aqu%C3%AD%20tratado,electr%C3%B3nicamente%2C%20proyectada%2C%20enviada%20por%20correo

Csico. (2021). *Cisco*. Obtenido de https://www.cisco.com/c/en/us/products/switches/campus-lan-switches-core-distribution/index

DBMG. (2021). *DBMG*. Obtenido de http://www.dbmg.cl/pro.php?id=3025

Díaz, M. R. (2020). *Scielo* . Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=es&nrm=iso&tlng=es

Ecured. (2021). *Ecured*. Obtenido de https://www.ecured.cu/Patch_Cord

educacion, M. d. (2013). *Subdirección de Desarrollo*. Obtenido de https://www.mineducacion.gov.co/1759/articles-327021_archivo_pdf_Dia2_1_Gestion_Riesgo.pdf

ESPINOSA, C. A. (2017). Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/7933/1/04%20RED%20185%20TRABAJO%20DE%20GRADO.pdf

Fortinet. (2021). *Fortinet* . Obtenido de https://www.fortinet.com/lat/products/next-generation-firewall/entry-level

Gobierno. (2021). *Gobierno de españa* . Obtenido de http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/isoirc_27001_pdca.html

Goujon, A. (2012). *Welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

Grup, I. (2020). *ID GRUP*. Obtenido de https://idgrup.com/firewall-que-es-y-como-funciona/#:~:text=Un%20firewall%2C%20tambi%C3%A9n%20llamado%20cortafuegos,ordenadores%20de%20una%20misma%20red.

Host. (2020). *HostDime* . Obtenido de https://www.comparahosting.com.co/?gclid=CjwKCAjwj8eJBhA5EiwAg3z0m4u-tkC-bfR9p1bUFglpiDG7lKr6-tui_djscEsfVzaKROfhOr-NIBoCJnMQAvD_BwE

Howard. (2020). *Fs comunidad*. Obtenido de https://community.fs.com/es/blog/how-to-choose-the-right-core-switch.html

IBM. (2021). *IBM*. Obtenido de Ibm.com

INCONTEC. (2013). *Norma Técnica NTC-ISO-IEC 27001.*

Informáticas, U. d. (2018). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Scielo*, 1.

International, F. S. (2020). IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. *Forensic Science International*, 1.

ISO. (2009). *ISO.* Obtenido de https://www.iso.org/standard/50341.html

ISO, N. (2013). *27001-2013.*

Izquierdo, F. (2019). *Repositorio institucional cud*. Obtenido de http://calderon.cud.uvigo.es/handle/123456789/318

kaspersky. (2017). *kaspersky*. Obtenido de https://latam.kaspersky.com/resource-center/threats/ddos-attacks

Lagorio, F. (2016). *Tecnologia Digital* . Obtenido de https://sites.google.com/site/tecnologiadigital20/home/riesgos-informaticos

manuez, v. (2018). Obtenido de https://vilmanunez.com/webinar-gratis-online-con-gotowebinar/#:~:text=GoToWebinar%20es%20una%20de%20las,solo%20siguiendo%20unos%20pocos%20pasos

Marsh. (2020). *MARSH*. Obtenido de https://www.marsh.com/co/insights/research/marsh-microsoft-encuesta-percepcion-riesgo-cibernetico-2019.html

Mendoza, M. Á. (2014). Obtenido de https://www.welivesecurity.com/la-es/2014/09/29/8-pasos-evaluacion-de-riesgos-1/

Merayo, P. (s.f.). *Maxima formacion*.

Microsoft. (2020). Obtenido de https://azure.microsoft.com/es-es/overview/what-is-azure/?ef_id=EAIaIQobChMIkMaFm_G98AIVgf7jBx3GnAyQEAAYASABEgJPzPD_BwE%3AG%3As&OCID=AID2100025_SEM_EAIaIQobChMIkMaFm_G98AIVgf7jBx3GnAyQEAAYASABEgJPzPD_BwE%3AG%3As&gclid=EAIaIQobChMIkMaFm_G98AIVgf7jBx3GnAyQE

Microsoft. (2020). Obtenido de https://support.microsoft.com/es-es/office/%C2%BFqu%C3%A9-es-onedrive-profesional-o-educativo-187f90af-056f-47c0-9656-

cc0ddca7fdc2#:~:text=OneDrive%20es%20el%20servicio%20en,lugar%20en%20todos%20tus%20dispositivos

Microsoft. (2019). Obtenido de https://support.microsoft.com/es-es/office/%C2%BFqu%C3%A9-es-sharepoint-97b915e6-651b-43b2-827d-fb25777f446f

MINTIC. (2016). *MinTic*. Obtenido de https://www.mintic.gov.co

Networks, K. (2019). *Kio*. Obtenido de https://www.kionetworks.com/blog/data-center/qu%C3%A9-es-un-data-center

(2006). *NORMA TÉCNICA NTC-ISO/IEC.* Bogota. Obtenido de https://www.normas-iso.com/iso-27001/

novoa, M. (2013). *Slide share*. Obtenido de https://es.slideshare.net/lorenatroncoso/servidores-5912221

PandaSecurity. (2020). *PandaSecurity*. Obtenido de https://www.pandasecurity.com/es/mediacenter/empresas/botnet-mirai-nueva-vulnerabilidad/

Panduit. (2021). *Panduit*. Obtenido de http://www1.panduit.com/es/products-and-services/products/gabinetes-administracion-de-temperatura-racks-y-armazones/gabinetes/gabinetes-de-red

Panduit. (2021). *Panduit* . Obtenido de http://www1.panduit.com/es/product/UTP6ASD5MBU

Pareja, D. (2020). *pirani* . Obtenido de https://www.piranirisk.com/es/blog/seguridad-informatica-uno-de-los-peores-riesgos-del-mundo

Polo, R. (2017). *GTI*. Obtenido de http://noticias.gti.es/fabricantes/que-es-una-pdu-y-para-que-sirve/

publica, F. (2021). *Funcion publica colombia* . Obtenido de Funcion publica

Rimac. (2021). *Rimac*. Obtenido de http://www.prevencionlaboralrimac.com/Herramientas/Matriz-riesgo

salazar, A. s. (2014). *Aspectos Contractuales de Cloud Computing.* Obtenido de http://ciiddi.org/congreso2014/images/documentos/aspectos%20contractuales%20de%20cloud%20computing%20zalazar.pdf

Salesforce. (2020). *Cloud Computing - Aplicaciones en un solo tacto.*

Sánchez, F. (2020). *blog smartekh*. Obtenido de https://blog.smartekh.com/4-de-las-principales-problematicas-y-riesgos-en-los-data-center

santander, U. i. (2016). *Unidad industrial de santander* . Obtenido de https://www.uis.edu.co/intranet/calidad/documentos/SEGUIMIENTO_INSTITUCIONAL/manuales/MSE.01.pdf

SARLAFT, R. (2021). *RIESGO SARLAFT*. Obtenido de http://riesgosarlaft2012-ii.blogspot.com/p/medicion-de-impacto-y-de-probabilidad.html

school, S. b. (2020). *Select business*. Obtenido de https://escuelaselect.com/siete-tipos-riesgos-laborales/

Seagate. (2021). *Seagate*. Obtenido de https://www.seagate.com/la/es/tech-insights/what-is-nas-master-ti/

services, K. (2021). *kiote*. Obtenido de https://kioteservices.com/cloud-computing

servicies, A. (2021). *Amazon*. Obtenido de https://aws.amazon.com/es/types-of-cloud-computing/

SoftwareLab.org. (2017). Obtenido de SoftwareLab.org: https://softwarelab.org/es/que-es-wifi-que-significa-y-para-que-sirve/

STATION, R. (2021). Obtenido de https://support.microsoft.com/es-es/office/%C2%BFqu%C3%A9-es-onedrive-profesional-o-educativo-187f90af-056f-47c0-9656-cc0ddca7fdc2#:~:text=OneDrive%20es%20el%20servicio%20en,lugar%20en%20todos%20tus%20dispositivos

Tectel. (2015). *Tectel*. Obtenido de http://www.tecnologiatelefonica.com/que-es-un-rack-y-para-que-se-usa

TIC, G. (2021). *Guia TIC*. Obtenido de https://guiatic.com/co/393-soluciones-para-el-mejoramiento-continuo-en-las-instituciones-educativas/363-kawak-administracion-del-sistema-de-gestion-de-calidad-y-el-mejoramiento-continuo-en-instituciones-academicas-documentacion-pl

TIC, G. (2021). *Guia TIC* . Obtenido de https://guiatic.com/co/24-software-contable/1313-novasoft-administrativo-y-financiero-niif-contabilidad-tesoreria-cuentas-por-pagar-cuentas-por-cobrar

Tiempo, E. (2020). Banca móvil e internet, canales más usados hoy por colombianos. *Tiempo*, 1.

tools, I. (2017). *ISO TOOLS*. Obtenido de https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/

VÁSQUEZ, F. (2018). Obtenido de https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/8436/Vasquez_ej.pdf?sequence=1&isAllowed=y

William. (2021). Obtenido de https://upcommons.upc.edu/bitstream/handle/2099.1/18520/ANEXO%20I.William%20T.Fine.PDF?sequence=3&isAllowed=y#:~:text=%E2%9E%A2%20Consecuencias%3A%20Se%20definen%20como,presenta%20la%20situaci%C3%B3n%20de%20riesgo.

Zone, R. (2020). *sergio de luz*. Obtenido de https://www.redeszone.net/mejores/switches/

Anexo 1

Certificación donde consta que la matriz de riesgo consolidada, se encuentra alineada con la infraestructura física y lógica de un data center en Colombia emitida, por un ingeniero especializado en la creación e implementación de data centers en Latinoamérica.

Señores

UNIVERSIDAD AGUSTINIANA

Ciudad

ASUNTO: REVISIÓN PROYECTO DE GRADO "ANALIZAR LOS RIESGOS Y VULNERABILIDADES DE UN DATA CENTER EN COLOMBIA PARA CREAR UNA MATRIZ DE RIESGO ACORDE A LO ESTABLECIDO EN LA NORMA ISO 27001:2013"

Respetados señores:

Mi nombre es **SAÚL PEÑALOZA GARZÓN**, identificado con Cédula de Ciudadanía No. 79.878.126 de Bogotá, Ingeniero Electricista con M.P # CN205-44267, especialista en Telecomunicaciones Móviles, diseñador certificado de Data Centers, siendo Accredited Tier Designer (ATD®) del UPTIME INSTITUTE® y Certified Computer Room Designer (CCRD®) de ICREA (International Computer Room Expert Association), con veinte (20) años de experiencia profesional, habiendo gerenciado e implementado proyectos en varios Data Centers en Latinoamérica, de compañías tales como LUMEN® (anteriormente denominada IMPSAT®, GLOBAL CROSSING® y LEVEL 3®) e IBM®. Actualmente Gerente de Ingeniería y Proyectos en ENERGY DATA INGENIERÍA SAS.

Me he permitido realizar revisión del Proyecto de Grado en referencia desarrollado por parte de los estudiantes **ESTEBAN CAMILO ORJUELA SUPELANO** y **CAMILO ANDRÉS ÑUSTES BERMÚDEZ** y encuentro que los riesgos claramente descritos en la Matriz Consolidada de Riesgos para el Data Center en Colombia aplican perfectamente para este tipo de instalaciones, por lo cual considero

Figura 40 Certificación numero 1 Hoja 1. Autoría propia (2021)

que el proyecto es totalmente viable y que al ser implementado claramente redundaría en un ostensible beneficio en la mejora de la seguridad de la información sensible que se administra y procesa dentro de un Data Center y que es clave para su correcta operación.

Cordialmente,

19/05/2021

I.E. SAÚL PEÑALOZA GARZÓN, ATD, CCRD

C.C. 79.878.126 de Bogotá

M.P. CN205-44267

E-mail: ingenieria@energydataing.com

Cel. +57-318-4321055

Figura 41 Certificación numero 1 hoja 2. Autoría propia (2021)

Anexo 2

Certificación donde consta que la matriz de riesgo consolidada, se encuentra alineada con la infraestructura física y lógica de un data center en Colombia emitida, por un ingeniero de telecomunicaciones inscrito al consejo profesional de ingenierías eléctricas.

Yo EDWIN GERARDO [redacted] identificado con CC [redacted], en mi calidad de Ingeniero en Telecomunicaciones con 6 años de experiencia en Sistemas de comunicaciones, tecnología empresarial y ejecución de proyectos de Datacenter a petición de los interesados.

CERTIFICO

Que el documento "MATRIZ CONSOLIDADA DE RIESOS PARA EL DATACENTER EN COLOMBIA" del trabajo de grado "Analizar los riesgos y vulnerabilidades de un data center en Colombia para crear una matriz de riesgo acorde lo establecido en la norma ISO 27001: 2013" de autoría de Esteban Camilo Orjuela Supelano y Camilo Andrés Ñustes Bermúdez de la Universitaria Agustiniana, se encuentra alineada con la infraestructura física y lógica de un data center en Colombia y en un largo plazo puede implementarse en una organización de telecomunicaciones con los debidos procesos legales y de confidencialidad requeridos para tal fin.

Lo anterior, a solicitud de los interesados.

Esta certificación se firma el 14 de mayo de 2021.

Atentamente,

[redacted]

NOMBRE: Edwin Gerardo [redacted]

C.C. [redacted]

MATRICULA PROFESIONAL No. [redacted]

Figura 42 Certificación numero 2. Autoría propia (2021)

Anexo 3

Concepto de aprobación del buen uso y dando da cumplimiento a los requisitos de la Norma ISO 27001:2013 en el componente de Gestión de Riesgos y enfocado al requisitos de Planificación por la empresa PGC Ltda. Planeación, Gestión y Control de la ciudad de Bogotá.

Concepto Trabajo de Grado
Preparado por: PGCC LTDA

CONCEPTO ALINEACION TRABAJO DE GRADO
SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACION
ISO 27001:2013

Preparado por: **PGCC LTDA** Fecha: **Mayo 20 de 2021**

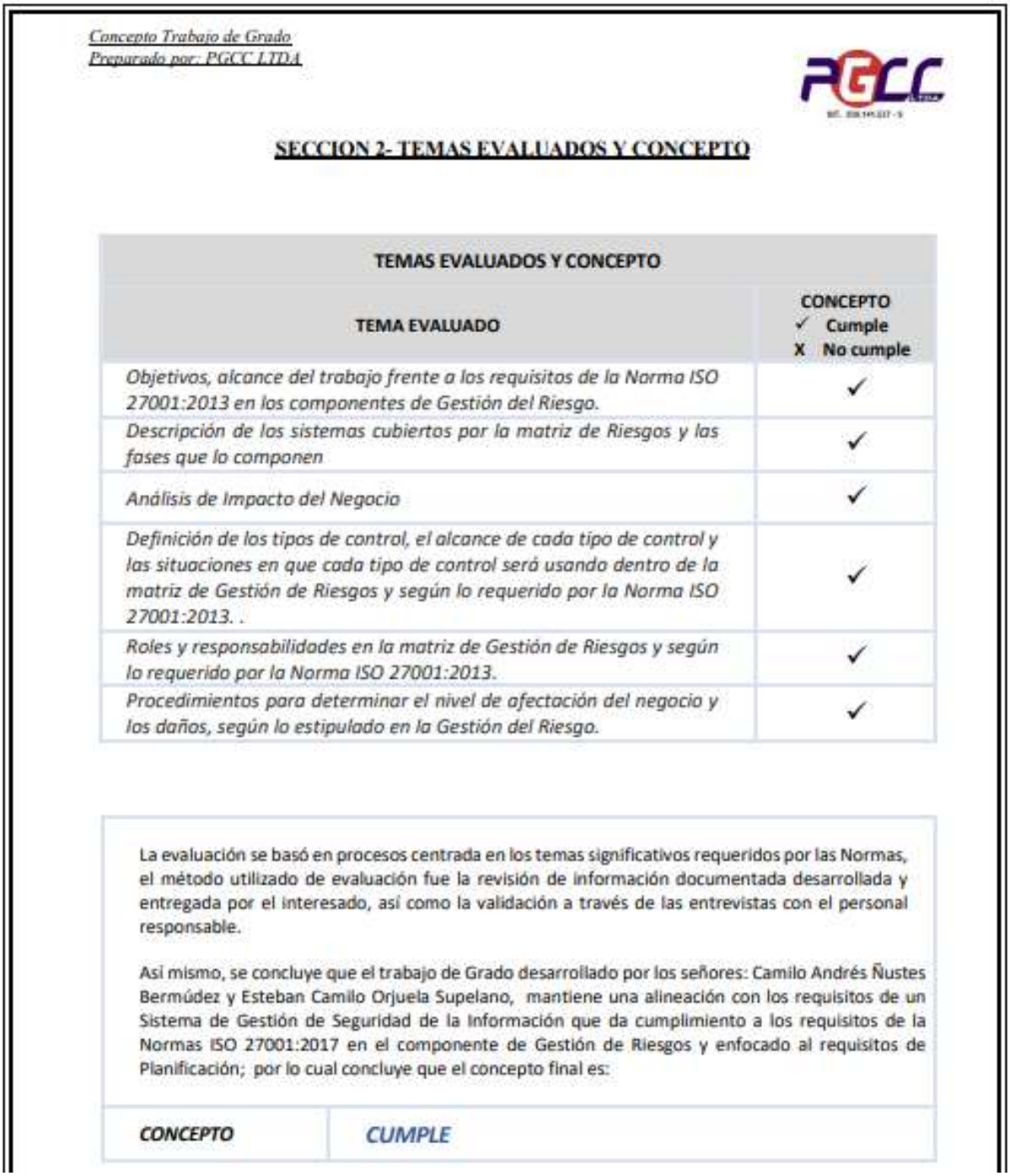
LISTA DE DISTRIBUCIÓN

Organización : UNIVERSIDAD AGUSTINIANA
Oficina PGCC LTDA : File – Conceptos

SECCION 1- PRESENTACION GENERAL DE LA ACTIVIDAD

NOMBRE DE LA ACTIVIDAD	*Revisión, evaluación y alineación del trabajo de Grado cuyo título es: "Analizar los riesgos y vulnerabilidades de un data center en Colombia para crear una matriz de riesgo acorde lo establecido en la norma ISO 27001: 2013"*
LUGAR	*Bogotá – Colombia*
OFICINA RESPONSABLE	*Gerencia de Procesos y Proyectos*
PERSONA CONTACTO DE LA ORGANIZACION	*Rafael Orjuela / Profesional Especializado*
EQUIPO ASIGNADO POR PGCC LTDA PARA LA EVALUACION	*Ing. Rafael Orjuela Viracachá / Evaluador Lider*
FECHA DE EVALUACIÓN	*17 y 18 de mayo de 2021*
FECHA DE ENTREGA DE CONCEPTO	*20 de mayo de 2021*

Figura 43 Concepto por la empresa PGCC Hoja 1. Autoría propia (2021)



Concepto Trabajo de Grado
Preparado por: PGCC LTDA

SECCION 2- TEMAS EVALUADOS Y CONCEPTO

TEMAS EVALUADOS Y CONCEPTO	
TEMA EVALUADO	**CONCEPTO** ✓ Cumple X No cumple
Objetivos, alcance del trabajo frente a los requisitos de la Norma ISO 27001:2013 en los componentes de Gestión del Riesgo.	✓
Descripción de los sistemas cubiertos por la matriz de Riesgos y las fases que lo componen	✓
Análisis de Impacto del Negocio	✓
Definición de los tipos de control, el alcance de cada tipo de control y las situaciones en que cada tipo de control será usando dentro de la matriz de Gestión de Riesgos y según lo requerido por la Norma ISO 27001:2013. .	✓
Roles y responsabilidades en la matriz de Gestión de Riesgos y según lo requerido por la Norma ISO 27001:2013.	✓
Procedimientos para determinar el nivel de afectación del negocio y los daños, según lo estipulado en la Gestión del Riesgo.	✓

La evaluación se basó en procesos centrada en los temas significativos requeridos por las Normas, el método utilizado de evaluación fue la revisión de información documentada desarrollada y entregada por el interesado, así como la validación a través de las entrevistas con el personal responsable.

Así mismo, se concluye que el trabajo de Grado desarrollado por los señores: Camilo Andrés Ñustes Bermúdez y Esteban Camilo Orjuela Supelano, mantiene una alineación con los requisitos de un Sistema de Gestión de Seguridad de la Información que da cumplimiento a los requisitos de la Normas ISO 27001:2017 en el componente de Gestión de Riesgos y enfocado al requisitos de Planificación; por lo cual concluye que el concepto final es:

CONCEPTO	***CUMPLE***

Figura 44 Concepto por la empresa PGCC Hoja 2. Autoría propia (2021)