IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN, RIESGOS Y CONTROLES ASOCIADOS PARA LA EMPRESA ESTRATEGIAS EMPRESARIALES DE COLOMBIA BAJO LA NORMA ISO 27001 E ISO 31000

PAUL CHRISTIAN BORRERO OCHOA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA

CALI - COLOMBIA

2018 – 2019

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN, RIESGOS Y CONTROLES ASOCIADOS PARA LA EMPRESA ESTRATEGIAS EMPRESARIALES DE COLOMBIA BAJO LA NORMA ISO 27001 E ISO 31000

PAUL CHRISTIAN BORRERO OCHOA

TRABAJO DE GRADO APLICADO COMO REQUISITO PARA OPTAR A:

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR: ING. LUIS FERNANDO ZAMBRANO HERNANDEZ

LÍNEA DE INVESTIGACIÓN

INFRAESTRUCTURA TECNOLÓGICA Y SEGURIDAD EN REDES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA

CALI - COLOMBIA

2018 – 2019

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

DEDICATORIA

A mi familia por ser el pilar de todos mis procesos formativos y profesionales.
A mis sobrinos que son el motivo de mi vida para ser cada vez mejor.

AGRADECIMIENTOS

A mis amigos y compañeros por estar siempre allí para apoyarme en todo momento. Al ingeniero LUIS FERNANDO ZAMBRANO HERNANDEZ, por orientarme en el presente proyecto.

RESUMEN

El identificar correctamente los activos necesarios para la gestión de la información, se constituye para las organizaciones, en una base que les permite gestionar cada uno de los riesgos sobre la seguridad que afectan específicamente la información, determinar eficientemente aquellos controles que resultan más apropiados y sus niveles de seguridad necesarios.

Cada uno de los activos presenta características específicas que requieren protección y monitoreo particular, ya sea por el tipo de información que contienen, el estado en el que se conservan o importancia relativa para la función y desarrollo de la empresa. Así mismo, se debe identificar, documentar y validar la responsabilidad del personal que tiene acceso a los activos, los roles que desempeñan y el papel que juegan en torno a su seguridad, de manera que se garantice la propiedades de disponibilidad (accesible en todo momento con autorización), integridad (exactitud en la información), confidencialidad (restricción especifica), autenticidad (sin alteración) y trazabilidad (registro de acceso y gestión) de la información de la empresa.

El cuantificar estas variables, permitirá determinar el valor que posee cada activo y la gestión a realizar sobre cada uno. Para el desarrollo del trabajo, se utilizará como guías la Norma ISO 27001:2013 sistema de seguridad de la información y la ISO 31000:2018 para la gestión de riesgos y controles. Esto para ser implementado en la empresa Estrategias Empresariales de Colombia, cuya razón social está centrada en la prestación de servicios y cuenta con sede en la ciudad de Cali y clientes en toda Colombia.

PALABRAS CLAVE

Activos de información, integridad, confidencialidad, disponibilidad, seguridad, riesgos, controles, información, inventario, clasificación.

ABSTRACT

Correctly identifying the necessary assets for information management, is constituted for organizations, on a basis that allows them to manage each of the security risks that specifically affect the information, efficiently determine those controls that are most appropriate and their Security levels needed.

Each of the assets has specific characteristics that require particular protection and monitoring, whether due to the type of information they contain, the state in which they are conserved or relative importance for the function and development of the company. Likewise, the responsibility of the personnel that has access to the assets, the roles they play and the role they play around their security must be identified, documented and validated, in order to guarantee availability properties (accessible at all times with authorization), integrity (accuracy of information), confidentiality (specific restriction), authenticity (without alteration) and traceability (access and management registration) of company information.

Quantifying these variables will determine the value of each asset and the management to be carried out on each one. For the development of the work, the ISO 27001: 2013 information security system and ISO 31000: 2018 guidelines for risk management and controls will be used as guides. This to be implemented in the Colombian Business Strategies company, whose corporate name is focused on the provision of services and has headquarters in the city of Cali and customers throughout Colombia.

KEYWORDS

Assets of information, integrity, confidentiality, availability, security, risks, controls, information, inventory, classification.

TABLA DE CONTENIDO

pág.

LISTADO DE TABLAS

LISTADO DE FIGURAS

1. INTRODUCCION

La información se encuentra catalogada como un activo de suma importancia para la continuidad y logro de objetivos para las organizaciones sin importar su actividad u objeto social. Asegurar esta información y de los sistemas bajos los cuales se gestionan, debe tener prioridad para las empresas e incluir esto como parte fundamental de su planeación estratégica, comprometer la asignación de recursos tanto físicos, financieros y humanos para que todo se desarrolle en las condiciones más favorables y benéficas para la empresa.

Un activo de información, es todo aquello que tiene información y valor para la empresa y que por lo tanto debe ser protegido, implementando las medidas más acordes a la relevancia que tiene el activo para el llevar a cabo las diferentes operaciones de las empresas.

Los activos de información pueden tener diferente presentación y estar en diferentes ubicaciones, bases de datos, contratos, documentos, repositorios, entre otros. El asignar un responsable para cada uno de ellos, permitirá tener un mejor control y asegurar en cierto grado su correcto mantenimiento, actualización y gestión.

El utilizar una guía que permita direccionar los esfuerzos de una forma lógica y ordenada en función de una correcta identificación de activos de información, es tan fundamental como la identificación en sí misma. La norma ISO 27001 proporciona la metodología, direccionamiento y medidas de consulta y apoyo que permiten de una manera específica, realizar una adecuada identificación de todos los activos de información, protegerlos y gestionarlos.

Para lograr esto, se hace necesario además, gestionar específicamente la seguridad relacionada a la información, utilizando metodologías documentadas, la cual permita objetivos para implementación claros en la organización en donde se visualice una adecuada evaluación de los riesgos que, de una manera u otra, puedan impactar sobre los activos de información.

El presente trabajo, toma como base la norma ISO 27001:2013 e ISO 31000:2018 como base para lograr la identificación de activos relativos a los datos e información así como la gestión de evaluación de los riesgos relacionados que se pueden presentar de manera específica.

2. PLANTEAMIENTO DEL PROBLEMA

Estrategias Empresariales de Colombia, es una empresa cuyo objeto social son las actividades de administración empresarial, se dedica a la asesoría y consultoría administrativa para diferentes empresas del sector servicios en el país, su valor agregado es el soporte que se presta para el desarrollo estratégico con soporte en procesos que usan herramientas tecnológicas que facilitan la operación de sus clientes.

En el cumplimiento de esas actividades, genera, procesa y conserva información esencial que le permite el cumplimiento de sus objetivos estratégicos y el de las empresas que asesora, sin embargo, carece de una correcta identificación de sus activos de información, no se tiene clara una metodología que permita cuantificar y valorar la importancia de estos para cada uno de sus procesos, y de qué manera, teniendo en cuenta los compromisos adquiridos con sus empresas cliente, debe salvaguardar sus activos, de manera que se dé un grado de certeza en este campo y se proyecte como una organización sólida en seguridad de información.

Es por ello que, se hace muy primordial, y para que la empresa pueda definir su sistema específico de seguridad para la gestión de la información, construir la guía, metodología y/o estrategia que permita la identificación, valoración y gestión para sus activos propios relativos a la información, estableciendo el valor representativo para desarrollar las actividades, que tan susceptibles son, que riesgos pueden presentar y los controles más adecuados de acuerdo con la información que maneja. Sin estructurar una adecuada metodología, la empresa, simplemente establece los controles que cree necesarios, pero sin tener en cuenta todas aquellas variables que determinan que tan importante es el activo, riesgos a los que está expuesto, controles que garantizan la protección o la mitigación del riesgo y el monitoreo y actualización correspondiente.

3. JUSTIFICACIÓN

El objetivo fundamental que debe tener toda empresa es consolidar su operación en el mercado, pero para lograrlo debe trazar una ruta que le permita conseguir esta meta. Identificar cuáles son esos componentes que facilitaran su gestión y más importante aún, priorizar cuál de todos son los que presentan mayor relevancia, es el núcleo sobre el cual deben versar su planeación estratégica.[1]

Sin importar cuál es su objeto social, toda organización establece sus pilares de desarrollo en el conocimiento y gestión de la información que maneja, ya sea la propia para llevar a cabo sus procedimientos internos o, la de los clientes y demás partes interesadas con las cuales se relaciona.

Estrategias Empresariales de Colombia, por ser una empresa de consultoría y asesorías, tiene acceso, gestiona y almacena información de sus actividades y las de sus clientes, pues es su principal recurso de trabajo y como tal debe establecer las medidas pertinentes que garanticen su seguridad y la proyección de esta sobre sus clientes, los cuales depositan en la empresa, toda su confianza para el cumplimiento de sus objetivos estratégicos.

Por esta razón, resulta imperativo realizar la identificación de todos esos activos que utiliza Estrategias Empresariales de Colombia, para gestionar la información, de manera que se tenga conocimiento pleno de cada uno, que controles se han implementado, la eficacia y pertinencia de los mismos, las responsabilidades del personal para su manejo, además de la gestión que permita su mantenimiento y actualización.

Esta última, de suma importancia, ya que los riesgos a los que se exponen son cada vez más cambiantes y si se hace un excelente trabajo inicial pero no se garantiza su mejora continua, los riesgos pueden materializarse sin que la empresa se encuentre preparada tan siquiera para su mitigación.

Lo anterior, redundará en un mayor valor frente a los clientes, que percibirán la empresa como una organización sólida, no solo a nivel de servicio, sino también con ese plus de seguridad y confianza, en saber que la información entregada y gestionada cumple con estándares reales de salvaguarda, confidencialidad e integridad.

[1] Aguirre & Aristizabal. Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la Ofrenda

4. OBJETIVOS

4.1. GENERAL

Identificar los activos de información en la empresa Estrategias Empresariales de Colombia, de manera que se conozcan los riesgos y controles necesarios para garantizar su correcto desempeño en el mercado en que se encuentra.

4.2. ESPECIFICOS

- ✓ Establecer una metodología para la identificación de los activos de información
- ✓ Definir y valorar los riesgos para los activos de información identificados
- ✓ Definir los controles a implementar acordes a los riesgos identificados

5. MARCO REFERENCIAL

5.1. MARCO LEGAL

ISO 27001

Tiene como objetivo proteger y resguardar los activos de información, independientemente de su categoría, sector u objeto. Considera como un activo de la información específicamente a cualquier agregado de datos el cual haya sido utilizado o creado por algunos de los procesos de una organización o empresa, al igual que el hardware y software, que es empleado para llevar a cabo su procesamiento o custodia, así como todos aquellos servicios gestionados para realizar su envío o además de cada una de las herramientas necesarias para la implementación así como el soporte de los sistemas de información corporativos.[2]

En el ámbito funcional, considera 3 factores:

Inventario de Activos: Se refiere a que los activos que forman parte de una organización, deben siempre estar perfectamente identificados, manteniendo además, el inventario actualizado de activos propios para la información, los cuales se consideren críticos o de gran relevancia para el desarrollo de las actividades.

El inventario, requiere contar con la respectiva valoración de cada uno de los activos identificados, teniendo en cuenta la respectiva escala que a bien tenga aprobada la alta dirección o a quien este designe como responsable, como por ejemplo, critico, medio o bajo. Así mismo, se considera fundamental, indicar cuales son aquellas propiedades que requieren ser protegidas por cada activo teniendo en cuenta su Confidencialidad, Integridad y Disponibilidad, dando una valoración respectiva por cada una de las propiedades. Además, en el inventario, se debe incluir la ubicación real del activo, quienes lo utilizan y sus respectivos responsables.

Propiedad de los Activos: En esta se indica que la información así como cada uno de los activos que se encuentran relacionados a los servicios para procesarla, deben contar con un encargado o responsable, el cual es asignado por la organización. Es así como en esta categoría se establece:

1. Propietario de la Información: corresponde a aquella parte o partes que se designan por la organización, como un cargo, proceso o equipo de trabajo en cuya gestión se tiene que definir cuál personal tiene acceso a la información, que se puede hacer con la información, hasta donde se tiene acceso, así como los criterios a cumplir con la finalidad que la información sea salvaguardada en caso de accesos externos que no cuenten con autorización, para de esta manera, impedir perdida o modificación de la

[2] Andrés Segovia. Advisera Expert Solutions (2018).

misma modificación, su destrucción intencionada o no, así como establecer su gestión una vez haya cumplido su ciclo y no sea requerida y proceder con su disposición final cumpliendo los requisitos internos y externos de tiempo, forma y demás asociados.

2. Custodio: se refiere aquella parte de una organización, normalmente un proceso, cargo o equipo de trabajo que se encarga de la administración y hacer efectivos todos los controles relativos a la seguridad, tales como copias de seguridad o backups, asignación de los privilegios a que hay lugar, en cuanto a acceso, edición o borrado, que se haya definido por parte del propietario de la información; todo ello teniendo como base los controles de seguridad así como los recursos que disponga la organización.

3. Usuario: se denota así, a la persona que se encarga de generar, obtener, utilizar, gestionar y/o conservar la información de las diferentes organizaciones en cualquier medio, ya sea digital, físico o valiéndose de redes y sistemas para la información que tenga implementados la organización. Esto quiere decir, toda aquella persona que emplea la información para llevar a cabo sus actividades asignadas y que cuenta con los permisos suficientes para el uso de la misma, dentro de lo relacionado en el inventario de la información. Por lo anterior, es fundamental que cada uno tenga definidos las responsabilidades, derechos y accesos específicos relacionados con los activos de información.

Directrices de Clasificación: establece, según la guía, que la información debe tener definida su clasificación, teniendo en cuenta el valor, la disposición legal, importancia y criticidad para la organización.

ISO 31000

Es la norma internacional aplicada a la Gestión de Riesgos. Esta indica los elementos y principios para que las organizaciones realicen la gestión, análisis y las respectivas evaluaciones sobre sus riesgos. Está dirigida tanto a empresas del sector público como privado, ya que en ella se encuentran relacionadas las principales actividades realizadas a nivel empresarial como los son planificación, gestión y procesos de comunicaciones. Si bien es cierto que la mayoría de las organizaciones realizan la gestión de riesgos utilizando diferentes metodologías, las buenas prácticas y recomendaciones a las que hace referencia esta norma internacional, están desarrolladas para influir y mejorar de manera significativa las operaciones de gestión.

Al estar orientada a cualquier tipo de organización, la norma busca que a través de la implementación de principios y directrices, se desarrolle un sistema de gestión para los riesgos, de manera que se convierta en una herramienta clave que reduzca los obstáculos que impiden a las empresas, alcanzar cada uno de sus objetivos estratégicos.

Esta norma, parte desde la ideología que, cada empresa implementa acciones para gestionar sus riesgos en mayor o menor medida, pero, en muchas ocasiones, sin coordinar ni alinear de manera efectiva, las actividades o prácticas que llevan a cabo para ello. Así mismo, que se trabaje de manera integral el sistema de gestión de riesgos con la administración y estrategia que se tiene para la operación, en sus procesos y en la cultura que sea estructurada.

Entre las bondades que supone este estándar en la gestión de los riesgos para las organizaciones que la implementan, se encuentran:

- ✓ Mejoramiento de manera significativa la eficacia en sus procesos y en su gobernabilidad.
- ✓ Alta confianza de las partes interesadas
- ✓ Reducción de perdidas aplicando controles a su sistema de análisis de riesgo
- ✓ Ser flexibles y responder de manera efectiva a los cambios del negocio

La gestión de riesgos debe ser siempre considerada como un proceso aplicado en forma dinámica, continua y fundamental para administrar de manera eficiente cualquier tipo de organización. Es por ello, que todas deben asegurarse de contar siempre con las herramientas necesarias que les proporcionen las capacidades requeridas para de manera eficiente, monitorear, priorizar y gestionar los riesgos internos que presentan, tomando como referente los cambios que se presenten tanto internos como externos.

5.2. MARCO TEORICO

Los activos de información son aquellos recursos que se utilizan dentro de los sistemas de gestión para la seguridad específica de la información, que son indispensables, ayudando a las empresas, a desarrollar sus operaciones y cumplir con los objetivos estratégicos que han sido trazados por parte de sus administradores.

Para lograr una adecuada identificación de los activos, poder hacer una valoración y establecimiento de controles existen diferentes metodologías, una de ellas es la establecida por las normas ISO 27001:2013 que trata del establecimiento de los sistemas de seguridad sobre la información, haciendo referencia al mantenimiento eficiente de los tres (3) pilares que tiene información: confidencialidad, disponibilidad e integridad, al igual que los sistemas y herramientas utilizados para su tratamiento en las organizaciones.[3]

Si entendemos la definición de estos tres conceptos:

[3] (ISO 27001:2013).

La confidencialidad se define como aquella información que no se revela ni se pone en conocimiento de terceros no autorizados

La integridad se define como el mantenimiento de la exactitud de la información y sus metodologías de procesamiento.

La disponibilidad se define como como el acceso y gestión de la información por parte de aquellos que así lo requieren.

Se puede concluir que, se constituyen en el pilar fundamental para la construcción y desarrollo de un método que permite realizar una correcta identificación y hacer una valoración sobre los activos de información teniendo como referente el sistema de seguridad propio para los datos e información que se utiliza en las empresas actualmente.

En el entendido, que solo con una identificación de activos y su categorización por criticidad, no basta para asegurar la información que contienen estos, se hace necesario introducir e implementar un análisis de riesgos el cual es un medio cualitativo y cuantitativo que permite hacer una valoración efectiva acerca de cada riesgo, que pueden afectar y a los que se exponen los activos en las organizaciones. Esta evaluación implica, validar el nivel de riesgo que este asociado, establecer criterios de razonabilidad, entendiéndose como aquello que se está dispuesto a tolerar o que permite el desarrollo de las operaciones del proceso responsable del riesgo, es decir su valor mínimo tolerable, esto, teniendo en cuenta que nunca por más controles que se implementen, se puede garantizar cero riesgo para un activo de información. Con esta evaluación, se establecerán probabilidades, amenazas, vulnerabilidades, impactos y activos críticos.

5.3. MARCO CONCEPTUAL

Activos. Tomando como referencia la seguridad aplicada a la información, trata de cualquier elemento o información, que se relacione con el tratamiento de la misma (por ejemplo edificaciones, individuos, sistemas...) y que posea algún tipo de valor significativo para la empresa.[4]

Amenazas. Son todas aquellas situaciones que pueden generar consecuencias negativas para la adecuada gestión de las funciones o actividades propias de la operación de las empresas, como, por ejemplo, accesos no autorizados, virus, desastres naturales y demás.

Confidencialidad: Se trata de aquella propiedad de la información que la hace indisponible o no ser de conocimiento o acceso a personal, empresas y/o procesos

[4] (iso27000.es, 2012).

no autorizados[5].

Controles. Medidas de protección que permiten gestionar y controlar cada uno de los riesgos que pueden llegar a presentarse sobre los activos y sistemas relativos a la información.

Disponibilidad: Hace referencia a que la información debe siempre encontrase accesible y utilizable para cuando así sea requerido por la entidad autorizada.[6]

Evaluación de riesgos: Se trata de comparar el resultado que arroje el análisis de riesgos con los criterios de los mismos, con esto, se determina si el riesgo, su magnitud o ambos son aceptables o tolerables (Icontec Internacional, 2011).

Impacto. Se refiere a las consecuencias que tienen la materialización de las diferentes amenazas que se tienen sobre cada activo de información.

Integridad: Es aquella propiedad relativa a la información que hace referencia a su exactitud y completitud (Organización Internacional de Normalización [ISO], 2014).

Proceso: Se trata de un conjunto de actividades lógicamente relacionadas entre sí, con la finalidad de transformar elementos de entrada en salida (iso27000.es, 2012).

Riesgos. Son todas aquellas situaciones que afectan los riesgos y que causan incertidumbre sobre el cumplimiento de los objetivos trazados.

Seguridad de la información: se refiere a conservar la confidencialidad, integridad y disponibilidad de la información.

Vulnerabilidades. Es aquella característica observada o que pueden presentar los activos y sistemas propios de la información y que pueden o no ser aprovechadas para generar caos, robar información y en general hacer algún tipo de daño sobre estos.

5.4. MARCO CONTEXTUAL

Una gestión efectiva y eficiente de los activos específicos de la información, que, den soporte a cada proceso de la organización, se constituye en uno de los requisitos específicos establecidos por la ISO 27001:2013, incluido en la lista de Controles del Anexo A.

Lo anterior, comprende desde la identificación a través del desarrollo de un inventario, determinar un propietario o responsable por cada uno de los activos, establecer el uso correcto y adecuado, así como de su recuperación en caso que sea requerido con el fin de prevenir su pérdida o distribución no controlada.

[5] Organización Internacional de Normalización [ISO], 2014
[6] ISO, op. cit.

En los controles especificados en la norma ISO 27001 2013, se especifica el realizar un completo inventario para los activos relacionados con la información, como valor fundamental para desarrollar el trabajo propio para su gestión, pues si las organizaciones desconocen o que tienen, resulta muy complejo establecer un control especifico y que además sea eficiente. Es necesario adicionalmente, establecer un protocolo de actualización de inventario continuo a lo largo del tiempo, por lo que se hace indispensable definir las revisiones periódicas a realizar y comunicar cualquier cambio que sea observado.[7]

La norma ISO27001:2013, indica que es fundamental que los activos de información, sean identificados claramente, se mantengan actualizados y se especifiquen cuales resultan importantes o críticos para la organización.

Según lo anterior, las organizaciones, deben identificar cada uno de los activos que utilizan para sus operaciones y documentar en relación a la importancia relativa que tienen cada uno. Este inventario de activos, debe incluir la información que se considere relevante para poder tener la habilidad de recuperación ante la ocurrencia de un desastre, por lo que se necesita que se incluya, el tipo de activo, el formato en el que se encuentra, sitio o ubicación, condiciones de backup, licencia y el valor de negocio. El inventario de activos no debería estar duplicado sino es estrictamente requerido, sin embargo, se debe garantizar que el contenido, está alineado y es complementario con el resto del inventario de la empresa.[8]

Estrategias Empresariales de Colombia, es una organización de carácter privada, ubicada en la ciudad de Santiago de Cali, cuyo objeto social son las actividades de asesorías administrativas, que incluyen procesos financieros, administrativos, comerciales, jurídicos, tesorería, auditoría, tecnología y comunicaciones para diferentes empresas de servicios transaccionales a nivel Nacional.

Misión. Lograr la excelencia en el servicio para facilitar la vida de nuestros clientes.

Visión. En los próximos cinco años, ser la empresa más importante en la prestación de asesorías para las redes transacciones de Colombia.

Como objetivos estratégicos, se tiene trazados el desarrollo del ser humano, presentar excelencia en el servicio y en la calidad del mismo, crecimiento, rentabilidad a través del tiempo e incluir la responsabilidad social corporativa.

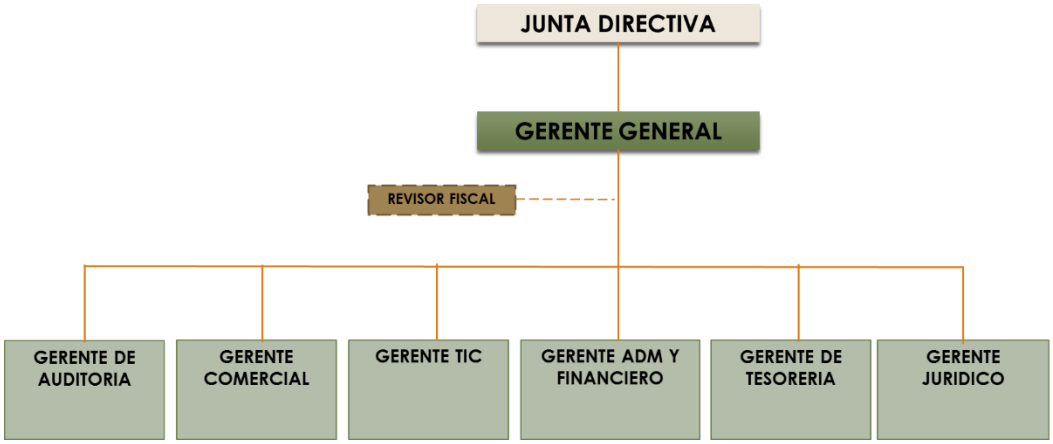
A continuación, se presenta la estructura organizativa con que cuenta la empresa:

Figura 1 Organigrama Corporativo.

[7] ISO, W. (2018). Los Activos de Información en la norma ISO 27001 2017

[8] ISOTOOLS. ¿Cómo clasificar los activos de seguridad en un SGSI? (2015)

ORGANIGRAMA



Fuente. Estrategias Empresariales

Cada gerencia representa un proceso productivo integrado por subprocesos y personal altamente calificado, que permiten el desarrollo operativo a la organización. La gerencia general, es quien orienta y monitorea que se cumplan los objetivos estratégicos, así como también determina el modo o mecanismos para realizar las operaciones y mejoras corporativas.

6. METODOLOGIA

6.1. DEFINICIÓN DE LAS METODOLOGÍAS EXISTENTES PARA EL ANÁLISIS DE RIESGOS SOBRE ACTIVOS DE INFORMACIÓN.

Teniendo en cuenta que se requiere definir una metodología que permita realizar el análisis de los riesgos asociados a los activos de información en Estrategias Empresariales, a continuación se realiza un contexto y definición de diferentes tipos de las metodologías que permiten realizar esta labor.

6.1.1 Octave. Operationally Critical Threat, Asset, and Vulnerability Evaluation. Se trata de una metodología que orienta a las organizaciones para que dirijan y gestionen de una manera efectiva sus evaluaciones de riesgos, de manera que se tomen decisiones tomando como base los riesgos, se protejan los activos de información más críticos y por último se comunique de manera efectiva la información específica y fundamental relacionada con la seguridad.[9]

Esta metodología, es considerada como una técnica o metodología fundamentada para la clasificación y proyección en lo que se tiene que ver con la seguridad de la información direccionada hacia el riesgo, la cual es basada en los siguientes métodos específicos: flexible, auto dirigido y evolucionado. Estos, son desarrollados a través de tres fases: el primero, perfiles de las amenazas que se basa en los activos de cada organización, el segundo, identificación de las vulnerabilidades que guardan relación directa con la infraestructura y por último, se trata del desarrollo de la estrategia así como los de los planes de seguridad.

Se encuentra basada en los siguientes criterios, que son los que regulan su proceso de implementación:

- ✓ Esta metodología precisa ser auto-dirigida. Implementando un equipo o grupo específico para el análisis con todas sus capacidades.
- ✓ Las medidas que sean tomadas, deben ser adaptables de acuerdo con las necesidades de la compañía. Aquí se debe establecer el inventario de buenas prácticas para la ejecución de actividades, el perfil asociado a cada una de las amenazas y por último referenciar de forma específica las vulnerabilidades.
- ✓ El proceso debe ser definido. En el entendido en que se deben establecer las actividades objeto de evaluación, documentar los resultados de esas evaluaciones y definir su alcance.
- ✓ El proceso debe ser continuo. Estableciendo el paso a paso a seguir, así como las prácticas a desarrollar.
- ✓ El proceso debe ser desarrollado con visión hacia el futuro. Enfocándose en los riesgos que vayan siendo identificados.

[9] Becerra, Claudia. Metodologías Para el Análisis de Riesgos en los SGSI. Tunja. 2015

- ✓ El proceso deberá centralizarse en un número reducido de riesgos. Teniendo en cuenta aquellos que resultan más críticos, para definir su evaluación y desarrollar actividades específicas o focalizadas.
- ✓ Debe haber una gestión integrada. Siempre estableciendo, la responsabilidad y el compromiso que debe tener la alta dirección, se deben integrar aspectos organizacionales y tecnológicos e incluir la participación activa de todo el personal clave y de tecnología.
- ✓ Debe existir comunicación abierta. Donde se informe e integre a todo el personal.
- ✓ Se debe conforma equipo de trabajo. Donde exista una capacidad alta para el análisis, se integren de manera armónica e interdisciplinar las áreas de la empresa y exista trabajo colaborativo.

Con este método, se orienta de manera operativa la implementación para la obtención de resultados. De manera que se tiene plan a corto plazo para ir avanzando y uno estratégico a largo plazo que va ayudando a mitigar los riesgos que sean detectados. Por último, después de implementar acciones a corto y largo plazo, establece una metodología detallada y específica, donde se soporta cada actividad realizada y se siguen metodologías estandarizadas.

6.1.2 Cramm. CCTA Risk Analysis and Management Method. Esta metodología ha sido desarrollada por el Central Communication and Telecommunication Agency (CCTA) establecida en el reino unido, orientada principalmente a grandes conglomerados industriales, así como, a entidades del sector público. Ha sido concebida en tres fases o etapas:

- ✓ Primera: establecimiento de objetivos de seguridad. Aquí se establece el alcance en implementación, el valor que representa la información en el actuar de la organización, la identificación y evaluación para sus activos físicos, así como también el software que hace parte del sistema de información.
- ✓ Segunda: analizar los riesgos. Se realiza la identificación y se valoran por tipo y por nivel, cada amenaza que puede llegar a impactar de manera significativa el sistema corporativo. Se valoran las vulnerabilidades y se cruzan con las amenazas de esta manera se puede calcular la medida para cada uno de los riesgos.
- ✓ Tercera: identificar y elegir las mejores salvaguardas. De aquí se obtienen informes de relacionados con el estudio, comportamiento, afectación y gestión de cada riesgo y se da la directriz acerca del plan para su implementación.

En síntesis, en esta se realiza una gestión integral de los riesgos, incluido su análisis respectivo, esto en miras a proporcionar confidencialidad, disponibilidad e integridad para sistemas relacionados con datos e información corporativa, utilizando evaluación mixta. Esto basado en un sistema tecnológico que soporta esta

herramienta, la cual cuenta con más de 400 tipos diferentes de activos, 25 tipos de impactos identificados y más de 3500 posibles salvaguardas a implementar.

6.1.3 Mehari. Esta fue estructurada por el club Francés de seguridad de la información (CLUSIF) alrededor de 1996, y es de libre acceso, no cuenta con restricciones, además, pensada para cualquier empresa. Se actualiza constantemente para ayudar a los oficiales, directores o responsables en las empresa, de la seguridad en sistemas de información, a ejecutar sus operaciones en seguridad informática, pero también es utilizada y ayuda a los auditores y gestores de riesgos en sus respectivas verificaciones.

Con esta metodología se lleva a cabo un estudio de manera rigurosa acerca de factores de riesgo que resultan primordiales, de manera que cuantitativamente se determine donde se requiere realizar un análisis minucioso. Se propone también, una integración entre el análisis de lo que a la organización le interesa en materia de seguridad contra el respectivo análisis de riesgos, valiéndose de diferentes herramientas de apoyo.

Se trata de proporcionarle a las organizaciones, una metodología aplicada que les permita evaluar de manera adecuada, la gestión de sus riesgos, basándose en el dominio especifico que hace referencia a la seguridad propia de la información, acorde a lo direccionado por ISO/IEC 27005.[10]

Lo que destaca de esta metodología se puede condensar en lo siguiente:

- ✓ Permite el modelamiento del riesgo a través de un modelo específico.
- ✓ Hace una evaluación objetiva, sobre cada política o directriz generada para la seguridad especifica de la información implementada en las empresas.
- ✓ Realiza una valoración y simular los diferentes niveles de riesgos a los que se encuentren expuestas.

Mehari, permite detectar vulnerabilidades a través de la implementación de auditorías, en las cuales se analizan todas aquellos escenarios de riesgos y el contexto en el cual se presentan. Se realiza de esta manera una evaluación exhaustiva y verídica acerca de los riesgos sobre los sistemas informáticos de la organización. Se destacan dentro de esta, tres fases fundamentales:

- ➢ Análisis, gestión y evaluación especifica sobre los riesgos que sean identificados
- ➢ Evaluación sobre seguridad, haciendo énfasis especial en la vulnerabilidades que se presentan
- ➢ Análisis especifico de amenazas

Estos módulos, deben ser compatibles con las políticas y las estrategias de cada organización que decida implementar el modelo o permitir que estos se adapten, de

[10] M. Crespo. (2014). El Análisis de Riesgos dentro de un Auditoría Informática: Pasos y Posibles Metodologías

esta manera, se pueden identificar y generar aquellos planes de acción que sean requeridos, a fin de implementar y sostener la seguridad de la información. [11]

6.1.4 Coras. Construct a Platform for Risk Analysis of Security Critical Systems. Este Proyecto es implementado aproximadamente a comienzos del 2001 y su principal objetivo o meta consiste en desarrollar una metodología para el trabajo específica en sistemas de información, en los cuales, por la operación, la seguridad de la información, resulta ser prioritaria o critica. Durante la implementación, pueden detectarse fallas en el entorno de la seguridad, redundancias y se exponen las diferentes vulnerabilidades de seguridad, explotadas en las siguientes etapas:

- ✓ Exposición o Presentación
- ✓ Análisis de elevado nivel
- ✓ Aprobación
- ✓ Caracterización de los riesgos asociados
- ✓ Calculo o apreciación de riesgos
- ✓ Evaluación de cada uno de los riesgos
- ✓ Tratamiento del riesgo[12]

Es un modelo que se integra por los siguientes elementos:

- ➢ Metodología de análisis de riesgos, cuya base fundamental es la elaboración de métodos o modelos.
- ➢ Lenguaje de tipo gráfico, el cual se basa en UML (Unified Modelling Language)
- ➢ Editor gráfico, para soportar la generación de los modelos más apropiados
- ➢ Base de datos de casos que pueden ser utilizados como guía
- ➢ Herramientas de gestión para los casos
- ➢ Representación textual basada en XML (eXtensible Mark-up Language)
- ➢ Establecimiento de estándares que definan la presentación de informes.[13]

En resumen, esta metodología durante su implementación, establece un editor de tipo gráfico, para diseñar modelos basados en lenguaje Microsoft Visio, con una librería en la que se encuentran diferentes casos que pueden ser consultados y utilizados, un gestionador de casos y un modelo o plantilla de informe para realizar una comunicación estándar de fácil comprensión, que permite en todo momento relacionar cada una de las partes del proceso establecido en el análisis de riesgos.[14]

6.1.5 NIST SP 800 – 30. (National Institute of Standards and Technology). La metodología propone recomendaciones y acciones a implementar para realizar una correcta gestión sobre cada riesgo para establecer un sistema de gestión en seguridad de información, el cual es acompañado por el compromiso y

[11] M. Crespo. (2013). El Análisis de Riesgos dentro de una Auditoría Informática.
[12] M. Juan. Análisis de riesgos de seguridad. (2006)
[13] Heidi E. Coras Security Advisors. (2014).
[14] C. Elvis, Metodología para el análisis de riesgos en seguridad informática.

responsabilidad del personal relacionado con la empresa en todos los niveles, para lograr cumplir con los objetivos trazados.
Está basada en una serie de pasos, cuya implementación es fundamental para lograr la implementación con éxito de la metodología:

- ✓ Caracterizar correctamente el sistema
- ✓ Identificar las amenazas y vulnerabilidades a las cuales se encuentra expuesto
- ✓ Realizar un análisis exhaustivo de la información
- ✓ Determinar y caracterizar el riesgo
- ✓ Analizar correctamente el impacto
- ✓ Recomendaciones de los controles específicos a implementar

Con esto, se proporciona una base sólida para desarrollar a nivel empresarial, un programa realmente eficaz que permite la gestión de manera integral sobre los riesgos, de manera que se puede orientar la evaluación y mitigación de estos en los sistemas de información. Se estructura como una guía, que permite realizar la gestión de los riesgos, a través de tres pasos fundamentales:

a- Evaluación
b- Mitigación
c- Análisis y evaluación de los riesgos.[15]

Es más orientada y destaca por ayudar a gestionar riesgos en proyectos de tecnología, logrando implementación satisfactoria en hardware, bases de datos, software, telecomunicaciones y redes, esto a través de criterios de seguridad que integra en su estructura entre los que se encuentran confidencialidad, integridad y disponibilidad, como base para valorar la materialización de amenazas y el impacto que ocasionan sobre los elementos que conforman las tecnologías de la información que integran las diferentes empresas en el mundo.

6.1.6 Magerit. Se desarrolló por el consejo superior de administración electrónica, esta se basa en dos objetivos fundamentales, primero estudiar cada uno de los riesgos que afectan el sistema de seguridad de la información y su contexto, y el segundo, se basa en las recomendaciones que se enmarcan con el fin de desarrollas las medidas apropiadas de adopción que permiten hacer una evaluación, prevenir reducir y controlar los riesgos que se hayan identificado. [16]

En Magerit, la seguridad es definida como “aquella capacidad de las redes y sistemas de información que permiten soportar, teniendo adecuado margen de confianza, los incidentes o actividades que de forma malintencionada ponen en compromiso la integridad, disponibilidad, autenticidad y confidencialidad para datos

[15] Comisión interamericana de Telecomunicaciones, gestión de riesgos de seguridad (2009)
[16] M. Juan. Planes de Contingencia: La Continuidad del Negocio en las Organizaciones (2006)

guardados o que son trasmitidos y de cada servicio que se ofrece a través de esas redes o sistemas" [17]

Dentro de los principales elementos que esta metodología acoge para el desarrollo del análisis relativo a riesgos, se encuentran:

- ✓ Activos de información
- ✓ Amenazas y vulnerabilidades
- ✓ Impactos
- ✓ Riesgos y salvaguardas o controles

De acuerdo con el desarrollo de esta metodología, se pueden resaltar las etapas en las cuales se basa para ser implementada:

a. Planificación
b. Análisis de los riesgos
c. Gestionar los riesgos
d. Selección de salvaguardas

Estas etapas son desarrolladas en a través de una metodología lógica basada en:

- ✓ Describir el paso a paso que permite realizar la validación del estado actual de los riesgos, y de esta manera gestionar su eficientemente su mitigación.
- ✓ Describir aquellas tareas que resultan básicas para desarrollar el análisis y gestión de los riesgos.
- ✓ Aspectos prácticos resultantes al evaluar las lecciones aprendidas, casos prácticos o experiencia que se obtiene a través del tiempo, para analizar de manera efectiva y eficiente los riesgos.[18]

A nivel organizacional, Magerit se centraliza en:

- ✓ Establecer conciencia sobre los encargados de los sistemas de información, que riesgos se pueden presentar en sus procesos y la necesidad, de contar con mecanismos implementados que permitan detectarlos de forma temprana.
- ✓ Ser una guía para de manera lógica y sistemática, analizar los riesgos.
- ✓ Seleccionar e implementar las salvaguardas más adecuadas para de manera oportuna, controlar efectivamente los riesgos.
- ✓ Preparar adecuadamente a las organizaciones que implementen esta metodología, para procesos de auditoria, o cuando se requieran certificaciones.

De acuerdo con lo anterior, los pasos para su implementación, se llevan a cabo a través de las actividades que se mencionan:

1. Realizar la identificación de los activos

[17] B. David y R. Camilo. Modelo para la cuantificación del riesgo telemático en una organización (2010)
[18] Guía avanzada de gestión de riesgos, Inteco (2008)

2. Hacer un diagnóstico para determinar las salvaguardas existentes
3. Valorar los activos.
4. Identificar amenazas
5. Identificar las vulnerabilidades a las cuales se está expuesto
6. Hacer un estimativo acerca de esas vulnerabilidades
7. Identificar el impacto
8. Evaluar los riesgos

6.2. SELECCIÓN DE LA METODOLOGÍA.

Teniendo en cuenta las metodologías anteriormente mencionadas, se realiza una tabla resumen, donde se identifican las principales características, ventajas y desventajas de cada una.

Tabla 1 Comparación de metodologías para el análisis de riesgos

METODOLOGIA	CARACTERISTICA	VENTAJA	DESVENTAJA
OCTAVE	Evalúa cada riesgo de seguridad específico para la información y establece propuesta que permite desarrollar el plan de mitigación. Hace una subdivisión de los activos en dos: 1. Sistemas 2. Personas.	✓ Comprende procesos relacionados con el análisis, observación y gestión sobre los riesgos ✓ Involucra a los trabajadores en todos los niveles de la organización. ✓ Es muy completa al involucrar cada proceso, departamentos, recursos, activos, las amenazas identificadas, al igual que las salvaguardas como elementos de análisis.	✓ Solo se puede aplicar en pequeñas y medianas empresas. ✓ No presenta compatibilidad con estándares. ✓ Se basa en demasiados documentos para analizar riesgos. ✓ No define claramente los activos de información ✓ Requiere de conocimientos técnicos para su implementación
MEHARI	Es principalmente un procedimiento de sistema de auditoria que permite la evaluación de riesgos, realiza un completo análisis de	✓ Usa un modelo cuantitativo y cualitativo para el análisis de riesgos. ✓ Evalúa y logra la disminución de riesgos de acuerdo	✓ Solo se enfoca en los pilares de confidencialidad, disponibilidad e integridad. ✓ La estimación acerca del impacto

	los riesgos en sistemas informáticos.	con el tipo de empresa. Particulariza el trabajo. ✓ Permite detectar vulnerabilidades mediante auditorias.	de los riesgos sobre los activos, se realiza en el proceso de evaluación y gestión.
MAGERIT	Realiza la implementación del proceso para la gestión de riesgos tomando como referencia que, cada órgano de administración y control tome decisiones, Integrando cada riesgo que puede llegar a derivarse por el uso de cada tecnología de la información así como de las telecomunicaciones que se tienen en la empresa.	✓ Comprende en su modelo el análisis y la gestión del riesgo. ✓ Es metódica. ✓ Realiza identificación de activos. ✓ No requiere actualización para su uso. ✓ Se encuentra muy bien documentada en lo que se refiere al uso de recursos de información, tipos de activos y sus amenazas.	✓ Requiere ser muy metodológico para su implementación. ✓ Tiene algunas debilidades a la hora de realizar inventario y establecimiento de políticas. ✓ Se centraliza mucho sobre activos.
CORAS	Proporciona un modelo de trabajo para sistemas en los que la seguridad resulta ser crítica. A través de este, se pueden detectar falencias relacionadas con la seguridad, inconsistencias, redundancia y poner al descubierto las vulnerabilidades de seguridad en términos de exposición, aprobación, análisis de alto nivel, identificación, cálculo, evaluación y tratamiento del riesgo.	✓ Se basa en modelos de seguridad críticos. ✓ Es un instrumento muy útil para desarrollar y sostener en el tiempo los sistemas nuevos. ✓ Entrega reporte de las vulnerabilidades que se hayan encontrado en el sistema.	✓ No cuenta con análisis de riesgo cuantitativo. ✓ No contempla elementos como procesos y dependencias.
CRAMM	Esta herramienta o metodología utilizada para el realizar un completo análisis y gestión sobre los	✓ Permite hacer una identificación, descripción y	✓ No examina como elementos a procesos y recursos dentro de

	riesgos, brinda pilares fundamentales referidos a la confidencialidad, integridad y disponibilidad de sistemas de información valiéndose de evaluaciones mixtas.	clasificación por cada activo de TIC ✓ Combina análisis con evaluación para los riesgos. ✓ Evalúa el impacto a nivel empresarial. ✓ Evalúa amenazas, vulnerabilidades, nivel de riesgo.	su entorno de evaluación.
NISP SP 800 - 30	En esta se exponen un agregado de sugerencias, recomendaciones y operaciones con miras a la correcta implementación de una gestión de riesgos, la cual sea parte fundamental en todo lo que se realice para la seguridad de la información.	✓ Bajo costo para su implementación. ✓ Posee herramientas de mitigación y valoración en riesgos. ✓ Proporciona mejora a la administración partiendo de aquellos informes o resultados que se han obtenido del análisis por cada riesgo identificado.	✓ No tiene contemplados procesos, dependencias o activos como elementos de análisis.

Fuente. Claudia Rodríguez. Metodologías Para el Análisis de Riesgos en los SGSI, en combinación con criterios del autor.

Teniendo en cuenta las metodologías descritas y los criterios de comparación establecidos, adicionalmente, que el presente trabajo se aplica a una empresa que se encarga de prestar asesorías administrativas, que tiene procesos definidos y que maneja información de sus empresas cliente, donde se requiere que se involucren tanto la identificación de activos de información, como también, una guía clara acerca de cómo gestionar los riesgos que sea metodológica, que diagnostique el estado actual y con base en ello se desarrolle un trabajo sistémico; se elige trabajar con la metodología Magerit, apoyado adicionalmente en que:

- ✓ Permite describir y planificar aquellas medidas necesarias para mantener los riesgos bajo control
- ✓ Al ser sistémica, se adapta a la forma de trabajo de la empresa.
- ✓ Ayuda a que se tome conciencia por parte de los líderes de proceso, acerca de los riesgos que pueden impactar sus actividades y que pueden afectar de manera significativa las operaciones.
- ✓ Las decisiones se toman sobre datos fundamentados y con soportes como evidencia.

- ✓ Permite que la empresa esté preparada para una auditoria externa y, así no sea prioridad al corto plazo para la alta dirección, estar preparada para una posible certificación.

6.3. DESARROLLO DE LA METODOLOGÍA

6.3.1 Ciclo Deming para el desarrollo del trabajo. Teniendo en cuenta lo establecido por la ISO 27001:2013, se aplica el ciclo para mejorar continuamente en el desarrollo de las actividades, además, esta metodología es expuesta a los líderes de proceso, para que en adelante se continúe con su mantenimiento y custodia. Con ello se busca que estos, propongan mejoras en la gestión de seguridad sobre los activos que tienen a su cargo.[19]

La aplicación del ciclo en la empresa se define a continuación:

Planear:

- ✓ Mediante la definición de lo que es un activo de información.
- ✓ Establecimiento de una metodología para identificar y valorar cada uno de los activos de información.
- ✓ Definición de un esquema que muestre la respectiva clasificación.
- ✓ Definir el respectivo tratamiento y el adecuado manejo para cada activo de información.

Hacer:

- ✓ Generar el levantamiento de la información de los activos de información que son utilizados y gestionados en los procesos de la empresa.
- ✓ Realizar la identificación y la respectiva valoración sobre cada activo de información.
- ✓ Desarrollar la clasificación de los activos que se utilizan para gestionar la información, teniendo en cuenta su importancia para el cumplimiento de las funciones.
- ✓ Participar activamente en las actividades diarias, en cada uno de los procesos, el tratamiento y manejo que se haya definido por cada nivel de clasificación y proceder con la integración en las diferentes metodologías como parte práctica y definitiva para garantizar de manera relativa la seguridad de los mismos.

Verificar:

- ✓ Aquí se revisan las valoraciones que se hayan realizado sobre los activos de información, para corregir en casos en los que se llegase a presentar cambios sustanciales en la empresa o mejoras en la tecnología.

[19] Franco Cárdenas. Gestión Integral de la Seguridad de la Información (2018)

- ✓ Llevar a cabo, la revisión de la información en términos de calidad.
- ✓ Monitorear, hacer seguimiento y auditorías internas para validar cumplimiento.

Actuar:

- ✓ Actualizar la información del inventario de activos de manera periódica.
- ✓ Aplicar las mejoras y recomendaciones que se generen de las revisiones que se realicen.[20]

Algunas de las actividades anteriormente mencionadas, se dejan como mejores prácticas, con el fin de que el trabajo realizado se incorpore en la cultura organizacional, y se vuelva parte de las labores que tienen prioridad alta para la empresa.

6.3.2 Clasificación de los activos de información. Para conseguir generar de forma adecuada la clasificación de los activos de la información, se tomó como guía lo establecido por la ISO 27001 y lo recomendado por el Ministerio de las Tecnologías y Telecomunicaciones MINTIC, que establece que se deben clasificar tomando como referente los tres pilares específicos para la información: confidencialidad, integridad y disponibilidad, tal como se describe a continuación:[21]

De acuerdo con la Confidencialidad

Esta hace referencia a que la información no debe estar revelada o expuesta a personal no autorizada. Se trabaja este ítem, con la clasificación dispuesta por el sistema integrado de gestión o calidad con el que cuenta la empresa:

Tabla 2 Clasificación de los activos por Confidencialidad

INFORMACIÒN RESTRINGIDA	Aquella Información que solo se encuentra disponible para un proceso especifico de la organización, por lo que de ser accedida por un tercero que no cuente con autorización, puede tener impacto negativo reflejado en materia operacional, económica, legal o inclusive, mala imagen operativa.
INFORMACIÒN PRIVADA	Información accesible para los procesos que integran la empresa, que en caso de ser accedida por un tercero, puede generar un impacto negativo en los procesos internos.

[20] Franco, op. cit
[21] Mintic (2016)

INFORMACIÒN PUBLICA	Aquella que se encuentra a disposición de personal tanto interno como externo, sin ningún tipo de restricción, y que su conocimiento no implica perjuicio para la empresa, procesos o personas.

Fuente: Mintic

De acuerdo con la Integridad

Este hace referencia a la disposición exacta y completa que debe tener la información, de manera que se garantiza que la información es completa, exacta y precisa desde que se genera hasta su disposición final.

Tabla 3 Clasificación de los activos por Integridad

A – Alta	Información que en caso de pérdida en su exactitud y completitud ocasionaría que se tenga impacto negativo en lo referente a lo legal, económico, interrumpir la operación o inclusive, ocasionar pérdida critica en la imagen corporativa.
M – Media	Información que en caso de perder su exactitud y completitud ocasionaría impacto negativo en relación a lo económico y legal, demorar las actividades en los procesos y sus operaciones, además de ocasionar pérdida de imagen moderada sobre los trabajadores de la empresa.
B – Baja	Información que en caso de sufrir pérdida de exactitud y completitud, representaría impacto poco significativo al interior de la organización y sus partes relacionadas.
No clasificada	Se referencia a los activos de Información que necesariamente deben hacer parte del inventario y que aún no se encuentren clasificados correctamente, los cuales deben ser gestionados como activos de integridad ALTA.

Fuente: Mintic

De acuerdo con la Disponibilidad

Hace referencia a que la información siempre debe estar accesible y útil para ser consultada por personas autorizadas en los tiempos y forma en que estas lo requieran.

Tabla 4 Clasificación de los activos por Disponibilidad

1 – Alta	La no disponibilidad que se pueda tener en la información puede ocasionar impacto negativo en relación a criterios legales y económicos, retrasar los procesos y actividades desarrolladas, o incluso conllevar a pérdidas críticas en la imagen de la

	empresa ante entes externos, clientes y partes interesadas.
2 – Media	La no disponibilidad que debe tener la información puede ocasionar impacto negativo en temas económicos, legales, interrumpir y demorar las actividades operativas, además de generar mala imagen corporativa de manera moderada.
3 – Baja	La no disponibilidad de la información puede afectar la continuidad en las operaciones de la empresa o entes relacionados, sin embargo, esto no tiene implicaciones de tipo legal, económico y degradación en la imagen corporativa.
4 – No clasificada	Aquellos activos de información, que se deben incluir en el inventario y que no se han clasifica, los cuales deben ser gestionados como activos de información de disponibilidad ALTA.

Fuente: Mintic

6.3.3 Identificación de activos. La identificación de activos de información le permite a las organizaciones hacer un reconocimiento efectivo de sus activos y como se encuentran relacionados con cada uno de los procesos organizacionales.[22]

En el desarrollo, se tienen en cuenta, aquellos activos que tienen significancia operativa para la empresa, es decir, aquellos que resultan fundamentales y permiten de forma práctica y efectiva, cumplir los objetivos estratégicos, de manera que la empresa los pueda categorizar y gestionar de manera eficiente.

Uno de los primeros pasos, es establecer y tener claridad de cuales activos se gestionan dentro de la empresa, para ellos se realiza una descripción detallada a los líderes de proceso, acerca de cuáles son los tipos de activos y como poder reconocer e identificar cada uno y la información que se gestiona o se puede gestionar:

[22] Franco D. Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma iso/iec 27001.

Figura 2 Tipos de activos de información.

Fuente: el autor.

6.3.4 Criticidad de los activos. Para determinar qué tan crítico resulta un activo para la empresa, se establece el siguiente criterio:

Tabla 5 Criterios de Calificación

Confidencialidad	Integridad	Disponibilidad
Información restringida	Alta	Alta
Información privada	Media	Media
Información pública	Baja	Baja
Información no publicada	No clasificada	No clasificada

Fuente Mintic

Donde:

Tabla 6 Criticidad de Activos.

CRITICIDAD	
ALTA	Aquellos activos en los cuales la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) se clasifica como alta.
MEDIA	Aquellos activos de información para los que la información resulta alta en al menos una propiedad o por lo menos una de estas es clasificada como nivel medio.
BAJA	Son los activos de información en los que su clasificación de información en cualquiera de los niveles se considera como baja.

Fuente Mintic

6.3.5 Categorías de activos. Una de las formas que se han establecido para facilitar la identificación y clasificación de los activos, es organizarlos en categorías, de esta forma resulta ideal para que los líderes de proceso entiendan que son y cómo pueden determinar cuáles son los que hacen parte de su proceso y de los que son responsables. Para el desarrollo del trabajo, se tienen las siguientes categorías:

Datos: Hace referencia a los datos (independientemente del formato en el cual se encuentren) que se generan, recopilan, tramitan y destruyen, como por ejemplo, las bases de datos corporativas, la gestión documental (procedimientos, manuales, formatos, etc.).

Aplicaciones: Se trata del software que es utilizado para llevar a cabo la gestión de los procesos de las organizaciones.

Hardware: Son los quipos físicos que son necesarios y requeridos para el desarrollo de las labores diarias, como por ejemplo pc, terminales, dispositivos móviles, entre otros.

Red: Hace referencia a los dispositivos que son utilizados para la conectividad de redes, tales como switches, pasarelas, routers, entre otros.

Tecnología: Equipos que se hacen necesarios, para la gestión de las personas y las operaciones de la misma para el cumplimiento de su objeto social, como lo son teléfonos, impresoras, cableado, servidores, entre otros.

Personal: Aquí se agrupan los colaboradores internos de cada organización, el personal con contrato indirecto, y personal en general que de una u otra manera, accede a información de tipo interna o confidencial de la empresa.

Instalaciones: Son los sitios en los cuales se ubican los sistemas relevantes, tales como oficinas, vehículos, entre otros.

Equipamiento auxiliar: Aquí se agrupan los activos que se utilizan para dar soporte a cada uno de los sistemas de información, y que no fueron relacionados en ninguno de los elementos anteriores. Aquí se pueden encontrar climatizadores, elementos para destruir datos, entre otros).[23]

6.3.6 Gestión de riesgos sobre los activos de información. Tiene como objetivo principal lograr hacer una correcta identificación para los riesgos a los que se exponen los activos de información, esto para elegir los controles más adecuados en temas de seguridad.

La correcta valoración para los riesgos, se fundamenta básicamente en valorar los activos, identificación de riesgos existentes en los procesos responsables y en los requisitos de seguridad que son propios por la operatividad de le empresa.

La metodología utilizada para realizar la valoración de los riesgos se basa en lo recomendado por la ISO 31000:2018 y buenas prácticas direccionadas por la norma ISO 27001:2013.

Se realiza levantamiento de la información con los procesos que hacen parte de la empresa, las entrevistas con el personal y en espacial con los líderes de proceso, permiten tener claridad hacer de cuáles son los riesgos que se han presentado y se pueden presentar, además de las causas que los generan, las vulnerabilidades no subsanadas y los pocos controles que se han implementado sobre los activos de información que se tienen en la empresa.

Durante las entrevistas, de manera coordinada con las gerencias, se definen los riesgos a tratar en el desarrollo del proyecto, tomando como referente aquellos que resultan con una criticidad alta para el proceso y para la empresa.

Se realiza énfasis en la identificación de las amenazas que están relacionadas, pues con ellas se direccionan los controles específicos que se requieren, de acuerdo con el tipo de activo que cada proceso maneja.

La información recopilada con los activos de información, se prioriza de manera que se identifique a cabalidad cual representa mayor riesgo para la empresa.

Se utiliza la metodología establecida y recomendada por la norma técnica colombiana ISO 31000, donde se realiza:

- ✓ Establecimiento de contexto
- ✓ Valoración del riesgo: identificar, estimar y evaluar
- ✓ Tratamiento o gestión de los riesgos encontrados

[23] INCIBE-CERT (2016). Inventario de activos y gestión de la seguridad en SCI

6.3.7 Identificación de amenazas y vulnerabilidades. Las organizaciones, al ejecutar sus actividades, se ven expuestas a diversas situaciones que pueden afectar de manera negativa el ejercicio y cumplimiento de sus obligaciones, una amenaza se define como aquella causa potencial que puede ocasionar daño sobre un activo, mientras que la vulnerabilidad es aquella debilidad que puede tener un activo y que es potencialmente aprovechable por una amenaza [24]

6.3.8 Estimación del Riesgo. Para lograr estimar el riesgo al que se encuentran expuestos cada activo de información, se establece y se pone a disposición de la gerencia las siguientes escalas de valoración, donde una vez aprobada se procedió con su implementación:

Tabla 7 Escala de calificación Impacto, probabilidad, riesgo

IMPACTO	PROBABILIDAD	RIESGO
Muy alto = 5 MA	Seguro= 5	Critico = C
Alto = 4 A	Probable= 4	Importante = I
Medio = 3 M	Posible= 3	Apreciable = A
Bajo = 2 B	Poco probable= 2	Bajo = B
Muy bajo= 1 MB	Muy raro= 1	Despreciable= MB

Fuente. El autor

En la siguiente tabla, se describe la escala utilizada para la valoración de riesgo:

Tabla 8 Nivel de riesgo.

Nivel del riesgo	Rango
Despreciable MB	1 - 4
Bajo B	5 - 9
Apreciable M	10 - 15
Importante A	16 - 20
Critico MA	21 - 25

Fuente el autor

6.3.9 Evaluación del riesgo. Teniendo en cuenta el objeto social de Estrategias Empresariales, calidad, flujo y volumen de información que maneja, una vez definidos los riesgos, se propone a la gerencia a través de este proyecto, realizar evaluación y proponer controles para aquellos que resultan apreciables, importantes y críticos. Con esto se realiza la evaluación y se generan las salvaguardas que más se ajustan a cada activo de manera específica.

[24] Yaneth & Enith (2008) Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO 27001:2013 para la empresa UNISANAR IPS de Quibdó

7. RESULTADOS Y ANALISIS

7.1.1. Clasificación de los activos. Se realiza levantamiento de información inicial o diagnóstico, de manera que se obtiene una base metodológica sobre la cual iniciar el proyecto y de esta forma realizar un comparativo más aterrizado entre lo que se tiene antes de iniciar con la ejecución de actividades comparado con el producto final.

La información se registra y presenta inicialmente a la gerencia, para que se conozca a nivel directivo, el estado que en esta materia se tiene de manera inicial. Así mismo, se hace énfasis en las bondades del trabajo, los resultados que se esperan obtener a corto, mediano y largo plazo, adicionalmente, como esto impacta de manera positiva las operaciones de la empresa.

Este trabajo, además de poder validar el estado inicial en el que se encuentra la empresa en cuanto a la identificación de los activos de información, se direcciona para evidenciar el conocimiento que se tiene en cuanto a la definición de activo de información y su importancia para la ejecución de las actividades propias del negocio en el que se encuentra.

Como parte del desarrollo, integración e implementación de herramientas que le permita a la empresa organizar de manera efectiva sus activos de información, se genera la identificación de activos, realizando un trabajo colaborativo con los líderes de proceso, primero de forma general, donde se explica de manera detallada que son los activos de información, como se gestionan, la necesidad de establecer responsabilidad sobre los mismos, que tan crítico puede resultar para el proceso y luego para la empresa.

Para desarrollar cada una de las actividades definidas en el proyecto, se puso en práctica la metodología descrita, realizando entrevistas sucesivas con los líderes de cada proceso en la empresa, de esta manera se logró realizar una determinación real acerca de los activos manejan, responsabilidades, riesgos identificados y controles implementados.

En estas entrevistas, se logró evidenciar que los responsables de proceso no tenían claridad de cómo realizar una correcta identificación de sus activos de información, aun cuando algunos de ellos manejan los más críticos para la empresa.

Adicional a ello, no se considera el personal como un activo de información ni la documentación física, tomando siempre como referencia únicamente los equipos tecnológicos con los cuales desarrollan sus operaciones.

Los pocos controles implementados, son los direccionados por el proceso de tecnología, quienes aplicaron los que consideran para los equipos y herramientas como lo son contraseñas de accesos, roles, permisos.

No se encontraron controles específicos del proceso, solo los generales para la

empresa y los que algún miembro del equipo de trabajo, conocía por su experiencia que deberían tener de acuerdo con la documentación y actividades que se realizan de manera particular.

Se resalta la importancia de identificar los activos del proceso con el fin de incluirlos en el desarrollo de la metodología y puedan evaluarse los riesgos y controles implementados o por implementarse, de esta manera se estará mejor preparado ante cualquier materialización de amenazas que puedan afectar de manera significativa el desarrollo de la operación de verse involucrados los activos que se manejan en el proceso.

Una vez definido los activos de información, se consolidan los datos por cada uno de los procesos, se realiza la identificación correspondiente y se procede con el registro de la información.

A manera de resumen, para la identificación de los activos se aplica:

- ✓ Identificar qué información se genera en cada proceso de la empresa
- ✓ Identificar qué información usa cada proceso que se genere en otros procesos, esto para determinar la interacción existente.
- ✓ Definir la clasificación de los activos identificados.
- ✓ Realizar una correcta identificación por cada uno de los activos.
- ✓ Definir la responsabilidad sobre los activos y generar proceso de mantenimiento y actualización.

Este último ítem, responsabilidad del activo, para la empresa se tiene definido que sea el dueño del proceso en que se genera, por lo tanto, será este quien decida que personal accede a la información, pues será su responsabilidad toda la gestión que se realice sobre los activos a su cargo. Con esto se logra que cada activo, tenga una cabeza visible y la responsabilidad en el manejo pueda estar segregada entre el personal que lo gestiona, siendo su dueño el que permita esa gestión, de acuerdo con las actividades realizadas.

Se establecieron los 14 activos de información claves sobre los cuales se centraliza la operación de Estrategias Empresariales. Estos permiten que las actividades se desarrollen en los términos requeridos, por lo que una afectación sobre estos, hacen que de manera significativa la empresa no pueda cumplir con el servicio tanto a nivel interno como de cara hacia cada uno de sus clientes.

El 90% de la información que la empresa gestiona para cumplir con sus responsabilidades específicas, se encuentra de manera digital o se digitaliza, por lo que resultan críticos, aquellos activos que se utilizan para su gestión.

De esta manera, el trabajo se centralizo sobre los activos importantes, apreciables y críticos que requieren consolidar mecanismos de protección a través de controles y definición de responsabilidades.

Definir la responsabilidad sobre los activos de información, permite que se

establezca la apropiación necesaria para que los controles que se definan, se implementen de manera efectiva pero ante todo, se realice el seguimiento y monitoreo. Esto es lo que se explica y se expone a cada responsable con el fin de poder definir los riesgos y controles implementados o potenciales de implementar.

Como resultado de las entrevistas, se presenta el resumen gráfico de lo obtenido:

Tabla 9 Procesos y personal entrevistado

PROCESO	*CARGO*
Auditoria	Gerente y director
Tic	Gerente y director
Comercial	Gerente y director
Financiero y administrativo	Gerente y director
Jurídico	Gerente y director
Tesorería	Gerente y director
TOTAL: 6 PROCESOS	**TOTAL: 12 PERSONAS**

Fuente: el autor

Tabla 10 Tipo de información manejada por proceso

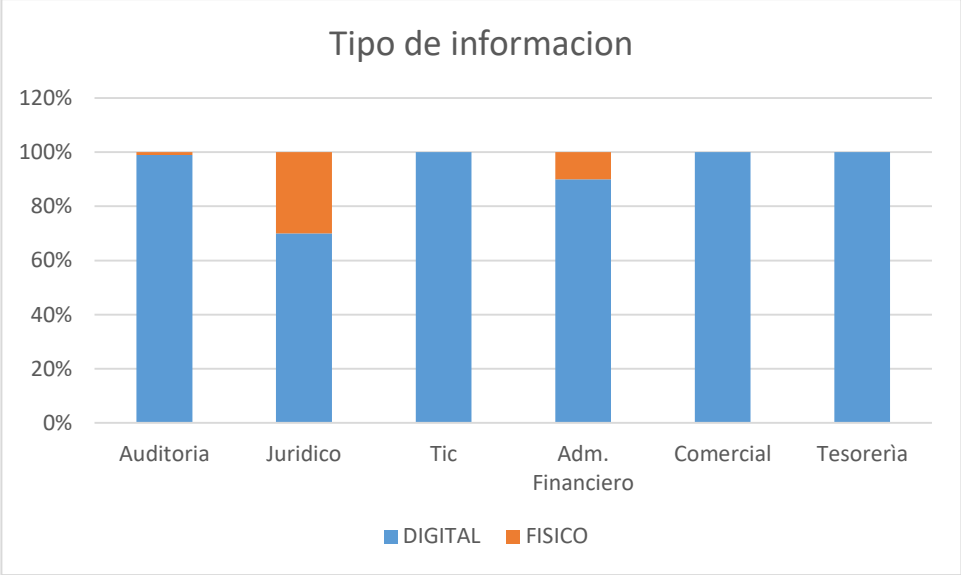
PROCESO	*TIPO DE INFORMACIÒN*
Auditoria	Cifras, datos personales
Tic	Configuración de herramientas, usuarios, bases de datos.
Comercial	Información de clientes, campañas publicitarias
Financiero y administrativo	Cifras, cuentas, estados financieros clientes
Jurídico	Procesos judiciales, disciplinarios y contratación.
Tesorería	Cifras, cuentas, información de clientes y proveedores
TOTAL: 6 PROCESOS	**TOTAL: 12 PERSONAS**

Fuente: el autor

Como se puede observar, la responsabilidad recae sobre la gerencia y dirección de cada proceso, por lo que las entrevistas se enfocaron en estos, quienes lograron identificar el tipo de información manejada y que tan relevante resulta para sus actividades.

En cuanto a cómo se maneja la información, se obtuvo el siguiente resultado:

Figura 2 Medio de manejo de información



Fuente: el autor

Como se puede evidenciar la mayoría de la información se gestiona de manera digital, a través de los diferentes aplicativos y herramientas que se manejan de manera interna, las cuales se ponen a disposición de los procesos. Lo único que se maneja en físico para el caso del administrativo corresponde a las hojas de vida del personal, para el caso del proceso jurídico, son los contratos firmados con los clientes.

De esta manera se observa que los activos donde se maneja la información digital, resulta crítico para el funcionamiento de la empresa.

Cuando se consulto acerca de cuáles son los activos de información que manejan, seis (6) de los seis (6) procesos encuestados no los identificaron de manera clara, por lo que después de la explicación, se logró obtener efectivamente cuales eran los que tiene realmente en el proceso.

En la tabla siguiente, se realiza el consolidado indicando el registro de los activos que fueron identificados:

Tabla 11 Identificación de activos.

IDENTIFICACIÒN DEL ACTIVO DE INFORMACIÒN				PROPIEDAD DEL ACTIVO		UBICACIÒN		NIVEL DE CLASIFICACIÒN DE LA INFORMACIÒN
ITEM	**PROCESO**	**NOMBRE DEL ACTIVO DE INFORMACIÒN**	**Descripción del activo**	**Propietario**	**Custodio**	**Físico**	**Digital**	**Confidencial, restringida, interno, público**
1	Comercial	Jaspersoft Comercial	Contiene información operacional que permite estadísticamente validar el comportamiento de los servicios ofrecidos	Director comercial	Director comercial		x	Restringida
2	Comercial	Trasfer de archivos	Herramienta destinada por la empresa para compartir archivos estadísticos y consolidativos de la operación propia y de los clientes	Directos comercial	Director comercial		x	Restringida
3	Financiero	Manager ERP	Contiene la información contable	Gerente Financiero	Director Financiero		x	Restringida
4	Financiero	Jaspersoft Financiero	Contiene los reportes de las transacciones contables realizadas, ordenados por empresa, concepto, cuenta y fecha	Gerente Financiero	Director Financiero		x	Restringida
5	TIC	Servidor Operacional	Contiene la información consolidada de los servicios, clientes, operaciones y transacciones	Gerente de TIC	Director de TIC		x	Restringida
6	TIC	Servidor de correo	Aloja los dominios, cuentas, usuarios y correos gestionados	Gerente de TIC	Coordinador de infraestructura y telecomunicaciones		x	Restringida
7	TIC	Controlador de dominio	Aloja la información de los equipos y la red	Gerente de TIC	Coordinador de infraestructura y telecomunicaciones		x	Restringida

8	TIC	Fortigate	Contiene la IP de los equipos y políticas de seguridad, control de navegación e intrusos	Gerente de TIC	Coordinador de infraestructura y telecomunicaciones		x	Restringida
9	TIC	Switch	Conexión de los equipos	Gerente de TIC	Coordinador de infraestructura y telecomunicaciones		x	Restringida
10	TIC	Router	Distribución web	Gerente de TIC	Coordinador de infraestructura y telecomunicaciones		x	Restringida
11	TIC	Intranet	Contiene los datos del personal de la empresa y clientes, aloja información interna	Gerente de TIC	Coordinador de infraestructura y telecomunicaciones		x	Restringida
12	TIC	Binaps	Permite la gestión documental	Gerente de TIC	Coordinador de infraestructura y telecomunicaciones		x	Restringida
13	Administrativo	Personal Clave	Personas que por su grado de preparación y cargo, se encargan de administrar información y procesos críticos	Gerente administrativo	Coordinador de RH		x	Restringida
14	Todos	PC	Permite la gestión operativa, contiene los archivos de gestión del personal	Todo el personal vinculado	Todo el personal vinculado		X	Restringida

Fuente el autor

Realizando el análisis de la información consignada en la anterior tabla, se logra evidenciar, la categoría en la cual se encuentra cada activo de información, su clasificación, criticidad, pero además, los procesos que tienen relación directa con cada uno de estos.

Efectivamente por el objeto social de la empresa, se observa que los activos críticos son aquellos utilizados en la gestión de la información a nivel digital, por lo que resultará critico el control sobre las políticas, configuraciones, accesos, roles y perfiles del personal que accede y administra cada uno de ellos.

Adicionalmente, se pregunto acerca de cuáles controles se tienen documentados, si estos documentos están socializados y evaluados por el personal que conforma sus equipos de trabajo:

Tabla 12 Generalidad de controles por proceso.

CONTROLES		
Proceso	Documentado	Socializado
Auditoria	No	No
Jurídico	No	No
Tic	No	No
Adm Financiero	No	No
Comercial	No	No
Tesorería	No	No

Fuente el autor.

Al indagar acerca de los controles que se tienen, todos los encuestados concluyeron en que se siguen los controles que son implementados por el proceso de tecnología, en cuyo caso hacen referencia a:

- ✓ Usuario
- ✓ Contraseña
- ✓ Política para solicitud de cambio o reasignación de usuarios y contraseñas

A pesar que cada líder o responsable de proceso es consciente de la información que maneja, se debió hacer una exposición de las diferentes clasificaciones de la información, para que estos lograran identificar en cuál de ellas se encasilla la información que utilizan en el desarrollo de sus actividades.

El inventario de los activos que son identificados, se registran en el formato establecido y aprobado por la Gerencia de la empresa:

Tabla 13 Formato registro activos de información.

Ítem	NOMBRE	TIPO DE ACTIVO	CATEGORIA	CLASIFICACIÓN	PROCESOS RELACIONADOS	CRITICIDAD
1	Jaspersoft Comercial	Software	Aplicaciones	Restringida	Comercial, financiero	Alta
2	Trasferencia de archivos	Software	Aplicaciones	Restringida	Comercial y Jurídico	Media
3	Manager ERP	Software	Aplicaciones	Restringida	Financiero y Tesorería	Alta
4	Jaspersoft Financiero	Software	Aplicaciones	Restringida	Financiero	Alta
5	Servidor Operacional	Software	hardware	Restringida	Todos los procesos de la empresa	Alta
6	Servidor de correo	Software	hardware	Restringida	Todos los procesos de la empresa	Media
7	Controlador de dominio	Software	Red	Restringida	Todos los procesos de la empresa	Alta
8	Fortigate	RED	Red	Restringida	Todos los procesos de la empresa	Media
9	Switch	RED	Red	Restringida	Todos los procesos de la empresa	Alta
10	Router	RED	Red	Restringida	Todos los procesos de la empresa	Alta
11	Intranet	Software	Red	Restringida	Todos los procesos de la empresa	Baja
12	Binaps	Software	Red	Restringida	Todos los procesos de la empresa	Baja

13	Personal Clave	Personal	Personal	Restringida	Todos los procesos de la empresa	Alta
14	PC	Hardware	Hardware	Restringida	Todos los procesos de la empresa	Alta

Fuente el autor

A continuación se establece la clasificación para cada uno de los activos de información según los tres pilares fundamentales de la información:

Tabla 14 Clasificación de los activos por pilar de información.

Ítem	NOMBRE	TIPO DE ACTIVO	CLASIFICACIÓN CONFIDENCIALIDAD	CLASIFICACIÓN DISPONIBILIDAD	CLASIFICACIÓN INTEGRIDA	CRITICIDAD
1	Jaspersoft Comercial	Software	Información Restringida	Alta	Alta	Alta
2	Trasferencia de archivos	Software	Información Restringida	Alta	Alta	Media
3	Manager ERP	Software	Información Restringida	Alta	Alta	Alta
4	Jaspersoft Financiero	Software	Información Restringida	Alta	Alta	Alta
5	Servidor Operacional	Software	Información Restringida	Alta	Alta	Alta
6	Servidor de correo	Software	Información Restringida	Alta	Alta	Media
7	Controlador de dominio	Software	Información Restringida	Alta	Alta	Alta
8	Fortigate	RED	Información Restringida	Alta	Alta	Media

9	Switch	RED	Información Restringida	Alta	Alta	Alta
10	Router	RED	Información Restringida	Alta	Alta	Alta
11	Intranet	Software	Información Restringida	Alta	Alta	Baja
12	Binaps	Software	Información Restringida	Alta	Alta	Baja
13	Personal Clave	Personal	Información Restringida	Alta	Alta	Alta
14	PC	Hardware	Información Restringida	Alta	Alta	Alta

Fuente el autor.

7.1.2. Identificación de riesgos. Siguiendo la metodología Magerit, se realizó evaluación cuantitativa de los activos identificados, teniendo en cuenta la escala definida,

Tabla 15 Valoración cuantitativa del riesgo

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
[pc] Equipos de computo	CRITICO	25	20	25	20	20	22
[network][switch]Switches	IMPORTANTE	15	15	20	15	15	16
[network][router] Router Internet	IMPORTANTE	20	20	20	20	20	20
[Media] soporte de información - Jaspersoft	CRITICO	20	25	25	20	25	23
[COM] REDES DE COMUNICACIONES - Trasfer de archivos	IMPORTANTE	15	9	15	20	20	16
[Media] SOPORTE DE INFORMACIÓN - Manager ERP	CRITICO	25	25	25	25	25	25
[hw] EQUIPAMENTO INFORMATICO Servidor operacional	APRECIABLE	15	9	15	9	9	11

[hw] EQUIPAMENTO INFORMATICO Servidor de correo electrónico	BAJO	9	9	9	9	9	9
[SW] SOFTWARE - Controlador de dominio	IMPORTANTE	20	20	9	20	20	18
[HW] EQUIPAMENTO INFORMÁTICO - Fortianalyzer	CRITICO	25	25	25	25	25	25
[S] SERVICIOS - Intranet	IMPORTANTE	20	20	15	20	20	19
[S] SERVICIOS - BINAPS	CRITICO	25	25	25	15	20	22
[int] Servidor de Impresión	APRECIABLE	15	15	4	9	9	10
[des] Personal TI	IMPORTANTE	20	15	9	20	20	17

Fuente el autor.

De lo anterior, se realiza la validación de aquellos activos cuyo valor resulta apreciable, importante y crítico, pues en entrevista con la gerencia general, son los que se atenderán de forma prioritaria y sobre los que se destinaran los recursos necesarios en el corto y mediano plazo. Asumiendo como apetito de riesgo aquellos cuya calificación ha resultado baja o muy baja.

Se observa como resulta crítica la información en cada proceso, esto es, porque los datos manejados constan de los propios, de sus clientes y proveedores. En estos, se aloja información sensible como datos personales, financieros, de configuraciones de seguridad para el acceso a herramientas corporativas y de procesamiento de información.

Uno de los activos más importantes, hace referencia al personal clave, pues tiene acceso a los datos e información clasificada como restringida de la empresa, para ello, se han establecido clausulas especiales de confidencialidad, soportada con componentes legales y económicos ante la evidencia de algún incumplimiento.

El manager ERP, resulta crítico para la operación, pues contiene todo el sistema de información contable con el que se llevan a cabo las transacciones financieras corporativas. El personal que lo manipula, es considerado como crítico para el proceso y son de los que más controles de monitoreo requieren.

Al ser una empresa que dedicada a los servicios de consultoría y asesoría, Estrategias Empresariales hace uso intensivo del correo electrónico corporativo y una herramienta para la trasferencia de información y archivos procesados con datos bastante sensibles, se utiliza un proceso de cifrado con doble clave, para los documentos que consideran.

Se emplean activos cuya configuración resulta fundamental para la operación y seguridad de la información, entre estos observamos el Fortigate, switch, router e inclusive el controlador de dominio, pues con estos se controla el personal que tiene permitido acceder a sistemas de información propios de la empresa, se aplican controles y políticas, estableciendo las restricciones que son direccionadas por la gerencia de tecnología con su equipo de trabajo y aprobadas por la gerencia general.

Uno de los puntos clave, además de lo anteriormente mencionado, es la distribución e identificación que se tiene sobre las estaciones de trabajo o pc que utiliza el personal, pues es a través de estos que acceden a la información. Se tiene diseño de diagrama de red, con sus respectivos puntos de conexión, IP asignada por colaborador. Para un mejor control, toda vez que cada uno tiene diferentes responsabilidades, se tiene diferenciado por proceso y a cada proceso se le aplican las reglas que le son correspondientes.

Por último, se estableció como alta la clasificación de disponibilidad e integridad y como restringida la confidencialidad, puesto que cada activo resulta fundamental para la operación de los procesos críticos definidos por la empresa, de esta manera se concientiza al personal sobre la importancia que tienen y como debe propenderse por su custodia de manera adecuada.

7.1.3. Amenazas y Vulnerabilidades. Las amenazas a las cuales se ve enfrentada Estrategias Empresariales, y que ponen en riesgo su operación, pueden observarse en la siguiente tabla:

Tabla 16 Amenazas y Vulnerabilidades.

No.	Vulnerabilidad	Amenaza	Descripción Amenaza
1	Falta de actualizaciones	Permeabilidad para el ingreso de malware	Acceso a información confidencial por parte de terceros no autorizados
2	Desconocimiento de las políticas de seguridad	Ingeniería social sobre el personal	Falta de medidas preventivas
3	Fallas en el fluido eléctrico	Pérdida o daño de los equipos	Perdida de la información y hardware
4	Uso de medios extraíbles sobre los equipos	Pérdida de información, ingreso de virus.	Propagación de software dañino para los activos
5	Software no licenciado	Programas sin soporte que garantice la seguridad del sistema	Posibles sanciones legales por utilizar software sin licencia.
6	Falta de copias de seguridad para la información	Inexistencia de información de respaldo	Perder la información de los procesos ocasiona fallas en la operación
7	Error en la configuración y aplicación de las políticas de seguridad	Facilidad para la intrucción de los sistemas de la empresa por externos	Posibilidad de acceso por terceros no autorizados al sistema
8	Control para el acceso a las comunicaciones por personal ajeno a la empresa	Acceso de personal no autorizado a la configuración de la red	Permitir acceso a personal no autorizado puede causar des configuraciones.
9	Conectividad a la red de equipos externos	Inadecuada configuración de la red para evitar conexiones de externos	Personal externo o interno no autorizado puede acceder a la red

Fuente el autor.

Al aterrizar estas amenazas descritas por los líderes de proceso y haciendo una integración con las amenazas conocidas y relacionadas con la metodología MAGERIT, se logra especificar aquellas que aplican por cada activo identificado. Se relacionan en la siguiente tabla los resultados obtenidos:

Tabla 17 Amenazas y vulnerabilidades

Activos de Información	No. De Amenazas y Vulnerabilidades	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	RIESGOS
[HW] EQUIPAMENTO INFORMÁTICO	1	[pc] Equipos de computo	22	[N1] Fuego	Falta de extintores específicos para equipos eléctricos	Perdida de equipos, perdida de información.
[HW] EQUIPAMENTO INFORMÁTICO	2	[pc] Equipos de computo	22	[N2] Daños por agua	Derrame de líquidos que usa el personal, falta de mantenimiento de tuberías.	Perdida de equipos, perdida de información, divulgación de información
[HW] EQUIPAMENTO INFORMÁTICO	3	[pc] Equipos de computo	22	[I5] Avería de origen físico o lógico	Daño en componentes, caídas, golpes.	Perdida de equipos, perdida de información
[HW] EQUIPAMENTO INFORMÁTICO	4	[pc] Equipos de computo	22	[I6] Corte del suministro eléctrico	Operatividad dependiente de la corriente eléctrica. Sin batería.	Daño sobre los equipos, interrupción de la operación de la empresa
[HW] EQUIPAMENTO INFORMÁTICO	5	[pc] Equipos de computo	22	[I7] Condiciones inadecuadas de temperatura o humedad	Falla en sistema de aire acondicionado, falta de medidores de temperatura y humedad.	Desgaste progresivo acelerado sobre los equipos, daños sobre la información contenida
[HW] EQUIPAMENTO INFORMÁTICO	6	[pc] Equipos de computo	22	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Fallo en hardware o Software	Pérdida de información, inoperatividad, pérdidas económicas
[HW] EQUIPAMENTO INFORMÁTICO	7	[pc] Equipos de computo	22	[E24] Caída del sistema por agotamiento de recursos	Falta de actualización de hardware de los equipos o cambio por obsolescencia.	Retrasos en la operación y prestación de los servicios. Pérdidas económicas.
[HW] EQUIPAMENTO INFORMÁTICO	8	[pc] Equipos de computo	22	[E25] Pérdida de equipos	Equipos sin guaya de seguridad, acceso a personal no autorizado.	Pérdidas económicas, alteración y consulta de la información por parte de personal no autorizado.
[HW] EQUIPAMENTO INFORMÁTICO	9	[pc] Equipos de computo	22	[A7] Uso no previsto	Falta de control acceso a personal a zonas no autorizadas, equipos disponibles para público.	Perdida de equipos, perdida de información, divulgación de información, alteración de información

[HW] EQUIPAMENTO INFORMÁTICO	10	[pc] Equipos de computo	22	[A11] Acceso no autorizado	Falta de control para el acceso de personal a zonas no autorizadas	Alteración y consulta de la información por parte de personal no autorizado.
[HW] EQUIPAMENTO INFORMÁTICO	11	[pc] Equipos de computo	22	[A25] Robo	Falta de control acceso a personal a zonas no autorizadas. Equipos de uso fuera de oficina.	Consulta de la información por parte de personal no autorizado, por inexistencia de controles de acceso.
[HW] EQUIPAMENTO INFORMÁTICO	12	[network][switch]Switches	16	[N1] Fuego	Se tienen extintores tipo ABC, los cuales no son específicos para eléctricos, por lo que puede presentarse daño.	Pérdidas económicas por cortos que produzcan llamas
[HW] EQUIPAMENTO INFORMÁTICO	13	[network][switch]Switches	16	[N2] Daños por agua	Derrame de vaso de agua, falta de mantenimiento de tuberías.	Pérdida de equipos
[HW] EQUIPAMENTO INFORMÁTICO	14	[network][switch]Switches	16	[I5] Avería de origen físico o lógico	Daño en componentes, caídas, golpes.	Suspensión de operaciones o actividades críticas de la empresa
[HW] EQUIPAMENTO INFORMÁTICO	15	[network][switch]Switches	16	[I6] Corte del suministro eléctrico	Falta de contingencia en sistema eléctrico	Perdida de equipos, perdida de información, divulgación de información
[HW] EQUIPAMENTO INFORMÁTICO	16	[network][switch]Switches	16	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Fallo en hardware o Software	Fallo de equipos, equipos vulnerables a ataques
[HW] EQUIPAMENTO INFORMÁTICO	17	[network][switch]Switches	16	[A11] Acceso no autorizado	Falta de control acceso a personal a zonas no autorizadas y filtrado de credenciales de acceso.	Perdida de equipos, perdida de información, divulgación de información, alteración de información
[HW] EQUIPAMENTO INFORMÁTICO	18	[network][switch]Switches	16	[A25] Robo	Falta de control acceso a personal a zonas no autorizadas.	Perdida de equipos, perdida de información, divulgación de información, alteración de información
[HW] EQUIPAMENTO INFORMÁTICO	19	[network][router] Router Internet	20	[N1] Fuego	Se tienen extintores tipo ABC, los cuales no son específicos para eléctricos, por lo que puede presentarse daño.	Daños de equipos, perdida de información
[HW] EQUIPAMENTO INFORMÁTICO	20	[network][router] Router Internet	20	[N2] Daños por agua	Falta de mantenimiento de tuberías.	Daños de equipos, perdida de información
[HW] EQUIPAMENTO INFORMÁTICO	21	[network][router] Router Internet	20	[I5] Avería de origen físico o lógico	Daño en componentes, caídas, golpes.	Pérdidas por falta de acceso a la red corporativa que impida la operación
[HW] EQUIPAMENTO INFORMÁTICO	22	[network][router] Router Internet	20	[I6] Corte del suministro eléctrico	Falta de contingencia en sistema eléctrico	Falla en la operación por imposibilidad de acceder a la red corporativa y fuentes externas

[HW] EQUIPAMENTO INFORMÁTICO	23	[network][router] Router Internet	20	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Fallo en hardware o Software	Pérdidas por falta de disponibilidad para el personal administrativo
[HW] EQUIPAMENTO INFORMÁTICO	24	[network][router] Router Internet	20	[A11] Acceso no autorizado	Falta de control para el acceso por parte de personal no autorizado.	Acceso a la configuración del dispositivo.
[HW] EQUIPAMENTO INFORMÁTICO	25	[network][router] Router Internet	20	[A7] Uso no previsto	Uso para fines no corporativos	Acceso a la red corporativa para fines no corporativos
[HW] EQUIPAMENTO INFORMÁTICO	26	[network][router] Router Internet	20	[A25] Robo	Falta de control acceso a personal a zonas no autorizadas.	Pérdida económica por robo de dispositivo
[HW] EQUIPAMENTO INFORMÁTICO	27	[Media] soporte de información - Jaspersoft	23	[I5] Avería de origen físico o lógico	Mala configuración en el acceso	Acceso a la información sensible de la empresa por parte de personal no autorizado
[HW] EQUIPAMENTO INFORMÁTICO	28	[Media] soporte de información - Jaspersoft	23	[I6] Corte del suministro eléctrico	Falta de contingencia en sistema eléctrico	Imposibilidad de acceder a la información crítica para la operación de la empresa
[HW] EQUIPAMENTO INFORMÁTICO	29	[Media] soporte de información - Jaspersoft	23	[A11] Acceso no autorizado	Falta de control acceso y filtrado de credenciales de acceso. Falta de actualizaciones firmware	Divulgación de información o alteración de la misma.
[HW] EQUIPAMENTO INFORMÁTICO	30	[Media] soporte de información - Jaspersoft	23	[A7] Uso no previsto	Falta de control acceso a personal a zonas no autorizadas	Uso de la información para beneficio de terceros
[HW] EQUIPAMENTO INFORMÁTICO	31	[COM] REDES DE COMUNICACIONES - Trasfer de archivos	16	[I8] Fallo de servicios de comunicaciones	Información compartida sin encriptar los datos	Interceptación de información sensible que sea compartida por este medio
[HW] EQUIPAMENTO INFORMÁTICO	32	[COM] REDES DE COMUNICACIONES - Trasfer de archivos	16	[E14] Escapes de información	Envió de información sin control por parte del líder de proceso	Fuga de información sensible de la empresa.
[HW] EQUIPAMENTO INFORMÁTICO	33	[COM] REDES DE COMUNICACIONES - Trasfer de archivos	16	[I5] Avería de origen físico o lógico	Daño en componentes, deterioro de los mismos.	Pérdida de información
[HW] EQUIPAMENTO INFORMÁTICO	34	[COM] REDES DE COMUNICACIONES - Trasfer de archivos	16	[I6] Corte del suministro eléctrico	Falta de contingencia en sistema eléctrico	Imposibilidad de envío de información crítica para la operación de la empresa y sus clientes
[HW] EQUIPAMENTO INFORMÁTICO	35	[COM] REDES DE COMUNICACIONES - Trasfer de archivos	16	[A19] Divulgación de información	Falla en aplicar controles de seguridad para el envío de información	Acceso a la información cuyo envío no se configure en las condiciones de seguridad adecuadas
[HW] EQUIPAMENTO INFORMÁTICO	36	[COM] REDES DE COMUNICACIONES - Trasfer de archivos	16	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Fallo en hardware o Software	Fallo del aplicativo por falta de control sobre las actualizaciones

[HW] EQUIPAMENTO INFORMÁTICO	37	[Media] SOPORTE DE INFORMACIÓN - Manager ERP	25	[E4] Errores de configuración	Varios usuarios con rol de administrador en el sistema	Cambios en la seguridad o configuración de la herramienta, ocasionando pérdida de integridad en la información.
[HW] EQUIPAMENTO INFORMÁTICO	38	[Media] SOPORTE DE INFORMACIÓN - Manager ERP	25	[A11] Acceso no autorizado	Falta de control en la asignación de usuarios y privilegios	Acceso a la información contable por parte de personal no autorizado
[HW] EQUIPAMENTO INFORMÁTICO	39	[Media] SOPORTE DE INFORMACIÓN - Manager ERP	25	[A7] Uso no previsto	Alteración de la información por personal con rol adm.	Fuga de información sensible de la empresa.
[HW] EQUIPAMENTO INFORMÁTICO	40	[Media] SOPORTE DE INFORMACIÓN - Manager ERP	25	[A15] Modificación deliberada de la información	Falta de controles de acceso.	Pérdida de integridad de la información para favorecimientos personales o de terceros
[HW] EQUIPAMENTO INFORMÁTICO	41	[hw] EQUIPAMENTO INFORMATICO Servidor operacional	11	[N1] Fuego	Falta de extintores específicos para evitar daño en caso de fuego en el servidor	Daños irreversibles en el servidor y pérdida de operación
[HW] EQUIPAMENTO INFORMÁTICO	42	[hw] EQUIPAMENTO INFORMATICO Servidor operacional	11	[N2] Daños por agua	Falta de mantenimiento de tuberías.	Daños sobre el componente eléctrico
[HW] EQUIPAMENTO INFORMÁTICO	43	[hw] EQUIPAMENTO INFORMATICO Servidor operacional	11	[I5] Avería de origen físico o lógico	Daño en componentes, por mala manipulación.	Pérdida de información
[HW] EQUIPAMENTO INFORMÁTICO	44	[hw] EQUIPAMENTO INFORMATICO Servidor operacional	11	[I6] Corte del suministro eléctrico	Falta de contingencia en sistema eléctrico	Daño sobre la información contenida por cortos eléctricos
[HW] EQUIPAMENTO INFORMÁTICO	45	[hw] EQUIPAMENTO INFORMATICO Servidor operacional	11	[A4] Manipulación de la configuración	Acceso al servidor por falta de control en los usuarios administradores	Acceso o alteración de la información.
[HW] EQUIPAMENTO INFORMÁTICO	46	[hw] EQUIPAMENTO INFORMATICO Servidor operacional	11	[E1] Errores de los usuarios	Manipulación errónea del servidor	Pérdida de integridad de la información para favorecimientos personales o de terceros
[HW] EQUIPAMENTO INFORMÁTICO	47	[hw] EQUIPAMENTO INFORMATICO Servidor de correo electrónico	9	[I8] Fallo de servicios de comunicaciones	Falta de acceso al correo corporativo	Falla en la operación por el no envío de información
[HW] EQUIPAMENTO INFORMÁTICO	48	[hw] EQUIPAMENTO INFORMATICO Servidor de correo electrónico	9	[E7] Deficiencias en la organización	Fallas en la comunicación	Retrasos en la operación de procesos que requieren activo el correo electrónico para su operación.
[HW] EQUIPAMENTO INFORMÁTICO	49	[hw] EQUIPAMENTO INFORMATICO Servidor de correo electrónico	9	[A5] Suplantación de la identidad del usuario	Falta de control sobre la información que se envía o se recibe	Envió y recepción de malware que afecte la red corporativa

[HW] EQUIPAMENTO INFORMÁTICO	50	[SW] SOFTWARE - Controlador de dominio	18	[A30] Ingeniería social	Falta de implementación de políticas de seguridad corporativa	Ingreso de malware al sistema o acceso a información sensible por parte de terceros
[HW] EQUIPAMENTO INFORMÁTICO	51	[SW] SOFTWARE - Controlador de dominio	18	[A4] Manipulación de la configuración	Alteración de las políticas configuradas	Vulnerabilidad de la información de la información almacenada en los equipos.
[HW] EQUIPAMENTO INFORMÁTICO	52	[SW] SOFTWARE - Controlador de dominio	18	[A15] Modificación deliberada de la información	Alteración de las funcionalidades para la administración de los equipos	Acceso a información corporativa, por reglas no aplicadas sobre los equipos
[HW] EQUIPAMENTO INFORMÁTICO	53	[HW] EQUIPAMENTO INFORMÁTICO - Fortianalyzer	25	[I5] Avería de origen físico o lógico	Daño en componentes	Ingreso de malware por políticas inactivas a nivel de red y seguridad perimetral
[HW] EQUIPAMENTO INFORMÁTICO	54	[HW] EQUIPAMENTO INFORMÁTICO - Fortianalyzer	25	[E2] Errores del administrador	Falta de políticas que impidan vulnerabilidad	Vulnerabilidad de la red corporativa
[HW] EQUIPAMENTO INFORMÁTICO	55	[HW] EQUIPAMENTO INFORMÁTICO - Fortianalyzer	25	[E20] Vulnerabilidades de los programas (software)	Falla en la configuración de acceso, políticas y monitoreo	Acceso de terceros a la red corporativa, vulnerabilidad de la información
[HW] EQUIPAMENTO INFORMÁTICO	56	[HW] EQUIPAMENTO INFORMÁTICO - Fortianalyzer	25	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Fallo en hardware o Software	Vulnerables a ataques por falta de seguridad o actualización de componentes y software
[HW] EQUIPAMENTO INFORMÁTICO	57	[S] SERVICIOS - Intranet	19	[A5] Suplantación de la identidad del usuario	Falta de credenciales de acceso interno	Divulgación de información en la red interna
[HW] EQUIPAMENTO INFORMÁTICO	58	[S] SERVICIOS - BINAPS	22	[A11] Acceso no autorizado	Acceso a la información por credenciales débiles en seguridad	Consulta, descarga y reenvío de documentación interna de la empresa
[HW] EQUIPAMENTO INFORMÁTICO	59	[S] SERVICIOS - BINAPS	22	[A19] Divulgación de información	Control débil para el ingreso a la administración de la herramienta	Uso de información para beneficios particulares
[HW] EQUIPAMENTO INFORMÁTICO	60	[int] Servidor de Impresión	10	[A5] Suplantación de la identidad del usuario	Contraseñas poco seguras y fácilmente descifrables	Impresión de información de la empresa por personal no autorizado
[HW] EQUIPAMENTO INFORMÁTICO	61	[int] Servidor de Impresión	10	[I8] Fallo de servicios de comunicaciones	Falla en el servicio por conexión cableada	Falla en la operación por documentos que sean requeridos ante indisponibilidad en el servicio
[HW] EQUIPAMENTO INFORMÁTICO	62	[int] Servidor de Impresión	10	[I6] Corte del suministro eléctrico	Indisponibilidad por falla en el fluido eléctrico	Falla en la operación por documentos que sean requeridos ante indisponibilidad en el servicio

[HW] EQUIPAMENTO INFORMÁTICO	63	[des] Personal TI	17	[A28] Indisponibilidad del personal	Falla en la funcionalidad de las herramientas y aplicaciones de la operación	Pérdida de operación, ante un fallo que no pueda ser corregido a nivel de aplicación o telecomunicaciones
[HW] EQUIPAMENTO INFORMÁTICO	64	[des] Personal TI	17	[E19] Fugas de información	Falta de controles en el ingreso del personal de TIC a la información y aplicaciones corporativas	Fuga de información sensible de la empresa.
[HW] EQUIPAMENTO INFORMÁTICO	65	[des] Personal TI	17	[A3] Manipulación de los registros de actividad (log)	Imposibilidad de conocer los cambios que se realizan sobre el sistema	Pérdida de integridad de la información, modificaciones en la configuración de bases de datos
[HW] EQUIPAMENTO INFORMÁTICO	66	[des] Personal TI	17	[A6] Abuso de privilegios de acceso	Permisos amplios sobre usuarios específicos en TIC	Acceso y modificación de la información sin que se deje rastro de lo realizado
[HW] EQUIPAMENTO INFORMÁTICO	67	[des] Personal TI	17	[A10] Alteración de secuencia	Falta de log en los desarrollos e implementaciones realizadas sobre las herramientas y contenedores de bases de datos.	Desvíos de información sensible de la empresa, ejecución de secuencias no previstas.

Fuente el autor.

Al no contar con un proceso de control sobre las licencias que se tienen para las herramientas y aplicativos utilizados, se tiene riesgo de seguridad ante un posible vencimiento de las mismas.

Se observó una vulnerabilidad grande en el tema de actualizaciones, pues una de las políticas aplicadas es la no instalación automática de las mismas, requiriendo personal con rol de administrador para que estas sean instaladas de manera correcta en cada uno de los equipos de la empresa.

Dentro de las recomendaciones que se realizaron como producto del presente trabajo y que fue aceptada por la gerencia, fue el programar las actualizaciones para su instalación de manera automática, toda vez que se expuso que con estas se instalan mejoras y parches de seguridad que resultan ser importantes para salvaguardar la información de los activos de información y sus aplicaciones que permiten la gestión.

No se evidenció un trabajo específico para generar cultura de seguridad sobre el personal, lo que es sin lugar a dudas, uno de los aspectos que resultan más críticos observados en el desarrollo del presente trabajo, pues a pesar de los controles, inversión en dispositivos y herramientas que ha realizado la administración, el factor humano resulta permeable ante el desconocimiento de las mínimas medidas de seguridad a tener en cuenta en lo que tiene que ver con la seguridad de los activos de información en la cual cada uno tiene injerencia directa e indirecta.

Otro de los aspectos evidenciados, fue el alto uso de medios extraíbles para la gestión de la información, esto sin que haya de por medio una política estricta que regule el empleo de estos, hace que el riesgo sobre los activos y su información sea muy alta por diferentes situaciones, ya sea por acceso no autorizado como por ingreso de malware entre algunos otros. Al realizar el análisis con la gerencia, se determinó restringir el uso solo para los líderes de proceso. Adicional, se recomendó establecer como proyecto de implementación, servicio de trabajo en línea con servidor propio para el almacenamiento de información, para de esta manera bloquear los puertos para medios extraíbles.

Una de las grandes falencias que presenta la empresa, es la ausencia de metodología para las copias de seguridad que debería tener implementada por el gran flujo de información que se maneja. Este proceso se está dejando a criterio de cada líder de proceso, quienes en aras de proteger su operación, lo realizan como mejor les parece, exponiendo en gran medida a la empresa ante una pérdida de datos.

Uno de los puntos incluidos y expuestos a la gerencia, es la creación de un proceso metodológico que permita estandarizar la generación de las copias de seguridad, en cuanto a tiempo, responsable, custodia y acceso a la misma, en cuyo caso se recomendó incluir este punto en específico, dentro del plan de continuidad corporativa.

En la validación realizada sobre la configuración de las aplicaciones y los accesos que se tienen permitidos sobre los activos de información, se encontró que no existía una correcta segregación de funciones, es decir, que la persona que realiza la configuración y asignación de permisos y roles, no tiene un proceso de monitoreo y/o aprobación. Por lo anterior, cuando se cometen errores, estos se identifican ya sobre la operación, lo que crea vulnerabilidad y reprocesos que han impactado el desarrollo en condiciones normales las actividades en reiteradas ocasiones.

Como medida para contrarrestar esto, se discutió con la gerencia para que dentro del equipo responsable en tecnología, se establezca una persona que se encargue de realizar aprobación y monitoreo de los permisos que se han asignado en los sistemas de información.

Con esta información se dio claridad acerca de los controles que se tienen implementados y por consiguiente, como resultado del análisis de la información, aquellos controles que se recomienda implementar para aumentar la seguridad sobre los activos con los cuales se gestiona la información en la empresa.

La cualificación se llevó a cabo con los líderes de cada proceso, así como de los responsables o custodios de los activos, de manera que resultó ser un proceso inclusivo y ajustado a la realidad operativa.

Los riesgos más altos se ven representados en el personal clave, servidores y configuraciones. Esto es debido a que un inadecuado proceso de configuración interna en los dispositivos y en la seguridad perimetral, hacen que la empresa se encuentre vulnerable al acceso por parte de terceros, ingreso de malware o fuga información. Sin la correcta implementación de una cultura de seguridad basada en una norma como guía de implementación, resulta en una posibilidad muy grande de exponer los datos sensibles de la empresa.

Con base en esta calificación, se identificaron los controles que cada proceso responsable de los activos tiene implementado y se discutieron los posible controles a implementar obteniendo resultados que se ponen en práctica y redundan en un mejor funcionamiento operativo.

7.1.4. Controles. La adopción de controles específicos que estén acordes a los riesgos identificados, se hace crucial para proteger cada activo utilizado para la gestión de datos e información. De acuerdo con los resultados observados en la valoración de los riesgos, se realizó la implementación de los siguientes controles:

Se implementó para la empresa con el direccionamiento del proceso de tecnología, la política de seguridad de telecomunicaciones, en la que se incluyen las medidas sobre los activos, el mejoramiento de la cultura de seguridad y el direccionamiento a las sanciones contenidas en el reglamento interno de trabajo cuando se presente incumplimiento. Anexo A

Implementación del procedimiento de seguridad operativa. En este se trazan los mecanismos, herramientas y actividades para garantizar de manera relativa, la operación de los sistemas de procesamiento y se establecen controles para código malicioso, copias de seguridad, accesos no autorizados, instalación de software. Anexo B.

A manera de resumen, se presenta lo direccionado para la empresa con el fin de contrarrestar las amenazas y vulnerabilidades encontradas, riesgos identificados y que fueron incluidas en los documentos mencionados.

Tabla 18 Controles.

CONTROL ADICIONAL RECOMENDADO	APARTE DE LA NORMA ISO 27001
Implementación de política de seguridad de la información	5.Politica de seguridad de la información
Restricción de medios extraíbles	6.Organizacion de la seguridad de la información
Sanciones por incumplimiento de normas internas	7.Seguridad del recurso humano
Capacitación en temas de seguridad de la información al personal	
Realizar control de accesos a través de configuración de perfiles	9.Control de acceso
Implementación de dominio corporativo	
Implementar medidas criptográficas para Trasferencia de información sensible	10. Criptografía
Controlar el acceso de personal externo	11. Seguridad física y del entorno
Establecer medidas de control sobre el servidor operacional	12. Seguridad de las Operaciones
Controlar el acceso sobre la red, re configurando las rutas, direccionamientos y depurando usuarios.	13. Seguridad de telecomunicaciones

Fuente el autor

Así mismo, para dar claridad acerca de lo recomendado después del análisis de los resultados obtenidos en el desarrollo del presente trabajo, a continuación, se mencionan de manera específica, los controles recomendados para cada uno de los activos de información identificados:

Tabla 19 Controles Específicos.

ACTIVO	CONTROL IMPLEMENTADO EN EL PROCESO RESPONSABLE	CONTROL ADICIONAL RECOMENDADO
Jaspersoft Comercial	Roles y permisos para cada persona que intervienen en el proceso	Configurar los reportes de manera particularizada para que cada persona acceda solo a lo que requiere.
Trasferencia de archivos	Envío de información solo a personal autorizado	Definir política para la trasferencia de archivos, clasificar por tamaño, tipo y contenido.
Manager ERP	Roles y permisos para cada persona que intervienen en el proceso	Monitoreo periódico de los permisos concedidos.
Jaspersoft Financiero	Roles y permisos para cada persona que intervienen en el proceso	Configurar los reportes de manera particularizada para que cada persona acceda solo a lo que requiere.
Servidor Operacional	Roles y permisos para cada persona que intervienen en el proceso	Limitar la información almacenada, definiendo periodos de retención.
Servidor de correo	Envío y recibo solo de información corporativa	Restringir el envío solo a los dominios de correo interno y de los clientes. Implementar listas de personal externo autorizado para el envío de información
Controlador de dominio	Políticas por grupos	Monitoreo de cambios en la implementación de políticas y excepciones, dejando registro por el responsable de implementación. Activar log de seguimiento.
Fortigate	Roles y permisos para el personal que configura la herramienta.	Asignar responsable para monitoreo de cambios en la configuración. No asignar usuario administrador o si se asigna activarlo solo en casos específicos.
Switch	Configuración inicial realizada por un experto	Documentar la configuración realizada y los cambios que se implementen. Asegurar la monitorización de los puertos. Establecer mínimo seguridad IEEE

Router	Administración por una sola persona	Autenticación doble para el ingreso a la configuración Documentar la configuración, tener una persona de respaldo que la maneje.
Intranet	Roles y permisos para cada persona que intervienen en el proceso	Definir administrador para el control de las publicaciones y eliminación de las mismas.
Binaps	Asignación de usuarios controlados por el administrador del sistema.	Solo contar con un administrador. Diferenciar roles para solo lectura de documentos.
Personal Clave	Acuerdos de confidencialidad	Incluir cláusulas de penalidades. Incluir clausula en el reglamento interno de trabajo
PC	Directorio activo Identificación de responsable	Segmentar por proceso Separa por vlan Monitorear las políticas aplicadas a usuarios y grupos

Fuente el autor.

De igual manera se estableció la declaración de aplicabilidad donde se consigna el estado o recomendación para cada control, teniendo en cuenta, cumplimiento especifico de lo establecido por el anexo A de la ISO/IEC 27001:2013. Documento que fue socializado con la gerencia. (Anexo C)

7.1.5. Actualización del inventario. Se estableció compromiso a través de acta con cada líder de proceso como responsable de su activo de información, para que sea este, quien se encargue de actualizar los activos que tiene a través de la identificación según los lineamientos estipulados en el desarrollo de este trabajo, adicionalmente, actualizar los controles o proponer nuevos cuando así lo considere conveniente.

La matriz de riesgos, será administrada por el equipo de tecnología, quienes, en conjunto con los líderes y responsables por cada proceso, pondrán en conocimiento respectivo a la gerencia, sobre aquellas situaciones que sean propensas a materializar esos riesgos sobre los activos de información, proponiendo los mejores mecanismos de protección con el fin, que se evalué y aprueben los recursos que sean necesarios.

Se propone, integrar el inventario de los activos de información y la matriz de riesgos al módulo respectivo en la herramienta Binaps, que ya tiene la empresa, pero que no está siendo utilizada por desconocimiento de su funcionamiento. A través de esta, se puede gestionar, actualizar y monitorear los activos de información, de

manera que resulta más practica realizar la tarea por parte de los responsables y de inclusión para los líderes de proceso y sus equipos de trabajo.

8. CONCLUSIONES

El primer paso para realizar una correcta identificación de activos, es entender que es un activo, cuales son los tipos de activos que maneja la empresa y la relevancia o prioridad que representan para el desarrollo de las actividades. De esta manera, se logró hacer extensiva la importancia de una adecuada identificación de los activos de información a cada líder de proceso, apropiarlos de su responsabilidad activa para su gestión y control, así como de los riesgos a los que se ven expuestos.

Estrategias Empresariales, por ser una empresa dedicada a las asesorías administrativas, se enfoca en los procesos operativos y no en la seguridad de sus activos de información, por lo que a través del desarrollo del proyecto, se estableció una metodología manual, donde se tienen en cuenta criterios como: valor para el proceso, valor para la empresa, tipo, criticidad y clasificación de cada activo de información, de esta manera, se incluyen aspectos relevantes que apoyados en la ISO 27001:2013 e ISO 31000:2018 constituyen en un método de reconocido valor para la organización.

La gestión de la seguridad de la información, es un gran reto para las empresas, por las implicaciones que tiene sobre los recursos físicos, financieros y humanos. La inversión que se deba realizar Estrategias Empresariales para el control de los activos de información, debe verse como algo que redunda en beneficio para la empresa de cara a la seguridad interna y a la imagen corporativa ante sus clientes y partes interesadas.

Estrategias Empresariales es una empresa que se encuentra en crecimiento, al reconocer cuales de sus activos resultan ser más críticos para sus operaciones, puede direccionar de manera específica los recursos a destinar para los proyectos relacionados a la seguridad de la información.

Se observó que los activos de información, tenían más de una causa generadora de riesgo, por lo que, al identificar la amenaza y la vulnerabilidad, se determinó de manera efectiva, la calificación de los riesgos asociados y que tan expuesta esta la empresa a su ocurrencia en cada uno de los procesos que la integra.

Se logró determinar los controles más apropiados que permiten salvaguardar de manera más específica, la integridad, disponibilidad y confidencialidad en cada activo utilizado para la gestión de la información, haciendo participes a los responsables de la misma, de manera que, al involucrarlos de manera activa al proyecto, se apropiaron del mismo y ahora son conscientes acerca de la importancia que representa para la empresa el velar de manera adecuada por la seguridad de los activos de información.

Aunque la empresa cuenta con varias herramientas que le permitirían gestionar los activos de información de manera práctica, el desconocimiento de las mismas, de su funcionalidad y gestión por parte del personal responsable, hace que el recurso se desaproveche y que el riesgo sea mayor ante la falta de identificación, monitoreo e implementación de controles.

Si bien es cierto que la empresa ha implementado algunos controles puntuales, para salvaguardar la información y el acceso a esta, no se observa documentación que soporte la actividad ya que se establecieron de manera práctica por conocimiento específico del personal que los estableció, sin seguir un lineamiento o estándar reconocido como el direccionado en el presente proyecto, por lo que la metodología Magerit resulta de importancia relevante para que Estrategias Empresariales pueda gestionar los riesgos de una manera eficiente e integrando de manera practica la matriz de riesgos generada a sus sistemas de control y seguimiento.

9. RECOMENDACIONES

Al finalizar el proyecto, se hace necesario establecer para Estrategias Empresariales, las siguientes recomendaciones, de manera que se ponen a disposición de la gerencia, haciendo claridad en las implicaciones positivas que pueden traer para su operación:

- ✓ Implementar un proceso de actualización automático que involucre matrices de seguimiento, validación y monitoreo, en el que se presenten alertas sobre cambios en la información o modificaciones sobre la misma, lo cual redundaría en un beneficio significativo para la empresa, toda vez que por su objeto social, el 90% de la operación se realiza de manera digital, y al no contar con la capacitación requerida sobre el personal, procesos automáticos podrían suplir esta necesidad.

- ✓ Implementar controles a todos los tipos de activos de información, sin importar que tan críticos son o no para las operaciones de la empresa, pues con los avances tecnológicos también se han desarrollado ataques en contra de las redes corporativas y dichos ataques pueden surgir por la más mínima brecha de seguridad que tenga la empresa, en especial por dispositivos móviles y el personal responsable que en términos generales, son (cuando no hay cultura) el eslabón más débil de toda la cadena operativa, como se refleja en Estrategias Empresariales.

- ✓ Estrategias Empresariales debería implementar la cultura relacionada con la seguridad de la información para el personal a todo nivel, haciendo énfasis en los líderes de proceso, como responsables para que el personal que tienen en sus diferentes cargos, acate de manera efectiva las medidas que se vayan implementado en materia de seguridad sobre los activos que gestionan en sus actividades.

- ✓ Establecer un reconocimiento de extremo a extremo para los activos de información, esto quiere decir que la empresa debe siempre considerar la protección de la información desde la fuente generadora hasta su uso o destinatario final, de esta manera se logrará tener de forma integral, control y seguridad desde el momento en que se genera, pasando por los dispositivos, herramientas y contenedores para la gestión de la información, hasta su disposición o repositorio de almacenamiento.

- ✓ Cobra relevancia, integrar procedimientos documentados para realizar pruebas especifica en seguridad sobre los activos de información, de manera que se tengan bases sólidas y registros para direccionar controles específicos que le permitan a Estrategias Empresariales, optimizar procesos en los que se realice gestión con los activos de información de manera segura y confiable,

resguardando en todo momento las propiedades fundamentales referidas a la confidencialidad, integridad y disponibilidad en su operación y la de sus empresas clientes.

- ✓ Evaluar la posibilidad de contratar con proveedores externos especializados, aquellos servicios de gestión de información que puedan resultar más críticos ante la falta de recursos propios, como lo son data center y servicios cloud.

- ✓ Tener en cuenta siempre los stakeholders para la gestión de los activos de información, no solo clientes y proveedores sino también entes de regulación y control, pues un incumplimiento en materia normativa que regula el sector tecnológico, puede afectar de manera significativa no solo la operación de la empresa sino también su reputación.

- ✓ Comprender siempre la integralidad que debe existir entre el sistema de planeación de recursos (enterprise resource planning - ERP), administración de riesgo empresarial (entreprise risk management – ERM) y la administración de las diferentes relaciones que se tiene con los clientes (customer relationship management – CRM), ya que en cualquiera de estos pueden presentarse riesgos que guarden relación directa con la seguridad de la información, que pueden afectar directa o indirectamente o influir la alineación de los programas tecnológicos con los objetivos estratégicos, el gobierno corporativo, la asignación de recursos e inclusive la comunicación de la red corporativa y con los clientes.

10. BIBLIOGRAFÍA

AGUIRRE, J. D., & ARISTIZABAL, C. (2013). Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la Ofrenda. {En linea} {12 diciembre 2019} Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

CARDENAS, F. A. 2018. NovaSec. ISO 27001 | Gestión Integral de la Seguridad de la Información | SGSI. {En linea} {14 noviembre 2019} Disponible en: http://www.novasec.co/blog/62-gestion-integral-de-la-seguridad-de-la-informacion

C. Elvis, Metodología para el análisis de riesgos en seguridad informática. {En linea} {14 noviembre 2019} Disponible en: http://msnseguridad.blogspot.com/2012/08/seguridad-informatica-la-seguridad.html

Comisión interamericana de Telecomunicaciones, gestión de riesgos de seguridad 2009). {En linea} {23 octubre 2019} Disponible en: http://www.oas.org/en/citel/infocitel/2009/septiembre/seguridad_e.asp

CRESPO Rin, María del Carmen (2014). El analisis de riesgos dentro de una auditoria informatica: pasos y posibles metodologías. Universisdad Carlos III de Madrid. {En linea} {21 julio 2019} Disponible en:: https://e-archivo.uc3m.es/handle/10016/16802

BRACHO DAVID, Carlos R. & ACURERO Alfredo. 2010 Modelo para la cuantificación del riesgo telemático en una organización. Universidad de Zulia. Revista Venezolana de información, tecnología y conocimiento. {En linea} {17 agosto 2019} Disponible en: https://www.researchgate.net/publication/47372038_Modelo_para_la_cuantificacion_del_riesgo_telematico_en_una_organizacion

FRANCO, Diana Elizabeth. 2015. Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001. Espol. Fiel Guayaquil: Escuela superior politécnica del litoral. 120p

GASPAR MARTÍNEZ, Juan 2004. Planes de contingencia: la continuidad del negocio en las organizaciones. Ediciones Díaz de Santos. {En linea} {17 agosto 2019}: Disponible en: https://www.editdiazdesantos.com/libros/gaspar-planes-de-contingencia-L03006470201.html?articulo=03006470201

Guía avanzada de gestión de riesgos. Instituto Nacional de Tecnologías de la Comunicación - Instituto Nacional de Tecnologías de la Comunicación - ITECO. {En

linea} {01 septiembre 2019} Disponible en: https://www.academia.edu/4075256/guia_avanzada_de_gestion_de_riesgos

Heidi E. I. Dahl. 2008 The Coras Methodod for security risk analysis. SINTEF. {En linea} {10 octubre 2019} Disponible en: http://coras.sourceforge.net/documents/080828TheCORASMethod.pdf

ALEMAN NOVOA Elena & BARRERA RODRIGUEZ Claudia. 2015. Metodologías para el analisis de riesgos en los SGSI. Fundación universitaria Juan de Castellanos. Publicaciones e invetigación. {En linea} {18 marzo 2019} Disponible en:http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

INCIBE-CERT 2016. INCIBE - CERT. Inventario de activos y gestión d la seguridad en SCI 2016. {En linea} {03 agosto 2019} Disponible en: https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci

ISO, W. (2018). Los Activos de Información en la norma ISO 27001 2017. {En linea} {25 noviembre 2019} Disponible en: https://isowin.org/blog/activos-ISO-27001/

ISOTOOLS. 2015. ¿Cómo clasificar los activos de seguridad en un SGSI? {En linea} {10 junio 2019} Disponible en: https://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/

GARCIA, Juan Manuel. 2006. Análisis y control de riesgos de seguridad informática: control adaptativo. Departamento de Sistemas y Computación Instituto Tecnológico de Morelia, Morelia, México. {En linea} {23 julio 2019} Disponible en: http://acistente.acis.org.co/typo43/fileadmin/Revista_105/JMGarcia.pdf

Mintic. 2016. Guía para la Gestión y Clasificación. {En linea} {25 junio 2019} Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

SEGOVIA, A. J. 2018. Advisera Expert Solutions. ¿Qué es norma ISO 27001? {En linea} {03 mayo 2019} Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/

PALOMEQUE Letty Yaneth., & PALACIOS Yaciry Enith. (2018). Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO 27001:2013 para la empresa UNISANAR IPS de Quibdó. {En linea} {17 mayo 2019} Disponible en: https://repository.unad.edu.co/handle/10596/15028

ANEXO A. SEGURIDAD EN LAS TELECOMUNICACIONES

SEGURIDAD EN LAS TELECOMUNICACIONES
OBJETIVO
Controlar, monitorear y gestionar el acceso lógico a la infraestructura de la organización, con el fin de evitar daños e interferencias a la red de la empresa por parte de entes externos e internos de la misma.
ALCANCE
La seguridad de las telecomunicaciones abarca la gestión en la seguridad de las redes de las sedes principales y puntos de venta, abarcando aspectos como: Controles de uso y manejo de la red. Mecanismos de seguridad en las telecomunicaciones asociadas a la red interna. Segmentación de la red interna De igual forma la seguridad de las telecomunicaciones en **ESTRATEGIAS EMPRESARIALES** cubre los aspectos de intercambio de información con entes relacionados, a través de la implementación de controles en: Manejo de la mensajería electrónica de la organización. Segmentación de red para invitados.
AUTORIDAD Y RESPONSABILIDAD
Autoridad Gerente **Responsabilidad** Director TIC Asistente de Comunicaciones
TÉRMINOS Y DEFINICIONES
Acceso a la información: se trata del derecho que posee toda persona para acceder, recopilar, recibir información, acorde a la política de seguridad de la información que se encuentre vigente. **Flujo de operación:** hace referencia a las entradas y salidas de una ruta de comunicación, especificando IP y puertos de origen y PI y puertos de destino. **Medios de procesamiento de información:** hace referencia a los dispositivos ya sean internos o externos, los cuales tengan la capacidad de procesamiento,

gestión y almacenamiento, y que es manipulado por el usuario, como lo son por ejemplo, discos duros externos, equipos de cómputo.

Seguridad perimetral: hace referencia a dispositivos firewall que permiten controlar el ingreso y salida de información no autorizada por la organización.

Vulnerabilidades: hace referencia a las brechas de seguridad detectadas en las redes e infraestructura que pueden llegar a representar la materialización de un riesgo por la falta o carencia de controles.

VPN: es el túnel establecido entre dos redes para garantizar la comunicación entre fuentes de información que cuenta con permisos restringidos, y que se encuentran establecidos por los responsables del proceso de comunicaciones.

POLÍTICAS INTERNAS

Controles de red:

El acceso a la información a través de la red solo se realiza a través de medios de procesamiento propios de la organización, por tal motivo en caso de que existan excepciones, siempre se requiere que se cuente con aprobación expresa de la gerencia y se deberá comunicar al proceso de TIC para que este proceda con la habilitación de acceso sobre los datos o información teniendo en cuenta los tiempos solicitados. El acceso a personal externo de la empresa se realizará a por medio de la red inalámbrica habilitada para invitados.

Dentro de la red institucional de la empresa se encuentra restringido:

La descarga de archivos con extensiones: .flv, .mp4, .mp3, .exe, .rar, .avi.

El ingreso a correo electrónico no institucional.

La descarga de archivos de sitio peer to peer.

La conexión hacia portales de streaming sin la autorización respectiva.

La conexión hacia portales de reproducción o descarga de música en línea.

La descarga de archivos desde sitios no seguros.

El acceso a sitios o páginas para adultos de contenido sexual.

El uso de servicios de escritorio remoto a través de internet diferentes a RDWEB, TeamViewer

Además, de cualquier sitio o servicio que conlleve un riesgo sobre la seguridad propia de la información corporativa.

Reglas de filtrado para control de acceso a usuarios internos y externos

Las reglas de filtrado estarán contenidas en el router principal y están condicionadas por los accesos aprobados por el proceso de TIC. En caso tal de

requerirse por parte de algún funcionario de TIC modificar el alcance de estas deberá contar con la autorización por medio de ticket del Jefe de Infraestructura y Telecomunicación.

Se deberá hacer uso de IPS de servicio o de trabajo cada vez que un grupo de usuarios finales necesiten acceder a cualquier sistema de información que pertenezca a la infraestructura privada de la empresa y de proveedores externos.

Administración de la red de puntos de venta

Todas las transacciones realizadas por la compañía desde los puntos de venta se realizarán por medio de una red privada propia, la cual se encuentra administrada por el personal de TIC de **ESTRATEGIAS EMPRESARIALES** quien será el encargado de habilitar dicho medio de comunicación.

Todo punto que se encuentre por fuera de la cobertura de la red inalámbrica y disponga de un servicio de internet, estará obligado a operar a través de una conexión VNP que será suministrada y monitoreada por el proceso de TIC.

Autenticación de usuarios para conexiones externas

El proceso de TIC tiene referenciados como servicios para la conexión externa SSL, VPN para trabajadores que por el desarrollo de sus funciones, necesiten acceder de manera remota a la red corporativa.

La autenticación a los servicios VPN para personal que requiere conexión externa, deberá solicitarse a través del formato de solicitud de acceso remoto (VPN), el cual debe estar firmado por la Gerencia.

Identificación de equipos en la Red

El proceso de TIC llevara control y realizara la identificación de cada equipo conectado a la red interna, utilizando controlador de dominio, haciendo designación de las IP condicionada a la MAC del equipo de cómputo asignado por la empresa.

El acceso WIFI se encuentra segmentado por proceso y su acceso está restringido solo a equipos que se encuentran registrados por el personal de comunicaciones, por medio de su dirección MAC.

Protección de los puertos de configuración y diagnostico remoto

Con el inventario de puertos y teniendo claro cuáles de ellos permiten el mantenimiento y prestar soporte remoto a servidores y equipos, se restringirá el uso de estos a solo los administradores de la red o de los servidores.

El personal interno deberá permitir el control remoto de los equipos a su cargo, solo al personal autorizado del proceso de tecnología, teniendo en cuenta, no

dejar en ningún momento el equipo desatendido mientras dura el soporte o mantenimiento, de esta manera se puede supervisar el trabajo y los accesos.

Gestión de vulnerabilidades en las redes e infraestructura

Cada dos meses el Asistente de Comunicaciones estará en la obligación de realizar la puesta en marcha del análisis de vulnerabilidades o en caso de presentarse una amenaza latente, adicionalmente deberá analizar la información para establecer acciones de mejora de acuerdo con las novedades evidenciadas.

La acción de mejora del análisis de vulnerabilidades será presentada por Asistente de Comunicaciones aprobado por la Gerencia.

Topología de la red

El único encargado de realizar el diseño de la red es el Asistente de Comunicaciones.

La implementación de nuevos enlaces deberá contemplar una acción de contingencia en caso de posibles fallas en la estructura establecida.

La topología de red de **ESTRATEGIAS EMPRESARIALES** debe conservar la política de uso de redes privadas para la administración de sus servicios de información, por tanto, todo nuevo enlace debe asegurar la no salida a canales externos (internet) de forma no controlada.

Mecanismos de seguridad asociados a servicios de red

Todo punto de venta y sede administrativa debe contar con un medio de acceso comunicación que le permita la interconexión con el router principal, el cual es administrado por el proceso de TIC.

El firewall que opere como principal en cada municipio deberá contar con herramientas de marcado de paquetes, marcado de rutas, manejo de tablas de enrutamientos, scripting sobre funciones automáticas de enrutamiento de contingencias, manejo de eventos particulares de la red y manejo de tabla de filtros y bloqueo de tráfico.

Todo equipo de la organización que tenga autorización para navegar en internet deberá trabajar por medio del servidor proxy de la compañía.

El único autorizado para administrar las reglas del servidor proxy es el Asistente de Comunicaciones

Todo equipo de cómputo de la compañía deberá estar configurado con el DNS propio de la organización.

La sincronización de relojes de equipos cliente y servidores se administrará a través del proveedor tecnológico.

Todo de equipo de cómputo de la sede administrativa deberá ser registrada dentro del listado tabla ARP de la compañía, y la administración y gestión de está estará en cabeza del Asistente de Comunicaciones.

La implementación de listas negras y blancas se instaurarán en: Wifi de la empresa, reglas de filtrado de la navegación, proxy, Directorio Activo (DA).

Toda la infraestructura de la organización será objeto de verificación para el análisis de vulnerabilidades, este sistema será administrado por el jefe de infraestructura o quien sea responsable de la misma.

Segmentación de la red

El proceso de TIC hará uso de dispositivos de seguridad — firewalls, para tener control sobre los accesos entre redes.

La segmentación se implementará para los equipos de enrutamiento, haciendo uso de configuraciones de listas de control de acceso, y de VLANS para los equipos y dispositivos propios de las comunicaciones internas, como lo son AP, routers y switch.

Manejo de la mensajería electrónica de la organización

La instalación de correo electrónico se realizará bajo la implementación de protocolos de internet IMAP y solo se almacenará en la mensajería de correo electrónico información de 2 meses anteriores.

Solo se permitirá el uso de mensajería instantánea por medio de la intranet (bitrix), chat de correo corporativo y servidor open fire.

En caso de requerirse instalar otros servicios de mensajería instantánea se deberá enviar un ticket a la mesa de ayuda.

Segmentación de red para invitados

Deberá existir una red inalámbrica con permisos restringidos hacia los sistemas de información internos, para que sea de uso de personal externo a la misma.

La segmentación de red para los invitados se realizará a través de VLANS y debe cumplir con el objeto de la premisa anterior.

Para permitir el acceso de un personal externo a navegación en internet, se deberá registrar el número de dirección MAC y posteriormente se facilitará el acceso al servicio de red de **INVITADOS**.

DESCRIPCIÓN DEL DOCUMENTO
Control de redes

Inicialmente se recepciona la solicitud por parte de la Mesa de ayuda quien se encarga de hacer la clasificación del ticket y de asignárselo al personal de TIC, en los siguientes casos:

Solicitud de ingreso sobre la red privada por parte de una nueva estación de trabajo.

Solicitud de un acceso a un sistema de información (páginas web, plataforma transaccional, software contable y software especializado)

Solicitud de ingreso a la red de invitados de un personal externo a la organización.

Apertura de un nuevo punto de venta.

Solicitud de creación de un nuevo segmento de red.

Posterior a la recepción del ticket el Asistente de Comunicaciones y/o Auxiliar de Mesa de ayuda verifican que se encuentre autorizado la asignación del permiso al segmento o estación de trabajo solicitado.

Una vez ha realizado la verificación se procede a la atención del ticket, de acuerdo a las políticas mencionadas en el ítem de control de red.

A continuación, se describen las acciones a emplear teniendo en cuenta, lo mencionado en los literales anteriores:

Solicitud de acceso a la red privada de la empresa de una nueva estación de trabajo

En caso tal de que se requiera una nueva estación de trabajo el Auxiliar de Mesa de ayuda encargado de establecer la respectiva configuración de la estación de trabajo consultará con el Asistente de Comunicaciones la IP y demás datos a asignarle de acuerdo con la tabla ARP.

Posterior a la recepción de la IP el Auxiliar de Mesa de ayuda configurará la IP, GATEWAY, máscara, DNS y el Proxy. Una vez se ha desarrollado esta actividad el jefe de comunicaciones habilitará los permisos de la IP asignada.

Con esta habilitación el asistente de Infraestructura y Telecomunicaciones procederá a informar al solicitante para que realice las pruebas de acceso respectivas.

Solicitud de un acceso a un sistema de información (páginas web, plataforma transaccional, software contable y/o software especializado)

El Asistente de Comunicaciones una vez reciba el ticket asignado, realiza la verificación de la estación de trabajo para identificar la IP origen y confirmar el flujo de la operación a realizar.

Posterior a la verificación se realiza la configuración en el router principal para hacer la correspondiente ruta y la habilitación del acceso, por medio de la

configuración de los mecanismos de seguridad asociados a los servicios de la red.

Solicitud de ingreso a la red de invitados de un personal externo a la organización

En caso de requerirse acceso para personal externo, el personal de **ESTRATEGIAS EMPRESARIALES** deberá enviar un ticket a la mesa de ayuda.

Posterior a esto el Auxiliar de Mesa de ayuda, solicitará el equipo al invitado para proceder con el enrolamiento del equipo a través de la dirección MAC de la interfaz inalámbrica, luego se hará el registro de dicha dirección en los dispositivos Access Point como en el router principal. Esta actividad solo tiene alcance para la oficina principal de la empresa.

Solicitud de creación de un nuevo segmento de red

Para la creación de un nuevo segmento de red se debe tener la autorización expresa de la Gerencia, una vez se tenga esta aprobación el Asistente de Comunicaciones procede a validar las condiciones de la infraestructura para identificar si esta soporta la operación.

Posteriormente se procede a la configuración de la VLANS y después de configura el router principal para hacer las correspondientes rutas y habilitaciones necesarios de acceso, por medio de la configuración de los mecanismos de seguridad asociados a los servicios de la red.

Gestión de las vulnerabilidades en la red

El Asistente de Comunicaciones de acuerdo con su programación realiza la puesta en marcha del análisis de vulnerabilidades por medio de una máquina virtual dentro de la VLAN de servidores ejecuta el aplicativo de análisis de vulnerabilidades.

Para esta actividad se debe seleccionar el objeto de evaluación del análisis de vulnerabilidades, los cuales pueden ser:

Sistemas operativos

IP y puertos

Tipos de dispositivos

Una vez se obtiene el resultado arrojado del aplicativo de análisis de vulnerabilidades se procede a analizar la información filtrarla de acuerdo con el nivel de afectación:

Afectan directamente el core bussiness del negocio de la organización.

Afectan a la infraestructura de redes de la organización comprometiendo la prestación del servicio.

Aparición de posibles puertos e IPS no controladas por el Asistente de Comunicaciones.

Una vez realizada la identificación, se documenta la acción para mejorar con el fin de determinar las actividades a realizar para atacar las vulnerabilidades, una vez se ha documentado la acción de mejora se procede a realizar la presentación a la Gerencia para su posterior evaluación y obtener la respectiva aprobación.

Una vez conseguida la aprobación de la Gerencia se procede a realizar la ejecución de la acción de mejora de acuerdo con los tiempos estimados de implementación y de avance, los cuales se le comunicaran a la Gerencia, con el ánimo de mostrar los resultados del plan de acción.

Intercambio de información con las partes externas:

Mensajería electrónica

Se recibe una solicitud de creación de correo electrónico, intranet corporativa u otro servicio de mensajería instantánea a través de ticket en la mesa de ayuda, posterior a esto el proceso de TIC realiza la asignación del ticket al Auxiliar de Mesa de ayuda para que proceda con la instalación del correo.

Una vez el Auxiliar de Mesa de ayuda recibe el ticket asignado, desarrolla las siguientes actividades de acuerdo con cada caso:

Si la solicitud es para la creación de un nuevo usuario en el correo electrónico y/o de intranet, el Auxiliar de Mesa de ayuda solicita adicionalmente el formato FO-GH-34 Solicitud de herramientas de trabajo firmado por el jefe inmediato.

Posteriormente el Auxiliar de Mesa de ayuda con toda la información adjunta procede a crear el usuario de correo electrónico y de intranet de acuerdo con las políticas anteriormente mencionadas de manejo de mensajería electrónica.

Si la solicitud es para la creación de un nuevo servicio de administración de mensajería instantánea, el Asistente de Infraestructura y Telecomunicaciones verifica las condiciones con la que se cuenta de infraestructura y posteriormente se realiza.

Una vez se ha procedido con la creación del servicio solicitado (correo electrónico, usuario de intranet y/u otro servicio de mensajería electrónica) se procede por parte del funcionario de TIC encargado de la resolución del ticket a entregar el usuario y la contraseña para acceder al servicio solicitado.

ANEXO B. SEGURIDAD DE LA OPERATIVIDAD

SEGURIDAD DE LA OPERATIVIDAD
OBJETIVO
Generar seguridad en la operación del sistema de procesamiento de información, implementando medidas, políticas y controles que contrarresten las potenciales amenazas sobre la seguridad de la información, evitando que sea afectado su sistema y cada usuario de la misma.
ALCANCE
La seguridad de la operatividad de ESTRATEGIAS EMPRESARIALES abarca el desarrollo de actividades tendientes a controlar aspectos de control como: ✓ Aparición de código malicioso ✓ Carencia de implementación de copias de seguridad ✓ Detección y registro de acceso autorizados y prevención de amenazas de acceso no autorizados. ✓ Instauración de software no permitido por la organización ✓ Aparición de vulnerabilidades y amenazas que afectan el normal funcionamiento de la seguridad establecidad sobre los sistemas de información.
AUTORIDAD Y RESPONSABILIDAD
Autoridad Gerente **Responsabilidad** Director de TIC Asistente de Comunicaciones Auxiliar de Servicios tecnológicos
TÉRMINOS Y DEFINICIONES
Acción de corrección: hace referencia a la actividad de mitigación en el corto plazo implementada para corregir en una primera medida la amenaza materializada.

Acción correctiva: se refiere a las acciones que se toman con el fin de eliminar las causas que ocasiona las no conformidades. Estas acciones se enfocan en el desarrollo de actividades de largo plazo.

Backups: se trata de las copias de seguridad que se realizan sobre la información, con el fin de tenerlas disponibles en caso de requerir recuperación ante alguna pérdida o evento que así lo requiera.

Flujo de operación: hace referencia a las entradas y salidas de una ruta de comunicación, especificando IP y puertos de origen y PI y puertos de destino.

Malware: se utiliza para señalar a aquel software considerado como invasivo u hostil. En este se incluyen los gusanos, virus, rootkits (generalmete), asi como spyware y otro software, de tipo malicioso.

Programa malicioso: trata de software cuyo objetivo principal es ingresar y causar daños sobre los equipos de cómputo sin que el propietario del mismo tenga conocimiento.

Usuarios operativos: hace referencia a las cuentas de usuario creadas dentro del árbol del directorio activo y que tienen privilegios restringidos.

Vulnerabilidades: hace referencia a las brechas de seguridad detectadas en las redes e infraestructura que pueden llegar a representar la materialización de un riesgo por la falta o carencia de controles.

Virus: son programas que se ejecutan y propagan, causando infección sobre otros softwares que se ejecuten dentro de un mismo equipo de cómputo.

POLÍTICAS INTERNAS

Control de código y software malicioso

El único autorizado para realizar la instalación de software y en general cualquier tipo de programa en las maquinas, es el personal de TIC encabezado por el Auxiliar de Servicios tecnológicos, en caso de detectarse la instalación software no licenciado se procederá a su desinstalación y notificación al proceso de gestión humana para que proceda a realizar el llamado de atención correspondiente.

Todo equipo de cómputo de los puntos de venta debe trabajar en un sistema operativo Linux basado en la imagen pre configurada por el proceso de TIC, adicionalmente debe contar con un usuario administrador local para brindar soporte y un usuario operativo con privilegios limitados para el colaborar.

Todo equipo de cómputo de las sedes administrativas debe tener instalado un antivirus o software que impida la propagación o ejecución de código malicioso, virus o malware. Esta actividad estará en cabeza del proceso de TIC.

Solo se podrá instalar software en los equipos de cómputo de las sedes administrativas por medio del usuario administrador local y el usuario administrador del dominio, los demás usuarios de los colaboradores tendrán permisos limitados para la instalación de software.

El proceso de TIC deberá gestionar la programación de análisis de código malicioso en los equipos de cómputo por medio del antivirus, en caso de encontrar novedades se deberá emplear medidas de acciones de mejora a través del formato correspondiente.

Dentro de la red institucional de la empresa para evitar la propagación de malware en los sistemas de información se encuentra restringido a través de una lista blanca de navegación que contiene todas las páginas web permitidas y usadas dentro de las labores de la información.

La red de servidores, de equipos administrativos y equipos de venta se encuentran debidamente segmentados.

Los diferentes equipos, servidores locales y equipos que se encuentran en la red deberán contar con las últimas versiones de software estables y parches de seguridad respectivos.

Almacenamiento de información (respaldo)

Los repositorios oficiales de la empresa para almacenar información digital son el servidor de archivos local y la intranet corporativa. No se garantiza respaldo o copia de seguridad sobre la información que no se almacene en estos servicios.

La información de los usuarios finales de la sede administrativa se almacena en el servidor de archivo local, por tanto, la información no se encuentra en los equipos de cómputo de cada funcionario.

El respaldo de la información de los usuarios de las sedes administrativas se realizará a través de un esquema de replicación del servidor de archivos y del directorio activo de la organización, el cual se realizará periódicamente de manera incremental cada 30 minutos.

La capacidad máxima de almacenamiento disponible para los usuarios de las sedes administrativas es de 5GB por mes.

La copia de la configuración del router principal se realizará a través de un script automático cada 7 días.

El respaldo de la información de la plataforma transaccional se ciñe bajo las políticas de gestión y respaldo del proveedor tecnológico.

El respaldo de la información manejada por medio de la nube de la intranet corporativa por ser un servicio externo el proveedor asegurará respaldo de la información 24/7.

Los servidores locales a excepción del VoIp se encuentran virtualizados y la copia de su configuración se realizará en otra participación del servidor, se debe generar esta imagen de la configuración completa cada dos semanas como copia de respaldo extra solo si:

Se realizan cambios de configuración significativos en la máquina de virtualización.

Si se crea una nueva máquina virtual (se crea copia de la máquina virtual).

El sistema de contingencia automática y de replicación se encuentra fuera de servicio.

Supervisión de la seguridad operativa

El registro de actividades se registrará internamente a través de logs, los cuales tienen como alcance:

- ✓ Servidores
- ✓ Rourtes

La administración, monitoreo y custodia de los logs de los servidores y rourtes estará en cabeza del Asistente de Comunicaciones

Los logs de servidores y rourtes se almacenarán con una periodicidad diaria y su almacenamiento no será superior a 6 meses.

La verificación de generación de los logs se realizará de manera trimestral, esta actividad se llevará a cabo por parte del Asistente de Comunicaciones

La custodia, mantenimiento, integridad, disponibilidad y continuidad de la generación de logs de la plataforma transaccional estarán en cabeza del operador tecnológico, por tal motivo en caso de requerirse dicha información se deberá enviar por parte del Asistente de Comunicaciones un correo con la solicitud correspondiente.

Control de la instalación de software

Los únicos autorizados para realizar la instalación de software es el Auxiliar de Servicios tecnológicos con previa autorización del director de TIC y/o Asistente de Comunicaciones

La instalación de software será controlada a través del dominio quien se encargará de restringir los permisos a los usuarios.

Solo la cuenta de administración de dominio y el administrador local contaran con los permisos de usuario que les permitan llevar a cabo la instalación y/o configuración de software.

Gestión de las vulnerabilidades técnicas

El encargado de analizar las vulnerabilidades técnicas es el director de TIC, coordinador de comunicaciones y/o Asistente de Comunicaciones, quien tienen el deber de detectar y clasificar las vulnerabilidades de acuerdo con las siguientes categorías:

- ✓ Lógico: son aquellas que comprometen la integridad en cada uno de los activos de información corporativa, al igual que las bases de datos, accesos a la misma o el software y que pueden ser causados por malware, manipulación indebida que altere, eliminen o destruya información.
- ✓ Físico: se trata de las situaciones o alteraciones que afectan o pueden afectar la vida útil de los equipos, como por ejemplo el mal trato o daño ocasionado por la mala manipulación del personal.
- ✓ Locativo: hace referencia a los elementos que ocasionan entornos inadecuados para la seguridad e integridad, de las herramientas, dispositivos, equipos y documentación relevante para la empresa.

Las vulnerabilidades provenientes de las incidencias de la red deberán ser gestionadas por el Asistente de Comunicaciones teniendo en cuenta cada directriz relacionada en el documento interno “Seguridad en las telecomunicaciones”

El seguimiento al avance de las acciones de mejora empleadas para mitigar la materialización de vulnerabilidades estará en cabeza del jefe de Servicios Tecnológicos y es de responsabilidad de éste presentar el estado de avance a la gerencia operativa.

Es de responsabilidad del director de TIC y/o Asistente de Comunicaciones, emplear el análisis de vulnerabilidades con una periodicidad no superior a dos meses.

DESCRIPCIÓN DEL DOCUMENTO
El presente procedimiento se encuentra dividido en cinco grandes fases, en una primera fase se encontrará todo lo concerniente a la gestión relacionada con la seguridad sobre redes y en una segunda fase se podrá divisar el intercambio de datos e información con externos relacionados. **Control de código malicioso** Inicialmente, se genera la notificación de la aparición de un código malicioso a través de los siguientes canales: El Auxiliar de Servicios tecnológicos detecta la aparición de un código malicioso en un equipo de cómputo. El usuario informa la aparición de mensajes anómalos presentados sobre su equipo asignado. Se presenta una afectación sobre un sistema de información o un servidor local o sobre la capacidad de un canal de comunicación, que sea detectada por el Asistente de Comunicaciones Una vez se tiene identificada la amenaza y sus posibles afectaciones, se procede a clasificar el tipo de vulnerabilidad, con el fin de definir el nivel de impacto que tiene para la operación de la organización y de los usuarios asociados al sistema de información afectados. Posteriormente el director de TIC y/o Asistente de Comunicaciones debe generar un plan de acción de mejora contemplando las siguientes actividades previas: Se debe desconectar el equipo de cómputo afectado de la red de la empresa. Se debe hacer un mantenimiento correctivo que incluya un escaneo profundo de equipo a través del antivirus. Se debe verificar que el software del equipo de cómputo afectado se encuentre actualizado y con los últimos parches. En caso de que la afectación sea sobre un servidor local se debe activar la contingencia con el fin de desconectar el equipo para proceder a un análisis a detallado. En caso tal de ser un canal de comunicaciones el afectado, se deberá realizar un análisis de red utilizando un Sniffer y un análisis de los registros del monitoreo del canal, sobre los equipos de red involucrados.

Una vez se ha desarrollado la fase de análisis el director de TIC, coordinador y/o asistente de Comunicaciones, deberá accionar y monitorear la implementación de las mejoras establecidas.

Copias de seguridad

Generación de copias de seguridad

El respaldo de copias de seguridad inicia con la programación realizada por parte del Asistente de Comunicaciones

Una vez se ha definido la fecha de realización del backup manual y la verificación de los backups que se ejecutan de manera automática, se procederá por parte del Asistente de Comunicaciones realizar las siguientes actividades:

Backup Manual

El Asistente de Comunicaciones deberá ingresar al servidor local, para proceder a realizar la copia de las imágenes de las máquinas virtuales y el traspaso a la otra partición.

Backup automático

Para el caso de los backups automáticos se debe revisar la lista de chequeo para los sistemas de información e identificar que se cumpla la generación de acuerdo con la periodicidad establecido en la política de este documento. Para poder hacer esta validación el Asistente de Comunicaciones procede a:

Revisar la cantidad de registros en términos de tamaño, a través de la comparación entre los servidores.

Verificar la última fecha de modificación de los archivos alojados en el servidor de respaldo.

Restauración de información

Para la restauración de los backups de los equipos de red, se debe proceder a identificar el último backup disponible, una vez se localice y se compruebe su veracidad, el Asistente de Comunicaciones debe proceder a cargar el backup en el equipo de contingencia designado. Una vez ha realizado la actividad si los afectados son usuarios finales procede a notificarles.

Supervisión de la seguridad operativa

El jefe de Infraestructura y Telecomuniciones procede a activar el registro de logs automático en el sistema local, con el fin de que queden registradas las cada uno de los movimientos realizados por los usuarios en el mismo.

Una vez se genera el registro de estas actividades o movimientos, se deberá proceder a verificar que se encuentren los registros de actividad, esta acción se llevará a cabo de acuerdo con la programación del Asistente de Comunicaciones y en los tiempos establecidos por la política.

Gestión de vulnerabilidades técnicas

El director de TIC y/o Asistente de Comunicaciones realiza la programación para realizar el análisis de vulnerabilidades en la organización, tomando como premisa que: "los periodos regulares para la implementación de un análisis de vulnerabilidades serán de un plazo no superior a dos meses", para esto deberá definir el alcance de la detección de acuerdo con las categorías (lógico, físico y locativo) mencionadas en la política de gestión de vulnerabilidades técnicas del presente documento.

Una vez se han definido el alcance a analizar, se procede a realizar el escaneo por parte del Asistente de Comunicaciones, en este proceso se valida la posible aparición del tipo de vulnerabilidades.

Para el proceso de escaneo se debe tener en consideración que de acuerdo con su tipo se podrán utilizar las siguientes herramientas de apoyo:

- ✓ Software especializado para el análisis de vulnerabilidades lógicas (Netsus), que se encarga de detectar posibles amenazas en el sistema de información.
- ✓ Para el caso de la física, se apoyará del proceso de auditoría para identificar las vulnerabilidades.
- ✓ Si el grupo de vulnerabilidades detectado materializan una amenaza, se procede por parte del director de TIC y/o Asistente de Comunicaciones a realizar las acciones de mejora e implementar los respectivos controles, para esto se deberá determinar las acciones de corrección y las acciones correctivas que permitirán mitigar, eliminar o trasferir las amenazas detectadas.

En caso de que el plan de acción estipulado en el formato de acciones de mejora se haya implementado y se llegan a presentar nuevos problemas se deberá implementar en conjunto con el responsable de las Comunicaciones las respectivas mejoras a que haya lugar o actualizar los controles existentes si es el caso.

Cuando ya se hayan implementado las respectivas acciones para la corrección, el coordinador o asistente de Comunicaciones deberá volver a realizar el escaneo de análisis de vulnerabilidades para identificar si aún persisten las amenazas o fueron solucionadas efectivamente.

ANEXO C. DECLARACIÓN DE APLICABILIDAD

ESTRATEGIAS EMPRESARIALES	Fecha de elaboración	20/11/2019
	Clasificación del documento	Privado
DECLARACIÓN DE APLICABILIDAD	Convenciones utilizadas en controles:	
	RL: Requerimiento legal,	
	OC: Obligación contractual,	
	RN: Requerimiento del negocio	
	MP: Mejores prácticas	

CONTROLES DEFINIDOS ANEXO A ISO 27001:2013			**Control**	**Justificación de exclusión**	**Controles**				**Documento**	**Responsable del control**
Dominio	**Sección**	**Objetivo de control/Control**			**RL**	**OC**	**RN**	**MP**		
Políticas de la Seguridad de la Información	A.5.1.1	Políticas para la seguridad de la información.	Implementación de la política de seguridad de la información					X	Política de Seguridad	Oficial seguridad de la información
	A.5.1.2	Revisión de las políticas de seguridad de la información.	Una vez implementada la política de seguridad de la información, se establece como periodo de revisión el último mes de cada año, o en su defecto, cada que ocurran cambios significativos en la organización					X	Política de Seguridad	Oficial seguridad de la información

Organización de la seguridad de la información	A.6.1	**ORGANIZACIÓN INTERNA**								
	A.6.1.1	Roles y responsabilidades para la seguridad de la información	Definición de los roles y responsabilidades aplicados para la seguridad de la información					X	Manual de responsabilidades específica para el sistema de gestión de seguridad de la información	Director de Gestión Humana
	A.6.1.2	Segregación de funciones y responsabilidades	Distribución de cargos por organigrama para el proceso de tecnología. Se realiza reestructuración de cargos					X	Mapa de procesos. Organigrama especifico por procesos.	Director de Gestión Humana
	A.6.1.3	Contacto con las autoridades	Establecer directorio de autoridades relacionadas con TIC					X	Directorio TIC	Gerente de TIC
	A.6.1.4	Contactos con grupos de interés especiales	Incluir en directorio TIC, los grupos de interés específicos, además de los proveedores					X	Directorio TIC	Gerente de TIC
	A.6.1.5	Seguridad de la información en la gestión de proyectos	Protocolo para pruebas técnicas y de calidad en seguridad de la información para los proyectos a implementar					X	Manual de pruebas de seguridad	Coordinador de desarrollo y Coordinador de telecomunicaciones
	A.6.2	**DISPOSITIVOS MOVILES Y TELETRABAJO**								
	A.6.2.1	Política para dispositivos móviles	Dentro de la política de seguridad de la información, definir					X	Política de seguridad de la información	Oficial de seguridad de la información

			dispositivos y aplicaciones permitidas							
	A.6.2.2	Teletrabajo	Incluir en manuales de funciones, reglamento interno de trabajo y política de seguridad de la información, responsabilidad, medidas reglamentarias y protocolo para el teletrabajo					X	Manual de funciones, reglamento interno, política de seguridad	Gerente de TIC y oficial de seguridad de la información.
Seguridad de los recursos humanos	A.7.1	**ANTES DE ASUMIR EL EMPLEO**								
	A.7.1.1	Selección	Procedimiento documentado para la selección y contratación de personal.			X			Procedimiento de selección y contratación	Director de Gestión Humana
	A.7.1.2	Términos y condiciones laborales	En cada contrato laboral quedaron específicos, términos y condiciones, así como las responsabilidades relacionadas a la seguridad de la información.			X			Contrato laboral	Director de Gestión Humana
	A.7.2	**DURANTE LA EJECUCIÓN DEL EMPLEO**								
	A.7.2.1	Responsabilidades de la dirección	Definir las responsabilidades y rol que se tiene respecto a la seguridad de la información.				X		Responsabilidades definidas en el SGSI.	Director de Gestión Humana

	A.7.2.2	Toma de conciencia, educación formación y concientización en la seguridad de la información.	Capacitación especifica en el SGSI a través de las inducciones y reinducciones periódicas al personal					X	Presentaciones digitales magnéticos Formatos de capacitación	Director de Gestión Humana
	A.7.2.3	Proceso disciplinario	Este procedimiento se encuentra documentado y está a cargo del proceso jurídico con acompañamiento de gestión humana. Adicional se encuentran reglamentadas sanciones en el reglamento interno de trabajo. Se debe reestructurar la parte de seguridad de la información.					X	Reglamento interno. Procedimiento disciplinario	Director de Gestión Humana
	A.7.3	**TERMINACIÓN Y CAMBIO DE EMPLEO**								
	A.7.3.1	Terminación o cambio de responsabilidades de empleo	Inclusión de clausula en los contratos donde se especifica de manera particular, cuales son las causales de terminación del contrato			X			Contrato laboral	Director de Gestión Humana
Gestión de activos	A.8.1	**RESPONSABILIDAD POR LOS ACTIVOS**								
	A.8.1.1	Inventario de activos	Establecer procedimientos de compras y para la gestión de los activos					X	Procedimiento compras Procedimiento de gestión de activos	Director de Gestión Humana

	A.8.1.2	Propiedad de los activos	Implementación del Procedimiento compras					X	Procedimiento compras	Director de Gestión Humana
	A.8.1.3	Uso aceptable de los activos	Implementación del Procedimiento compras					X	Procedimiento compras	Director de Gestión Humana
	A.8.1.4	Devolución de activos	Implementación del Procedimiento compras					X	Procedimiento compras	Director de Gestión Humana
	A.8.3	**MANEJO DE MEDIOS**								
	A.8.3.1	Gestión de los medios removibles	Implementar procedimiento para la gestión de medios removibles					X	Procedimiento para la gestión de medios removibles	Oficial de seguridad de la información
Control del acceso	**A.9.1**	**REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO**								
	A.9.1.1	Política de control de acceso	Establecer e implementar el procedimiento para el control de acceso				X		Procedimiento de control de acceso	Oficial de seguridad de la información
	A.9.1.2	Acceso a redes y servicios en red	Establecer e implementar el procedimiento para el control de acceso				X		Procedimiento de control de acceso	Oficial de seguridad de la información
	A.9.2	**GESTIÓN DEL ACCESO DE USUARIOS**								
	A.9.2.1	Registro y cancelación de usuarios	Establecer procedimiento para la asignación y cancelación de usuarios					X	Procedimiento asignación y cancelación de usuarios	Oficial de seguridad de la información

	A.9.2.2	Suministro de acceso de usuarios	Establecer procedimiento para la asignación y cancelación de usuarios					X	Procedimiento asignación y cancelación de usuarios	Oficial de seguridad de la información
	A.9.2.3	Gestión de derechos de acceso privilegiado	Establecer procedimiento para la asignación y cancelación de usuarios					X	Procedimiento asignación y cancelación de usuarios	Oficial de seguridad de la información
	A.9.2.4	Gestión de información de autenticación secreta de usuarios - Contraseñas	Establecer procedimiento para la asignación y cancelación de usuarios					X	Procedimiento asignación y cancelación de usuarios	Oficial de seguridad de la información
	A.9.2.5	Revisión de los derechos de acceso de los usuarios	Establecer procedimiento para la asignación y cancelación de usuarios					X	Procedimiento asignación y cancelación de usuarios	Oficial de seguridad de la información
	A.9.2.6	Supresión, o modificación de los derechos definidos para el acceso de usuarios	Establecer procedimiento para la asignación y cancelación de usuarios					X	Procedimiento asignación y cancelación de usuarios	Oficial de seguridad de la información
	A.9.3	**RESPONSABILIDADES DE LOS USUARIOS**								
	A.9.3.1	Uso de información de autenticación secreta (contraseñas)	Establecer procedimiento para la asignación y cancelación de usuarios				X		Procedimiento asignación y cancelación de usuarios	Oficial de seguridad de la información
	A.9.4	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**								

	A.9.4.1	Restricción de acceso a la información	Diseño y aplicación del procedimiento de control de para el acceso					X	Procedimiento para el control de acceso	Oficial de seguridad de la información
	A.9.4.2	Procedimientos de ingreso seguro	Diseño y aplicación del procedimiento de control de para el acceso					X	Procedimiento para el control de acceso	Oficial de seguridad de la información
	A.9.4.3	Sistema de gestión de contraseñas	Diseño y aplicación del procedimiento de control de para el acceso					X	Procedimiento para el control de acceso	Oficial de seguridad de la información
	A.9.4.4	Uso de programas utilitarios privilegiados	Diseño y aplicación del procedimiento de control de para el acceso					X	Procedimiento para el control de acceso	Oficial de seguridad de la información
	A.9.4.5	Control de acceso al código fuente de los programas	Diseño y aplicación del procedimiento de control de para el acceso					X	Procedimiento para el control de acceso	Oficial de seguridad de la información
Seguridad física y del entorno	A.11.1	**AREAS SEGURAS**								
	A.11.1.1	Perímetro de seguridad física	Implementar procedimiento para la gestión de la seguridad física					X	Gestión para la seguridad física	Oficial de seguridad de la información
	A.11.1.2	Controles de acceso físico	Implementar procedimiento para la gestión de la seguridad física					X	Gestión para la seguridad física	Oficial de seguridad de la información
	A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Implementar procedimiento para la gestión de la seguridad física					X	Gestión para la seguridad física	Oficial de seguridad de la información
	A.11.1.4	Protección contra amenazas externas y ambientales	Implementar procedimiento para la					X	Gestión para la seguridad física	Oficial de seguridad de la información

			gestión de la seguridad física							
	A.11.1.5	Trabajo en áreas seguras	Implementar procedimiento para la gestión de la seguridad física					X	Gestión para la seguridad física	Oficial de seguridad de la información
	A.11.1.6	Áreas de carga, despacho y acceso público	Implementar procedimiento para la gestión de la seguridad física					X	Gestión para la seguridad física	Oficial de seguridad de la información
Seguridad de las Operaciones	A.12.1	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**								
	A.12.1.2	Gestión de cambios	Implementar procedimiento de gestión de cambios y de capacidad				X		Procedimiento de gestión de cambios y capacidad	Jefe de infraestructura y servicios
	A.12.1.3	Gestión de la capacidad	Implementar procedimiento de gestión de cambios y de capacidad				X		Procedimiento de gestión de cambios y capacidad	Jefe de infraestructura y servicios
Seguridad de las comunicaciones	**A.13.1**	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**								
	A.13.1.1	Control de redes	Implementar procedimiento o protocolo para la seguridad de la red				X		Gestión de la seguridad de la red	Coordinador de telecomunicaciones
	A.13.1.2	Seguridad de los servicios de red	Implementar procedimiento o protocolo para la seguridad de la red				X		Gestión de la seguridad de la red	Coordinador de telecomunicaciones
	A.13.1.3	Separación en las redes	Implementar procedimiento o protocolo para la seguridad de la red					X	Gestión de la seguridad de la red	Coordinador de telecomunicaciones
	A.13.2	**TRANSFERENCIA DE INFORMACIÓN**								

	A.13.2.1	Políticas y procedimientos de transferencia de información	Implementar procedimiento o protocolo para la seguridad de la red					X	Gestión de la seguridad de la red	Oficial de seguridad de la información
Adquisición, desarrollo y mantenimiento de sistemas	A.14.1	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**								
	A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Exclusión	Las aplicaciones de la empresa no circulan a través de redes públicas					–	–
	A.14.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**								
	A.14.2.1	Política de desarrollo seguro	Establecer protocolo para desarrollos y pruebas en ambientes controlados				X		Desarrollos y pruebas en ambientes controlados	Coordinador de desarrollo
	A.14.2.2	Procedimientos de control de cambios en sistemas	Implementación de procedimiento de gestión de cambios					X	Gestión de cambios	Coordinador de desarrollo
	A.14.2.5	Principios de construcción de los sistemas seguros	Establecer protocolo para desarrollos y pruebas en ambientes controlados				X		Desarrollos y pruebas en ambientes controlados	Coordinador de desarrollo
	A.14.2.6	Ambiente de desarrollo seguro	Establecer protocolo para desarrollos y pruebas en ambientes controlados					X	Desarrollos y pruebas en ambientes controlados	Coordinador de desarrollo
	A.16.1	**GESTIÓN DE LOS INCIDENTES Y LAS MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**								

Gestión de los incidentes de la seguridad de la información	A.16.1.1	Responsabilidades y procedimientos	Diseño e implementación del procedimiento de gestión de incidentes y reportes					X	Procedimiento de gestión de incidentes y reportes	Oficial de seguridad de la información
	A.16.1.2	Reporte de eventos de seguridad de la información	Diseño e implementación del procedimiento de gestión de incidentes y reportes					X	Procedimiento de gestión de incidentes y reportes	Oficial de seguridad de la información
	A.16.1.3	Reporte sobre las debilidades de la seguridad	Diseño e implementación del procedimiento de gestión de incidentes y reportes					X	Procedimiento de gestión de incidentes y reportes	Oficial de seguridad de la información
	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Diseño e implementación del procedimiento de gestión de incidentes y reportes					X	Procedimiento de gestión de incidentes y reportes	Oficial de seguridad de la información
	A.16.1.5	Respuesta a incidentes de seguridad de la información	Diseño e implementación del procedimiento de gestión de incidentes y reportes					X	Procedimiento de gestión de incidentes y reportes	Oficial de seguridad de la información
	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Diseño e implementación del procedimiento de gestión de incidentes y reportes					X	Procedimiento de gestión de incidentes y reportes	Oficial de seguridad de la información
	A.16.1.7	Recolección de evidencia	Diseño e implementación del procedimiento de gestión de incidentes y reportes					X	Procedimiento de gestión de incidentes y reportes	Oficial de seguridad de la información

gestión de la continuidad del negocio	A.17.1	**CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN**								
	A.17.1.1	Planificación de la continuidad de la seguridad de la información	Documentar el plan de continuidad del negocio		X				Plan de continuidad del negocio	Gerente TIC y Coordinado BCP
	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Documentar el plan de continuidad del negocio		X				Plan de continuidad del negocio	Gerente TIC y Coordinado BCP
cumplimiento	**A.18.1**	**CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES**								
	A.18.1.3	Protección de los registros	Política de protección de datos personales		X				Política de protección de datos personales	Coordinador BCP
	A.18.1.4	Privacidad y protección de información de datos personales	Política de protección de datos personales		X				Política de protección de datos personales	Coordinador BCP
	A.18.1.5	Reglamentación de los controles criptográficos	Establecer protocolo para control de la criptografía corporativa					X	Protocolo para el control criptográfico	Oficial de seguridad de la información
	A.18.2	**REVISIONES DE SEGURIDAD DE LA INFORMACIÓN**								
	A.18.2.1	Revisión independiente de la seguridad de la información	Resultados de auditorías internas y externas					X	Practica semestral	Coordinador de auditoria
	A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Plan de auditoria TIC que incluya monitoreo de políticas					X	Practica semestral	Coordinador de auditoria
	A.18.2.3	Revisión del cumplimiento técnico	Se propone incluir pruebas periódicas en el plan de implementación anual					X	Practica semestral	Gerente de TIC, coordinador de auditoria y

			de TIC, pruebas de conectividad y carga que se realicen sobre las aplicaciones y con monitoreo de auditoria TIC que certifique la capacidad de procesamiento							oficial de seguridad de la información