Universidad Hispanoamericana

Escuela de Ingeniería Informática

Licenciatura en Sistemas de Información

Tema de estudio:

Desarrollo de una política de seguridad informática bajo las normas ISO/IEC 27001 e ISO/IEC 27002 para salvaguardar los activos informáticos de la empresa Ali-mentos S.A.

Proyecto de graduación para optar por el grado de licenciatura en Ingeniería Informática con énfasis en sistemas de comunicación

Elaborado por:

Luis C. Ilama Torres

Tutor:

Lic. Pedro Leiva Chinchilla

Heredia, Costa Rica

Fecha: marzo 2021

Tabla de Contenido

Índice de Tablas

Índice de Figuras

Declaración Jurada

DECLARACIÓN JURADA

Yo Luis Cristian Ilama Torres, con número de cédula 1-0862-0200 egresado de la carrera de Ingeniería Informática con énfasis en sistemas de comunicación de la universidad Hispanoamericana, hago constar por medio de este acto y debidamente apercibido y entiendo de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura en Ingeniería Informática, juro solemnemente que mi trabajo de investigación que lleva como título: Desarrollo de una política de seguridad informática bajo las normas ISO/IEC 27001 e ISO/IEC 27002 para salvaguardar los activos informáticos de la empresa Ali-mentos. S.A., es obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982; incluyendo el numeral 70 de dicha ley que advierte; artículo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que esto no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad Hispanoamérica se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los 23 días del mes de 07 del año dos mil veintiuno.

LUIS CRISTIAN ILAMA TORRES (FIRMA)

Firmado digitalmente por LUIS CRISTIAN ILAMA TORRES (FIRMA)
Fecha: 2022.01.27 16:32:50 -06'00'

Firma del estudiante
Cédula: 1-0862-0200

Carta Aprobación del Tutor y Contraparte

CARTA DEL TUTOR

San José, 29 de Enero del 2022

Ing. Maria Isabel Losilla Barrientos.
Facultad de Computación
Universidad Hispanoamericana

Estimada señora:

El estudiante Luis C. Ilama Torres, cédula de identidad número 1-0862-0200, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado "Desarrollo de una política de seguridad informática bajo las normas ISO/IEC 27001 e ISO/IEC 27002 para salvaguardar los activos informáticos de la empresa Ali-mentos S. A.", el cual ha elaborado para optar por el grado académico de Licenciatura en Ingeniería Informática.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	10%
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	15%
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACIÓN	30%	30%
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	15%
e)	CALIDAD, DETALLE DEL MARCO TEÓRICO	20%	20%
	TOTAL		90%

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

Firmado digitalmente por PEDRO IGNACIO LEIVA CHINCHILLA (FIRMA)
Fecha: 2022.01.29 20:21:20 -06'00'

MS.c. Pedro Ignacio Leiva Chinchilla
1-1394-0453

CARTA DE LECTOR

San José,

Universidad Hispanoamericana
Sede Llorente
Carrera de Informática

Estimado señor

El estudiante Luis C. llama Torres, cédula de identidad 1-0862-0200, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado " Desarrollo de una política de seguridad informática bajo las normas ISO/IEC 27001 e ISO/IEC 27002 para salvaguardar los activos informáticos de la empresa Ali-mentos S.A.", el cual ha elaborado para obtener su grado de Licenciatura en Ingeniería Informática con énfasis en sistemas de comunicación.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.

Randall Vargas Villalobos

Firmado digitalmente por Randall Vargas Villalobos
Fecha: 2022.02.10 15:06:53 -06'00'

Firma
Randall Vargas Villalobos
Cédula: 1-1140-0113

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 27 de enero 2022

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Luis Cristian Ilama Torres con número de identificación 108620200 autor (a) del trabajo de graduación titulado **Desarrollo de una política de seguridad informática bajo las normas ISO/IEC 27001 e ISO/IEC 27002 para salvaguardar los activos informáticos de la empresa Ali-mentos S.A.** presentado y aprobado en el año 2022 como requisito para optar por el título de Licenciatura en Ingeniería Informática; si autorizo al Centro de Información Tecnológico (CENIT) para que, con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento esto por solicitud del director y supervisor del proyecto de la Empresa.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

LUIS CRISTIAN ILAMA TORRES (FIRMA)

Firmado digitalmente por LUIS CRISTIAN ILAMA TORRES (FIRMA)
Fecha: 2022.01.27 16:04:30 -06'00'

Firma y Documento de Identidad

Dedicatoria

Esta tesis es dedicada a Dios por darme salud para lograr terminar mi carrera y así cumplir mi sueño de obtener el título aprendiendo, a mi Madre quién ha sido el motor de motivación para no desmayar cuando ya mis fuerzas parecían acabarse, y a toda mi familia que me han motivado a estudiar viendo en mi un ejemplo para todos ellos.

Agradecimientos

Mi agradecimiento a Dios por darme la oportunidad de estudiar y aprender, darme entendimiento para sobrellevar cada una de las pruebas y salud para lograr con éxito el alcance de la meta.

A mi madre quién siempre estuvo a mi lado y me ayudó en los momentos difíciles de mi carrera, brindándome apoyo y motivándome a seguir adelante.

A mi familia a quienes no pude atender para seguir estudiando, quienes sacrificaron algunos momentos de compartir y que no pude estar ahí para dedicarle el tiempo necesario a los trabajos y proyectos.

A todos los profesores y los directores de la carrera quienes siempre estuvieron ahí para darme la mano en cada situación.

A mi tutor quien me guio y aconsejó por todo el proceso de la tesis.

Abreviaturas

- **MAGERIT**: Metodología de análsis y gestión de riesgos.
- **COBIT**: Objetivos de Control para Tecnología de Información y Tecnologías relacionadas.
- **ISO**: Organización Internacional de Normalización.
- **IEC**: Comisión Electrotécnica Internacional.
- **TI**: Tecnología de la Información.
- **BRC**: Consorcio Británico de Minoristas
- **CENAM**: Centroamérica y el Caribe
- **DBA**: Administrador de base de datos.
- **REDES SAS**: Conectado en serie.
- **OECD**: Organización para la Cooperación y el Desarrollo Económicos.
- **VPN**: Red privada virtual.
- **SGSI**: Sistema de seguridad de la información.
- **PHVA**: Planear, hacer, verificar y actuar.
- **UNED**; Universidad Estatal a Distancia.
- **INTECO**: Instituto de Normas Técnicas de Costa Rica.
- **WEB**: Red informática mundial.
- **TEC**: Tecnológico de Costa Rica.
- **RyD**: Investigación y Desarrollo.
- **AP**: Punto de acceso.
- **RDP**: Protocolo de escritorio remoto.
- **UPS**: Sistema de Alimentación Ininterrumpida.
- **WIFI**: Fidelidad inalámbrica.
- **HP**: Hewlett Packard.
- **CA**: Corriente Alterna.
- **ERP**: Sistema de planificación de recursos empresariales.
- **BIOS**: Sistema básico de entrada y salida.

Resumen

Este estudio tuvo como fin diseñar una política de seguridad informática para la empresa Ali-mentos S.A. de Costa Rica, basada en ISO/IEC 27001 e ISO/IEC 27002 para el uso adecuado de sus activos informáticos, y con esto ayudar a reforzar la integridad, confidencialidad y disponibilidad de los datos.

El alcance de este estudio tuvo como objetivo la revisión a los procedimientos actuales, en general, en el manejo de los activos que se está realizando en la empresa a nivel de hardware e información interna importante para la compañía y los usuarios.

Lo anterior con la intención de diseñar la política general de seguridad informática para los usuarios de los sistemas informáticos y el manejo de datos cuando se esté laborando dentro y fuera de la compañía.

Con un análisis de riesgo, se revisaron los riesgos potenciales a nivel de uso de activos informáticos, se aplicó la herramienta MAGERIT V.3 y se complementó con alguna información de COBIT 5 en su apartado APO013, esto ayudó a guiar este trabajo y a alcanzar los resultados para la propuesta de la política de seguridad informática.

También se usó las normas ISO/IEC 27001 e ISO/IEC 27002 para establecer el marco de referencia que se usó para crear la política de seguridad informática para la compañía que ayude en el buen uso de sus activos informáticos.

Una vez que se obtuvo los resultados y todos los entregables, se entregaron a la dirección, junto con la propuesta de la política que podrán implementar en la compañía

para resguardar la integridad y asegurar la disponibilidad de los datos que necesitan para la toma de decisiones.

Esta política es a nivel general y será implementada por la dirección del departamento de TI, el cual le dará el seguimiento adecuado para que esta sea de cumplimiento obligatorio por todos los usuarios de la compañía, tanto a lo interno como a lo externo cuando se aplique trabajo en casa.

Capítulo 1 : Problema del Proyecto

Las nuevas tecnologías y los modernos procedimientos en los trabajos, la búsqueda de competir en el mercado de una manera profesional lleva a las empresas a buscar la forma de mantenerse en pie de lucha y de ser competitivos en el mercado que dominan según su nicho.

Al pasar los años, las empresas han adoptado nuevos conocimientos, en estos tiempos la estructura, políticas, procedimientos y la administración han cambiado de forma radical, es por esto por lo que, para ser competitivos en estos días, hay que estar actualizados en todos los aspectos que confieren el desarrollo y la actualización de los procesos informáticos para la toma de decisiones.

Hoy en día las compañías cuentan con muchas herramientas que les ayudan a participar y a mantenerse a un alto nivel de competencia, las certificaciones como ISO, BRC, herramientas como MAGERIT, COBIT y muchas otras, son opciones que pueden elegir para asegurase un campo en la competencia de los proveedores de servicios y/o productos.

Entre estos están los que son dirigidos a salvaguardar uno de los activos esenciales de las compañías, la información, ya que esta se usa para la toma de decisiones y ayuda a mantener a la compañía en el mercado dándole las bases para cumplir con su misión.

En este trabajo se utiliza algunas de estas herramientas, por ejemplo, MAGERIT- versión 3.0 que es una metodología para el análisis de riesgo y gestión de estos a nivel de sistemas de información, y se apoya en las recomendaciones de COBIT 5 y su apartado APO13.

Lo anterior con el fin de realizar un análisis para la empresa Ali-mentos S.A. en sus activos informáticos, revisar sus procesos y diseñar una política de seguridad informática basada en ISO/IEC 27001 e ISO/IEC 27002.

Con esta política de seguridad informática, se quiere garantizar la integridad, confidencialidad y disponibilidad de la información, además, reducir el riesgo de pérdida de activos durante su manipulación.

1.1. Planteamiento del Tema

Para comprender la razón de ser de Ali-mentos S.A., en este capítulo se va a revisar su propósito, el valor, la visión y misión a través de sus antecedentes y su cultura, se detallará la fecha de cuando fue creada y sus actuales metas en el mercado de los Alimentos.

En la justificación del proyecto se describe por qué se decidió este tema de seguridad informática y cuáles son las causas principales que están afectando a la compañía para realizar un cambio en los procesos en el manejo de sus activos.

1.2. Antecedentes

En esta sección se describe, en un pequeño resumen, el nacimiento de la compañía, como fue que su creador tuvo una visión futurista para alcanzar el éxito de esta, y su trayectoria hasta lo que es hoy Ali-mentos S.A.

1.2.1. Marco de Referencia Empresarial y Contextual

La Empresa Ali-mentos S.A. fue fundada en 1919 y la Revista Digital Alimentaria de la cámara Costarricense de la Industria Alimentaria, cuenta lo siguiente:

Ali-mentos S.A. inició hace un siglo como una pequeña empresa familiar, con la convicción de que el alimento no solamente proviene de lo que hay en el plato sino de lo que hay “dentro del corazón”.

Desde entonces, se ha enfocado en el desarrollo de soluciones a la medida de las necesidades y deseos de los consumidores en términos de sabor, textura, seguridad, desempeño, salud y nutrición, conveniencia y mucho más.

Hoy cuentan con una diversidad de productos que van desde salsas, aderezos, marinadores, sazonadores hasta mezclas de panadería, también ingredientes para la industria cárnica, sistemas de cobertura, bases culinarias, mezclas funcionales y mezclas para hacer helados.

En pleno conocimiento del rol trascendental que juega la innovación colaborativa, la compañía se ha esmerado por evolucionar para satisfacer y servir las necesidades de no solo las personas, sino del planeta. De esta forma trabajan con sus clientes alrededor del mundo para crear productos relevantes en sus consumidores, de una manera respetuosa con el medio ambiente (CACIA, 2019).

Ali-mentos S.A. se rige bajo la norma BRC por sus siglas en inglés que es un estándar mundial para la seguridad de los alimentos y fue creada bajo el Consorcio Británico de Minoristas, Ali-mentos S.A. S.A. alcanzó en marzo 2021, su nuevo certificado AA bajo esta norma.

Esta norma tiene doble finalidad que es asegurar el cumplimiento de los proveedores y además proporcionar a los minoristas una herramienta, la cual es

garantizar la calidad y seguridad de los productos alimenticios que comercializan (Anexia, Tecnologías, 2018).

La estrategia de la compañía se rige por sus valores, misión y objetivos que se detalla:

1.2.1.1. Misión. Crear resultados: Somos responsables de cumplir nuestros compromisos, realizándolos con excelencia, valorando los resultados y premiando el éxito.

1.2.1.2. Visión. Mejorar el Futuro: A través de la imaginación y la innovación, fomentamos un espíritu optimista que motiva para asumir riesgos y persistir para realizar nuestros sueños. Siempre creemos que el futuro puede ser incluso mejor.

1.2.1.3. Objetivos. Crear el éxito de tus clientes: Reconociendo que nuestro éxito depende del éxito de nuestros clientes, trabajamos para crear valor, generando crecimiento y prosperidad para nuestros clientes.

1.2.1.4. Organización. El tipo de organización es familiar ya que viene precedida de generaciones anteriores y se ha ido heredando a través de los años.

1.2.1.5. Negocio al que se Dedica. Ali-mentos S.A. es un socio de desarrollo de productos especializado en ingredientes alimentarios, proveedor de empresas de alimentación mundiales y regionales de todo el planeta.

1.2.1.6. Equipo de Trabajo TI. La dirección de TI es la que está a cargo de todo lo que tiene que ver con el soporte, funciones, mantenimiento, infraestructura, seguridad informática (soporte), creación de roles, proyectos, hardware, software, base

de datos, análisis de datos, oportunidad e inteligencia del negocio y todo el soporte a la Gerencia General en temas informáticos.

Por lo anterior se va a realizar un pequeño resumen de la estructura de este departamento, esto con el fin de guiar este trabajo en función de cada rol y tener claro a quien se le debe consultar en caso de que se requiera alguna información del área que maneja cado uno.

1.2.1.6.1. Organigrama de la Dirección de Tecnología de Información CENAM. En el siguiente organigrama se puede ver la estructura del departamento de TI y el área en que se desempeña cada colaborador. En la dirección de TI, en el primer nivel del organigrama, está el Director de TI quien tiene a cargo directamente a cada uno de los colaboradores del departamento.

Vemos que la estructura del departamento es plana ya que son solo dos niveles y centralizada en su director, cada colaborador le reporta directamente al director y no hay delegaciones, esto ayuda al departamento a ser mucho más productivos ya que, en la toma de decisiones, están involucrados cada uno de ellos.

Con base a la definición anterior, se puede decir que trabajan en función de productividad en todo lo que hacen en el día a día.

La Figura 1.1 ayuda a comprender la estructura del departamento de TI en abril 2021, el fin de esta es ayudar en este trabajo a identificar los roles de cada colaborador y así saber a quién consultar sobre cada tema que se requiera profundizar.

Figura 1.1

Organigrama de la Dirección de TI, abril 2021

1.2.1.6.2. Descripción de Puestos y Roles. Seguidamente, con base al organigrama anterior se va a presentar la tabla 1-1 donde se ve reflejado cada rol del equipo de trabajo del departamento de TI, este consta de cuatro columnas donde se describe el nombre del colaborador, el puesto que desempeña y su rol en el departamento, también si es parte o si tiene algún rol en el proyecto.

Se presenta el detalle de cada posición y sus roles:

Tabla 1-1:

Descripción y Roles del equipo de TI, abril 2021

Colaborador	Posición	Responsabilidades	Rol en el Proyecto
Gerencia	Director de TI	Administrador general de la dirección (continuidad del negocio)	Patrocinador, aprobación de cambios, supervisión de avances y aprobación o rechazo de la política de seguridad.

Colaborador	Posición	Responsabilidades	Rol en el Proyecto
Analista	Analista de Negocios y Sistemas TI	Colaborador y apoyo en los sistemas de TI	Consultado en aspectos técnicos
Técnico TI	Soporte Técnico TI	Soporte técnico en Hardware y Software	Consultado en aspectos técnicos
Analista	Analista de Negocios y Sistemas TI	Colaborador y apoyo en los sistemas de TI	Consultado en aspectos técnicos
Analista	Inteligencia de negocios y DBA TI	Apoyo en el análisis de datos y mantenimiento de la base de datos	Consultado en aspectos técnicos
Analista	Administrador de Infraestructura TI	Apoyo en la infraestructura, soporte técnico y telecomunicaciones	Consultado en aspectos técnicos
Técnico TI	Asistente de Soporte TI	Soporte técnico en Hardware y Software	Consultado en aspectos técnicos

1.2.2. Proyectos Similares

A continuación, se detalla algunos proyectos que se encontraron en la red y que son tomados en cuenta para la aplicación de este trabajo, con las experiencias de estos, se recolecta información importante para este trabajo.

1.2.2.1. Diseño e Implementación de Políticas de Seguridad Informática, Red y Virtualización Apoyadas con Software Libre en la Compañía Tecnología y Redes S.A.S. Se ha tomado en cuenta para este proyecto, el proyecto de grado

presentado para optar al título de ingeniero de sistemas de Javier Orlando Alarcón Vargas y que fue publicado el 16 de noviembre de 2016 en Bogotá D.C.

Donde el objetivo del trabajo fue la implementación de un plan integral de optimización de los procesos de infraestructura tecnológica, esta fue aplicado en la Compañía Tecnología y Redes SAS y uno de los fines fue la aplicación de políticas de seguridad informática, red y virtualización.

En este proyecto y según los resultados de los análisis de riegos que se realizó, encontraron que la empresa no contaba con esquemas de alta disponibilidad, por lo que la continuidad del negocio estaba sin ninguna garantía, tampoco contaban con un servicio de réplica alterna (Data Center Alterno), lineamientos de arquitectura empresarial bien definidos ni estándares internacionales.

El otro tema es la calidad de la seguridad de la información que no contaba con políticas que garantizarán la integridad, disponibilidad y la confidencialidad de la información, y que, al igual que lo anterior, afecta directamente a la continuidad del negocio.

Se puede ver en el trabajo, que una vez que se ha realizado el análisis de riesgo, se tiene los cimientos para la política de la seguridad de la información, la propuesta de las políticas son una herramienta importante para garantizar la integridad, disponibilidad y confidencialidad de la información que se usa para la toma de decisiones y garantizar la continuidad del negocio.

Entre las propuestas están las siguiente:

Una política para el uso de correo electrónico que tiene como fin aplicar directrices y lineamientos para su buen uso a nivel, según el trabajo, corporativo e interno.

Una política de control de acceso a todos los activos informáticos que usen información de la compañía y las bases de datos.

Una política de *backup* y restauración con el fin de realizar los respaldos necesarios para información que se manipula en los sistemas informáticos, además, mantener en otro lugar la información actualizada por si se necesita realizar una restauración de la información.

Una política de gestión de activos informáticos con el cual se pueda llevar un inventario de estos y definir responsabilidades para cada usuario para su adecuada manipulación.

Una política de gestión de comunicaciones y operaciones que ayuda a la anterior con el uso correcto de los activos informáticos.

También se propuso políticas para el uso de los servicios de red y licenciamiento y uso de software, con los que se asegura el uso correcto de los servicios internos y el apropiado uso en la red (Alarcón, 2016).

1.2.2.2. Diseño del Plan De Seguridad Informática del Sistema de Información Misional de la Procuraduría General de la Nación. Este trabajo de Grado de Iván Andrés Alfaro Viana y Edwin Vargas León para optar al título de especialista en seguridad informática, presenta un interesante proyecto donde su

objetivo general es el de diseñar un plan de seguridad informática para el sistema de información de la Procuraduría General de la Nación en Colombia.

OBJETIVO GENERAL. Diseñar un plan de seguridad informática para el sistema de información misional de la Procuraduría General de la Nación mediante la aplicación de buenas prácticas de seguridad, que permita desarrollar políticas y estándares claros para la preservación de confidencialidad, integridad y disponibilidad (Alfaro & Vargas, 2016, p.18).

En la redacción de la pregunta del problema del proyecto se busca proteger la información institucional:

PROBLEMA. "¿De qué forma se puede proteger la información institucional que se maneja en el sistema de información misional –SIM- de la Procuraduría General de la Nación?" (Alfaro & Vargas, 2016, p.17).

Se puede ver en los objetivos especificos como los proyectos siguien en la misma línea para alcazar el mismo resultado, politicas y herramientas que ayuden a mantener la integridad, confidencialidad e intergridad de los datos:

OBJETIVO ESPECÍFICOS

- Analizar el estado actual de seguridad informática para el sistema misional de la Procuraduría General de la Nación.
- Verificar la metodología utilizada para el análisis de riesgo usada en el sistema de información misional.
- Identificar los riesgos asociados al sistema de información misional.

- Determinar las posibles políticas de seguridad informática del sistema de información misional SIM.
- Plantear las medidas y procedimientos adecuados para dar cumplimiento a las políticas de seguridad informática del sistema de información misional (Alfaro & Vargas, 2016).

Se puede ver como el manejo de la información en cualquier sistema de cualquier parte del mundo, necesita los controles necesarios para garantizar la integridad, confidencialidad y disponibilidad de la información y de los activos informáticos.

Se logra entender en el objetivo general, la línea que siguen basados en el desarrollo de políticas y estándares para lograr su objetivo, y así, realizar con éxito su proyecto asegurando con esto, alcanzar las metas propuestas sin evadir los detalles importantes gracias a las herramientas como lo son COBIT y MAGERIT, ISO y muchas otras.

Igual al proyecto anterior o muchos otros que se han realizado en los temas de seguridad informática, este proyecto comienza con el análisis de estado actual de la seguridad informática, revisando las metodologías que se usaban en ese momento, identificando los riesgos a los que se enfrentaba el sistema, luego con los resultados, diseñar las políticas de seguridad que se ajusten a estos sistemas y el cómo hacer para que sean aplicadas en toda la compañía.

Poco a poco, conforme avanza la lectura de este trabajo, se va desarrollando cada una de las etapas de análisis, y con los hallazgos, se va definiendo y proponiendo

cada una de las mitigaciones para cada punto, además, en las conclusiones y recomendación se hace énfasis en la importancia de utilizar las metodologías correctas para identificar las debilidades y los riesgos en cualquier mejora que se vaya a realizar en los sistemas.

Se puede ver que las políticas de seguridad son el resultado de la mayoría de las propuestas para la mitigación de riesgos de cualquier empresa, y que la mayoría de las recomendaciones es usar políticas de seguridad que ayuden a dar continuidad a las propuestas de cambio, se asegure que se cumplan los procedimientos establecidos y que se garantice la continuidad de la operación.

1.3. Justificación del Proyecto

"Las políticas de seguridad informática son una serie de normas y directrices que garantizan la confidencialidad, integridad y disponibilidad de la información" (UNIR - Universidad Internacional de La Rioja, 2020).

También indica que:

> Estas políticas a alto nivel, ayuda a minimizar el riesgo que puedan afectar directa o indirectamente a los activos informáticos de la compañía, a proteger y proveer controles que se deben implementar en los procedimientos internos por medio de instrucciones técnicas (UNIR - Universidad Internacional de La Rioja, 2020).

Es por lo anterior que es importante tomar en cuenta que contar con las herramientas necesarias para proteger la información que se recibe a diario en los sistemas informáticos, es una obligación, no un lujo que se pueda tomar o no.

Con estas herramientas se debe asegurar que los activos informáticos como hardware, software y datos, no se vean afectados por algún tipo de amenaza o mala manipulación de los usuarios, o por falta de políticas de seguridad informática que les ayuden a salvaguardar a estos, lo anterior debido a que son usados por la compañía para la continuidad del negocio.

En el año pasado 2020, debido a la pandemia se incrementó el trabajo en casa, y Ali-mentos S.A., como la mayoría de las compañías, tuvo que cambiar los procesos y amoldarse a esta modalidad que, aunque ya estaba siendo usada en algunas compañías, en Ali-mentos S.A. no había surgido la necesidad de aplicarla.

Debido a esto, el director de TI, en la reunión para ver el tema que se podría aplicar como oportunidad de negocio en este proyecto, propuso realizar la revisión de los procesos de salida de hardware de la compañía y el manejo de la información cuando no están conectados al servidor, y con los resultados, proponer una política general de seguridad informática para el uso de estos activos tan importantes para la empresa.

También se va a tomar en cuenta en este trabajo, el manejo interno de estos activos en los diferentes departamentos, para que la política pueda abarcar toda la compañía en general.

El trabajo en general tarda seis meses en realizarlo y cuatro de esos seis meses serán utilizados para el trabajo de campo en la empresa Ali-mentos S.A. de Costa Rica.

1.4. Definición del Problema

En esta sección se plantea el porqué de la necesidad de una política de seguridad informática en la compañía Ali-mentos S.A. y los beneficios que puede generar este trabajo.

1.4.1. Problemática

Debido a la situación creada por la pandemia Covit-19 en el año 2020, muchas organizaciones tuvieron que restructurar sus procesos para lograr continuar con la operación de sus negocios, reducción de jornadas laborales, de personal, de salarios y muchas otras estrategias más que sirvieron para mantenerse en el mercado.

Ali-mentos S.A. no fue la excepción, y aunque no tuvo la necesidad de las reducciones antes mencionadas, tuvo que realizar ajustes en su estructura para permitir que la operación siguiera adelante. En la parte operativa los cambios fueron mínimos debido a que son pocas las personas que se pudieron enviar a trabajar desde la casa, esto por la naturaleza de sus trabajos.

Sin embargo, a nivel Administrativo se realizó rápidamente cambios en los sistemas y activos informáticos para que tuvieran el acceso a la red interna de la compañía, esto sin perder la seguridad de los datos y asegurando que tuvieran el acceso de todas las herramientas necesarias para la operación.

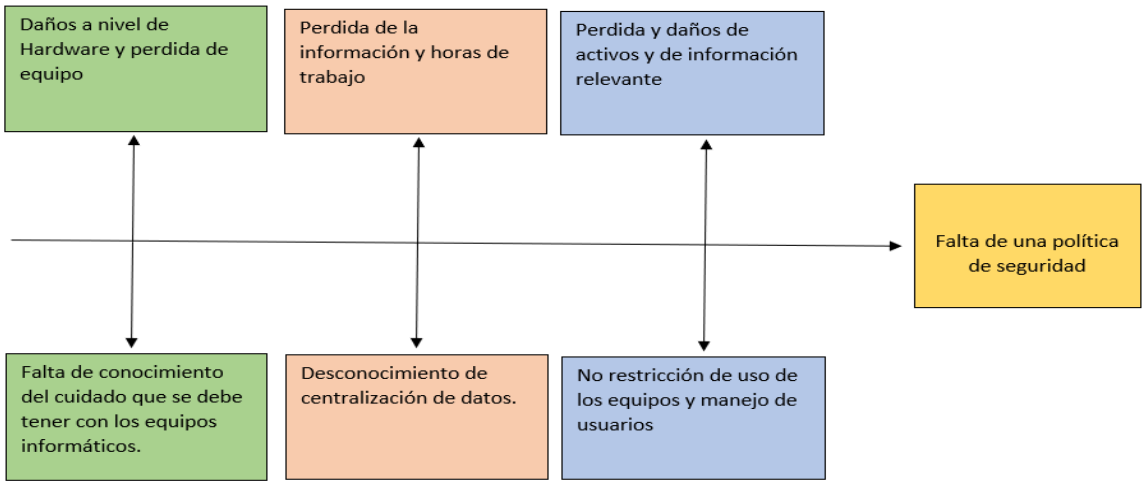
Debido al crecimiento tan rápido y obligatorio de la implementación de trabajo en casa, se ve la necesidad por parte de la dirección de TI de establecer una política de seguridad informática general, para el manejo de la información, hardware y software que salen de la compañía para ser utilizadas desde la casa.

Además, se va a aprovechar este trabajo para realizar una revisión general y fortalecer, con la misma política, la seguridad interna del uso de computadores y de información en todos los departamentos de la compañía donde exista un activo informático que debe conectarse a la red para guardar información.

1.4.1.1. Diagrama Causa-Efecto. En la siguiente figura 1.2 Esquema de Diagrama de Causa y Efecto, se puede ver como la falta de una política de seguridad informática afecta directamente a los activos informáticos de la empresa.

Figura 1.2

Esquema de Diagrama Causa-Efecto



La falta de conocimiento de los usuarios en Ali-mentos S.A. en el uso de los equipos informáticos o manejo adecuado, puede generar graves daños al hardware y software, esto podría ocasionar pérdida de equipos.

El desconocimiento de la centralización de datos en Ali-mentos S.A. de los usuarios que no son de TI, puede causar pérdidas de información y tiempo de trabajos realizados, esto al no saber que, si no se guarda los trabajos en el lugar adecuado (Base de datos, Servidores, La nube…), puede causar la pérdida total o parcial de estos si el equipo llega a fallar.

El acceso a los equipos de la compañía sin la definición de roles y/o herramientas que controlen el ingreso a estos y a los sistemas, puede generar pérdidas de información relevante para Ali-mentos S.A. y para los usuarios.

1.4.2. Problema General

¿Cómo minimizar el riesgo en la integridad, la confidencialidad y disponibilidad de la información en el uso de activos informáticos por medio de una política de seguridad informática en la Empresa Ali-mentos S.A.?

1.4.3. Problemas Específicos

¿Cómo minimizar los riesgos que afectan en los procesos de manipulación de los activos informáticos de la Empresa?

¿Cómo garantizar la confidencialidad de la información en los procesos informáticos de la compañía?

¿De qué manera se puede asegurar la integridad y disponibilidad de la información de los activos informáticos?

1.5. Objetivo General y Objetivos Específicos

Se detalla en seguida los objetivos del proyecto.

1.5.1. Objetivo General

Desarrollar una política de seguridad informática usando las normas ISO/IEC 27001 e ISO/IEC 27002 para el aseguramiento de la confidencialidad, integridad y disponibilidad de la información en el uso de los activos informáticos de la Empresa Alimentos S.A.

1.5.2. Objetivos Específicos

I. Identificar la situación actual de la compañía.

II. Realizar un análisis de riesgo en los procesos de uso de activos informáticos.

III. Evaluar los controles necesarios para mitigar o eliminar los riesgos encontrados en el análisis de riesgo.

IV. Desarrollar una política de seguridad informática acorde a los resultados del análisis de riesgo de este trabajo para presentarla a la Dirección de TI de la empresa.

1.6. Alcance y Limitaciones

En este apartado, el lector del trabajo puede tener una idea resumida de lo que puede encontrar con precisión en la investigación y los fines que busca este proyecto, también las limitantes que se presenten en la elaboración del trabajo de campo.

1.6.1. Alcance

A continuación, los principales alcances de este proyecto:

1.6.1.1. Identificación de la Situación Actual de la Compañía en Procesos del Manejo de Activos Informáticos. Mediante un análisis de riesgo, se revisarán los

procesos actuales en el manejo de los activos informáticos, esto a nivel de hardware, software e información que se almacene en los equipos.

Se realizará una revisión del uso de los sistemas y activos informáticos en todos los departamentos que tenga al menos un equipo que se deba conectar a la red para utilizarlo, también a los equipos que usan para realizar trabajo en casa.

1.6.1.2. Mitigación y/o Eliminación de los Riesgos que se Detecten Basados en el Análisis de estos en el Uso de Activos Informáticos. Con los resultados de la revisión de sistemas y la ayuda de las herramientas seleccionadas para este trabajo, COBIT, MAGERIT, se buscará las mejores opciones para la mitigación o eliminación de los hallazgos en el tema de riesgos.

1.6.1.3. Desarrollo de una Política de Seguridad Informática General Para el Manejo de los Activos. Con base a las normas ISO/IEC 27001/ISO/IEC 27002 y los resultados de la revisión en sistemas, se desarrollará la política de seguridad informática que es el objetivo principal de este trabajo, el cual pretende establecer el alineamiento de este proyecto con la estrategia de la empresa.

No se incluye en el proyecto:

- La implementación y/o desarrollo de Software.
- Manipulación de los procesos actualmente establecidos.
- Al ser un proyecto basado en el uso de los activos informáticos, no se revisará la estructura interna de la base de datos, del funcionamiento del sistema interno ni del hardware de la compañía a nivel de procesos del departamento de TI.

1.6.2. Limitaciones del Proyecto

Dentro de las limitaciones está la Información confidencial de la compañía sobre sus procesos de producción, sus fórmulas y productos.

1.7. Cronograma de Actividades

Se trabajará por fases para asegurarnos un marco de trabajo ordenado y así ayudar a obtener los resultados, en el apartado de los apéndices podremos encontrar, en el Apéndice A, el detalle del cronograma de trabajo y sus diferentes fases.

Con esta herramienta se podrá revisar el avance del proyecto y al contener fechas, se podrá monitorear los tiempos establecidos para cada proceso del proyecto, estas fechas podría variar según el avance del trabajo de campo y las restricciones por el tema de la pandemia.

Estas son las fases en términos general:

Fase l

Reunión con el director de TI para hablar sobre el inicio del proyecto.

Reunión sobre lo aprendido y ver consultas con el equipo de TI.

Fase ll

Identificación de los lugares donde hay colocados activos informáticos de la compañía.

Construcción de diagrama de posición de las áreas donde hay equipos dentro de la compañía.

Identificación de los activos que salen de la compañía para trabajo en casa.

Fase lll

Revisión de Roles

Revisión de Procesos

Fase IV

Análisis de Riesgos aplicando MAGERIT v3

Elaboración Matriz de Riegos base (sin plan de mitigación)

Registro e informe de Hallazgos

Fase V

Respuesta a los Hallazgos

Plan de mitigación

Matriz de Riegos (con el plan de mitigación)

Diseño del informe final

Aplicación de ISO 27001 y 27002

Diseño de la política de Seguridad Informática.

Fase VI

Reunión de cierre

Revisión del Plan de mitigación

Entrega de Matriz de Riegos (con el plan de mitigación)

Entrega del informe final.

Revisión de la política de Seguridad Informática.

Capítulo 2 : Marco Teórico

En este capítulo se detalla conceptos principales del tema en estudio para guiar al investigador en la comprensión del contenido y elaboración de instrumentos de aplicación en el trabajo de campo, el análisis y la propuesta para resolver el problema general (Ulate & Vargas, 2016).

Los fundamentos de la investigación junto con las bases teóricas son mostrados en los siguientes puntos de la estructura de este capítulo, donde se explica y se le da fundamento a las variables establecidas en los objetivos específicos que ayudan a alcanzar el objetivo general del proyecto (Ulate & Vargas, 2016).

La mayor ventaja es la prevención de incorporar teorías obsoletas, y así construir con teorías adecuadas en los tiempos correctos y usando las herramientas correctas, esto para obtener resultados adecuados para las nuevas tecnologías (Ulate & Vargas, 2016).

2.1. Marco contextual Organizacional

Ali-mentos S.A. es una empresa estadounidense que fue fundada en 1919 y llegó a Costa Rica en 1971, empezó en el área básica que fueron las salsas para restaurantes, la mezclas y aditivos para la industria alimentaria.

Gracias al gran trabajo que realizaron y sus resultados cuando la planta estaba en otra ubicación, en julio del 2003 compraron el edificio en Heredia donde actualmente desarrolla los procesos, el crecimiento a nivel operativo y estructural ayudo a alcanzar las metas fijadas hasta hoy.

Hoy en día, abril 2021, Ali-mentos S.A. cuenta con presencia activa en seis continentes con el propósito de nutrir al mundo fusionando creatividad y cuidado,

ayudando a los clientes a satisfacer las necesidades y las de los consumidores, velando en conjunto para que se respete el medio ambiente y así ayudar al mundo.

Hoy Ali-mentos S.A. Costa Rica, aunque sigue el mismo objetivo, ha creado nuevos productos para los clientes y además tiene una nueva línea de productos que vende directamente a los distribuidores en todo el país.

La compañía está estructurada, en Costa Rica, en departamentos y estos centralizados en el presidente de la compañía, lo que ayuda a que la operación sea más productiva y eficiente, los gerentes de cada departamento toman decisiones y, además, están muy cerca del personal para apoyarlos en solucionar cualquier eventualidad donde se debe tomar acciones.

Al ser una empresa familiar, la compañía está enfoca a que sus empleados tengan calidad de vida dentro y fuera de la empresa, motivan y ayudan a los empleados a superarse y a sentirse seguros con sus puestos, dándoles oportunidades de superación y motivándoles con muchas garantías que pueden ayudar en sus vidas personales.

Ali-mentos S.A. está certificada con el estándar europeo BRC que ayuda a dar seguridad a sus clientes de que van a adquirir productos de calidad y al estar respaldados por esta certificación, las garantías internas se ven reflejadas en los productos y resultados.

2.2. Marco Referencial

A continuación, se detallan algunos conceptos básicos utilizados como marco de referencia en este trabajo y como herramientas para la obtención de resultados,

también ayudan con el alineamiento de este en el objetivo general del proyecto, empezando con las variables de los objetivos específicos que son la base para el desarrollo de este trabajo.

2.2.1. Análisis de riesgo

En la primera variable de esta investigación se necesita saber cuál es la situación actual de la empresa en los procesos de uso de activos, para ello se debe realizar una valoración de los sistemas y procesos, clasificarlos según su valoración, y, además, en paralelo realizar una identificación de amenazas por el mal uso o falta de controles de los activos informáticos.

Para la obtención de la información que se necesita y la identificación de las amenazas, se requiere realizar un análisis de riesgo y con este, revisar cuidadosamente el actual proceso que se realiza en los diferentes departamentos.

Pero ¿qué es y cómo se puede realizar un análisis de riesgo?, para esto hay algunos conceptos de los expertos que se deben de revisar:

2.2.1.1. Seguridad: Es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

El objetivo que se debe proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

2.2.1.2. Activos informáticos. Existen muchos tipos de activos, incluyendo:

a) información: archivos y bases de datos, contratos y acuerdos, documentación de sistemas, información de investigaciones, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes de continuidad del negocio, procedimientos de vuelta atrás, pistas de auditoría e información archivada;

b) activos de software: software de aplicación, software de sistemas, herramientas de desarrollo y utilitarios;

c) activos físicos: computadoras, equipos de comunicaciones, medios removibles y otros equipos;

d) servicios: servicios de procesamiento y comunicaciones, servicios generales, por ejemplo: calefacción, iluminación, suministro de energía y aire acondicionado;

e) recursos humanos, y su calificación, habilidades y experiencia;

f) intangibles, tales como reputación e imagen de la organización.

Los inventarios de activos ayudan a garantizar que se logre la protección eficaz de los activos, pero también pueden ser requeridos para otros propósitos del negocio, como por ejemplo por razones de salud y seguridad, financieras o de seguros (gestión de activos). El proceso de compilar un inventario de activos es un prerrequisito importante de la gestión de riesgos. (INTECO, 2014)

2.2.1.3. Disponibilidad. O disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

2.2.1.4. Integridad. O mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

2.2.1.5. Confidencialidad. O que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

A estas dimensiones adecuadas de la seguridad se pueden añadir otras derivadas que acerquen a la percepción de los usuarios de los sistemas de información:

2.2.1.6. Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

2.2.1.7. Trazabilidad. Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual que haya que poner medios y esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

2.2.1.8. Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

2.2.1.9. Análisis de riesgos. Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización… (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

2.2.1.10. Tratamiento de los riesgos. proceso destinado a modificar el riesgo.

Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al indicio de calidad que se requiere

> del servicio. Es más, a veces aceptamos riesgos operacionales para acometer actividades que pueden reportarnos un beneficio que supera al riesgo, o que se tiene la obligación de afrontar. Es por ello por lo que a veces se emplean definiciones más amplias de riesgo…
>
> La evaluación de riesgos es uno de los pasos clave para la implementación de cualquier sistema de gestión de riesgos. Es vital identificar las amenazas que pudieran frenar la consecución de los objetivos de la organización, o generar un incumplimiento que causara un perjuicio.
>
> Gracias a una adecuada evaluación del riesgo, la organización podrá adoptar las medidas necesarias para el cumplimiento. Para ello es importante detectar los riesgos que se pudieran producir y como afectarían a la organización y a su desempeño (ISOTools, Excellence, 2021, párr 2).

Se puede observar, en estos párrafos, la importancia de la aplicación de análisis de riesgo para los sistemas informáticos, y no solo informáticos, esto es aplicable en la mayoría de los procesos de las empresas, pero el enfoque de este trabajo es a nivel informático, por eso el enfoque es solo en los sistemas informáticos.

Se afirma que solo con una adecuada y acertada evaluación puede ayudar a eliminar y/o mitigar las amenazas que estén presentes en los sistemas y procesos.

A nivel de gestión de la seguridad, indica la OECD “debe estar fundada en la evaluación del riesgo, abarcando todos los niveles de las actividades en la operación sin dejar por fuera las posibles respuestas a riesgos emergentes y la prevención de estos” (OECD, 2004).

También indica que las políticas de seguridad deben de estar coordinadas e integradas en la creación de los sistemas coherentes de seguridad, todo esto enfocado en los requerimientos de los sistemas y de los roles de los usuarios de estos (OECD, 2004).

2.2.2. Controles para mitigar o eliminar riesgos informáticos

Una vez que se tiene la información del estado actual de la empresa y de haber realizado el análisis de riesgo, se debe de clasificar los hallazgos según su impacto al proceso, con esto se puede tomar la decisión de que riesgos se deben de mitigar o eliminar según su efecto ante el proceso.

Para ello, se debe controlar los hallazgos con herramientas que proveen las políticas de seguridad que se implementen para los sistemas, sin dejar a un lado la actitud de los usuarios de los sistemas informáticos, ya que de estos depende el buen funcionamiento y las buenas prácticas de uso.

Sobre el tratamiento del riesgo está lo siguiente:

La Dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información.

Hay dos grandes opciones:

- reducir el riesgo residual (aceptar un menor riesgo)
- ampliar el riesgo residual (aceptar un mayor riesgo)

Para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que cubre una amplia visión de consideraciones de las que podemos apuntar algunas sin pretender ser exhaustivos:

- cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos internos, misión de la Organización, responsabilidad corporativa, etc.
- posibles beneficios derivados de una actividad que en sí entraña riesgos
- condicionantes técnicos, económicos, culturales, políticos, etc.
- equilibrio con otros tipos de riesgos: comerciales, financieros, regulatorios, medioambientales, laborales, …

En condiciones de riesgo residual extremo, casi la única opción es reducir el riesgo.

En condiciones de riesgo residual aceptable, podemos optar entre aceptar el nivel actual o ampliar el riesgo asumido. En cualquier caso, hay que mantener una monitorización continua de las circunstancias para que el riesgo formal cuadre con la experiencia real y reaccionemos ante cualquier desviación significativa.

En condiciones de riesgo residual medio, podemos observar otras características como las pérdidas y ganancias que pueden verse afectadas por el escenario presente, o incluso analizar el estado del sector en el que operamos para compararnos con la “norma”.

En términos de las zonas de riesgo que se expusieron anteriormente,

- zona 1 – riesgos muy probables y de muy alto impacto; posiblemente se plantee sacarlos de esta zona
- zona 2 – riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones

- zona 3 – riesgos improbables y de bajo impacto; o los dejamos como están, o se permite que suban a mayores si ello ofreciera alguna ventaja o beneficio en otro terreno
- zona 4 – riesgos improbables, pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera.

También conviene considerar la incertidumbre del análisis. Hay veces que sospechamos las consecuencias, pero hay un amplio rango de opiniones sobre su magnitud (incertidumbre en el impacto). En otras ocasiones la incertidumbre afecta a la probabilidad.

Estos escenarios suelen afectar a las zonas 4 y 3, pues cuando la probabilidad es alta, normalmente adquirimos experiencia, propia o ajena, con rapidez y salimos de la incertidumbre. En cualquier caso, toda incertidumbre debe considerarse como mala y debemos hacer algo:

- buscar formas de mejorar la previsión, típicamente indagando en foros, centros de respuesta a incidentes o expertos en la materia;
- evitar el riesgo cambiando algún aspecto, componente o arquitectura del sistema; o

- tener preparados sistemas de alerta temprana y procedimientos flexibles de contención, limitación y recuperación del posible incidente.

Hay veces que estos escenarios de incertidumbre ocurren en un terreno en el que hay obligaciones de cumplimiento y la propia normativa elimina o reduce notablemente las opciones disponibles; es decir, el sistema se protege por obligación más que por certidumbre del riesgo.

A la vista de estas consideraciones se tomarán las decisiones de tratamiento (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

2.2.3. Políticas de Seguridad Informática

"Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan…" (UNIR - Universidad Internacional de La Rioja, 2020).

"Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización." (Rodriguez & Ribón Zarco, s.f.).

En los párrafos anteriores se afirma que las políticas de seguridad informáticas ayudan a garantizar las tres palabras claves de este proyecto que se necesitan garantizar, también se puede ver que de nuevo se menciona la importancia de estas para minimizar los riesgos que afectan a los sistemas informáticos.

Las políticas de seguridad informática deben considerar elementos esenciales:

- El alcance, donde se incluya facilidades, sistemas y las personas a quien está dirigidas.
- Los objetivos y los elementos involucrados en la definición.
- Requerimientos mínimos de la configuración de la seguridad del alcance de la política de los sistemas involucrados.
- Definición de sanciones por el no cumplimiento de las políticas establecidas.
- Cultura de responsabilidad de los usuarios con accesos a la información sensible para la compañía (Rodriguez & Ribón Zarco, s.f.).

En la siguiente figura 2.1 se puede ver parámetros que se debe considerar para establecer las políticas de seguridad y que se detallan a continuación:

Figura 2.1:

Parámetros para establecer políticas de seguridad informática, mayo 2021

- Realizar un análisis de riego informático con el fin de valorar la situación actual de los procesos para que las políticas estén de acorde a lo que necesite la empresa.

- Acercamiento al departamento de TI para establecer, con su experiencia, el alcance y definir cuáles son las violaciones a las prácticas.
- La comunicación a todo el personal del desarrollo de la política, que incluya beneficios, riesgos de recursos y los elementos de seguridad.
- Acercamiento con los encargados de cada departamento para el seguimiento de la aplicación de buenas prácticas en las políticas establecidas y su seguimiento.
- Actualización oportuna de las políticas con el monitoreo periódico de los procedimientos y operaciones de la empresa, y
- Hacer énfasis en la redacción del alcance para evitar futuros mal entendidos cuando se requiera actualizar algún proceso con mecanismos de seguridad (Rodriguez & Ribón Zarco, s.f.).

Luego de lo anterior, se implementa el plan de trabajo con los encargados de los departamentos, ellos son los que más conocen de los procesos y de los flujos de trabajo, la estructura del este plan se detalla en la siguiente figura 2.2 y que tiene seis fases en total:

Figura 2.2:

Plan de trabajo con los encargados de los departamentos, mayo 2021

- Realizar un cronograma de acercamiento con los jefes y coordinadores de los departamentos, en especial con los de TI quienes tienen los conocimientos de los sistemas que se van a proteger.
- Se debe destacar la afectación, en general, de la pérdida de información para la compañía y los usuarios.
- Dejar claro en estas reuniones, la importancia de comprometerse con las buenas prácticas en la manipulación de datos en la red.
- Realizar propuestas con los coordinadores y personal a cargo para definir las medidas de seguridad que se van a implementar.
- Revisar las medidas de seguridad a implementar.
- Revisar los accesos a Internet.
- Revisar los respaldos de la información.
- Revisar grupos de perfiles según los roles.

- Revisar los permisos de acceso, escritura, lectura de archivos y carpetas de acuerdo con el cargo asignado (Rodriguez & Ribón Zarco, s.f.).

En la siguiente figura 2.3 se representa las recomendaciones para la implementación de las políticas:

Figura 2.3:

Recomendaciones para la implementación de políticas de seguridad informática, mayo 2021

- Analizar los componentes físicos de la red y la estructura de la información para buscar y saber cuáles son los riesgos informáticos a los que están expuestos.
- Se debe verificar, con los encargados de los departamentos, si la información anterior es correcta y verificar que todo se está tomando en cuenta.
- Con el personal de cada departamento, se debe explicar las ventajas de implementar las políticas de seguridad y cuáles son los riesgos de no implementarla.

- Cada responsable de los departamentos debe tener claro las políticas y concientizar las responsabilidades que tienen con respecto a la aplicación y seguimiento de todos los empleados, incluyéndolos.
- Implementar herramientas para auditar los elementos físicos de la red y el desempeño de los usuarios.

Se indica en esta sección algunos conceptos importantes que van de la mano con el tema de las políticas de seguridad informática, y estas, a la vez son herramientas que ayudan a conseguir la aplicación correcta desde el enfoque del análisis para la redacción de la política que se desee implementar:

> Una política de seguridad se define a alto nivel, esto es qué se debe proteger y cómo, es decir, el conjunto de controles que se deben implementar. Esta se desarrolla en una serie de procedimientos e instrucciones técnicas que recogen las medidas técnicas y organizativas que se establecen para dar cumplimiento a dicha política.
>
> La definición de una política de seguridad debe estar basada en una identificación y análisis previo de los riesgos a los que está expuesta la información y debe incluir todos los procesos, sistemas y personal de la organización. Además, tiene que haber sido aprobada por la dirección de la organización y comunicada a todo el personal (UNIR - Universidad Internacional de La Rioja, 2020).

En las siguientes definiciones se puede conocer algunos procedimientos y políticas que son importantes para el aseguramiento de los activos informáticos y que ayudan a garantizar la integridad, confidencialidad y la disponibilidad de estos:

2.2.3.1 Buenas prácticas. El documento de buenas prácticas de seguridad de la Información —puede ser un documento específico, cláusulas anexas a los contratos de los empleados, etc.— debería recoger, entre otras cosas, el uso aceptable de los sistemas y la información por parte del personal, las directrices para mantener el puesto de trabajo despejado, el bloqueo de equipo desatendido, la protección de contraseñas… (UNIR - Universidad Internacional de La Rioja, 2020).

2.2.3.2. Procedimiento de control de accesos. Recoge las medidas técnicas y organizativas relacionadas con los permisos de acceso a las instalaciones y sistemas que albergan la información de la organización, así como el acceso a la propia información. Los controles de acceso pueden ser físicos o lógicos… (UNIR - Universidad Internacional de La Rioja, 2020).

2.2.3.3. Controles de acceso físico. Mecanismos y sistemas implementados para controlar el acceso de personas a las instalaciones de la organización como, por ejemplo, tornos, barreras, cámaras, alarmas, sistemas de apertura de puertas biométricos o por tarjeta, etc. Otros ejemplos de controles de acceso físico son también: albergar la información en armarios cerrados con llave y, en general, cualquier medio físico que dificulte o no permita el acceso no autorizado a la información (UNIR - Universidad Internacional de La Rioja, 2020).

2.2.3.4. Controles de acceso lógico. Sistemas implementados para controlar el acceso de los usuarios a los distintos sistemas que albergan la información o el acceso a la propia información. Ejemplos de controles de acceso lógico son la implementación de un NAC (control de acceso de equipos y usuarios a la red), la configuración de permisos de lectura y escritura sobre los propios archivos de información, sistemas de seguridad de entrada en los distintos sistemas, autorizaciones de acceso remoto de los usuarios a la red a través de una VPN, etc. (UNIR - Universidad Internacional de La Rioja, 2020).

2.2.3.5. Procedimiento de gestión de usuarios. Recoge las instrucciones precisas a realizar para el alta, cambio de puesto de trabajo y baja (voluntaria o cese) de los usuarios en los distintos sistemas de información, así como para la concesión de los permisos de acceso tanto físicos como lógicos que deberían tener a las instalaciones, sistemas y a la propia información. Este procedimiento se debería basar y recoger una definición clara y concisa de los diferentes roles y responsabilidades de los usuarios, es decir, en función de los roles y responsabilidades del personal se le tendrían que conceder diferentes accesos y permisos, los mínimos y necesarios para el desempeño de su trabajo (UNIR - Universidad Internacional de La Rioja, 2020).

2.2.3.6. Procedimiento de clasificación y tratamiento de la información. “Incluye las instrucciones acerca de cómo clasificar la información de acuerdo con su valor, requisitos legales, sensibilidad y criticidad para la organización y las medidas de protección y manipulación/tratamiento del mismo acorde a su clasificación” (UNIR - Universidad Internacional de La Rioja, 2020).

2.2.3.7. Procedimiento de gestión de incidentes de seguridad de la información. “Instrucciones para la notificación de incidentes, de respuesta a los mismos con las acciones a realizar al ser detectados, etc.” (UNIR - Universidad Internacional de La Rioja, 2020).

2.2.3.8. Otros procedimientos. “Gestión de activos de información, copias de seguridad de la información, seguridad de la red, antimalware, registro y supervisión de eventos, actualización y parcheo de sistemas y equipos…” (UNIR - Universidad Internacional de La Rioja, 2020).

En resumen, las políticas de seguridad informática de una empresa u organismo deben adaptarse a todas sus necesidades y, en la medida de lo posible, ser atemporales. Es por ello por lo que cada vez se hace más necesario el rol del experto en ciberseguridad dentro de las organizaciones, un perfil profesional especializado en ciberseguridad y que responde a las nuevas necesidades en materia seguridad en un contexto de digitalización de las organizaciones (UNIR - Universidad Internacional de La Rioja, 2020).

2.2.3.9. Sistemas de Gestión y la Seguridad de la Información. ISO/IEC 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO/IEC 27001:2013 para los sistemas gestión de la seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO/IEC-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización. La gestión de la seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO/IEC 27002.

Norma ISO/IEC 27001

Estructura de la norma ISO/IEC 27001

1. **Objeto y campo de aplicación:** La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.
2. **Referencias Normativas:** Recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO/IEC 27001.
3. **Términos y Definiciones:** Describe la terminología aplicable a este estándar.
4. **Contexto de la Organización:** Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.
5. **Liderazgo:** Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad informática que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.

6. **Planificación:** Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un sistema de gestión de seguridad de la Información, así como de establecer objetivos de seguridad de la Información y el modo de lograrlos.
7. **Soporte:** En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.
8. **Operación:** Para cumplir con los requisitos de seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la seguridad de la Información y un tratamiento de ellos
9. **Evaluación del Desempeño:** En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del sistema de gestión de seguridad de la Información, para asegurar que funciona según lo planificado.
10. **Mejora:** Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI (ISOTools, EXCELLENCE, 2021).

Novedades de la ISO/IEC 27001:2013

Esta norma fue publicada recientemente, aportó una serie de cambios con respecto a su antecesora que los usuarios de los SGSI tienen que asimilar para continuar gestionando de forma eficaz la seguridad de la Información. Las novedades que manifiesta son:

- No aparece la sección “Enfoque a procesos” con su respectiva metodología basada en el ciclo PHVA, ahora ofrece mayor flexibilidad.
- Se elimina la obligatoriedad de algunos documentos, conservando únicamente la declaración de aplicabilidad.
- Se han revisado los requisitos y controles.
- Se apuesta por un enfoque del análisis del riesgo en la fase de planificación y operación (ISOTools, EXCELLENCE, 2021).

Aspectos clave del diseño e implantación de la norma ISO 27001.

Los SGSI basados en la ISO 27001 tiene aspectos claves por si solo y otros relacionados con las normas ISO 22301 e ISO/IEC 20000 que se describen a continuación.

Es una solución de mejora continua en base a la cual puede desarrollarse un SGSI que permita evaluar todo tipo de riesgo o amanezcas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros.

Permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros.

Es un sistema basado en enfoque basado en el ciclo de mejora continua o de Deming, el cual consiste en Planificar-Hacer-Verificar-Actuar (PDCA por sus siglas en inglés).

Este ciclo que es planteado por el ISO 27001 se dividen cada uno de ellos en una serie de acciones:

Planificar: Definir la política de seguridad Establecer al alcance del SGSI Realizar el análisis de riesgo Seleccionar los controles Definir competencias Establecer un mapa de procesos Definir autoridades y responsabilidades.

Hacer: Implantar el plan de gestión de riesgos Implantar el SGSI Implantar los controles.

Controlar: Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección.

Actuar: Adoptar acciones correctivas Adoptar acciones de mejora (ISOTools, Excellence, 2021, pág 4-5)

Además, ISOTools dice que ISO 27001 está enfocada en la parte informática de la empresa y tiene puntos en común con las normas ISO 23301 de continuidad de negocio y la ISO/IEC 20000 de gestión de servicios TI (ISOTools, Excellence, 2021, pág 5-6).

La ISO 22301 trabaja el tema de la seguridad de la empresa desde la perspectiva general y global, asegurando la continuidad del negocio influyendo en

aspectos como activos financieros, contabilidad, legales y los factores ligados con la producción y la operativa (ISOTools, Excellence, 2021, pág 5-6).

Esta norma toma en cuenta los tiempos de recuperación el cual es crucial para poder evaluar el plan de contingencia y reanudar la actividad de la organización en niveles aceptables (ISOTools, Excellence, 2021, pág 5-6).

La norma ISO 27001 estable algunas fases para la elaboración de un SGS basado en el sistema PDCA:

1. Análisis y evaluación de riesgos: Se fundamenta en la identificación y análisis de amenazas para una adecuada gestión de riesgos, en sus consecuencias y criticidad.

2. Implementación de controles: Esta norma estable hasta 113 puntos de control los cuales están divididos por grandes objetivos, políticas de seguridad de la información y controles operacionales.

3. Definición de un plan de tratamiento de los riesgos o esquema de mejora: Debe de tomar en cuenta las distintas consecuencias potenciales de los riesgos estableciendo criticidad para cada uno de ellos para evaluar con objetividad las diferentes amenazas, para luego afrontar el riesgo eliminándolo, mitigándolo o trasladándolo.

4. Alcance de la gestión: La definición del alcance para la implementación del SGSI en la organización es una muy parte importante para saber cómo implantar este, esto puede variar según el tamaño de la empresa y sus activos.

5. Contexto de organización: Permite determinar los problemas internos y externos de la organización, sus debilidades, amenazas, fortalezas y oportunidades, para esto ISO se apoya con el método DAFO uno de los más comunes y aceptados.

6. Partes interesadas: Los proveedores de servicios de información y de equipamiento de tecnologías de la información, clientes en la protección de datos personales, fuerzas de seguridad de cada estado y autoridades jurídicas, la participación en foros profesionales y la sociedad en general son parte de este grupo del que se debe tener claro las necesidades y expectativas.

7. Fijación y medición de objetivos: Es necesario la fijación de objetivos que sean medibles, comunicados a los empleados de la empresa, además que estos empleados posean competencias necesarias en materia de seguridad informática según su puesto.

8. Proceso documental: ISO 27001 hace énfasis en la documentación estableciendo de manera muy estricta como se debe gestionar la documentación y exigiendo que la organización cuente con un procedimiento documentado para esta gestión, esto es para fundamental para obtener la certificación.

9. Auditorías internas y externas: Existen dos grandes tipos de auditorias internas de gestión donde se supervisa el liderazgo y el contexto y de controles donde son auditados los 113 controles mencionados anteriormente y que son revisados por personal altamente calificad y por la dirección de la la organización (ISOTools, Excellence, 2021, pág 6-18).

La Plataforma ISOTools facilita la automatización de la ISO 27001

La ISO 27001 para los SGSI es sencilla de implantar, automatizar y mantener con la Plataforma Tecnológica ISOTools.

Con ISOTools se da cumplimiento a los requisitos basados en el ciclo PHVA (Planear – Hacer – Verificar – Actuar) para establecer, implementar, mantener y mejorar el Sistema Gestión de la Seguridad de la Información, así como se da cumplimiento de manera complementaria a las buenas prácticas o controles establecidos en ISO 27002.

ISOTools también permite aplicar los requisitos de otras normas de Seguridad de la Información como PMG SSI de los Servicios Públicos de Chile, entre otros.

Este software, permite integrar la ISO 27001 con otras normas, como ISO 9001, ISO 14001 y OHSAS 18001 de una forma sencilla gracias a su estructura modular (ISOTools, Excellence, 2021).

Capítulo 3 : Marco Metodológico

En una tesis, el capítulo que explica la metodología es muy importante, ya que informa la manera de realizar la investigación y de obtener los datos para el análisis; también se describen los instrumentos y las técnicas empleadas para recolectar los datos. En síntesis, corresponde detallar todos los procedimientos ejecutados y con ello demostrar la validez y autenticidad de la investigación (Ulate & Vargas, 2016).

Según lo anterior, este capítulo ayudará a evaluar si las herramientas que se van a utilizar son las adecuadas para obtener lo necesario para el éxito del proyecto. En su estructura se define las técnicas y los instrumentos que serán aplicados en la obtención de datos para realizar este trabajo.

También se define el tipo de investigación, alcance, procedimientos metodológicos y la definición de las variables de los objetivos específicos de este trabajo.

El total del trabajo está dado en dos modalidades:

Trabajo de campo: Este se aplica directamente en las localidades de los activos informáticos, con entrevistas, análisis de la información que se obtiene de los resultados de cada etapa para conseguir resultados que se ajusten a los objetivos del trabajo.

Información Bibliográfica: Lectura de casos de éxito, tesis e información de la red de profesionales en la materia, además, el marco de referencia que usamos en este trabajo que es ISO 27001 e ISO 27002.

3.1. Tipo de Investigación

"La investigación es concebida no solamente como un ejercicio académico, sino como un acto recurrente en la vida de los seres humanos (Ulate & Vargas, 2016, pág. 3)."

En todo momento el ser humano tiene la necesidad de investigar para sobrevivir, aprendemos desde que nacemos con el primer paso que es respirar fuera del vientre de nuestra madre, seguimos aprendiendo día tras día y cada vez más, cuando empezamos a caminar, a distinguir sabores, cuando ingresamos a la escuela, siempre hay esa necesidad de aprender e investigar.

La Metodología para elaborar una tesis también indica que la curiosidad es generada por el interés que tienen las personas sobre temas variados, también por las situaciones que se presentan en la vida cotidiana que afectan directamente al ser humano (Ulate & Vargas, 2016).

Por esta razón es que los proyectos de investigación que se desarrollan en las carreras universitarias son cada vez más utilizados para el aprendizaje de los estudiantes y profesores, y es por esto por lo que ahora se están aplicando en la secundaria y en las escuelas.

3.1.1 Enfoque de la Investigación

Hay dos tipos de investigación que se utilizan en un proyecto y que tienen su origen en Atenas, en la Grecia clásica del siglo IV antes de Cristo. Esto por cuanto Platón y Aristóteles fundaron las bases filosóficas en las que más tarde

se enmarcarían las distintas aproximaciones y desarrollos de las perspectivas cualitativa y cuantitativa (Gurdián-Fernández, 2010).

El tipo de esta investigación para este trabajo es de tipo mixto, esto debido a que, del análisis de riesgo se tomarán los datos para la toma de decisiones, y, con las variables del proyecto, se identificará la posición actual del manejo de los activos informáticos, y con estos resultados formular el tipo de política necesaria para la compañía, es por esto por lo que el enfoque mixto será utilizado en este proyecto.

La Figura 3.1 ofrece una visión general de la unión de este tipo de investigación, donde se explica que la investigación mixta es el resultado de la unión de la cualitativa y la cuantitativa.

Figura 3.1:

Tipos de investigación

También se puede decir que este trabajo tiene un enfoque tecnológico y aplicado, esto debido a que se realizará un trabajo basado en los resultados de un análisis de riesgo, y que tiene como fin la implementación de una política de seguridad

de la información para garantizar la integridad, confidencialidad y disponibilidad de la información que se utiliza para la toma de decisiones.

3.2. Alcance de la investigación

La riqueza del tipo de investigación mixto consiste en que se pueden abordar los problemas que enfrentan actualmente las ciencias desde diferentes ópticas, y de esta manera obtener mucha riqueza en los resultados a los problemas complejos y diversos ((Ulate & Vargas, 2016) como lo mencionó Hernández et al., 2010).

También Hernández se refiere al alcance descriptivo como:

> Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar cómo se relacionan éstas (Ulate & Vargas, 2016, pág 80).

Por lo anterior se puede afirmar que este trabajo de investigación es de alcance descriptivo, debido a que la propuesta de la política de seguridad informática se realizará con base al análisis de riesgo que se va a aplicar, con el cual se pretende medir y recoger información de los diferentes perfiles de los usuarios.

Se indagará en las propiedades y características del actual proceso para buscar las debilidades del sistema en la relación que pueda existir entre los usuarios y este, también las oportunidades de cambio para asegurar la integridad y disponibilidad de los activos informáticos.

3.3. Fuentes de Información

Las fuentes de información son las herramientas más importantes para un trabajo de investigación, sin ella no sería posible realizar los proyectos de investigación debido a que no habría materia prima para resolver y justificar el proyecto.

“Las fuentes de información primarias y secundarias representan el origen de los principales datos de una investigación” (Por Investigadores, 2020).

Como se puede ver, estas fuentes, al ser el origen de los principales datos del trabajo, conlleva una alta responsabilidad en materia de la revisión adecuada para el éxito del proyecto, si la fuente de origen no es la adecuada o no es verdadera, el trabajo en sí no tendría una justificación en los resultados.

Por esto la importancia de leer y buscar en varias fuentes de información para ver las diferentes perspectivas del tema, y así, obtener no solo lo que necesitamos para el proyecto, también información veraz y probable.

3.3.1. Fuentes primarias

Como fuentes primarias está la información que se obtiene de primera mano, esto quiere decir que son documentos originales que cuenta la información de su creador, de una entrevista que se realizó a algún participante del proyecto o de algún libro especifico.

Por la naturaleza de este proyecto y debido a la utilidad de estas herramientas para el desarrollo y el éxito que se pretende obtener, se va a utilizar como fuente primaria lo siguiente:

Para la estructura del trabajo, el libro electrónico “Metodología para elaborar una

TESIS, de la UNED, elaborado por Ileana Ulate Soto, Elizarda Vargas Morúa, EUNED, 2016.

a) Para la aplicación del trabajo de campo MAGERIT v3 y COBIT 5
b) Para la implementación de la política de seguridad informática la norma INTE/ISO/IEC 27001:2013, primera edición INTECO.

3.3.2. Fuentes secundarias

"En las ciencias sociales, una fuente secundaria suele ser un libro académico, un artículo de revista o un documento digital o impreso creado por alguien que no experimentó o participó directamente en los eventos o condiciones bajo la investigación" (Ulate & Vargas, 2016).

En la estructura de este proyecto se va a utilizar las siguientes fuentes secundarias con el fin de aprovechar el conocimiento y la experiencia de las personas que documentaron los trabajos sobre el tema que se está realizando:

a. Sitios web correspondiente.
b. Trabajos finales de graduación y tesis de diferentes instituciones.
c. Publicaciones.

3.4. Instrumentos y técnicas de recolección de datos

Los instrumentos y técnicas de recolección son herramientas que se utilizan en los proyectos para la obtención de datos, experiencias de los autores y la información de los procedimientos que los usuarios realizan en los procesos.

Entre estas, indica Hernández et al. (2010), están las que se utilizan en investigaciones sociales como (escala de actitudes, cuestionarios, recolección de contenidos para análisis cuantitativo, observación cuantitativa, pruebas estandarizadas, archivos y otras.

También Hernández et al. (2010) indica que estas van de acuerdo con la investigación que se esté realizando y derivado de esto, escoger la técnica y los instrumentos necesarios para la obtención de datos.

En el siguiente cuadro se puede revisar las usuales técnicas usadas para las diferentes investigaciones, ya sea cuantitativa o cualitativa:

Figura 3.2:

Usuales Técnicas de Investigación

Usuales técnicas de investigaciones cuantitativas	Usuales técnicas de investigaciones cualitativas
• Cuestionarios cerrados • Registros de datos estadísticos • Pruebas estandarizadas • Diferentes tipos de entrevistas • Encuestas	• Observación • Entrevistas profundas • Sesiones de grupos • Biografías • Revisión de archivos • Etnografías

Fuente: Hernández *et al.* (2010).

Al ser este trabajo de tipo mixto, se ha utilizado para la recolección de datos en Ali-mentos S.A. dos de estas herramientas, la entrevista y la observación, y con estas obtener la situación actual de los procesos en el uso de activos y, además, realizar el análisis de riesgo basado en los hallazgos.

3.4.1. La Entrevista

La entrevista permite al investigador obtener información de primera mano y la puede aplicar de diferentes formas, como, por ejemplo: personal, por teléfono, correo electrónico, video conferencia o cualquier herramienta electrónica que pueda usar para comunicarse con los usuarios de los procesos (Ulate & Vargas, 2016).

Es necesario determinar cuáles sujetos pueden ofrecer información sobre el tema de estudio, por su experiencia, manejo de los activos, uso de la información y/o por su conocimiento en los procesos intervenidos en el proyecto (Ulate & Vargas, 2016).

Las entrevistas pueden ser estructuradas o no estructuras, pero Ulate et al. (2016) recomienda el uso de las estructuradas y que sea personal siempre y cuando se pueda aplicar de esta forma, esto ayuda a que la información sea detalla y profunda (p.77).

En el caso de este proyecto se realiza entrevistas estructuradas para facilitar la aplicación por medio del formato que se encuentra en el área de los apéndices, con el fin de mejorar la información que se obtiene realizando preguntas asertivas y útiles, también para agilizar el proceso de recolección de datos y no usar mucho tiempo de los actores y que puedan seguir con sus labores.

3.4.2. La observación

La observación es el procedimiento para obtener datos de la realidad mediante la percepción intencionada y selectiva de un objeto o fenómeno determinado. El objeto de estudio son las conductas manifiestas de uno o varios individuos

dentro de cierto contexto ((Ulate & Vargas, 2016) como lo mencionó Ortiz y García, 2008).

Con este recurso es recomendable sistematizar los procesos iniciando con la definición de los aspectos, eventos y/o las conductas de interés, se debe definir las unidades de observación en días, horas, minutos, luego se toman las muestras representativas de las observaciones para al final categorizar y subcategorizarlas (Ulate & Vargas, 2016).

En este proyecto esta técnica se va a utilizar para observar los procesos del manejo de activos en Ali-mentos S.A., con lo que se pretende conocer los métodos que utilizan los usuarios actualmente y revisar los puntos de mejora que se puedan aplicar en estos procesos.

Además, la observación será la base para la aplicación del análisis de riesgo, revisión de la situación del hardware y su ubicación, la manipulación y los controles actuales para la salida de estos de la compañía, el inventario de activos y que se aplicará por medio de la plantilla correspondiente para este proceso en el apéndice C.

3.4.3. Documentación

Como se indicó en la metodología de este proyecto, la información que viene de experiencias de los conocedores del tema es de suma importancia para la elaboración de este proyecto y de cualquier otro, ya que esta es la base para obtener un resultado positivo en cualquier proyecto.

La revisión de la documentación permite conocer el mejor camino a seguir para la aplicación de técnicas ya desarrolladas, y, con los casos de éxito de proyectos similares, tener claro los pasos a seguir para alcanzar los objetivos propuestos.

En este trabajo se utilizó fuentes bibliográficas de libros, normas para la política de seguridad, tesis, información de internet relacionada con el tema de estudio y marcos de referencia para la aplicación del análisis y mitigación de riesgos.

También se hizo una revisión de los procesos internos para la seguridad informática de la compañía donde hay procedimientos para procesamiento de virus, administración y control de claves de acceso, uso de dispositivos portátiles y el ingreso y salida del personal que labora en la compañía.

3.5. Procedimientos Metodológicos de la Investigación

Los procedimientos metodológicos en esta sección hacen énfasis en la población de estudio, y en el cual se desglosa el tamaño de la muestra y la unidad de esta para hacer la diferencia con la unidad informante.

A continuación, se detalla cuáles son estos procedimientos para la compañía, los totales que se van a revisar y como se realizó la distribución y selección.

3.5.1. Población de Estudio

La población de estudio es el total de elementos que se revisa o que abarca la revisión en los proyectos, en el caso de este trabajo sería el total de los activos en la compañía Ali-mentos S.A. en junio 2021 y que son 203.

En la siguiente página, en la figura 3.3 se puede ver le detalle de la estructura del universo, muestra y de la unidad de medida para este trabajo:

Figura 3.3:

Representación gráfica del Universo, muestra y población, mayo 2021

FUENTE: Elaboración propia a través de un ejemplo una imagen de Internet.

Al ser una investigación mixta se toman en cuenta estos datos para determinar los valores resultantes de los puntos de mejora que se puedan aplicar en los hallazgos del análisis de riesgo y a cuantos equipos del Universo se deben de intervenir.

3.5.2. Tipo de Muestreo

El tipo de muestreo es la estrategia que se utiliza para justificar el tamaño de la muestra, esta puede ser "…aleatorio, a juicio o por conveniencia…" (Ulate & Vargas, 2016).

En el caso de este trabajo se decide aplicar el tipo “por conveniencia” para las entrevistas con los usuarios de Ali-mentos S.A. ya que no es posible realizar esta a todos los usuarios debido a la naturaleza de sus labores, por ejemplo, el equipo de Ventas que siempre están laborando fuera de la compañía al lado del cliente.

Del total de activos se decidió hacer entrevista a 23 usuarios de 23 activos calificados como críticos para el proceso, esto es el 11.3% del total de activos en uso.

3.5.3. Tamaño de la Muestra

El tamaño de la muestra es del 11.3% de los activos informativos, esto a nivel de entrevistas, ya que la revisión y el análisis de riesgo si se aplicará a todos los activos de la compañía.

3.5.4. Selección y Distribución de la Muestra

Como se indicó en el tipo de muestreo, la selección de la muestra para las entrevistas se realiza por conveniencia, empleando el formulario del apéndice E para realizar la recolección de datos, además de la lluvia de ideas para saber si tienen alguna aportación para mejorar la seguridad.

3.5.5. Unidad de Muestreo

La unidad de muestreo es diferente a la unidad informante debido a que, para esta última, se utilizará un usuario experto del departamento de TI, y las entrevistas son a los usuarios en general.

3.5.6. Unidad Informante

La unidad informante, a parte del director de TI, se toma en cuenta al compañero del departamento de soporte, él fue el asignado por el director de TI para dar la información necesaria, precisa y que se puede incluir en este trabajo, en la tabla 3-1 se hace referencia a los informantes.

Tabla 3-1:

Definición de sujetos de información, mayo 2021

Posición	A cargo de	Experiencia	Relación con el tema
Director de TI	Gerencia de TI	7 años en la compañía como Gerente de TI	Está a cargo de la aprobación del proyecto y propuso el tema
Soporte Técnico de TI	Soporte y Mantenimiento de TI	12 años y 7 meses en el área de mantenimiento de TI	Consultante de la parte técnica

3.6. Definición, Operacionalización e Instrumentalización de las Variables

"...la variable es un aspecto de un fenómeno caracterizado por la capacidad de asumir valores, ya sea cuantitativa o cualitativamente." (Ulate & Vargas, 2016).

Otras definiciones son:

Las variables en un estudio de investigación son todo aquello que medimos, la información que colectamos, o bien, los datos que se recaban con la finalidad de responder las preguntas de investigación, las cuales habitualmente están especificadas en los objetivos (Villasís-Keever & Miranda-Novales, 2016, pág. p. 304).

Además, Villasís-Keever & Miranda-Novales indican que hay cuatro tipos de variables que se pueden clasificar en un trabajo desde el punto de vista metodológico, aunque no todos los estudios de investigación contienen las cuatro, variable dependiente, independiente, de confusión y universal (2016, pág. p. 304)

Para este trabajo se utilizó la clasificación del libro Metodología para elaborar una tesis, el cual clasifica estas variables como:

1. **Variable Independiente:** elemento que explica, condiciona o determina la presencia de otro.
2. **Variable Dependiente:** elemento explicado en función de otro.
3. **Variable de Interviniente**: elemento que interviene tanto en una variable independiente como en una dependiente, es decir, cuando influye en la aparición de otro elemento, pero solo en forma indirecta (Ulate & Vargas, 2016).

También se tiene la medición de la variable según el tipo de dato en la escala que se presenta a continuación en la figura 3.4:

Figura 3.4:

Escala de variables de estudio

NOTA: Fuente: cpicmha.sld.cu, Capítulo 5 Las variables de un estudio http://www.cpicmha.sld.cu/literaturapatrionial/A-Manual%20metodologia/JAPV3346/Cap%EDtulo205.html

En la figura anterior se puede observar la escala de variables y su ramificación, se puede ver que las variables cuantitativas pueden ser continuas o discretas y las variables cualitativas pueden ser nominales u ordinales, estas últimas se subdividen en politómicas (más de dos alternativas) y/o dicotómicas (solo dos alternativas).

Para terminar, junto con estos tipos de valores se necesita usar una escala de variables de estudio que se pueda relacionar con esto datos y así, lograr unificar toda la información en la tabla de variables que consolidamos en la siguiente tabla de variables.

En la siguiente tabla 3-2, se detalla en una tabla tomada de una tesis para la elaboración de un catálogo de servicio, la escala, subescala y la descripción de cada una de estas:

Tabla 3-2:

Escala de Variables de Estudio

Escala	Subescala	Descripción
Cuantitativa	Continua	Representa valores enteros o fraccionarios
	Discreta	Representa únicamente valores enteros
Cualitativa	Ordinal dicotómica	Únicamente puede tomar dos valores posibles.

	Ordinal politómica	Puede tomar tres o más valores posibles.
	Nominal	Los valores no representan criterios de orden.

FUENTE: Elaboración propia a partir de Villasís-Keever & Miranda-Novales, 2016, mencionado en (Madrigal Vargas, 2019, pág. 92)

Se detalla en la tabla 3-3, los objetivos específicos de este trabajo, las variables de estudio que son extraídas de estos objetivos, la definición conceptual de cada aplicación que se debe realizar a las variables, los indicadores que ayudan a definir la situación actual de la compañía en el uso de los activos informáticos y las herramientas para conseguir lo necesario para la toma de decisiones.

Esta herramienta da el norte a seguir para la consecución de los resultados, más adelante se presenta otra tabla que es el complemento de esta, y que juntas ayudan a organizar la recolecta de la información y los pasos a seguir para la ejecución del este proyecto.

Tabla 3-3:

Variables de estudio

Objetivo específico	Variables de estudio	Definición conceptual	Indicadores	Tipo	Escala	Valores
Identificar la situación actual de la compañía.	Situación actual de la compañía.	Revisión detallada de la situación en sí, de los procesos a Identificar.	Procedimientos actuales en el uso de activos informáticos.	Independiente	Cualitativa Ordinal Dicotómica	Existen o no existen

Objetivo específico	Variables de estudio	Definición conceptual	Indicadores	Tipo	Escala	Valores
Realizar un Análisis de riesgo en los procesos de uso de activos informáticos.	Activos Informáticos	Componente o funcionalidad de un sistema de información.	Inventario actual de activos informáticos	Independiente	Cuantitativa Discreta	Números enteros
			Importancia del activo en la continuidad del negocio.	Dependiente	Cualitativa Ordinal Dicotómica	¿Es importante para la continuidad del negocio? sí o no
	Análisis de riesgo.	Analizar y evaluar los riesgos en los procesos.	Identificación, análisis y evaluación de riesgos.	Independiente	Cualitativa Ordinal Dicotómica	Existen o no existen
Evaluar los controles necesarios para mitigar o eliminar los riesgos encontrados en el análisis de riesgo.	Controles para mitigar o eliminar los riesgos.	Medidas de prevención a que los riesgos se materialicen.	Controles necesarios según los hallazgos para mitigarlos y/o eliminarlos.	Dependiente	Cualitativa Nominal	N/A

Objetivo específico	Variables de estudio	Definición conceptual	Indicadores	Tipo	Escala	Valores
Desarrollar una política de seguridad informática acorde a los resultados del análisis de este trabajo para presentarla a la Dirección de TI de la empresa.	Política de seguridad informática.	Serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información.	Tipos de políticas que se alinean con el proceso de la compañía.	Dependiente	Cualitativa Nominal	N/A
	Resultados del análisis	Información obtenía de la aplicación del proyecto.	Resultados obtenidos de la situación actual de la compañía en los procesos de usos de activos	Dependiente	Cualitativa Nominal	N/A

3.7. Metodología de Desarrollo

Luego del análisis de las variables y los instrumentos de recolección de datos, se necesita una guía o método para el desarrollo del proyecto, en esta se describe las técnicas y procesos que se van a realizar durante la aplicación de las fases de la investigación.

En la siguiente figura 3.5 se detalla las fases de la metodología utilizada para llevar a cabo la aplicación de este proyecto y que se explican a continuación:

Figura 3.5:

Fases de la Metodología de Desarrollo

3.7.1. Fases de la Metodología de Desarrollo

En la figura anterior se puede ver las fases a seguir para conseguir el producto final que es el desarrollo de la política de seguridad informática, el cual es el objetivo de este trabajo.

A continuación, se describe cada una de estas fases con el fin de entender los procesos que conlleva cada una en su aplicación:

3.7.1.1 Recolección de la Información. En la recolección de la información se utiliza las técnicas establecidas en este capítulo, la observación es la primera, y se usa para revisar las localidades de los activos informáticos y su distribución en la compañía.

En esta fase también se toma en cuenta la revisión de diferentes fuentes de información sobre el tema de estudio, por ejemplo: información en la WEB, libros, Tesis y algunas normas con marcos de referencia para el desarrollo del proyecto.

Con los datos del inventario de los activos, se obtiene cuántos equipos informáticos hay que analizar y la clasificación de estos según su importancia para el desarrollo de los procesos internos.

Otro dato importante es la cantidad de equipos que utilizan fuera de la compañía para el desarrollo de sus labores, ya sea en la casa, donde un cliente o de viaje cuando salen del país.

La identificación de la situación actual de la compañía es parte de esta fase de la recolección de la información, como están los procesos, como están y donde están los equipos, si necesitan o no protección, importancia del activo en la continuidad del negocio entre otras, se reflejan en la información que se recolecta.

También con el total de equipos, la identificación de estos y la situación actual de la compañía, se prepara el camino para el siguiente paso a seguir que es el análisis del riesgo.

3.7.1.2. Análisis de Riesgo. En el análisis de riesgo se evalúan los posibles eventos que pueden causar algún daño a los activos informáticos, con la identificación y la evaluación de cada activo, se utiliza para este análisis, las herramientas recomendadas por las normas ISO y MAGERIT.

3.7.1.3. Análisis de Resultados. Una vez que se tiene los hallazgos en el análisis de riesgo, se evalúa cada uno de estos en los activos que son importantes para los procesos internos, con los resultados se realiza la evaluación de controles para la mitigación que se ajuste a cada uno de estos.

Además, se revisa los resultados obtenidos a nivel general de este proyecto para la toma de decisiones y para buscar la mejor opción para la última fase de este trabajo.

3.7.1.4. Desarrollo de la Política de Seguridad Informática.

El desarrollo de la política de seguridad informática depende de los resultados obtenidos en las fases anteriores, la recolección de la información para tener claro la situación de la compañía, el análisis de riesgo y el análisis de la información en general, son los pilares donde se afianza el desarrollo para la política de seguridad que se debe entregar como objetivo principal de este proyecto.

3.7.2. Matriz Metodológica del Proyecto

En la tabla 3-4 se detalla la matriz metodológica en relación de los objetivos específicos y las variables del proyecto, esta matriz la encontré en la tesis del señor Gabriel Andrés Madrigal Vargas en su proyecto del TEC y me pareció muy acertada en su estructura para usarla en este proyecto, solo se toma la estructura de la tabla y sus encabezados.

Tabla 3-4:

Matriz Metodológica del Proyecto

Fase	Objetivos específicos	Preguntas	Actividades	Herramientas	Resultados
1	Identificar la situación actual de la compañía.	¿Cuál es la estructura del sistema en la compañía a nivel físico?	Realizar un esquema de la estructura para ver las localidades de los equipos.	Observación de cada activo por departamento y su lugar en el edificio.	Esquema de la estructura general de la compañía con ubicación de las áreas

Fase	Objetivos específicos	Preguntas	Actividades	Herramientas	Resultados
		¿Cuántos equipos informáticos hay en la compañía?	Inventario de activos por departamentos.	Listado para recolectar los datos de los equipos existentes. (Apéndice C).	Cantidad de activos informáticos
		¿Cuántos usuarios usan equipo compartido?	Identificación de usuarios y roles.	Consultas a la unidad informante para recolectar la información (Apéndice D).	Cantidad de usuarios que comparten los equipos para sus labores diarias
		¿Cuántos equipos salen de la compañía?	Identificación de activos para trabajo fuera de la empresa.	Listado de la etapa anterior. (Apéndice C).	Cantidad total de equipos portátiles que se utilizan fuera de la empresa
2	Realizar un análisis de riesgo en los procesos de uso de activos informáticos.	¿Se encuentran protegidos los activos informáticos en el sitio para cualquier evento?	Revisión general de los equipos en el sitio.	Levantamiento del documento con los hallazgos	Detalle de la situación actual de los activos
		¿Existen políticas de seguridad informática para el uso de los equipos?	Consultar si existen o si tienen conocimiento de alguna política para el uso de activos.	Entrevista cerrada, ¿sí o no? (Apéndice E)	Resultado positivo o negativo.

Fase	Objetivos específicos	Preguntas	Actividades	Herramientas	Resultados
		¿Existe control de accesos (claves, firma digital, otros) para el uso de estos equipos?	Consultar a los usuarios si tienen control de acceso.	Lista de chequeo para recolectar la información (Apéndice E)	Listado con el total de tipo de control de acceso.
		¿Existe la división de cuentas para cada usuario si usan el mismo equipo?	Consultar a los usuarios si tienen cuentas separadas para registrarse.	Lista de chequeo para recolectar la información (Apéndice E)	Cantidad de usuarios que no tengan cuentas únicas.
		¿Existe algún tipo de protección para los equipos que salen de la compañía?	Consulta a la unidad informante del proyecto.	Entrevista cerrada, ¿sí o no? (Apéndice E)	Resultado positivo o negativo.
3 Evaluar los controles necesarios para mitigar o eliminar los riesgos encontrados en el análisis de riesgo.		¿Hay riegos importantes que puedan afectar la continuidad del negocio por falta de ese activo?	Análisis de los hallazgos en la fase 2.	Matriz de calor.	Resultado de los activos que necesitan intervención con prioridades.
		¿Se puede eliminar, mitigar o	Análisis de los resultados en el punto anterior.	Paquete de Salvaguardas.	Eliminación, mitigación o aceptación del riesgo.

Fase	Objetivos específicos	Preguntas	Actividades	Herramientas	Resultados
		asumir el riesgo?			
		¿Qué control se puede utilizar para mitigar el riesgo encontrado?	Análisis de las salvaguardas asignadas.	MAGERIT e ISO 27001 / ISO 27002	Controles para mantener el cumplimiento de las salvaguardas asignadas.
4	Desarrollar una política de seguridad informática acorde a los resultados del análisis de este trabajo para presentarla a la Dirección de TI de la empresa.	¿Es suficiente los resultados obtenidos en el proyecto para desarrollar una política de seguridad informática?	Análisis de los resultados del proyecto en general.	ISO 27001 / ISO 27002	Si son o no suficientes los resultados para desarrollar una política de seguridad informática para la compañía.
		¿Qué política de seguridad se alinea con la estrategia de la compañía y con los resultados obtenidos?	Análisis y revisión de políticas de seguridad informáticas existentes	ISO 27001 / ISO 27002	Una política de seguridad informática actualizada y que se ajuste a las necesidades de la compañía.

NOTA: Elaboración compartida, la estructura de la Tesis del señor Gabriel Andrés Madrigal Vargas y la información fue sacada de los objetivos específicos de este proyecto.

Se puede ver, en la tabla anterior, las fases de la metodología que se usa en este proyecto, 4 en total, se realiza una pregunta basada en lo que se necesita conocer para alcanzar el objetivo específico del proyecto, a esto se le agregó tres columnas más donde se puede revisar las actividades que conlleva para responder a la pregunta formulada, además, las herramientas a utilizar y los resultados que se esperan alcanzar según las actividades realizadas.

Capítulo 4 : Resultados, Interpretación y Discusión

Este capítulo está designado para mostrar los datos recopilados en este trabajo, los datos tomados de la observación que se realizó en el sitio y los de las entrevistas que ayudaron a responder algunas de las consultas que nacieron de las variables de estudio, en el apéndice E se puede encontrar el formato utilizado para las entrevistas.

Cabe destacar que estas consultas están alineas con los controles de las normas ISO/IEC 27001, los controles son necesarios para este tipo de trabajo y se detallan a continuación.

4.1. Identificar la Situación Actual de la Compañía

Ali-mentos S.A. al ser una compañía a nivel global, tiene una estructura del sistema centralizado en Estados Unidos de América, donde el Corporativo tiene la Casa Matriz y donde se tiene todos los controles, políticas, almacenamiento y seguridad de toda la información electrónica para la continuidad del negocio.

Debido a las políticas del Corporativo, el alcance de este proyecto es solo a nivel local, en Costa Rica, y hay restricciones para obtener más información del sistema en este proyecto, pero si se cuenta con lo necesario para los objetivos específicos que se detallan a continuación.

4.1.1. ¿Cuál es la Estructura del Sistema en la Compañía a Nivel Físico?

El edificio de Ali-mentos S.A. fue comprado hace poco menos de 19 años y antes de pasar todo el personal, este fue remodelado en su totalidad para adaptarlo a la operación, por lo que se puede decir que la estructura de la compañía a nivel de redes se fue ampliando según la necesidad y el crecimiento que ha experimentado la empresa.

El *Datacenter* está localizado en un punto estratégico en la segunda planta del área administrativa por lo que está fuera del alcance de alguna inundación, este cuarto está equipado con aire acondicionado el cual es monitoreado por el *Netbotz* que se controla desde una de las pantallas en TI de las antes mencionadas en el inventario.

> Este *Datacenter*, indica nuestra unidad informante, tiene los equipos de comunicación con Corporativo y el resto de la planta, a este llegan los enlaces internacionales (Internet Corporativo) y el internet local (red Wireless para visitas), aquí está el *router* y los *switches* de distribución, el firewall local y demás equipos.
>
> Desde el *Datacenter*, continúa describiendo, a través de enlaces de fibra óptica hacia el rack del departamento de Calidad, *RyD* y TI, se distribuye la red a toda la empresa, en el rack de TI hay un *switch*, en el de *RyD* hay dos y en el de Control de Calidad tres más, para un total de nueve *switches*, además a esta estructura se ha agregado un nuevo rack en la bodega nueva de materia prima.
>
> También en la entrevista vía TEAMS, la unidad informante indica que Alimentos S.A. cuenta con dos redes Wireless conectadas a la red global, una red es para los dispositivos de usuario final (computadoras) y de esta red hay *AP´s* en oficinas y planta, la otra red Wireless es única y exclusivamente para conectar dispositivos dentro de la planta, como *hand helds* y *tablets*, y solo hay señal ahí dentro, no se pueden conectar ningún otro dispositivo como laptops a esa Wireless.

> Nuestros servidores, indica el informante, son virtualizados vía *VMware*, hay dos servidores físicos aquí en Costa Rica, nuestro ambiente cuenta con servidores separados para bases de datos (uno para producción y otro para desarrollo), para file server (documentos de usuario final), servidores RDP (2 servidores para aplicaciones y dos *Broker* o de respaldo para alta disponibilidad) para el acceso remoto de aplicaciones, que por cierto, su uso se intensificó con el teletrabajo, un servidor controlador de dominio.
>
> Termina indicando que hay una tercera red Wireless, pero esta es un enlace de internet con un proveedor local, y es meramente para dar señal a las visitas como auditores, técnicos de otras empresas, proveedores y otro tipo de visitas, esta red no tiene conexión con la red global.

En el Apéndice B se puede encontrar un esquema con la estructura del edificio de la compañía y la ubicación de cada área de trabajo, seis en total, en las cuales se desarrolla el día a día de la compañía para cumplir con su misión.

Se debe de tomar en cuenta que la tienda que aparece en este esquema es parte de la Asociación Solidarista y es por eso por lo que se excluye de este análisis, lo mismo con la oficina de la Asociación que está dentro del inmueble pero que su administración está fuera del alcance de la administración de la empresa.

Con el área de seguridad es la misma situación, ya que estos son de la empresa K9 que es subcontratada por la compañía para hacer efectiva la seguridad de la empresa y que están a cargo, en sus funciones principales, del ingreso y la salida de personas autorizadas al edificio.

Algunas áreas están divididas en departamentos para cumplir con uno de los enfoques de las compañías a través de las auditorias, la división de trabajo para el reparto de responsabilidades, a continuación, se detalla en la tabla 4-1, la cantidad de departamentos por área:

Tabla 4-1:

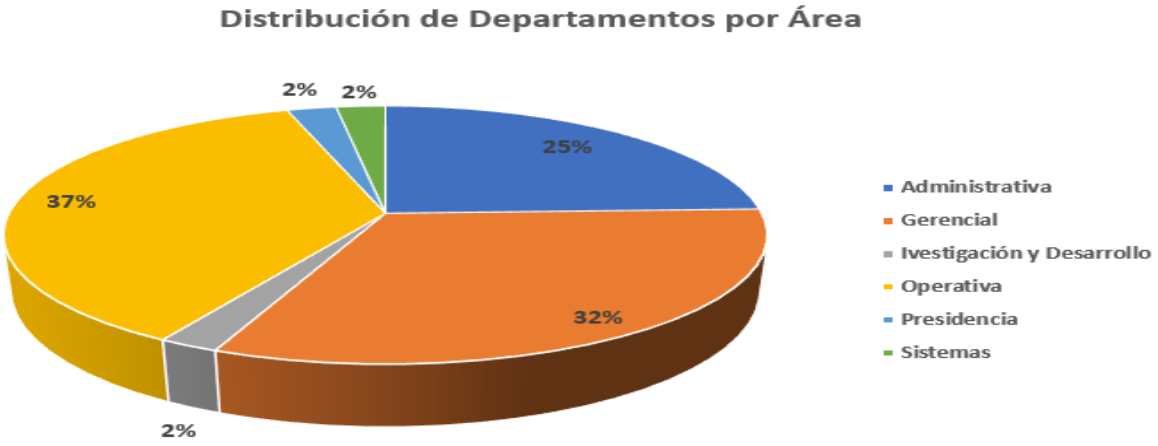
Departamentos por Área, junio 2021

Área	Departamentos por Área
Operativa	15
Gerencial	13
Administrativa	10
Presidencia	1
Investigación y Desarrollo (R&D)	1
Sistemas	1
Total	41

En la siguiente figura 4.1 se detalla la información de la tabla anterior en porcentaje de distribución de los departamentos por área:

Figura 4.1:

Distribución de Departamento por Área, junio 2021



4.1.1.1 Análisis de los Resultados. Se puede observar en el gráfico anterior, que el área operativa cuenta con más divisiones de departamentos debido a la naturaleza de sus funciones, en un treinta y siete por ciento del total, entre estos se puede mencionar un segundo nivel de división, los departamentos de Bodegas, Producción, Control de Calidad, Mantenimiento y Salud Ocupacional que le pertenecen.

Estos cinco departamentos son conocidos como departamentos críticos para la continuidad del negocio, y no es que los otros sean menos importantes, pero si las bodegas colapsan, no se podría recibir ni despachar productos, lo mismo si no hay un control de calidad sobre la producción, en la parte de mantenimiento si falla alguna máquina de proceso se detiene la producción, y, si no se asegura la salud de los operarios, no se podría avanzar en el proceso.

El segundo con más departamentos en su control es el área que refleja un treinta y dos por ciento del total, es el área gerencial, esto debido a que, en el segundo nivel de división en la estructura de la compañía, hay un gerente asignado a cada una de estas subáreas, esto se puede detallar en la tabla 4-2.

Tabla 4-2:

Gerencias por Departamento

Departamento con Área Gerencial	Cantidad de Gerentes por Departamento
Producción	2
Calidad	1
Finanzas	1
Gerencia	1

Departamento con Área Gerencial	Cantidad de Gerentes por Departamento
Logística	1
Mantenimiento	1
Negociaciones	1
Programación	1
R&D	1
SAC	1
TI	1
Ventas	1
Total:	13

El tercer grupo con más departamentos a cargo es el área administrativa el cual tiene un veinticuatro por ciento del total de los departamentos, entre ellos algunos asistentes de Gerencia, Recursos humanos, Finanzas, Servicio al cliente, Ventas, Negociaciones, Logística, Programación, Proyectos y Mercadeo.

Los otros grupos, no menos importantes, tiene a cargo solo un departamento que es el mismos que controlan, pero se desenvuelven por sí solos para dar algunos servicios a los departamentos antes mencionados, estos son dos, Sistemas e Investigación y Desarrollo. y por último está la Presidencia de la compañía donde está centralizada la toma de decisión cuando sea necesaria su participación.

4.1.2. ¿Cuántos Equipos Informáticos hay en la Compañía?

La importancia de saber cuántos activos va a cubrir la política de seguridad es esencial para este proyecto, esto porque cada equipo tiene su naturaleza y se comportan de diferente manera, con la cantidad y tipos de equipos, se puede saber que

tantos equipos salen de la compañía y cuantos se utilizan dentro, también para clasificar estos en el análisis de riesgo.

4.1.2.1. Recolección de la Información. En esta fase se utilizó una de las herramientas establecidas para este trabajo, la observación, con esta se asistió a cada departamento para revisar los activos informáticos y levantar un inventario.

Luego de la revisión se comparó la información recolectada contra el inventario de TI para confirmar si estaba conforme a este, y lo estaba, en el Anexo C se encuentra la plantilla utilizada para la recolección de estos datos.

4.1.2.1.1. Inventario de Activos. En los resultados se tiene que actualmente la compañía cuenta con un total de doscientos tres activos entre todos los departamentos, entre ellos hay varios tipos de activos informáticos que se detallan a continuación con sus cantidades por tipo en la tabla 4-3:

Tabla 4-3:

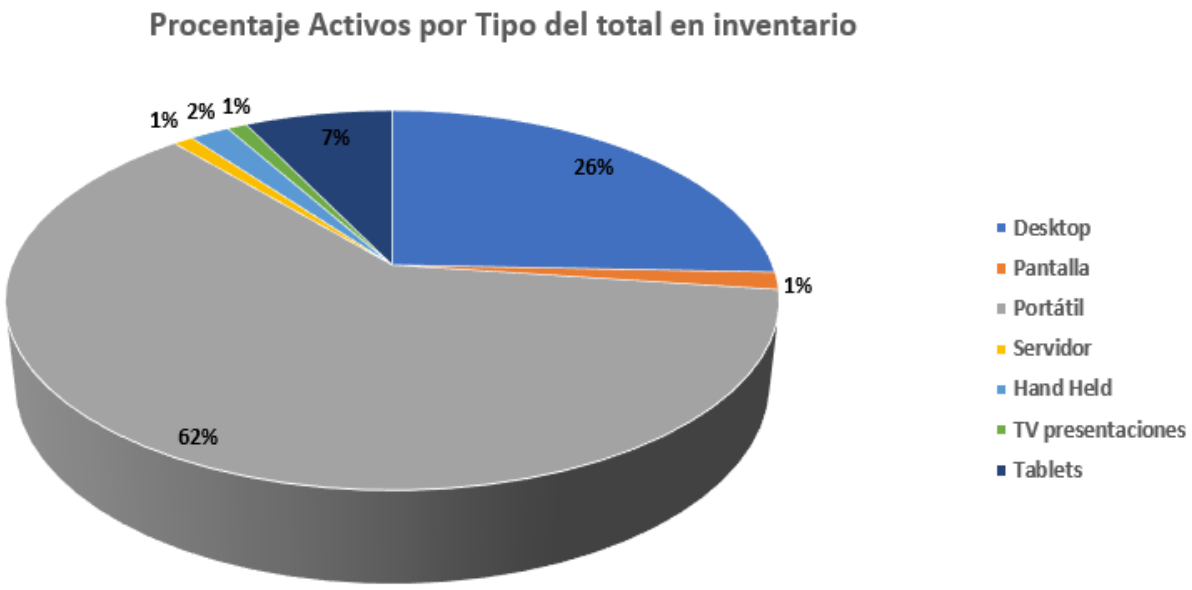
Inventario de Equipos, junio 2021

Tipo de Activo	Total de Equipos
Portátil	125
Desktop	52
Tablets	15
Hand Held	4
Pantallas de información	3
Servidores	2
TV para Presentaciones	2
Total unidades:	**203**

En la figura figura 4.2, se detalla el porcentaje de cada tipo de activo del total del inventario:

Figura 4.2:

Activos por Tipo, junio 2021



4.1.2.1.2. Análisis de los Resultados. En el diagrama anterior se observa que la mayoría del inventario, el sesenta y dos por ciento de doscientos tres del total de los activos que se utilizan para el día a día son computadores portátiles marca Hewlett Packard de tres tipos de modelos Series 800, 1040 y X360, con el sistema operativo Windows 10 E y Microsoft office 365 Enterprise.

El veintiséis por ciento del total de activos, son computadores tipo PC mini y todas son marca Hewlett Packard con tres tipos de modelos, series 300, 400 y 500, todas tiene el mismo sistema operativo y el office 365 igual que las portátiles.

Entre otros activos la compañía cuenta con cuatro *hand held* que se utiliza en las bodegas para el alisto y recibo de productos, tres pantallas que usan para las presentaciones de los equipos de trabajo y las otras dos son para monitoreo, una monitorea las condiciones ambientales del cuarto de servidores y la otra está con el monitoreo de condiciones ambientales, estatus UPS, alarma incendio y puertas.

En el cuarto de servidores hay dos servidores físicos, y en ambiente virtual *VMWare*: 10 servidores para la base de datos (producción y pruebas), file server, *Domain Controller, Remote Desktop* (dos para las aplicaciones y dos *broker*), *Backup*.

4.1.3. ¿Cuántos Usuarios Usan Equipo Compartido?

En esta revisión se utilizó el mismo formulario para la toma del inventario que se encuentra en el Apéndice C, se consultó con los supervisores del área y se constató con el consultante de TI, debido a que la compañía labora a tres turnos es muy común que, en los departamentos de operaciones, exista un usuario por cada turno que utilizan el mismo equipo que usan en los otros turnos.

También se constató que hay equipos en las bodegas que son usados por el personal de piso, estos para realizar verificaciones en el sistema o correos con información sobre carga y descarga de producto, el detalle en la tabla 4-4

Tabla 4-4:

Usuarios por tipo de equipos, junio 2021

Nombre del Equipo	Cantidad de Equipos	Cantidad de Usuarios	Diferencia
Desktop	52	107	55
TV Presentaciones	2	16	14
Tablets	15	22	7
Hand Held	4	8	4

Nombre del Equipo	Cantidad de Equipos	Cantidad de Usuarios	Diferencia
Portátil	125	127	2
Pantalla	3	3	0
Servidor	2	2	0
Total	**203**	**285**	**82**

4.1.3.1. Análisis de resultados. Se puede ver en los resultados anteriores que las desktops son los activos que más usan compartidos los usuarios, estos equipos, como se mencionó antes, son usados por hasta 8 usuarios en diferentes turnos, por ejemplo, los alistadores del turno uno de 6:00 am a 2:00 pm, los del turno dos de 2:00 pm a 10:00 pm y los del turno tres que comprende el horario de 10:00 pm a 6:00 am.

En la siguiente tabla 4-5 se detalla los tipos de usuarios y la cantidad de estos según sus cargos en la empresa, además solo se presentan los equipos que tienen más de un usuario:

Tabla 4-5:

Cantidad de Usuarios por Equipo, junio 2021

Usuarios	Equipo	Cantidad de Usuarios por equipo
Mejora Continua	TV presentaciones	16
Usuarios de piso MP	*Desktop*	15
Bachador + Lider	*Desktop*	15
Bodega de Producto terminado	*Desktop*	13
	Hand Held	8
	Tablets	15
Analista Calidad	*Desktop*	8
Usuarios de piso	*Desktop*	6
Bodeguero de Repuestos	*Desktop*	3
Aduaneros	*Desktop*	3

Usuarios	Equipo	Cantidad de Usuarios por equipo
Asistente de Bodega	*Desktop*	3
Supervisor turno por turno	*Portátil*	3
Asistente de Cocina	*Desktop*	3
Supervisor Producción Líquidos	*Desktop*	3
Controllers	*Desktop*	3
Supervisor Producción Polvos	*Desktop*	2
TOTAL		**119**

En el análisis de riesgo se detallará el uso de estos en cuanto a usuarios, roles y claves de acceso, por el momento se tiene que en el área operativa es la que presenta más equipos que son compartidos, esto por la naturaleza de la operación y que las otras áreas trabajan en un solo turno, el total de usuarios que utilizan equipo compartido es bastante alto, 119 usuarios en total.

4.1.4. ¿Cuántos Equipos Salen de la Compañía?

Como se mencionó al principio de este trabajo, Ali-mentos S.A. al igual que muchas compañías, tuvo que hacer un cambio radical en sus operaciones y esto hizo que muchos de los usuarios de *desktop* se tuvieran que pasaran a usar portátiles, y con esta estrategia, lograr que más personas lograran trabajar desde la casa en la red interna.

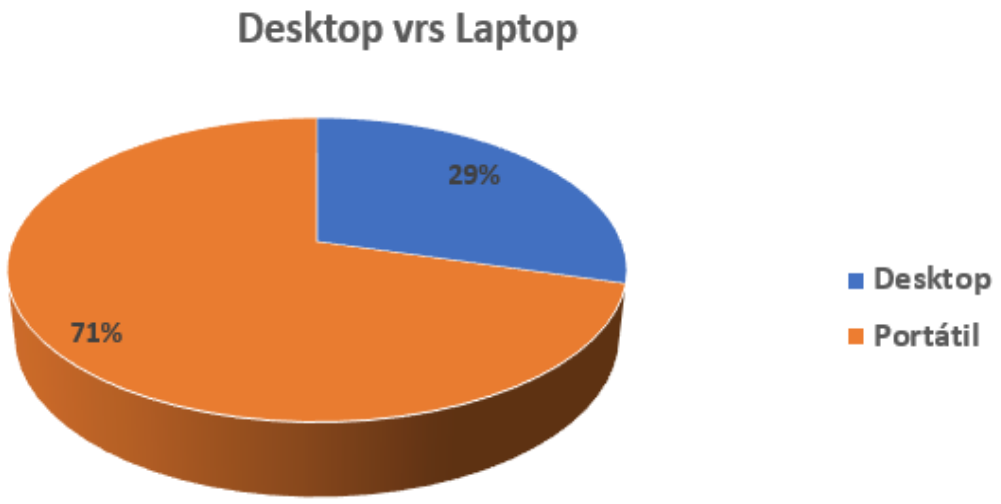
Lo anterior provocó que el número de unidades que salen de la compañía se acrecentara y superara en número a las demás unidades que se utilizan en la compañía para el trabajo diario, si comparamos los datos de los dos activos que tienen más inventario, se puede ver que las portátiles, al mes de julio del 2021, superan en

más del doble al desktop, esto era muy diferente hace dos años que el trabajo presencial era el más usado en la empresa.

En la figura 4.3 se detalla la comparación del número de desktop contra el número de las unidades portátiles con que cuenta hoy la empresa a dos años que comenzó la pandemia:

Figura 4.3:

Comparativa de existencia de unidades de desktop vs laptops a julio 2021



4.1.4.1. Análisis de Resultados. En el diagrama anterior se puede ver que las portátiles superan a las desktops con un setenta y uno por ciento contra el veintinueve por ciento de un total parcial entre estos dos de ciento setenta y siete activos, además se observa el cambio que ha tenido la compañía con respecto a la utilización de portátiles para la operación, estas cantidades eran muy difíciles de ver hace dos años en cualquier empresa que su trayecto siempre ha sido de trabajo presencial.

Se observa también que la cantidad de ciento veinticinco portátiles es la cantidad de activos que pueden salir en cualquier momento de la compañía, estableciendo así este número como respuesta a la pregunta de esta fase.

4.2. Análisis de Riesgo

Este análisis de riesgo se realizó con el fin de apoyar a la política de seguridad informática y tener un marco de referencia donde se pueda trabajar en mejorar los procedimientos en el uso de activos en la compañía Ali-mentos S.A.

Como está indicado en el capítulo 3.4.1 y 3.4.2, se usaron las dos herramientas establecidas para la recolección de la información, la observación en las localidades y las entrevistas con el formulario que se puede acceder en los Apéndice E.

Cabe destacar que la compañía al estar certificada con las normas BRC, está comprometida con la seguridad de toda su estructura y de sus empleados, también para los equipos que se utilizan en la operación y que tienen acceso los usuarios.

> Hay dos activos esenciales, la información que se maneja y los servicios que se prestan ya que marcan los requisitos de seguridad para todos los demás componentes, se deben de tomar algunas características formales, personales, con requisitos legales o alguna clasificación de seguridad (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

Con esta base se realizó este análisis de riesgo que se puede revisar en las siguientes líneas de este trabajo.

4.2.1 ¿Se Encuentran Protegidos los Activos Informáticos en el Sitio para Cualquier Evento?

En este punto se detalla la situación actual de los activos en todos los departamentos, el levantamiento de los hallazgos que se realizó por medio de la observación y la revisión general de los equipos en cada localidad, este punto está alineado con A.11 Seguridad Física y del Ambiente ISO 27001 donde su objetivo es “Prevenir el acceso físico no autorizado, daños e interferencia a la información y a los recursos de procesamiento de la información de la organización”.

- En el área administrativa, todas las computadoras se usan, cuando están en la compañía, dentro de las oficinas, por lo que están fuera del alcance de humedad, polvo o algún accidente físico por caídas de objetos, pueden estar conectadas directamente a la red por Ethernet o vía WIFI.
- Se observó que la mayoría de las computadoras de esta área, cuentan con monitores extra que se encuentran apoyados en brazos de hierro, estos monitores ayudan a simplificar la búsqueda de información y el uso de los sistemas, también ayudan a que las pantallas donde observan las entradas y salidas de información, no se vea limitadas por el tamaño de pantalla de las portátiles.
- Actualmente en 2021, se está trabajando en un proyecto donde solo las personas autorizadas puedan ingresar a las oficinas, esto por medio de huella digital con un dispositivo que va a estar al lado de las puertas, por el momento la

seguridad solo está a cargo de la compañía de seguridad K9 quien es la que permite o no, el ingreso del edificio.

- Todas las oficinas cuentan con puertas de acceso, y tienen la llave, solo los que pertenecen a ese departamento, las únicas computadoras que están expuestas a todo el personal las 24 horas, son 40 unidades que están en el área operativa, algunas de estas son protegidas por medio de forros plásticos cuando hacen limpieza profunda y/o la planta está detenida por alguna razón, fines de semana, feriados o vacaciones.

En la tabla 4-6 se presenta el detalle de los equipos que se utilizan fuera de las oficinas, a estos equipos se les aplica un cuidado diferente en las áreas descritas debido a que están expuestos a más riesgos por las labores que se realizan en estos departamentos.

Tabla 4-6:

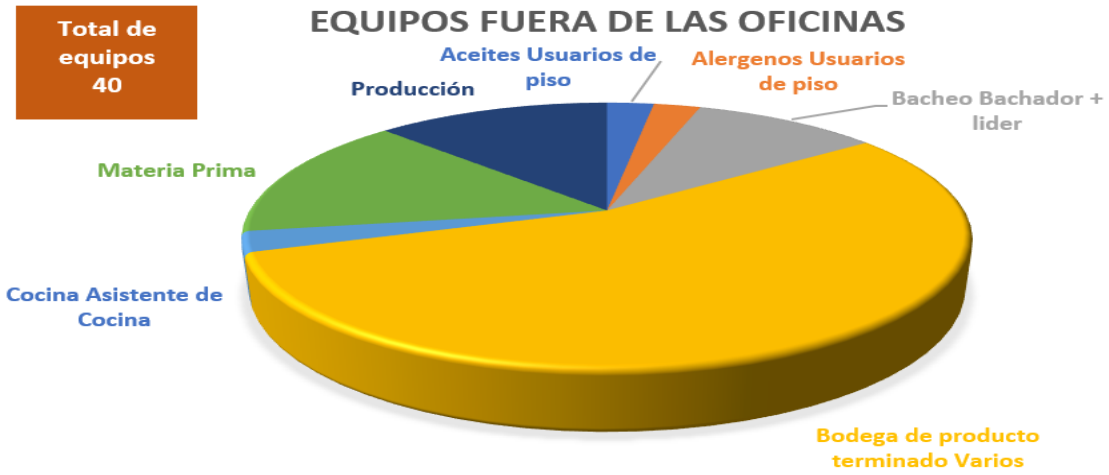
Equipos que se usan fuera de la protección de las oficinas, julio 2021

Departamento	Usuario	Equipos
Bodega de producto terminado	Varios	22
Materia Prima	Bodegueros	6
Producción	Operarios	5
Bacheo	Bachador + Lider	4
Aceites	Usuarios de piso	1
Alergenos	Usuarios de piso	1
Cocina	Asistente	1
Total		40

En la figura 4.4 se presenta esta información en un gráfico para tener una mejor visibilidad de estos datos:

Figura 4.4:

Equipos Usados Fuera de las Oficinas, julio 2021



4.2.1.2 Análisis de Resultados. En la tabla anterior se refleja que el departamento de Bodega de producto terminado es el que tiene más computadores fuera de las oficinas, tiene veintidós, dieciséis más que la bodega de materias primas que cuenta con seis unidades en piso, luego le sigue producción con cinco unidades y bacheo con cuatro, los otros tres departamentos cuentan con solo un activo.

De lo anterior se deduce que producto terminado es el departamento que debe de proteger más equipos que están expuestos en el área de la operación, aunque de los otros tres departamentos se suman 15 unidades que también requieren de atención para no versen afectados por algún evento.

Además, están los siguientes hallazgos:

- A nivel de altos voltajes, aunque la compañía está protegida con la tercera línea

de protección en la electricidad (línea a tierra), la mayoría de las computadoras no tienen protección de UPS para la protección de picos (altos y bajos voltajes), esto a nivel de desktop ya que las laptops tienen protección sobre estos picos de corriente eléctrica, esto según la siguiente publicación del soporte al cliente de Hewlett Packard:

> HP considera la seguridad muy seriamente y se asegura de que todos los equipos HP cumplan con las normas de seguridad internacionales. Dado que las computadoras son sistemas eléctricos complejos, la seguridad frente a las descargas eléctricas es una prioridad. A pesar de que el sistema eléctrico en el interior de un equipo HP no presenta riesgos inherentes, ciertas condiciones ambientales y/o el uso inadecuado de este pueden hacer que se produzcan descargas eléctricas si no se toman las precauciones necesarias.
>
> El adaptador de CA, que es la fuente de la energía eléctrica del equipo, está diseñado para usarse con un cable de energía de tres hilos. Sin embargo, el adaptador de CA está ampliamente probado, según las normas de seguridad internacionales, con un cable de dos hilos.
>
> Hay tres tipos de condiciones de descargas eléctricas: Descarga electrostática (ESD), Corriente de baja intensidad (que provoca una sensación de hormigueo) y Descarga eléctrica peligrosa (Hewlett Packard, 2021).

- Las desktops minis no tienen batería, aunque tiene un adaptador para la alimentación de corriente, al no contar con una batería interna, en el momento que se corte el fluido eléctrico, ellas se apagarán, si hay altos y bajos voltajes en la corriente eléctrica, puede afectar estas computadoras.
- Se hace la observación que en la compañía tienen una planta eléctrica para la continuidad del negocio cuando falle el servicio eléctrico, pero este se enciende hasta 2 minutos después del corte según indica el informante, por lo que todos los sistemas eléctricos que no estén protegidos experimentan una pérdida de corriente al apagarse y luego entra de golpe la nueva conexión.
- En la parte de planta, en el área de operaciones, el cableado de la red está distribuida en estructuras solo para ellos y todo es aéreo, la parte que está más baja se encuentra aproximadamente a dos metros de altura desde el piso y la más alta alcanza hasta los siete metros.
- Los dispositivos para la distribución de la red antes mencionados, están a alturas desde hasta cuatro metros, suspendidas por medio de tubos de acero que están colgando desde el cielorraso de la compañía y protegidos por medio de un tipo de campana de acero, por debajo tienen una especie de plástico por si llega de alguna forma, algún tipo de líquido.
- Los *switches* de distribución que están en el área operativa, están en cajas de metal con puertas de un material plástico transparente, ya que no es permito ningún objeto de vidrio dentro de la planta, esto para los controles de la

producción, estos *switches* están conectados a su unidad de protección UPS por cualquier evento que se pueda presentar.

- Se logró observar que algunos equipos en el área de operaciones no cuentan con UPS y tampoco están conectados a alguna regleta para su protección, los equipos están conectados directamente al tomacorriente y sin algún filtro que evite las fluctuaciones de tensión, inclusive se encontró varios equipos conectados con un distribuidor o toma corriente de cuatro entradas que se conecta directamente al tomacorriente.
- Se observó cuatro relojes digitales en los pasillos de planta, estos son para que los colaboradores, por medio de huella digital, registren sus ingresos y salidas, estos no están protegidos contra ningún tipo de accidente, aunque hay un tipo de separación en el pasillo para que pasen los montacargas, si ocurriera algún evento, estos podrían sufrir algún golpe o daño por salpicaduras de líquidos.
- En el área de cajas se observó una computadora que estaba sin bloqueo de pantalla y no había algún colaborador usándola en ese momento, puede que se acababa de levantar de su lugar de trabajo, pero no dejó la computadora bloqueada al levantarse.
- La mayoría de los equipos en el área administrativa son conectados directamente a los tomacorrientes y estos están por debajo de los escritorios, lo que causa, aparte de lo que vimos anteriormente sobre el filtro de fluctuaciones de tensión, el difícil acceso a conectar y desconectar estos equipos,

complicando la desconexión si ocurriera algún evento que necesite el corte inmediato de la corriente eléctrica al equipo.

- Las tabletas se encuentran empotradas en los estibadores, estas sujetas con un brazo que le ayuda al operario a manipularlas, cuando alguna necesita que se carga la batería, se conecta a un tomacorriente de 12 v. que está en los estibadores, no se observó ninguna protección en ellas.
- Las pantallas están colgadas con una base firme a la pared, solo hay una en el pasadizo de producción que está expuesta a algún golpe o situación que le pueda afectar para su buen funcionamiento, por ejemplo, salpicaduras de líquidos o polvo de los productos que se procesan en la planta.
- Los servidores están resguardados en un segundo piso bajo llave, solo el personal de TI tiene acceso a este cuarto por medio de una tarjeta electrónica, este tiene un sensor de movimiento, el cuarto cuenta con aire acondicionado para mantener la temperatura adecuada, además, tiene cámara de seguridad para darles el seguimiento necesario desde TI.
- Estos servidores junto con todo lo del Data Center, tienen un monitoreo continuo las 24 horas del día por medio de un sistema llamado *Netbotz* el cual, cada vez que se abre la puerta, genera una secuencia de 10 fotografías, una por segundo y se envían al correo electrónico al departamento de TI.
- TI también cuenta con *Display Orion* que es para el monitoreo de equipos y servicios críticos, para el área de operaciones en el departamento de Control de Calidad, TI tiene en el gabinete designado para este, una pantalla de monitoreo

de condiciones ambientales, *status* UPS, alarma de incendios y puertas, todo controlado por el equipo de soporte de TI.

- Los equipos de *hand held* son manipulados de mano en mano, se lo pasan entre los usuarios y cuenta con una faja que se ajusta a la muñeca, esto para evitar que el dispositivo sufra una caída si se resbala de la mano del operario, aparte de eso solo cuentan con su estructura para su protección.

4.2.2. ¿Existen políticas de seguridad informática para el uso de los equipos?

En los objetivos de control y controles de ISO27001 A.5 Políticas de seguridad de la información, se alinea esta parte del trabajo donde el objetivo principal es "Proporcionar dirección de la gestión y soporte para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes".

En la documentación que se obtuvo de la unidad informante, se recibió cinco procedimientos internos que están activos hasta el momento:

P-TI-001 Procedimiento para seguridad informática.

P-TI-003 Procedimiento para el procesamiento de Virus.

P-TI-006 Procedimiento para el control de administración de claves de acceso.

P-TI-008 Procedimiento para derechos de acceso.

P-TI-009 Procedimiento para uso de computadoras portátiles.

Entre ellos se detalla sus objetivos resumidos para su revisión.

4.2.2.1. P-TI-001 Procedimiento para la Seguridad Informática. El cual fue creado para definir la aplicación de la seguridad informática en general y tiene alcance a todos los recursos tecnológicos y sistemas de información de Ali-mentos S.A.

- La restricción al cuarto de servidores por medio de una puerta con sistema electrónico de bloqueo por tarjeta y solo el personal de TI tiene esa tarjeta y autorización para entrar.
- En caso de que una persona ajena al departamento necesite ingresar, debe ser acompañado por un miembro del equipo de TI.
- Este cuarto tiene su propio control de temperatura y debe mantenerse a veintitrés grados centígrados.
- El *Netbotz* también tiene funciones de monitoreo de temperatura, humedad relativa y punto de rocío para el control de las condiciones imperantes del cuarto.

4.2.2.2. P-TI-003 Procedimiento Para el Procesamiento de Virus. Realizado para comunicar y aclarar las políticas del proceso de eliminación de malwares en todas sus versiones de virus, este con un alcance a todos los recursos tecnológicos y sistemas de información de Ali-mentos S.A.

- El antivirus que se use, debe ser el estándar corporativo y con actualizaciones automáticas, estas no podrán ser cambiadas por el usuario final ni podrá ser deshabilitado ni desinstalado.
- Se detalla el refuerzo de nuevas herramientas y el proceso para la eliminación de virus del equipo y archivos, en el cual queda establecido

como encargado de realizar esta labor el encargado de soporte de TI se detalla cómo se hace la revisión y que se debe hacer cuando se detecte una amenaza.

4.2.2.5 P-TI-006 Procedimiento para control y administración de claves de acceso. Su propósito es el de definir la administración y control de las claves de acceso a los diferentes recursos tecnológicos.

- Establece en sí, el formato de cantidad de caracteres mínimos y lo que debe de cumplirse para la correcta asignación de la clave de ingreso, también el establece el tiempo para el cambio de esta y la cantidad de los intentos fallidos antes que la clave se bloquee.
- También describe el proceso que se debe de realizar en TI cuando ingresa o sale algún colaborador de la compañía, también menciona la clave de acceso a los servidores, sus administradores y sus limitantes.

4.2.2.5 P-TI-008 Procedimiento Para el Derecho de Accesos. Definir el procedimiento para la aplicación de la seguridad informática, tanto física como lógica es su propósito y tiene el alcance a todos los recursos tecnológicos y sistemas de información de Ali-mentos S.A.

Este procedimiento alinea la asignación, modificación y/o eliminación de derechos sobre información sensible con el protocolo de seguridad exigido por Corporativo y el comité de “Security Formula”.

También indica el procedimiento sobre la creación de usuarios y sus permisos donde el encargado de esta solicitud es el jefe de cada área, y las personas

responsables de la creación de estos es la persona de TI si se cumple con todos los requisitos en la solicitud.

4.2.2.5 P-TI-009 Procedimiento Para Uso de Computadoras Portátiles. El cual se creó para el uso y cuidado de estos activos en Ali-mentos S.A. y terceros, tiene un alcance a todos los usuarios de estos equipos y este procedimiento es actualizado al menos cada año por el departamento de TI.

- Entre sus puntos más importantes están la vida útil de cada equipo establecida a cinco años como máximo si sigue en uso, pero con una revisión para evaluar si puede seguir operando, esto a criterio de TI que son los expertos del tema.
- El remplazo de cualquier equipo es realizado por el encargado de soporte de TI y si se debe comprar, debe ser aprobado por el director de cada área.
- El sistema operativo, antivirus y demás funciones serán bajo el estándar de Corporativo.
- De ser necesario alguna herramienta que no esté establecida, solo el encargado de soporte de TI puede realizar la instalación.
- Es responsabilidad del usuario en caso de robo del equipo, reportar a lo interno al equipo de TI y presentar la denuncia ante la autoridad judicial.
- Si debe viajar, el usuario es responsable de tomar las previsiones de caso para el manejo de estos equipos, por ejemplo, equipaje de mano o anclar

con candado si tiene que asistir algún evento donde no deba llevar este equipo.

Todos estos procedimientos son a nivel local y están alineados con los procedimientos de Corporativo, se pudo constatar en la información que se comparte en estas, la mayoría son para los procesos del departamento de TI y además las que tienen el alcance a todos los usuarios, no son conocidos por estos o no se acuerdan de que existan procedimientos para el uso de activos.

Según indica la unidad informante, los procedimientos anteriores son actualizados y publicados una vez al año, son revisados por la auditoría externa y compartidos en el centro de documentación, una vez ahí se notifica a todo el personal de la actualización de estos a todos los departamentos.

4.2.3. ¿Existe Control de Accesos como Claves, Firma Digital para el Uso de Estos Equipos?

A.9 Control de acceso de ISO27001 es el punto donde se alinea esta parte del trabajo, este control tiene como objetivo principal “Limitar el acceso a la información y a los recursos de procesamiento de la información”.

Todos los equipos de la compañía son accedidos por medio del control de usuario y la clave corporativa que tiene un mínimo de caracteres y requisitos para ser válido, la firma digital no es usada por ningún usuario hasta el momento.

Para los equipos tipo laptop, aparte de este control de acceso, tiene el control de dos factores “DUO Mobile” este es una app que facilita la autentificación y que, con solo aprobar desde el celular o dispositivo Android, se confirma el acceso en caso de

que quieran entrar a la red, esto es solo para conectarse a la red interna desde afuera, los equipos cuando están en Ali-mentos S.A. no necesitan esta aprobación.

Las claves están configuradas para cambiarse cada noventa días, esto por medio del sistema operativo quien obliga al usuario a actualizar su contraseña para aumentar la seguridad del equipo y la información, el sistema avisa catorce días antes, todos los días del vencimiento y cambio, de no realizar la actualización, no se puede ingresar al equipo y se deberá contactar a soporte de TI.

4.2.4. ¿Existe la División de Cuentas para Cada Usuario si Usan el Mismo Equipo?

Este objetivo está alineado bajo el A.9 Control de acceso de los controles de ISO27001 al igual que el apartado anterior y el cual tiene como objetivo “Limitar el acceso a la información y a los recursos de procesamiento de la información”.

- Todos los colaboradores que usan activos informáticos tienen un usuario, su clave y además un rol que les permite tener privilegios según su puesto y departamento, en los equipos que son usados por varios colaboradores, el que termine su turno debe cerrar su sesión, de lo contrario el compañero que ingrese luego, tendrá acceso a su información y, además, todos los movimientos y/o transacciones que realice, quedaran en el historial del sistema a su nombre.
- El colaborador que inicio su turno, debe hacerlo con su usuario y contraseña, esto ayuda al sistema que se registren sus transacciones correctamente y que tenga la información que necesita para su día a día a la mano, además, al

registrase correctamente tendrá acceso a los servicios que tiene en su rol y a su correo corporativo, tampoco se verá restringido para realizar su trabajo.

- Para el acceso a las carpetas del servidor los usuarios deben de tener permiso para entrar a cualquier carpeta que esté en ese lugar, cada departamento tiene acceso a una ubicación en el servidor para el respaldo de su documentación y el uso de carpetas compartidas, si alguna persona de otro departamento necesita ingresar a alguna carpeta para obtener información, debe solicitar por medio de correo electrónico, permiso al gerente de esa área y con copia a los compañeros de soporte.

  Una vez aprobado el acceso, el usuario debe de crear un tiquete en el sistema para que los compañeros de soporte le den el permiso, este debe venir con las indicaciones si es solo lectura, escritura o ambas, el borrado no está permitido por ningún acceso de otra área.

4.2.5. ¿Existe Algún Tipo de Protección para los Equipos que Salen de la Compañía?

En el control A.6 Organización de la seguridad de la información de ISO27001 en su punto A.6.2 dispositivos móviles y teletrabajo, se dan las bases para alinear este control con los hallazgos de esta fase, ya que su objetivo principal es “Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles”.

A continuación, los resultados:

- Los equipos que salen de la compañía están protegidos por medio la cuenta de usuario y la clave que es, la primera vez, asignada por el soporte de TI, una vez

que ha ingresado el usuario debe de realizar el cambio de contraseña, aunque esto no es obligatorio ya que no hay un control donde deba realizar el cambio, hay usuarios que se mantienen con la calve asignada hasta que el sistema le pide actualización de clave.

Se debe de tomar en cuenta que solo con estos dos controles se puede ingresar a la información que hay en la computadora, pero no así a la red de la compañía si el activo está fuera, por lo que se puede tener acceso a toda la información que se guarda local en el equipo sin restricciones.

Una vez dentro del sistema y para conectarse al VPN corporativo, es necesario colocar de nuevo la clave, y luego se debe de hacer un reconocimiento por medio de la aplicación DUO Mobile quien genera un código tipo mensaje al teléfono donde se debe de aprobar la conexión a la red interna, por lo que es necesario disponer de los dos dispositivos para lograr conectarse a la red.

- Para el control físico, luego que se ha obtenido el permiso de salida de activos firmado por el departamento de TI y el área de control de activos de Finanzas, se debe llenar un formulario de salida en la caseta de seguridad, sin estos tres controles no es posible disponer de este activo fuera de la compañía.
- Las computadoras se entregan físicamente sin ninguna protección que evite los golpes, humedad, raspones, caídas y elementos extraños en los equipos como polvo o algún otro material que le pueda causar un daño físico o sistemático, algunos usuarios les compran un bolso para movilizarlos, pero otros no.

- No hay algún control de cifrado a nivel del sistema para evitar, en el caso de que sea extraviado o robado el equipo, que este sea utilizado y/o accedido si logran obtener la clave, por lo que el equipo y su información están expuestos a estos eventos.
- En la entrevista que se le realizó a la unidad informante indica que antes se encriptaba los equipos definidos como críticos pero que estos causaban dificultades por que si había daño en algún equipo o disco duro, al estar encriptados estos quedaban ligados uno del otro y al querer cambiar el disco o el equipo, estos no eran reconocidos por los nuevos componentes.

4.2.6. ¿Hay Alguna Persona Encargada de la Seguridad de TI a Nivel Local?

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización es el objetivo del apartado A.6. Organización de la seguridad de la información de ISO27001 y el cual sirvió de marco para revisar este punto.

A nivel local no existe algún encargado de la seguridad de TI, toda la seguridad pasiva o activa, vía hardware o software es administrada por Corporativo, indica el informante, el soporte local da apoyo realizando tareas que el equipo de Security Global les pida.

4.2.7. ¿Cuáles son activos críticos para la continuidad del negocio?

Este punto se alineo con el A.8 Gestión de activos de ISO27001, este tiene como objetivo “Identificar los activos de la organización y definir las responsabilidades

para la apropiada protección”, y dentro de este control, el control de inventario de activos.

En la entrevista la unidad informante indica lo siguiente sobre la criticidad de los activos para la operación:

> Evidentemente, además de los servidores como tales, todos los equipos de comunicación son críticos, desde el *router* de internet hasta los *switches* de la red local; como el ERP es *cloud*, el acceso a internet es crítico, y con cualquier fallo en los *switches*, se pierde conexión de red local; sin embargo, hay planes de contingencia para asegurar la continuidad del negocio.

Como se pudo evidenciar por el experto de TI, cada equipo tiene un proceso importante en el rol de la operación, todos los equipos, en el inventario que se realizó, tienen un papel importante para la consecución de las metas personales y grupales.

Aun así, debería estar identificados por categorías de criticidad, esto debido que no es lo mismo que deje de funcionar un *switch* que un *router*, menos si es un *hand held* a que deje de funcionar un servidor, es por eso por lo que es importante tener claro que equipos pueden tener un impacto menor o mayor en la continuidad del negocio a la hora de fallar.

4.2.8. ¿Sabe de Algún Contrato de Confidencialidad para los Usuarios de Activos informáticos?

En el Control A.7 Seguridad ligada a lo recursos humanos de ISO27001, en su punto A.7.1, indica que su objetivo es “Asegurar que los empleados y contratistas

entiendan sus responsabilidades, y que sean aptos para los roles para los cuales están siendo considerados", se toma como base para este punto.

- Todos los entrevistados indican haber firmado, en el momento que son contratados, una norma de confidencialidad que incluye varias cláusulas como seguridad y salvaguardas de la información, procedimientos internos, secretos empresariales, uso de recursos y algunos puntos más fuera del tema de este trabajo.

4.3. Evaluar los Controles Necesarios para Mitigar o Eliminar los Riesgos Encontrados en el Análisis de Riesgo.

Luego de la revisión física y las entrevistas se logró, junto con el análisis de riesgo, determinar en los hallazgos las amenazas que deberían ser revisadas por el departamento de TI, ya sea minimizar, eliminar, aceptar el riesgo o compartirlo con los departamentos involucrados.

ISO 27002 en su control A.9 Seguridad Física y del Ambiente da el marco para la consecución de áreas seguras, seguridad de centros de comunicación, salas de equipos, seguridad física, controles, localidades seguras y otros controles que ayudaron con la evaluación de los puntos de las variables de este trabajo.

Por el objetivo principal de este trabajo, se alinearon entre otras, dos controles de la norma ISO 27002 que fueron las bases para la revisión y el análisis de riesgo, el anterior mencionado A.9 y el punto 7 Gestión de Activos, esto junto con los otros mencionados en los puntos anteriores, dieron las bases para los siguientes resultados.

4.3.1 Análisis de Resultados.

Es en esta parte del trabajo donde se ve reflejado el análisis de resultados que ayudaron a tener una fotografía de la situación de actual de la compañía y que dio las bases para el siguiente paso que es realizar la política de seguridad informática.

Para los valores asignados en este análisis, se tomó en cuenta la opinión y la experiencia de la unidad informante quien es el que da soporte a todos estos activos analizados, en conjunto con la revisión y además mi experiencia de 19 años en los procesos internos de la operación, ayudaron a la asignación de los valores de probabilidades.

Otra variable que ayudó para los siguientes cálculos, es la afectación en la confidencialidad, integridad y disponibilidad, además el ámbito que se puede ver afectado si se materializa alguno de los riesgos encontrados.

4.3.1.1. ¿Hay Riegos Importantes que Puedan Afectar la Continuidad del Negocio por Falta de ese Activo?

El resultado de la revisión y el análisis de riesgo es bastante interesante debido a que, aunque la mayoría de los equipos en la empresa están protegidos de amenazas mayores, los hallazgos apuntan a algunas correcciones que son pequeñas, pero que, al repetirse en varias áreas de la compañía, pueden volverse un problema grande para la continuidad de la operación.

En la siguiente lista está el valor de probabilidad que se asignó a las vulnerabilidades, esta lista se generó con base a las técnicas específicas y recomendaciones de MAGERIT en su punto 2.1 Análisis mediante tablas del libro 3,

estimación del riesgo, esta se basa en una escala de 5 valores para los hallazgos encontrados:

5- Altamente Probable

4- Muy probable

3- Probable

2- Poco Probable

1- Probabilidad Despreciable

El punto 5 “Altamente Probable” es el valor más alto de esta escala de trabajo y, por ende, si apareciera algún riesgo con este valor, habría que darle la prioridad del caso y atacarlo de una vez con la salvaguarda adecuada.

Para este trabajo los resultados van a verse reflejados en el mapa de calor que está a continuación, se debe de tomar en cuenta que, según los valores obtenidos, dependen de las jefaturas de los departamentos el erradicarlos o no, según me comentó la unidad informante, para ello en este trabajo quedará las recomendaciones.

Como lo indica los objetivos de este trabajo, el análisis de riesgo va con el fin de la protección de los activos informáticos, tanto físicos como a nivel de la información y los servicios, es por esto por lo que se debe de tomar en cuenta para el análisis, lo que se verá afectado en caso de materializarse el riesgo, en este caso la disponibilidad (DISP), integridad (INTE) y confidencialidad (CONF) de la información.

Además de lo anterior, se debe de tomar en cuenta el ámbito para el análisis del impacto al negocio si se vieran comprometidos los conceptos antes mencionados (DISP, INTE, CONF), para estos están los posibles ámbitos que se pueden afectar:

- Económico
- Operativo
- Daño a la persona
- Imagen de la Empresa ante sus Clientes

Se muestra en la tabla 4-7 la valoración de los ámbitos alineados a la compañía:

Tabla 4-7:

Valoración de los Ámbitos de Impacto

Ámbitos de impacto	ECONÓMICO	OPERATIVO	DAÑO A LA PERSONA	IMAGEN ANTE EL CLIENTE
1. Muy Bajo (MB)	Menor que $500	Uso de la clave temporal	-	-
2. Bajo (B)	Entre $500 y $1,000	Perdida de datos del usuario	Cita Médica	-
3.Medio (M)	Entre $1,000 y $3,000	Acceso no autorizado a los datos de un usuario	Incapacidad 3 días	Perdida de información de su cuenta
4.Alto (A)	Entre $3,000 y $5,000	No alineamiento con Corporativo en el uso de activos informáticos	Incapacidad 1 mes	Servicio interrumpido
5.Muy alto (MA)	Mas de $5,000	Afectación a la continuidad del negocio	Incapacidad más de 1 mes	Acceso a Información sensible de su cuenta por un tercero

Los valores anteriores están alineados a la empresa y sus procesos, cabe mencionar que el alcance del proyecto está dado al uso de los activos y en el cual hay dos escenarios, los usados internamente en la compañía y los activos que son usados fuera de la compañía para realizar trabajo en casa.

Se puede ver que el valor en el ámbito económico está establecido muy bajo antes de los $500 debido a que la mayoría de los equipos son alquilados y el riesgo de su afectación son compartidos para las dos compañías según el contrato actual.

En el ámbito Operativo sus valores más altos están dados por el riesgo de que los equipos sean utilizados diferente a lo que está establecido por el corporativo y que esto genere alguna afectación a la continuidad del negocio, los accesos no autorizados dentro de la compañía serían por parte del personal que labora en esta, y, es por esto por lo que sus valores son bajos.

Sin embargo, si los equipos que salen de la compañía se perdieran o fuesen robados, pueden afectar la imagen de la empresa ante el Cliente si sus datos se ven expuestos ante un tercero o la competencia.

La afectación de las personas es un poco compleja de definir en cuanto a valor, es por esto por lo que se ha realizado con base a los días de incapacidad, esto ya que afecta directamente a la empresa por no contar con ese operario o administrador por algunos días.

Y, por último, la imagen de la compañía es muy importante para existir y mantenerse en el mercado, si la empresa se ve involucrada en algún tema que le

afecte a algún cliente, esto podría causar la pérdida del cliente y que otros más pierdan la confianza de la operación que realiza la compañía.

Las probabilidades están dadas por los valores de la tabla anterior y según los riesgos, así se tiene lo siguiente:

Para todos los casos solo hay dos casos posibles, así que se aplica si se da el evento o no se da esto se representa No=0/ Si=1, para eso se usa la fórmula de la probabilidad de un evento simple que está dada por probabilidad P(A) =casos favorables/ total de casos posibles.

En la siguiente tabla 4-8 se detalla los resultados para las posibilidades:

Tabla 4-8:

Cálculo de Probabilidad

Riesgo	**Caso Favorable**	**Casos Posibles**	**Caso favorable / Casos Posibles**	**5 niveles de Probabilidad // Factor=5/100**
R1	1	2	50%	2.5
R2	1	2	50%	2.5
R3	3	4	75%	3.75
R4	1	2	50%	2.5
R5	1	2	50%	2.5
R6	1	2	50%	2.5
R7	1	2	50%	2.5
R8	1	2	50%	2.5
R9	1	2	50%	2.5

Se puede ver en los resultados que la mayoría menos uno tiene valor 2.5 (3 redondeado) en la escalada de probabilidades y que para el próximo cálculo se va a redondear hacia arriba para que dé un valor existente en la escala, esto sería valor 3.

Además, en el caso de riesgo R3 se tiene que al haber dos riesgos que se pueden manifestar (calentamiento de cables / corto circuito) suben los casos posibles a 4, (se puede dar uno, el otro, los dos o ninguno) y los casos favorables también suben a 3 (se puede dar uno, el otro o los dos), es por eso por lo que el valor cambia y sube la probabilidad.

Entonces se tiene la tabla final de posibilidades con los valores redondeados como se detalla:

Tabla 4-9:

Relación de Riesgo y Posibilidad

Riesgo	Posibilidad
R1	3
R2	3
R3	4
R4	3
R5	3
R6	3
R7	3
R8	3
R9	3

En la tabla 4-8 que se presenta en la siguiente página, se realiza un resumen de

los hallazgos y los riesgos que existen, también en la primera columna está el número de capítulo donde se encuentra el detalle, además el valor de probabilidad según el listado anterior y lo que este riesgo puede afectar, junto a estos, el ámbito que se vería afectado.

La probabilidad se alineó con base a lo que realmente es importante que se tome en cuenta y para esto la experiencia de la unidad informante ayudó con la clasificación, como se menciona en este trabajo en 5.1, la responsabilidad de la seguridad de los activos informáticos no recae solo en el departamento de TI, sino en todos los involucrados en el uso de los activos y por eso es bueno asignar responsables para cada activo.

A continuación, el detalle en la siguiente página:

Tabla 4-10:

Hallazgos y Riesgos

En el documento	Hallazgo	Riesgo	Afecta a	Probabilidad	Ámbito que afecta
4.2.1.1.	Varios usuarios responsables del mismo equipo.	Perdida de confidencialidad e integridad de los datos del usuario por acceso no autorizado.	CONF / INTE	3	Operativo
	Los equipos se tapan con forros plásticos cuando hay limpieza profunda.	Daños físicos e interrupción del servicio por contaminación física.	DISP	3	Económico

En el documento	Hallazgo	Riesgo	Afecta a	Probabilidad	Ámbito que afecta
	Activos expuestos al polvo y la humedad.	Daños físicos e interrupción del servicio por contaminación física.	DISP	3	Económico
4.2.1.2.	Falta de UPS para las Desktop.	Daño físico e interrupción de servicios por descargas eléctricas.	DISP	3	Económico
4.2.1.6.	Falta de UPS para las Desktop.	Daño físico e interrupción de servicios por descargas eléctricas.	DISP	3	Económico
	Falta de regletas de protección.	Daño físico e interrupción de servicios por descargas eléctricas.	DISP	3	Económico
	Varios objetos eléctricos conectados a un distribuidor de corriente de cuatro entradas sin protección.	Daño físico al equipo y al usuario por calentamiento de cables y/o corto circuito.	DISP	4	Económico// Daño a la persona
4.2.1.7.	Relojes marcadores sin protección.	Daños físicos e interrupción del servicio por golpes o contaminación física.	DISP	3	Económico

En el documento	Hallazgo	Riesgo	Afecta a	Probabilidad	Ámbito que afecta
4.2.1.8.	Equipo sin bloqueo y no estaba el usuario.	Perdida en la integridad y confidencialidad de la información por acceso no autorizado.	CONF / INTE	3	Operativo
4.2.1.9.	Ubicación de los tomacorrientes en el área administrativa.	Daño físico para el Usuario a la hora de conectar o desconectar los equipos.	N/A	3	Daño a la persona
4.2.1.10.	Falta de protección para las *tablets* contra caídas.	Daños físicos e interrupción del servicio por manipulación.	DISP	3	Económico
4.2.1.11.	Pantalla sin protección en el pasadizo.	Daños físicos e interrupción del servicio por golpes con la maquinaria.	DISP	3	Económico
4.2.1.13.	*Hand Held* sin protección.	Daños físicos e interrupción del servicio por manipulación.	DISP	3	Económico
4.2.2.	Procedimientos no conocidos por los Usuarios.	Uso diferente de los equipos con lo establecido por el Corporativo.	DISP/INTE/CONF	3	Operativo

En el documento	Hallazgo	Riesgo	Afecta a	Probabilidad	Ámbito que afecta
4.2.3.1	No hay cifrado de disco ni de BIOS.	Perdida de la confidencialidad de la información si el equipo es robado.	DISP/INTE/CONF	3	Imagen de la Empresa ante sus Clientes
4.2.4.1.	Los usuarios puede que bloqueen o no el acceso al sistema.	Perdida de la confidencialidad e integridad de la información por acceso no autorizado.	INTE/CONF	3	Operativo
4.2.5.1	Uso de la clave temporal hasta que el sistema le pida una nueva para ingresar.	Perdida de confidencialidad e integridad por acceso no autorizado debido a una clave en común.	INTE/CONF	3	Operativo
	No hay protección para los equipos que salen de la compañía, esto en la parte física.	Daños físicos e interrupción del servicio por mala manipulación.	DISP	3	Económico
4.2.5.4.	No hay Procedimiento de seguridad a nivel local o no lo conocen.	Uso diferente y/o inadecuado de los equipos con lo establecido por el Corporativo.	DISP/INTE/CONF	3	Operativo

En el documento	Hallazgo	Riesgo	Afecta a	Probabilidad	Ámbito que afecta
4.2.7.	Identificación de activos críticos.	Pérdida de priorización cuando hay algún evento que perjudique la continuidad del negocio.	DISP	3	Operativo

De lo anterior se basó para el análisis de los hallazgos según su impacto en los dos procesos que existen en el uso de activos y su afectación en la confidencialidad, integridad y disponibilidad de la información:

En la tabla 4-9 se presenta la información de relación (Riesgo= Probabilidad x Impacto), los riesgos fueron consolidados para obtener el valor de cada uno y así represarlos en el mapa de calor de riesgos que se muestra a continuación:

Tabla 4-11:

Relación Riesgo=Probabilidad x Impacto, julio 2021

Prefijo	Riesgo	Probabilidad	Impacto	R=P*I
R3	Calentamiento de cables y/o corto circuito.	4	5	20
R8	Robo de equipo	3	5	15
R2	Afectación en la continuidad del negocio.	3	5	15
R9	Uso diferente y/o inadecuado de los equipos con lo establecido por el Corporativo.	3	4	12
R5	Daño físico para el Usuario	3	4	12
R6	Daños físicos al activo	3	2	6
R4	Contaminación física en el activo	3	2	6
R1	Acceso no autorizado.	3	2	6
R7	Interrupción del servicio	3	1	3

En la siguiente tabla 4-10, se muestra el mapa de calor para obtener una imagen gráfica de los resultados de la tabla 4-9:

Tabla 4-12:

Mapa de Calor de Riesgos, julio 2021

Probabilidad e Impacto		Impacto				
		1- Muy Bajo	**2- Bajo**	**3- Medio**	**4- Alto**	**5- Muy Alto**
Probabilidad	**5-Altamente Probable**					
	4-Muy probable					**R3**
	3-Probable	**R7**	**R1/ R4 /R6**		**R5/R9**	**R2 / R8**
	2-Poco Probable					
	1-Probabilidad Despreciable					

En la tabla anterior se refleja los riesgos que deben de ser revisados con prioridad debido a que al estar en la escala donde la probabilidad y el impacto tienen un valor muy alto y puede materializarse en cualquier momento, entre ellos los riesgos 2,3 y 8.

También se puede ver que muy cerca de la zona roja están los riesgos 5 y 9 que, aunque no tienen el mismo impacto que los anteriores, tienen un riesgo de hasta 12 puntos, por lo que deberán revisarse para ver si es posible mitigarlos la antes posible debido a que su impacto si se llegan a materializar es alto.

Los riesgos 1, 4 y 6 aunque su posibilidad es 3 que es probable que se materialicen, su impacto es bajo por lo que valdría la pena revisarlo para ver si es necesario corregirlo o mitigarlo para no exponer a estos activos a algún daño físico.

El último riesgo 7 pueden causar una pequeña interrupción en el servicio debido a que se tenga que cambiar el activo y configurar el nuevo dispositivo para su uso, se revisará en las salvaguardas si hay algo que se pueda hacer para minimizar este riesgo.

Capítulo 5 : Propuesta de Solución

5.1. ¿Se Puede Eliminar, Mitigar o Asumir los Riesgos encontrados?

Todo riesgo puede ser evaluado para saber si se puede intervenir y tomar decisiones de ataques para, si es posible, llegar a eliminarlo por completo y, para esto, la salvaguarda es el procedimiento tecnológico que reduce el riesgo.

Como se mencionó al principio de esta fase, ISO-27002 entre sus objetivos y controles del punto 9- Seguridad Física y del Ambiente, el cual indica que se debe prevenir accesos físicos no autorizados, daños e interferencias en las instalaciones y en la información, también alienta a tener los equipos, con información sensible, bajo perímetros de seguridad adecuados.

La importancia en el control de accesos, protección de amenazas externas y del ambiente, seguridad del equipo en cuanto a acceso y localización, cableado, mantenimiento y algunas otras más, ayudan a alinear los resultados obtenidos con estos controles.

Se sabe que, aunque TI es el responsable de los sistemas de información y su buen funcionamiento, los departamentos en sí son responsables de velar por la buena utilización de los activos informáticos que utilizan para los procesos diarios, es por esta razón que no es solo responsable TI de que se realicen, de ser necesario, los cambio para la intervención de los hallazgos de este trabajo.

En este punto revisando la tabla anterior con los riesgos encontrados, se pueda afirmar que si es posible la eliminación de algunos riesgos con pequeños cambios que se pueden realizar, también es posible mitigar algunos de ellos para ayudar a que baje la probabilidad de que se manifieste, y, por último, también es afirmativo que se pueden

asumir algunos riesgos debido a que algunos encontrados son de bajo impacto para la compañía.

Pero ¿cuáles son las salvaguardas que pueden ayudar a realizar lo descripto anteriormente?, esto lo vamos a resolver en el siguiente punto 5.1.1. de este capítulo, donde se va a alinear los hallazgos con el marco de referencia de MAGERIT e ISO-27002

En los siguientes puntos se va a dar respuesta a esta fase basados en los resultados del análisis de riesgo y los hallazgos encontrados en la revisión física que se realizó en las diferentes áreas de la compañía.

5.1.1. ¿Qué Controles se Puede Utilizar Para Mitigar los Riesgos Encontrados?

Las salvaguardas permiten hacer frente a las amenazas y estas varían al igual que las técnicas con el avance tecnológico, esto por se crean nuevas tecnologías o desaparece las antiguas, cambio de activos en cuanto a tipo o por que los atacantes cada vez son más ágiles para encontrar formas de acceder a la información (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

Es por lo anterior que se debe de realizar la búsqueda de las salvaguardas correctas con base a lo que se requiere atacar, es un proceso que debe de venir justificado para cada caso y es por eso por lo que se está usando dos herramientas que han ayudado a tener un marco de referencia en este trabajo y que además aparte de la experiencia, tienen años de estar buscando soluciones para los temas de riesgos.

En la tabla 5-1 a continuación se muestra el alineamiento de ISO-27002 con los hallazgos y los riesgos que resultaron de la revisión que se realizó en la compañía y que se encuentran con detalle en el capítulo 4.2 de este trabajo, en esta se detalla los controles que se pueden utilizar como base para buscar las salvaguardas que permitan atacar los riesgos que pueden afectar en los procesos de la compañía.

Tabla 5-1:

Alineamiento con los Controles de ISO27001, agosto 2021

Hallazgo	Riesgo	Control ISO27002
Varios usuarios responsables del mismo equipo	Perdida de confidencialidad e integridad de los datos del usuario por acceso no autorizado.	11 control de Acceso
Los equipos se tapan con forros plásticos cuando hay limpieza profunda	Daños físicos e interrupción del servicio por contaminación física.	9.2 Seguridad del Equipo
Activos expuestos al polvo y la humedad	Daños físicos e interrupción del servicio por contaminación física.	9.2 Seguridad del Equipo
Falta de UPS para las desktops	Daño físico e interrupción de servicios por descargas eléctricas.	9.2.2. Elementos de soporte
Falta de UPS para las Desktop	Daño físico e interrupción de servicios por descargas eléctricas.	9.2.2. Elementos de soporte
Falta de regletas de protección.	Daño físico e interrupción de servicios por descargas eléctricas.	9.2.2. Elementos de soporte
Varios objetos eléctricos conectados a un distribuidor de corriente de cuatro entradas sin protección	Daño físico al equipo y al usuario por calentamiento de claves y/o corto circuito.	9.2.2. Elementos de soporte
Relojes marcadores sin protección.	Daños físicos e interrupción del servicio por golpes o contaminación física.	9.2 Seguridad del Equipo
Equipo sin bloqueo y no estaba el usuario.	Perdida en la integridad y confidencialidad de la información por acceso no autorizado.	11- Control de Acceso

Hallazgo	Riesgo	Control ISO27002
Ubicación de los tomacorrientes en el área administrativa.	Daño físico para el Usuario a la hora de conectar o desconectar los equipos.	8. Seguridad Ligada A Los Recursos Humanos
Falta de protección para las tablets contra caídas.	Daños físicos e interrupción del servicio por manipulación.	9.2 Seguridad del Equipo
Pantalla sin protección en el pasadizo de Producción.	Daños físicos e interrupción del servicio por golpes con la maquinaria.	9.2 Seguridad del Equipo
Hand Held sin protección.	Daños físicos e interrupción del servicio por mala manipulación.	9.2 Seguridad del Equipo
Procedimientos no conocidos por los Usuarios.	Uso diferente de los equipos con lo establecido por el Corporativo.	13- Gestión de incidentes de la seguridad de la información
No hay cifrado de disco ni de BIOS.	Perdida de la confidencialidad de la información si el equipo es robado.	9.2.5 Seguridad del equipo fuera del entorno habitual
Los usuarios puede que bloqueen o no el acceso al sistema.	Perdida de la confidencialidad e integridad de la información por acceso no autorizado.	11. Control de Acceso
Uso de la clave temporal hasta que el sistema le pida una nueva para ingresar.	Perdida de la confidencialidad e integridad de la información por acceso no autorizado.	11. Control de Acceso
No hay protección para los equipos que salen de la compañía, esto en la parte física.	Daños físicos e interrupción del servicio por mala manipulación	9.2 Seguridad del Equipo
No hay Procedimiento de seguridad a nivel local o no lo conocen.	Uso diferente y/o inadecuado de los equipos con lo establecido por el Corporativo.	13- Gestión de incidentes de la seguridad de la información
Identificación de activos críticos	Pérdida de priorización cuando hay algún evento que perjudique la continuidad del negocio.	14- Gestión de la continuidad del negocio

Además de esta tabla, está el resumen de los riesgos encontrados y que se utilizó para la asignación de las salvaguardas que se necesitan en cada caso, de la tabla 4-9 se ha tomado este resumen que se presenta en la siguiente tabla 5-2 para empezar con la revisión y si es posible eliminar, mitigar o asumir estos riesgos por parte de los departamentos involucrados en los procesos.

Tabla 5-2:

Resumen de Riesgos Encontrados

Prefijo	Riesgo
R1	Acceso no autorizado
R2	Afectación en la continuidad del negocio
R3	Calentamiento de cables y/o corto circuito
R4	Contaminación física en el activo
R5	Daño físico para el Usuario
R6	Daños físicos al activo
R7	Interrupción del servicio
R8	Robo de equipo
R9	Uso diferente y/o inadecuado de los equipos con lo establecido por el Corporativo

De la tabla anterior se detalla cada riesgo con la posible solución según los controles asignados en la tabla 5-1.

R1. Acceso no autorizado

Este riesgo está alineado con el control 11-Control de Acceso de ISO-27002 y se tiene cuatro hallazgos que tienen que ver directamente con el acceso no autorizado a los equipos, estos fueron encontrados en diferentes áreas de la empresa y se da por diversas situaciones que se detallan:

- Varios usuarios responsables del mismo equipo.
- Equipo sin bloqueo y no estaba el usuario.
- Los usuarios puede que bloqueen o no el acceso al sistema.
- Uso de la clave temporal hasta que el sistema le pida una nueva para ingresar.

El objetivo del control 11 de ISO-27002 es controlar el acceso a la información, e indica que estos deberían ser controlados con base a los requisitos del negocio y a la seguridad de este, la propuesta es políticas de distribución y autorización de la información.

En la revisión y con los resultados obtenidos, se sabe que todos los usuarios tienen su control de acceso a las computadoras, tienen asignado un role y una clave de acceso que son la base para poder ingresar a sus equipos, por ello se puede decir que, si hay una política de control de acceso, pero se debe de reforzar haciéndole llegar las reglas de control y derechos de acceso a cada usuario en una política que contenga estos puntos claramente definidos.

R2. Afectación en la continuidad del negocio

La Gestión de la continuidad del negocio es uno de los temas delicados para cualquier empresa, en este punto 14 de ISO-27002 aconseja contrarrestar interrupciones a las actividades del negocio y proteger los procesos críticos contra los efectos de fallas en los sistemas de información y desastres.

En la revisión se identificó este riesgo debido a que no hay un listado donde se pueda revisar, en caso de un evento que se vea afectado un activo, a cuál se debe de

dar prioridad, se confirmó que si hay una prioridad cuando es un servidor el que tiene el problema o algún activo que dependan todos los sistemas, como la caída de la red.

Cabe mencionar que, para este riesgo, según indicó la parte informante, hay planes de contingencia por si algún activo deja de funcionar y esto es lo que aconseja ISO-27002 para mitigar este riesgo.

R3 Calentamiento de cables y/o corto circuito.

El control 9.2 Seguridad del equipo en su nivel 9.2.2 de ISO-27002 indica que se debería proteger los equipos contra posibles fallas o interrupciones de energía por la situación de los elementos de soporte, sean UPS, cables, ventilación, aire acondicionado y muchos otros que ayudan al equipo a su correcto funcionamiento.

En la revisión en el área de bacheo se observó varios equipos conectados a solo una salida del tomacorriente con un distribuidor para 4 equipos, este no tenía UPS ni alguna regleta que le diera protección.

Lo recomendable para la conexión de equipos es que cuenten con una UPS o un sistema de alimentación interrumpida con capacidad para toda la carga de equipos conectados o algún mecanismo de suministro de energía interrumpida para equipos críticos, si no es posible, al menos una regleta que contenga un fusible que pueda desconectar el equipo de la corriente eléctrica en caso de algún evento por picos elevados de corriente eléctrica o sobre carga.

R4 Contaminación física en el activo

En los hallazgos con posibilidades de este riesgo están los equipos que están en

las áreas de operaciones, estos son equipos que están en medio del proceso de la producción, estos controlan el empiezo y el fin de la producción.

Estos equipos están expuestos al polvo y al agua en cualquier momento que el usuario se descuide y no lo proteja a tiempo, hay algunos que están protegidos en muebles de acero inoxidable, pero a la hora de usarlos deben de sacar el teclado, el ratón o en algunas ocasiones abrir la tapa donde se encuentra protegido.

Entre los hallazgos están los siguientes:

Los equipos se tapan con forros plásticos cuando hay limpieza profunda, lo que lo deja expuesto a que no sea bien cubierto y le pueda entrar agua.

Activos expuestos al polvo y la humedad debido a su posición, en la revisión se logró observar que algunos equipos se ven afectados en su acceso por tarimas de productos que están en proceso para pasarlas a la bodega.

ISO-27002 en su control 9.2 Seguridad del Equipo en su punto 9.2.5 habla de la seguridad del equipo fuera del entorno habitual y sugiere entre otra protección especial como cubiertas para el teclado, minimizar el acceso innecesario de los equipos a las áreas de trabajo y además estar aislados para reducir el nivel general de protección.

R5 Daño físico para el Usuario

Este riesgo al no ser directamente al activo queda fuera del marco de referencia de ISO-27002 pero el riesgo existe y se debería tomar en cuenta, al estar los tomacorrientes debajo de los escritorios o módulos de trabajo, el usuario debe de correr la silla y agacharse para lograr tener acceso a los tomacorrientes asignados para ese proceso.

La propuesta de solución es colocar regletas de protección y que estas sean colocadas encima de los escritorios o módulos donde estén accesibles para los usuarios, esto evita que el usuario tenga que realizar maniobras que le puedan causar daños físicos, caídas o golpes.

R6 Daño físico al activo

Algunos equipos están expuestos a golpes, caídas, rayones, mala manipulación por parte del usuario y esto causa daños físicos que podría hacer que el equipo funcione incorrectamente o deje de funcionar.

Volviendo al control 9.2 Seguridad del Equipo que indica que los equipos deberían ubicarse en sitios adecuados o protegerse para reducir los riesgos ocasionados por amenazas y peligros ambientales, los equipos más pequeños como *hand held* y las *tablets* que son manipulables por los usuarios, están expuestos a este riesgo, también las computadoras portátiles están expuestas a este tipo de riesgos.

La recomendación es situar a los equipos en bases sólidas donde se minimice su movimiento y si se debe de mover, usar la protección de estuches y bolsos en el caso de las portátiles, esto ayuda a minimizar los accidentes de caídas y de que se deteriore más rápido el activo.

R7 Interrupción del servicio

La interrupción de servicio está dada por algunos de los eventos que se vieron anteriormente, daños físicos a los equipos por golpes, contaminación física o ambiental, mala manipulación del activo tanto físico como en el sistema, desconocimiento de procedimientos para el uso de los equipos y muchos otros eventos

que pueden casuar que este riesgo se materialice.

Es por esto por lo que, si se trabaja en los riegos anteriores, este riesgo se puede eliminar o mitigar según se corrijan los hallazgos y se implementen las salvaguardas recomendadas.

R8 Robo de equipo

En los equipos portátiles que se materialice este riesgo es una probabilidad que depende totalmente del usuario, aunque es difícil mitigar este riesgo porque siempre va a estar presente, cada vez que un equipo salga de la compañía, inclusive dentro, se puede buscar la forma que el impacto no sea más allá del valor económico del activo.

Si el equipo es robado y accedido a los datos, puede que en este se encuentre información crítica para la compañía y sus clientes, y esta información en manos de terceros es un riesgo alto de perdida de imagen ante el cliente y puede llevar a la pérdida del contrato y por ende el retiro del cliente de la cartera.

Es por eso por lo que se recomienda el cifrado de al menos el disco duro, esto para proteger la información del equipo, aunque este se dé por perdido, con esto se sabe que la información va a estar protegida y no podrá ser accedida.

R9 Uso diferente y/o inadecuado de los equipos con lo establecido por el Corporativo

En el control 8.1.1 Roles y responsabilidades se habla de los empleados, contratistas y usuarios y sus obligaciones con respecto a sus responsabilidades de seguridad a la hora de usar los equipos de la compañía.

Este indica que estos deberían implementar y actuar con las políticas de seguridad de la información de la organización, que se deben de proteger los activos de accesos no autorizados, divulgaciones, destrucciones o interferencias y que deben de reportar eventos de riesgos potenciales de seguridad ante los encargados.

Es por eso importante que los usuarios conozcan y apliquen las políticas que están establecidas por la compañía y el Corporativo en cuanto la seguridad informática, uso seguro de activos informáticos, procedimientos internos, división de responsabilidades en el área de TI para saber a quién buscar cuando tienen alguna situación adversa y sus roles de usuarios para que sepa hasta dónde puede llegar en los sistemas.

5.3. Desarrollar Una Política de Seguridad Informática Acorde a los Resultados del Análisis de este Trabajo para Presentarla a la Dirección

Las políticas de seguridad informáticas es un conjunto de pautas que se aplican a actividades y los recursos de una organización incluyendo áreas tales como seguridad física, personal, administrativa y seguridad de la red (Normasiso27001, 2017).

Las políticas de seguridad deben de ser fáciles de entender y explicar de forma resumida, para que sirve su aplicación en la empresa, la utilidad y los responsables de su debida aplicación (Normasiso27001, 2017).

La norma ISO27001 deben de estar disponibles como información documentada, ser comunicada dentro de la organización y estar disponible para las

partes interesadas, adecuada para el propósito de la organización y que incluya objetivos de seguridad (Normasiso27001, 2017).

Una de las mejores definiciones encontradas es la de Rubén Rodriguez y José Ribón Zarco que dice en la definición de políticas de seguridad de su trabajo:

> Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.
>
> No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y el porqué de ellos, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos, así como un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal. (Rodriguez & Ribón Zarco, s.f.)

Con base a la información anterior se procede con el análisis de la información para responder a las siguientes preguntas de las variables establecidas para este trabajo y que están alineas con los objetivos específicos.

5.3.1. ¿Es Suficiente los Resultados Obtenidos en el Proyecto para Desarrollar una Política de Seguridad Informática?

En el análisis de riesgo se observó que, aunque hay algunos procedimientos internos, el 100% de los entrevistados no saben de algún procedimiento más el de la

cláusula de confidencialidad que firman cuando ingresa a la compañía, esta cláusula es a nivel general de la información y no va con el enfoque que debería tener si fuese de TI sobre la manipulación de información a nivel de sistemas.

En los resultados de este trabajo a nivel general, se confirmó algunos riesgos en la confidencialidad, integridad y disponibilidad de la información debido a varias situaciones que si bien, la mayoría son en la manipulación y localidades de los activos, vienen dadas por falta del conocimiento de políticas que ayuden a guiar al usuario bajo un marco estratégico para minimizar los riesgos.

Los resultados obtenidos en este trabajo sí son los suficientes para crear una política de seguridad informática basa en la situación actual de la compañía con base a los procedimientos para el uso de los activos informáticos tanto a lo interno como a lo externo de la empresa.

5.3.2. ¿Qué Política de Seguridad se Alinea con la Estrategia de la Compañía y con los Resultados Obtenidos?

> El objetivo de una política de seguridad de la información es proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.
>
> La dirección debería establecer una orientación clara de la política en línea con los objetivos de negocio y demostrar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización (INTECO, 2014).

En ISO27001 existen varias opciones que se pueden alinear al trabajo y a cualquier resultado según su categoría o ámbito de afectación, esta variabilidad ayuda a que se cuente con herramientas que se puedan usar casi que en todos los resultados de cada tipo de riesgo encontrado.

Algunos ejemplos que tiene ISO27001 sobre el tema de políticas de seguridad se detallan a continuación:

Política de control de Acceso

Política de clasificación y manejo de la información

Política de seguridad física y ambiental

Política de temas finales orientados al usuario como:

Política de uso aceptable de activos

Política de escritorio y pantallas limpios

Política de transferencia de información

Política para dispositivos móviles y teletrabajo

Política restricciones a las instalaciones y uso del software

Política copias de seguridad (INTECO, 2014).

Y muchas otras que ayudas a las TI a lograr el control de los activos, aunque no estén ellos en el sitio.

De acuerdo con los resultados de este trabajo se usó algunos de estos temas para la creación de la política seguridad informática que es el objetivo principal de este proyecto.

Se debe de tomar en cuenta que hay algunos riesgos que no son alcanzados por este trabajo ni por la política general, estos están dados por decisiones que se han tomado en otras áreas y no por TI, y que deben ser corregidas por ellos mismos, por ejemplo, el riesgo 5 daño físico para el usuario, esto debido a que los tomacorrientes de la compañía fueron instalados debajo de los escritorios y esto no es un tema del alcance de este proyecto, aunque si se toma para hacer la observación y recomendaciones.

Entre los temas que se obtuvieron y están reflejados en los hallazgos de este trabajo se tienen los siguientes controles según ISO27002 que se alinean con los hallazgos y que se muestran en la siguiente tabla 5-3:

Tabla 5-3:

Controles ISO27001

Número de Control en ISO27002	**Nombre del Control**	**Objetivo de Control**
7	Gestión de Activos	Implementar y mantener una adecuada protección sobre los activos de la organización
8	Seguridad Ligada a los Recursos Humanos	El objetivo ligado a este control se da para no dejar este punto huérfano por ISO27002, ya que la protección al usuario es parte de este trabajo.
9	Seguridad Física y del Ambiente	Prevenir accesos físicos no autorizados, daños e interferencias contra las instalaciones y la información de la organización.

11	Control de Acceso	Controlar el acceso a la información.
13	Gestión de Incidentes de la Seguridad de la Información	Asegurarse de que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de manera que permita tomar acciones correctivas oportunamente.
14	Gestión de la Continuidad del Negocio	Contrarrestar interrupciones a las actividades del negocio y proteger los procesos críticos del negocio contra los efectos de fallas importantes en los sistemas de información o desastres, y asegurarse de su restauración oportuna.

Según estos resultados la política que se alinea con la compañía debe de tomar en cuenta la seguridad ligada a los recursos humanos para revisar que las acciones que se dan cuando se instale un nuevo módulo o equipo en la compañía.

El segundo tema que debe de quedar plasmado en la política es la seguridad física y de ambiente para prevenir los accesos no autorizados o daños contra los activos y la información de la compañía.

El tercer punto que se debe de alinear a la política es del control de acceso, esto para que los usuarios estén al tanto de la importancia de la información para la compañía, que sepa que hay información sensible que no es debido compartir ya que puede afectar la confidencialidad del negocio.

La gestión de incidentes de la seguridad de la información es el otro tema que ataca directamente a las debilidades de la seguridad de la información y por lo tanto se debe agregar en la política de seguridad.

Por último, está la gestión de la continuidad del negocio que contrarresta las interrupciones sufridas y ayuda a minimizar las fallas en activos críticos o en los sistemas de información, estos si se ven afectados por alguna situación adversa, puede generar situaciones que afecten directamente la continuidad del negocio.

Con base a esta información se trabajó en la política de seguridad que fue entregada a la Gerencia de TI para su revisión, y, si se alinea con los procesos y requerimientos de la organización, sea aprobada y presentada como política de seguridad de información de Ali-mentos S.A.

Una vez claro el alineamiento de los controles necesarios con los hallazgos, se debe saber cómo crear la política de seguridad informática y para esto se necesita la información de lo que conlleva la estructura de este desarrollo.

Para ello, como se menciona en el título de este proyecto, se va a usar ISO27001:2013 e ISO27002:2013 como marco de referencia para la estructura de la política, y con esto asegurar el alineamiento de los controles con lo que realmente necesita la compañía según los hallazgos.

En el capítulo 5 Políticas de seguridad de la información en su apartado 5.1 Directrices de gestión de la seguridad indica que le objetivo es proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativas pertinentes.

El apartado 5.1.1 Políticas para la seguridad de la información da la guía para la implementación de la política iniciando con el control que indica “Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la

dirección, publicado y comunicado a los empleados y parte externas relevantes" (INTECO, 2014).

En la guía de implantación se recomienda lo siguiente:

La organización debería definir una "política de seguridad de la información" al máximo nivel que sea aprobada por la dirección y establezca el enfoque de la organización para gestionar sus objetivos de seguridad de la información (INTECO, 2014).

También se indica que esta política debería considerar requisitos creados por la estrategia del negocio, la normativa, legislación y contratos, el entorno actual y previsto de amenazas para la seguridad de la información.

Debería incluir la definición de la seguridad de la información, de sus objetivos y principios para orientar todas las actividades concernientes a esta, además la asignación de responsabilidad generales y específicas en materia de gestión de la seguridad de la información para los roles definidos.

El apartado 5.1.2 habla de la revisión de las políticas para la seguridad de la información que deberían revisarse a intervalos planificados o siempre que se produzca cambios significativos, para asegurar la idoneidad, adecuación y eficacia de la política con alineamiento de la estrategia de la compañía.

Para esto se recomienda un propietario asignado por la dirección para el desarrollo de esta revisión y evaluación, el cual deberá incluir la evaluación de oportunidades de mejora y en enfoque de gestión de la seguridad en respuesta a los cambios del entorno, las circunstancias, condiciones legales, reglamentarias o

contractuales o entorno técnico de la organización, además, debe tomar en cuenta la revisión y aprobación de la dirección (INTECO, 2014).

La política fue desarrollada con base a todo este trabajo que se realizó y para el cual ayudaron las herramientas seleccionas para este fin.

La política de seguridad informática se puede encontrar en el apéndice F de este documento y fue entregado a la dirección de TI vía correo electrónico y según se había indicado al inicio de este proyecto, con todos los documentos de los entregables para su análsis.

Capítulo 6 : Conclusiones y Recomendaciones

6.1 Conclusiones

- Los cambios que se han realizado en los dos últimos años en muchas compañías han dejado huella para futuros proyectos que las empresas quieran realizar, un cambio como el que se vivió debido a la pandemia llevó a muchas empresas a recrear sus procesos para soportar y salir adelante con sus negocios.
- Al asumir nuevos procesos vienen cambios en todo aspecto, operativo, personales, tecnológicos y muchos otros que comprometen a todos los colaborados de la empresa a apoderarse de funciones nuevas y comprometerse a realizar un cambio de mentalidad con respecto a sus funciones en el uso de nuevas técnicas de trabajo.
- Pero con esto también vienen nuevos riesgos para los procesos y es acá donde este trabajo viene a ayudar a la Gerencia de TI para dar las nuevas pautas para la seguridad informática de la compañía en sus procesos, esto con una política de seguridad informática actualizada y alineada con los viejos y nuevos procesos de la operación.
- En el problema general de este trabajo, y según los resultados, se logra confirmar que las políticas de seguridad informáticas ayudan a la integridad, confidencialidad y disponibilidad de la información dando marcos de referencia para los usuarios, concientizando a los usuarios en las buenas prácticas de uso de los activos informáticos y asignando responsabilidades para cada uno de ellos.

- En los problemas específicos, para minimizar los riesgos que afectan los procesos de manipulación en los activos se realizó un análisis de la situación de la compañía, ya que la identificación de los riesgos es el primer paso para saber que hay que corregir y da el alcance que debe cubrir el análisis de riesgo.
- Con el análisis de riesgo, aparte de lograr la mitigación de algunos riesgos encontrados, se garantizó herramientas de control actualizadas y políticas de seguridad alineas a los procesos, garantizando con esto la confidencialidad, integridad y disponibilidad de la información en los procesos informáticos.
- Las herramientas utilizadas para conseguir el objetivo de este proyecto (observación/ entrevistas, MARGERTI V.3, COBIT 5, ISO27001/ISO27002) ayudaron como marco de referencia para la consecución de los objetivos, y estos fueron la base para el desarrollo de la política de seguridad con los resultados esperados en cuanto al alineamiento de este trabajo con la estrategia de la compañía.
- En la revisión de la situación actual de la compañía se logró confirmar que los procedimientos para el uso de activos no son conocidos por los usuarios y ellos lo hicieron ver así en las entrevistas realizadas, también se observó que los pocos procedimientos que hay, en su mayoría, están diseñados para el uso interno de TI, se evidenció que la compañía carece de una política de seguridad informática actualizada a nivel local que ayude a minimizar los riesgos de los activos esenciales que fueron analizados en este proyecto.

- Se pudo confirmar que el inventario de activos si existe y es controlado por los compañeros de soporte de TI, hay 203 activos actualmente, junio 2021, con este inventario se logró realizar el análisis de riesgo a los activos y se constató que todos ellos son parte importante para la operación y la continuidad del negocio.
- En el análisis de riesgo se pudo constatar que la mayoría de los activos de la compañía están protegidos en todos los niveles en el tema seguridad informática como es el caso de los servidores, los racks donde están los switches y las computadoras que se utilizan en el área administrativa.

  Sí existen riesgos que se obtuvieron durante el análisis, de las 203 unidades totales del inventario, hay un total de 119 usuarios que comparten algún equipo para sus labores, estos equipos están expuestos a más riegos que los demás equipos que son utilizados por un solo usuario por lo que se debe de establecer los límites de uso mediante políticas bien definidas para este tema.
- Los equipos que salen de la compañía son 125 unidades, un 61.5% del total del inventario, estos equipos están expuestos, aparte de los mismos riesgos de los demás, a otros riesgos que aumentan las probabilidades de que se puedan dañar, ser robadas, contaminar físicamente, dar mala manipulación por parte de terceros y accesos no autorizados a la información, es por eso por lo que se debe de dar un tratamiento diferente para protegerlos.
- La evaluación de los controles necesarios está alineada a las normas y controles de ISO-27001 e ISO27002, estos son el resultado de la respuesta al

análisis de riesgo y sus hallazgos, y esto quedó plasmado en el desarrollo de la política de seguridad informática que se realizó en este trabajo.

- La búsqueda de los tipos de políticas de seguridad informáticas que se alinearan con el proceso de la compañía se dio por medio de los efectos obtenidos en el análisis de resultados, los análisis que se realizaron en este trabajo aseguraron que se desarrollaran políticas actualizadas y alineas con los procesos actuales de la compañía.

6.2 Recomendaciones

En este trabajo queda reflejando el interés de la Gerencia de TI en los temas de seguridad informática, este tema no es de un solo departamento ni de solo una persona, la seguridad informática debe ser un asunto de todos los usuarios de la compañía, de los contratistas y terceras partes que interactúen con algún activo informático de Ali-mentos S.A.

El tema de seguridad informática debe ser conocido por todos los involucrados, hacer saber que existen y que todos somos responsables de que se cumplan los procedimientos y políticas establecidas para el funcionamiento correcto de los activos informáticos.

Se debe de capacitar y concientizar a los usuarios en los temas de seguridad informática y en el uso correcto de los equipos, esto puede ayudar a que sean menos los equipos que se le tengan que dar soporte físico o lógico y a su vez libera al personal de TI de problemas repetitivos que se dan por falta de conocimiento.

Los mantenimientos de los equipos deben de establecerse con regularidad para

evitar que los riesgos por falta de estos se agudicen y que el personal de soporte tenga más arreglos de equipos que mantenimientos en su agenda.

Las revisiones periódicas a los equipos en las operaciones, dan como resultado la prevención de riesgos por descuido o por falta de conocimiento en los procesos de los activos informáticos, en las revisiones que se hicieron se encontraron algunos riesgos que se pueden corregir, pero que el personal al no tener conocimiento sobre algunos temas, no se dan cuenta del riesgo que puede correr un activo en algunas circunstancias lo que un usuario experto de TI puede ver de inmediato gracias a su conocimiento en el tema de seguridad informática.

En el análisis de riesgo se encontraron 7 riesgos con los que se trabajó el mapa de calor y como resultado tres de ellos están en un estado muy alto y 2 más a nivel alto, por lo que se recomienda revisarlos con los departamentos encargado para realizar lo antes posible los cambio y así evitar que estos riesgos se materialicen y causen algún daño a los activos o los usuarios.

Se recomiendo también revisar los demás riesgos que están en esta tabla y analizar si se pueden mitigar o si no es necesario debido a si poco impacto.

Si bien es cierto que las políticas de seguridad informáticas vienen a dar solución para evitar riesgos a los activos de información, se debe de buscar la forma de que todos los usuarios estén enterados de que existe políticas para el manejo de los riesgos en el uso de activos y además que son políticas de carácter obligatorio para todos los usuarios, tanto los colaboradores del departamento de TI como los jefes de las áreas, deben de ayudar a que estas políticas le lleguen a todos los involucrados.

Referencias

Alarcón, J. O. (16 de Noviembre de 2016). Diseño e implementación de políticas de seguridad informática, red y virtualización apoyadas con software libre en la compañía tecnología y redes S.A.S. (Trabajo de Grado). Universidad Piloto de Colombia. Bogotá, Colombia. Obtenido de https://repository.libertadores.edu.co/bitstream/handle/11371/1332/alarconjavier2016.pdf?sequence=1&isAllowed=y

Alfaro, A., & Vargas, E. (2016). *DISEÑO DEL PLAN DE SEGURIDAD INFORMÁTICA DEL SISTEMA DE INFORMACIÓN MISIONAL DE LA PROCURADURÍA GENERAL DE LA NACIÓN.* Obtenido de http://polux.unipiloto.edu.co:8080/00003023.pdf

Anexia, Tecnologías. (29 de 08 de 2018). *Certificado BRC, ¿qué es y para que sirve?* (A. C. S.L.U, Editor, & Copyright 2021 Anexia Consultoría S.L.U) Obtenido de Anexia, Consultoría: https://consultoria.anexia.es/blog/certificado-brc-que-es-y-para-que-sirve

CACIA. (8 de julio de 2019). *ALI-MENTOS CELEBRA SUS 100 AÑOS*. (CACIA, Editor, & C. C. Alimentaria, Productor) Obtenido de Revista Digital Alimentaria Cámara Costarricense de la Industria Alimentaria: http://alimentaria.cacia.org/digital/ali-mentos-celebra-sus-100-anos/

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT -Versión 3.0 Metodología de*

Análisis y Gestión de Riesgos de los Sistemas de Información (Vol. Libro 1). (M. d. Públicas, Ed.) Madrid, España.

Hewlett Packard. (2021). *Seguridad contra descargas eléctricas.* Obtenido de Equipos portátiles HP: https://support.hp.com/pe-es/document/c02847414

INTECO. (30 de 01 de 2014). Tecnología de la información – Técnicas de Seguridad – Directrices para la gestión de la seguridad de la información para las organizaciones de telecomunicaciones basada en la INTE/ISO/IEC 27002:2009. (Primera). (I. d. Rica, Ed.) Costa Rica: INTECO.

ISOTools EXELLENCE . (2021). Obtenido de La norma ISO 27001 Aspectos clave de su diseño e implantación: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

ISOTools, Excellence. (30 de 03 de 2021). *Metodologías de evaluación de Riesgos*. (I. ©2021, Editor) Obtenido de ISOTools.org: https://www.isotools.org/2021/03/30/metodologias-de-evaluacion-de-riesgos/

ISOTools, EXCELLENCE. (2021). *Software ISO Riesgos y Seguridad*. Obtenido de PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Madrigal Vargas, G. A. (junio de 2019). Elaboración del catálogo de servicios de TI para la Direccion de tecnología de información de la Universidad EARTH basado en el marco de referencia de ITIL 2011. *TESIS*. Cartago, Cartago.

Normasiso27001. (08 de 2017). *FASE 3 ELABORACIÓN DE LA POLÍTICA. OBJETIVOS DEL SGSI.* Obtenido de A5 Políticas de Seguridad de la

Información - ISO 27001: https://normaiso27001.es/fase-3-elaboracion-de-la-politica-objetivos-del-sgsi/

OECD. (2004). *Directrices de la OCDE para la seguridad de sistemas y redes de información.* Obtenido de OECD BETTER POLICIES FOR BETTER LIVES: https://www.oecd.org/sti/ieconomy/34912912.pdf

Por Investigadores. (23 de marzo de 2020). *Fuentes de información primarias, secundarias y terciarias*. (USCLibraries, Productor, & USCUniversity of Southern California) Obtenido de TÉCNICAS DE INVESTIGACIÓN: https://tecnicasdeinvestigacion.com/fuentes-de-informacion-primaria-y-secundaria-y-terciaria/

Rodriguez, R., & Ribón Zarco, J. (s.f.). *POLITICAS DE SEGURIDAD INFORMÁTICA.* Obtenido de Centro Inca: https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf

Ulate, I., & Vargas, E. (2016). *Metodología para elaborar una Teisis.* (E. U. EUNED, Ed.) San José, San José, Costa Rica: Patricia Gómez Figueroa.

UNIR - Universidad Internacional de La Rioja. (14 de 05 de 2020). *Claves de las políticas de seguridad informática*. Obtenido de UNIR LA UNIVERSIDAD EN INTERNET: https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

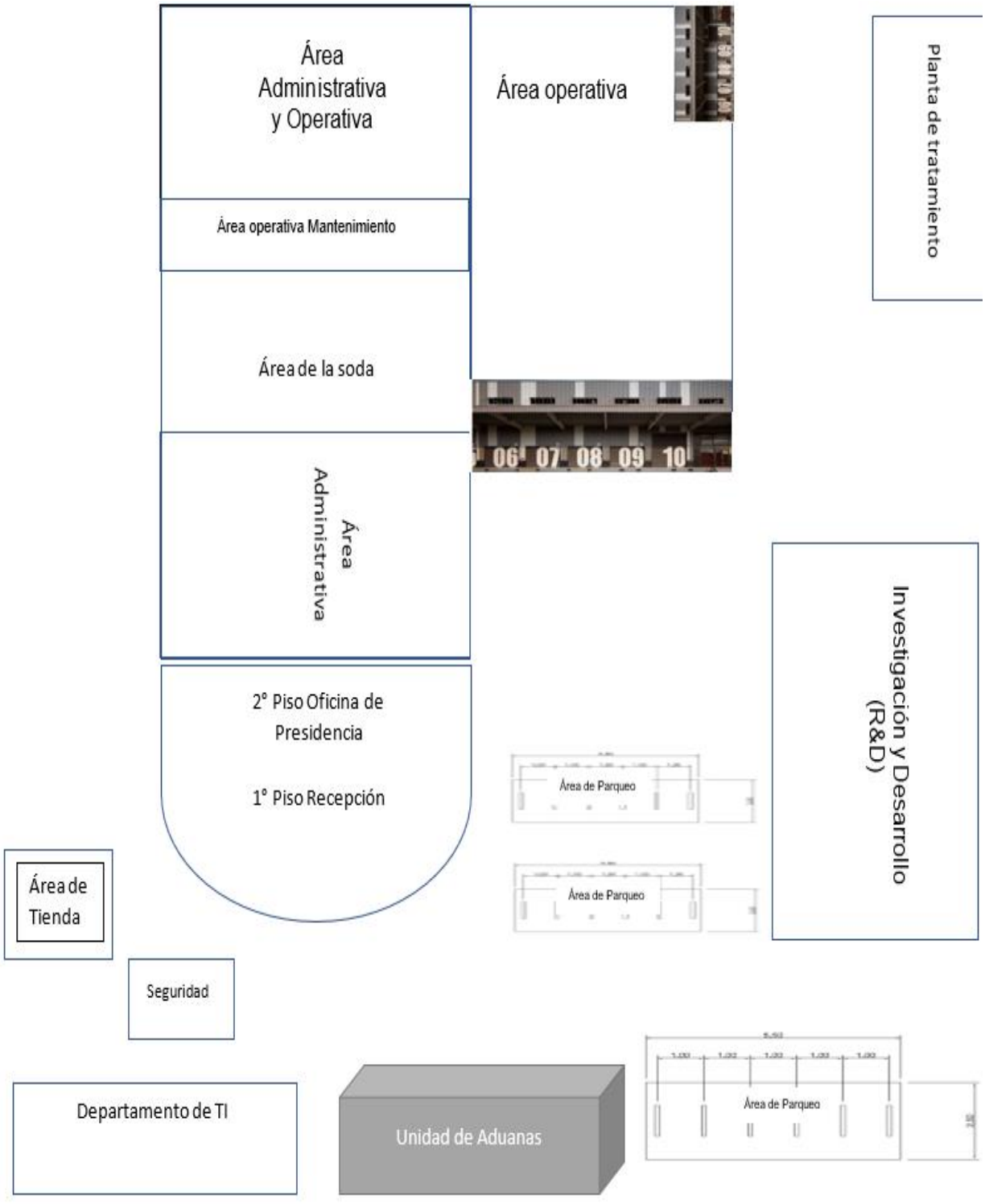
Villasís-Keever, M. Á., & Miranda-Novales, M. G. (11 de mayo de 2016). *El protocolo de investigación IV: las variables de estudio.* Obtenido de redalyc.org: https://www.redalyc.org/articulo.oa?id=486755025003

Apéndices

Apéndice A. Cronograma Inicial del Proyecto

Cronograma del Proyecto para la propuesta de una política de seguridad			
Nombre de la tarea	Duración	Inicio	Fin
-Planeación del Proyecto	5 meses	**04/03/2021**	**01/08/2021**
-Cierre Capitulo uno.		**10/03/2021**	**10/03/2021**
-Agendas y cronogramas		**12/03/2021**	**28/02/2021**
-Reunión de Inicio del proyecto con el gerente de área		14/03/2021	17/03/2021
-Definición de Objetivos		19/03/2021	24/03/2021
-Definición del Plan de trabajo		26/03/2021	27/03/2021
-Agendar reuniones		28/03/2021	28/03/2021
-Revisión de entrada a planta para el análisis de riesgo		30/03/2021	30/03/2021
-Trabajo de área		**02/04/2021**	**19/05/2021**
-Entrevistas con el equipo de TI		02/04/2021	07/04/2021
-Apliación de Análisis de Riesgo en los procesos informáticos		09/04/2021	14/04/2021
-Entrevistas con los empleados Administrativos		16/04/2021	21/04/2021
.-Investigación de casos de éxito en la aplicación de políticas de seguridad		23/04/2021	28/04/2021
-Entregable formularios de entrevistas		07/05/2021	12/05/2021
-Análisis de Resultados		**21/05/2021**	**16/06/2021**
-Revisión del análisis de Riesgo efectuado		21/05/2021	26/05/2021
-Análisis de los resultados de la revisón de procesos		28/05/2021	02/06/2021
-Análisis de las entrevistas de empleados		04/06/2021	09/06/2021
-Análisis de los hallazgos		11/06/2021	16/06/2021
-Preparación de documentos para entregar los resultados		**19/06/2021**	**27/06/2021**
-Consolidación de resultados obtenidos		19/06/2021	22/06/2021
-Confección de documentos y revisón de entregables		20/06/2021	22/06/2021
-Confección del documento electrónico para la Gerencia		21/06/2021	23/06/2021
-Envío de información vía electrónica		25/06/2021	27/06/2021
-Entrega de Resultados		**04/07/2021**	**04/07/2021**
-Entrega documental de los resultados		04/07/2021	04/07/2021
-Entrega de resultados del cumplimiento del cronograma		04/07/2021	04/07/2021
-Entrega de la política propuesta para la compañía		04/07/2021	04/07/2021
-Cierre del proyecto de Investigación		04/07/2021	04/07/2021

Apéndice B. Estructura General de la Compañía



Apéndice C. Formato para la toma del Inventario de Equipos

Formato para la toma del inventario de Equipos				
Desarrollo de una política de seguridad informática bajo las normas ISO/IEC 27001 e ISO/IEC 27002 para salvaguardar los activos informáticos de la empresa Ali-mentos S.A.				
Área	Departamento	Usuario	Equipo	Cantidad de Usuarios

Apéndice D. Formato Para la Toma de Cantidad Usuarios y Roles

Formato para la toma del inventario de Equipos				
Desarrollo de una política de seguridad informática bajo las normas ISO/IEC 27001 e ISO/IEC 27002 para salvaguardar los activos informáticos de la empresa Ali-mentos S.A.				
Área	Departamento	Usuario	Equipo	Rol de Usuarios

Apéndice E. Formato para las Entrevistas.

Entrevista de Análisis de la Situación en Ali-mentos S.A.									
Fecha	Nombre	Cargo	Control de acceso si/no?	Conoce si existen políticas o procedimientos para el uso de de activos si/no / Cuál?	Tienen cuentas separadas para registrarse.	¿Existe algún tipo de protección para los equipos que salen de la compañía?	Activos Críticos	Ha firmado o sabe de algún contrato de confidencialidad?	Sabe si Hay alguien encargado de la seguridad en TI?

ALI-MENTOS S.A.

Política de Seguridad Informática Bajo las Normas ISO/IEC27001 y 27002

Ali-mentos S.A.

Introducción

Como estrategia de la Gerencia de TI para salvaguardar los activos informáticos que se han convertido en una de las herramientas clave para el alcance de los objetivos de la compañía, se ha establecido estas políticas generales de seguridad informática para asegurar el conocimiento de las mejores prácticas en el uso de los activos informáticos y de la información.

Las políticas de seguridad informática tienen como objetivo principal salvaguardar dos de los valores más importantes de la operación en cualquier compañía, la información y los servicios prestados, esto a nivel de sistemas informáticos.

Lo anterior se logra concientizando a los usuarios de los activos informáticos con políticas de seguridad informáticas actualizadas y que ayuden a proteger la confidencialidad, integridad y disponibilidad de la información que tiene un valor muy alto para la empresa.

Por lo anterior se muestra este documento donde queda plasmadas algunas de las políticas de seguridad informática que se alinean con el día a día de las operaciones de Ali-mentos S.A. y que se convierten en un tema de conocimiento obligatorio para todos los empleados que utilicen alguno activo informático de la compañía.

1. Objetivo de la Política de Seguridad Informática.

Esta política de seguridad informática tiene como objetivo principal salvaguardar los activos informáticos de la compañía de las amenazas internas y externas de cualquier índole, además, minimizar los riesgos que se puedan presentar debido a la mala manipulación o desconocimiento en los procesos de uso adecuado en cuanto a los temas de seguridad informática y la seguridad física de los activos, y, con esto asegurar la continuidad del negocio.

Todo lo anterior con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información, el cumplimiento de leyes y regulaciones por parte del Corporativo, el entrenamiento de todos los empleados en temas de seguridad informática y el cumplimiento de las obligaciones contractuales de los Clientes y Proveedores.

2. Alcance de la Política de Seguridad de la Información.

El alcance de esta política de seguridad informática está dado para todos los activos de información de la empresa Ali-mentos S.A. y a todos los usuarios de estos activos, esto debido a que fue creada para proteger de estos, la información que contiene, todos los usuarios, consultores, contratistas y terceros deberán conocer y acatar las recomendaciones del manejo de los activos dentro y fuera de la compañía.

Más allá de conocer la política, todos los usuarios deberán ayudar a fortalecer, con el buen uso de los activos, la confidencialidad de la información y mitigar los riesgos que se puedan presentar a nivel físico y lógico por mala manipulación en el uso de estos activos.

3. Requisitos Reglamentarios o Legales.

Para la creación de esta política y su alineamiento con el negocio, esta está alineada por las políticas establecidas por Corporativo y por las leyes en el marco jurídico y normativo de la compañía, estas son las bases y las limitantes en el desarrollo de esta política.

4. Términos y Definiciones.

Para la referencia y entendimiento de todos los lectores de esta política de seguridad informática, se describen algunos términos que son usados en la redacción de este documento:

Usuario:

Todo colaborador que manipula algún activo informático para consulta, ejecución y/o envío de información electrónica en el proceso de sus labores en la compañía.

Activo informático:

Son todos aquellos elementos (hardware y software) que se utilizan para el proceso de comunicación electrónica, para el manejo de la información y el proceso de los datos electrónicos.

Hardware:

Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático y es usado para la instalación y ejecución de los diferentes softwares.

Software:

Conjunto de programas y rutinas que permiten a los activos informáticos realizar

determinadas tareas como las hojas de cálculos, de escritura, enviar y recibir correos y muchos otros más.

Sistema Informático:

Es todo aquel que está compuesto por hardware y software para la consecución de objetivos.

TI:

Término utilizado para hacer referencia a tecnología de la información, se utiliza mucho para mencionar al departamento de sistemas de la compañía quien es el encargado de esta tecnología.

Salvaguarda:

En informática son mecanismos de control para la protección de los activos informáticos, son controles que ayudan a mitigar los riesgos que puedan manifestarse en el entorno de la seguridad informática.

Riesgo:

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

Seguridad Informática:

Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema informático que pueda causar daños sobre la información.

Confidencialidad de la Información:

Garantía de que la información personal o de la compañía, será protegida para no ser divulgada sin consentimiento del dueño de esta, se establecen reglas de

acceso para evitar accesos no autorizados.

Integridad de la Información:

Mantenimiento de las características de completitud y corrección de los datos.

Disponibilidad de la Información:

Disposición de los servicios a ser usados cuando sea necesario.

Mitigación de Riesgos:

Uso de mecanismos para reducir los riesgos en los sistemas informáticos y en los activos, haciendo que, si algún riesgo se materializa, se pueda disminuir el impacto que pueda generar.

Negligencia:

Falta de cuidado, aplicación y diligencia de una persona en lo que hace, en especial en el cumplimiento de una obligación.

5. Compromiso de la Dirección

Al presentar esta política de seguridad de la información, se evidencia el compromiso de la Dirección con la implementación de mecanismos que ayuden a la seguridad de los activos informáticos y a la información que es crítica para la empresa Ali-mentos S.A.

La Dirección debe establecer para el aseguramiento de la confidencialidad, integridad y disponibilidad de la información, políticas de seguridad, responsabilidad y funciones para el seguimiento del cumplimiento de estas, y, los comunicados de su importancia y existencia a todos los usuarios de activos informáticos.

5.1 Comunicado de la política a los Usuarios

La Dirección de TI debe asignar los responsables de comunicar a nivel general la existencia de la política de seguridad informática y asegurar que este comunicado llegue a todos los usuarios, además que esta política esté en un lugar donde la puedan acceder siempre que lo necesiten.

5.2 Actualización de la Política

Esta política debe ser actualizada como mínimo cada 12 meses o cada vez que se genere algún cambio en la estrategia de la compañía en el tema de seguridad informática, la Dirección de TI es la encarga de asignar el responsable de llevar este control, y, al que se le asigne, será el encargado de cumplir con los tiempos establecidos.

6. Compromiso de los Usuarios

Todos los usuarios y contratistas deben leer y acatar las políticas de seguridad informática que estén aprobadas por la dirección de la empresa Ali-mentos S.A., sus aplicaciones en el uso de activos informáticos son de carácter obligatorio y de no cumplir con lo establecido por estas, podrían ser motivo para acciones disciplinarias e inclusive podrían ser separados del cargo si se demuestra su incumplimiento por negligencia.

7. Alcance del documento

Este documento alcanza los siguientes aspectos de seguridad informática que son tomados de ISO 27001:2013 como marco conceptual para el desarrollo de esta política de seguridad informática:

- **a.** Gestión de Activos
- **b.** Seguridad Ligada a los Recursos Humanos

c. Seguridad Física y del Ambiente

d. Control de Acceso

e. Gestión de Incidentes de la Seguridad de la Información

f. Gestión de la Continuidad del Negocio

8. Políticas de Seguridad de Ali-mentos S.A. S.A.

A continuación, se detallan las políticas que están alineadas con la estrategia de la compañía y que son de carácter obligatorio una vez que esté aprobada por el Gerente de TI, estas políticas se basan en las normas ISO 27001 e ISO 27002 que son un estándar y marco de referencia para las buenas prácticas y mejora continua de la seguridad informática.

8.1. Política para la Gestión de Activos.

Objetivo: Implementar y mantener una adecuada protección sobre los activos de la organización.

Alcance: Todos los activos informáticos y todos los usuarios de estos en la empresa Ali-mentos S.A. y sus administradores.

Descripción del tema: Todos los activos deberían tenerse en cuenta y tener un propietario para cada uno de ellos.

Se debe identificar propietarios para todos los activos y asignar la responsabilidad del mantenimiento de los controles apropiados. La implementación de controles

específicos sobre un activo podría ser delegada por su propietario, pero éste continúa manteniendo la responsabilidad por la protección del activo.

1. Todos los activos informáticos deben de tenerse en cuenta y tener un propietario a cada uno de ellos, esto con el fin de asentar responsabilidades cuando se presente alguna negligencia a la seguridad de la información.
2. Todos los activos deben ser claramente identificados y debe haber un inventario de todos ellos.
3. Es responsabilidad del usuario las buenas prácticas de uso de los equipos y de la información, además del uso aceptable de estos equipos.
4. La asignación de los responsables no es responsabilidad de TI, esta debe ser dada al departamento de TI por el Gerente del departamento que contrate algún colaborador y necesite un equipo, y, este debe dejarle claro a su colaborador, la responsabilidad del uso de este equipo y sus limitantes.
5. Cuando el usuario deje de laborar para la compañía, debe de devolver el equipo al Gerente del departamento o al jefe inmediato y deja de ser el responsable de este, además deja de tener acceso al activo.

8.2. Política para la Seguridad Ligada a los Recursos Humanos

Objetivo: Asegurar que los empleados, contratistas y usuarios de terceras partes (en adelante “Los usuarios de parte de terceros”) entiendan sus responsabilidades, sean aptos para los roles para los cuales están siendo considerados y para reducir el riesgo de hurto, fraude o mal uso de los servicios.

Alcance: Todos los empleados, contratistas y usuarios de terceras partes de la empresa Ali-mentos S.A.

Descripción del tema: Las responsabilidades de seguridad deberían ser tratadas en descripciones de puesto adecuadas y en términos y condiciones del empleo antes de contratar al personal.

Todos los candidatos para el empleo, contratistas y usuarios de terceras partes deberían ser seleccionados adecuadamente, especialmente para tareas sensibles.

Los usuarios de recursos de procesamiento de información ya sean empleados, contratistas y de terceras partes deberían firmar un acuerdo sobre sus roles y responsabilidades de seguridad.

1. Los roles y responsabilidades de seguridad de empleados, contratistas y usuarios de terceras partes deben estar definidos y documentados según las políticas internas de seguridad de la información.
2. Los usuarios de parte de terceros a la compañía Ali-mentos S.A., deben de implementar y actuar de acuerdo con las políticas internas de seguridad informáticas de la información.
3. Los usuarios de parte de terceros deben de proteger los activos de accesos no autorizados, divulgación, modificación, destrucción o interferencia.
4. Los usuarios de parte de terceros deben de ejecutar procesos o actividades particulares de seguridad.
5. Los usuarios de parte de terceros deben de asegurar que la responsabilidad por acciones tomadas sea asignada al individuo por acciones tomadas.

6. Los usuarios de parte de terceros deben de reportar eventos potenciales de seguridad u otros riesgos de seguridad para la organización.
7. Los roles y responsabilidades de seguridad deberían ser definidos y claramente comunicados a los candidatos al puesto durante el proceso de preempleo.

8.3 Política para la Seguridad Física y del Ambiente

Objetivo: Prevenir accesos físicos no autorizados, daños e interferencia contra las instalaciones y a la información de la organización.

Alcance: Todos los usuarios y departamentos que contengan al menos un activo informático considerado crítico o sensible para la empresa Ali-mentos S.A.

Descripción del tema: Los recursos de procesamiento de información críticos o sensible de la organización deberían estar ubicados en áreas seguras y resguardados por un perímetro de seguridad definido, con barreras de seguridad y controles de acceso apropiados. Deberían estar físicamente protegidos contra accesos no autorizados, daños e interferencias.

La protección provista debería ser proporcional a los riesgos identificados.

1. Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de entrada controladas por tarjeta o puestos de recepción) para proteger las áreas que contiene información y recursos de procesamiento de información sensible.

2. Donde sea aplicable, se debe construir barreras físicas para evitar el acceso físico no autorizado y la contaminación del entorno.
3. Los recursos de procesamiento de información gestionados por la organización deben estar separados físicamente de aquellos gestionados por terceras partes.
4. Las áreas seguras deben estar protegidas por controles de acceso apropiados, que aseguren que sólo se permite el acceso a personal autorizado.

8.4 Política para el Control de Acceso

Objetivo: Controlar el acceso a la información.

Alcance: Todos los activos informáticos y a todos los usuarios de estos activos en la empresa Ali-mentos S.A.

Descripción del tema: Los accesos a la información, a los recursos de procesamiento de la información y a los procesos del negocio deberían ser controlados con base en los requisitos del negocio y de la seguridad.

Las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.

1. Los accesos a la información, a los recursos de procesamiento de la información y a los procesos del negocio deben ser controlados con base a los requisitos del negocio y de la seguridad.
2. Los requisitos de seguridad de aplicaciones del negocio son individuales para cada usuario y este no debe ser compartido.

3. Debe haber perfiles estándar de acceso de usuarios para roles comunes en la organización.
4. Debe de haber separación de roles de control de acceso, por ejemplo, pedido de acceso, autorización de acceso y administración de acceso.
5. El usuario debe utilizar los requisitos establecidos para la autorización formal de pedidos de acceso y la de la revocación de derechos de acceso.
6. Los usuarios son los responsables de salvaguardar la información de autentificación y TI es el encargado de asignar los mecanismos para el control de autentificación a los sistemas.
7. Los usuarios deben de impedir el acceso no autorizado a los sistemas y aplicaciones restringiendo el acceso a la información, procedimientos de conexión (log-on) seguros, usando el sistema de gestión de contraseñas correctamente.
8. El usuario, contraseña, pin o códigos que asigna TI a cada usuario debe ser único y el usuario no debe de compartir estos datos con ninguna otra persona, inclusive si es el encargado del área.
9. Se debe de forzar el cambio de contraseñas iniciales.

8.5 Política para la Gestión de Incidentes de la Seguridad de la Información

Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de manera que permita tomar acciones correctivas oportunamente.

Alcance: Todos los empleados de la empresa Ali-mentos S.A., contratistas y usuarios de terceras partes.

Descripción del tema: Se debe de establecer procedimientos formales de reporte y escalamiento de eventos y todas las partes deberían tener conocimiento de ellos para reportar los diversos tipos de eventos y debilidades que puedan tener impacto en la seguridad de activos de la organización.

Establecer responsabilidades y procedimientos para el manejo de eventos y debilidades de la seguridad de la información con eficacia una vez que se hayan reportado, además de aplicar un proceso de mejora continua para la respuesta, seguimiento, evaluación y gestión general del incidente de seguridad de la información.

1. Se debe de establecer procedimientos para manejar diversos tipos de incidentes de seguridad de la información incluyendo fallos del sistema de información, pérdida de servicio, código malicioso, errores producidos por datos del negocio incompletos o inexactos, negación del servicio, violaciones de la confidencialidad e integridad y el uso inadecuado de los sistemas de información.
2. El usuario debe de reportar cualquier incidente a los encargados de soporte de TI o en su defecto a cualquier otro colaborador de esta área si no se encuentran los de soporte o están en otro evento.
3. Se debe de planificar e implementar acciones correctivas para prevenir que suceda de nuevo ese evento.

4. Se debe se realizar, por parte de TI, un análisis interno del problema junto con el usuario para revisar la raíz de la situación y corregirlo, esto para que no vuelva a suceder.
5. Solo el personal claramente identificado y autorizado se le permite el acceso a los sistemas y datos en producción.
6. Se debe de documentar todas las acciones de emergencia ejecutadas detalladamente.

8.6 Política para la Gestión de Continuidad del Negocio

Objetivo: Contrarrestar interrupciones a las actividades del negocio y proteger los procesos críticos del negocio contra los efectos de fallas importantes en los sistemas de información o desastres, y asegurarse de su restauración oportuna.

Alcance: Todos los empleados de la empresa Ali-mentos S.A.,

contratistas y usuarios de terceras partes.

Descripción del tema: Se debería implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto en la organización y recuperarse por la pérdida de activos de información (la cual puede ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

Este proceso debería identificar los procesos críticos del negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio

con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal de apoyo, materiales, transporte y recursos.

La gestión de la continuidad del negocio debería incluir controles para identificar y reducir riesgos, además del proceso general de valoración de riesgos, limitar las consecuencias de los incidentes dañinos y garantizar la rápida disponibilidad de la información requerida para los procesos del negocio.

1. Se debe de desarrollar y mantener un proceso de gestión de la continuidad del negocio en toda la organización, con los requisitos de seguridad de la información necesarios para la continuidad del negocio.
2. TI debe de tener identificados todos los activos involucrados en los procesos críticos del negocio.
3. Debe de haber una identificación y consideración de la implementación de controles preventivos y mitigantes adicionales.
4. Se debe de realizar pruebas y actualizaciones regulares de los planes y procesos establecidos.

_____

Firma de aprobación

Gerencia de TI