UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

"PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA FINANCIERA DE EMPRESAS COMERCIALIZADORAS DE AUTOMÓVILES DEL MUNICIPIO DE ANTIGUO CUSCATLÁN"

TRABAJO DE INVESTIGACIÓN PRESENTADO POR:

Nicolás Santiago Colon Campos

Norma Del Carmen Coreas Villanueva

Claudia Vanessa Sánchez Oliva

PARA OPTAR EL GRADO DE:

LICENCIATURA EN CONTADURÍA PÚBLICA

MARZO, 2021

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	: Msc. Roger Armando Arias Alvarado
Secretario General	: Ing. Francisco Antonio Alarcón Sandoval
Decano de la Facultad de Ciencias Económicas	: Msc. Nixon Rogelio Hernández Vásquez
Secretaria de la Facultad de Ciencias Económicas	: Licda. Vilma Marisol Mejía Trujillo
Director de la Escuela de Contaduría Pública	: Lic. Gilberto Díaz Alfaro
Coordinador General de Procesos de Grado de la Facultad de Ciencias Económicas	: Lic. Mauricio Ernesto Magaña Menéndez
Coordinador de Procesos de Grado de la Escuela de Contaduría Pública	: Lic. Daniel Nehemías Reyes López
Docente Asesor	: Lic. Mauricio Ernesto Magaña Menéndez
Tribunal Evaluador	: Lic. Daniel Nehemías Reyes López
	: Lic. Mauricio Ernesto Magaña Menéndez
	: Lic. Abraham de Jesús Ortega Chacón

MARZO, 2021

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

AGRADECIMIENTOS

Agradezco a Dios todo poderoso por darme la oportunidad de poder finalizar mis estudios, a mi madre Blanca Angélica Evelyn Colon por su cariño y apoyo a lo largo de mi vida; de la misma manera a mis compañeras de tesis Norma del Carmen Coreas Villanueva quien se ha visto involucrada en mi crecimiento profesional no solo en el camino de la carrera, sino a lo largo de finalización de este proceso y Claudia Vanessa Sánchez Oliva con quien hemos tenido buenas relaciones de estudio y me ha apoyado en todo momento.

Nicolás Santiago Colón Campos

Que privilegio poder darle las gracias a Dios, por su infinito amor y bondad permitiéndome culminar esta etapa; infinitas gracias porque me ha concedido tener una familia que ha creído en mí desde el primer día y por ser el motor que impulsa mi vida, gracias por darme tanto de todo y todo de ustedes. También agradezco por todas las personas que formaron parte de mi crecimiento personal y profesional, las cuales se convirtieron en instrumentos de bendición.

Norma Del Carmen Coreas Villanueva

Agradezco a Dios todo poderoso por guiarme y brindarme la sabiduría necesaria para culminar y alcanzar este logro con éxito, a mis padres y hermana por darme su cariño y apoyo incondicional en todo momento, a mis familiares y amigos que de alguna manera me ayudaron y me dieron su apoyo, a mis compañeros por su esfuerzo y dedicación en este proceso, y a todas las personas que contribuyeron para mi crecimiento personal y profesional.

Claudia Vanessa Sánchez Oliva

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

Las empresas comercializadoras de vehículos son una fuente fundamental para el desarrollo del comercio nacional e internacional, y El Salvador pese a ser pequeño en territorio mantiene un fuerte ritmo en el sector automotor y se cuenta con importantes empresas representantes de marcas multinacionales las cuales se han ido adaptando al proceso de modernización como a los avances tecnológicos.

Uno de los pasos importantes que se deben tomar en cuenta para la seguridad de la información es estar conscientes del entorno donde se desarrollan las actividades económicas, por ello que se deben identificar los aspectos internos y externos y la medida en que podrían afectar al propósito de la entidad; y es que en la actualidad, el entorno está prácticamente controlado por las nuevas tecnologías, que cada día están en constante evolución, brindando mayores herramientas para mejorar la productividad y poder explorar más allá de las fronteras nacionales, pero traen consigo beneficios como amenazas, y generalmente no se cuenta con elementos o planes de contingencia para la protección de los activos tecnológicos.

Es fundamental saber qué recursos se necesitan para obtener seguridad en los sistemas de información y la mayor inversión de las entidades no debe ser en recursos tecnológicos, generalmente es menos de la mitad de la inversión necesaria; la mayor proporción se debe destinar al desarrollo de políticas y procedimientos que contribuyan a generar una cultura de buenas prácticas, como también debe destinarse a la capacitación y concienciación de los recursos humanos, puesto que el comportamiento de todos los miembros de la empresa determina colectivamente la cultura de la empresa.

Por lo que la presente investigación se centra en brindar políticas y controles, que contribuyan al fortalecimiento de los procesos clave involucrados en la generación de la información financiera, tomando como el principal actor a los recursos humanos, específicamente a los profesionales en contaduría pública que tienen la inmensa responsabilidad de proteger la información de vital importancia para las entidades, que son denominados como activos de una institución, los cuales deben ser protegidos para evitar su pérdida, modificación o el uso inadecuado de su contenido.

Se utilizó el método cualitativo, debido a que se necesita información detallada y como también observar el comportamiento de los recursos humanos, por lo tanto, los resultados necesarios para esta investigación fueron descriptivos. El instrumento de medición implementado fueron las entrevistas con los principales actores de la generación de la información financiera, en el análisis de las respuestas obtenidas se detallan las características del problema que se presenta en este sector empresarial, con lo que se pudo concluir que los controles actuales no son suficientes ya que no se cuenta con marco de actuación basado en los estándares internacionales de mejores prácticas.

Se recomienda trabajar en la implementación del plan de seguridad de la información ya que comprende un conjunto de políticas y controles en las que compromete a todas las áreas y actividades de la actividad empresarial, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

INTRODUCCIÓN

La seguridad de la información engloba un conjunto de técnicas y medidas para controlar todos los datos que se manejen dentro de una empresa, tiene como objetivo principal proteger la información de las estas, además de asegurar aspectos fundamentales como: la confidencialidad, la disponibilidad y la integridad. Se genera una opinión que los controles asociados a la seguridad de la información solo están orientados a la informática, es importante aclarar que se toman en cuenta aspectos relacionados a la información, como son los medios por los que se transfiere datos, los sistemas que la manejan y soportan.

La seguridad de la información no solo debe enfocarse a lo tecnológico, se consideran también aspectos como seguridad de las organizaciones y recursos humanos, gestión de activos, control de accesos y mejora continua. Los sistemas y las redes de las empresas se enfrentan a amenazas de diferentes tipos, incluyendo fraudes por computadora, espionaje, sabotajes, y ciberataques que están orientados a la información almacenada en sus bases de datos.

Por ello, es importante la ciberseguridad en el entorno empresarial, en este caso enfocada en las empresas comercializadoras de automóviles, ya que estas se reflejan en el aporte y la contribución que hacen a la sociedad en el desarrollo económico del país y es un tema que a diario acapara más atención debido al aumento mundial de ataques y riesgos asociados al entorno digital, por lo que, se desarrolla la presente propuesta de un plan de seguridad de la información, acorde a sus necesidades y condiciones de operación.

Inicialmente, se presenta el Planteamiento del Problema en el Capítulo I, en el cual se expone la situación problemática objeto de estudio, incluye la delimitación, justificación, los objetivos y las hipótesis de la investigación. Además de presentar el Marco Teórico, donde se

aborda la situación actual de la seguridad de información en las empresas objeto de estudio, las principales definiciones y finalmente se desarrolla el marco técnico y legal aplicable a la seguridad de la información.

El capítulo II expone la metodología que fue empleada para la conseguir los resultados finales de la investigación, así también, se da a conocer las unidades de análisis, el universo y muestra, la técnica e instrumento para la recolección de datos y se realiza el análisis de los resultados obtenidos en la investigación.

Posteriormente en Capítulo III, se desarrolla la propuesta que consiste en la elaboración de un Plan de Seguridad de la Información que contiene políticas y controles, para contribuir a la obtención de un nivel razonable de protección en su información. Finalmente se presentan las conclusiones y recomendaciones del estudio de datos obtenidos en la investigación.

CAPITULO I – PLANTEAMIENTO DEL PROBLEMA Y MARCO TEÓRICO

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Estado actual de la problemática de las empresas comercializadoras de vehículos.

Las empresas comercializadoras de vehículos, cada día se vuelven más vulnerables debido a diversos motivos que pueden dañar su información integral y, sobre todo sus actividades o procesos; probablemente hace algunos años, estos tipos de problemas no preocupaban demasiado, pero la situación actualmente no se puede simplemente ignorar; ya que la información de los clientes, la información financiera de una empresa y las contraseñas de los usuarios, son de los datos más valiosos para cometer crímenes cibernéticos en la actualidad.

Durante el 2019 Toyota reconoció que una brecha de seguridad expuso los datos de 3,1 millones de clientes, lograron violar los sistemas de TI de la empresa y obtuvieron detalles exclusivos sobre muchas de las subsidiarias de ventas, sostiene que no hubo robo de información financiera, pero se pudo haber accedido a datos privados incluidos nombres, ID de correo electrónico y direcciones.

Esta es la declaración del Grupo Toyota publicada en su página web global (Blog de Itech Sas , 2019):

«Pedimos disculpas a todos los que han estado usando los vehículos Toyota y Lexus por la gran preocupación. Tomamos esta situación seriamente, e implementaremos de manera exhaustiva las medidas de seguridad de la información en los concesionarios y en todo el Grupo Toyota”. (Blog de Itech Sas , 2019)

En El Salvador, desde hace muchos años se han registrado frecuentes tipos de violaciones a la seguridad de la información de las empresas; sin embargo, no se le había dado la importancia que representa, pero es en 2016 cuando se promueven pólizas de seguro contra ataques cibernéticos, las cuales marcaron un paso importante en la materia; dichas pólizas incorporan ciertas condiciones, en vista de que los informes financieros son susceptible de un atentado y en el peor de los casos que se haga mal uso de los mismos.

Los ataques y las violaciones a la seguridad de la información actualmente suceden a cada minuto y comprende una gran dificultad el intentar localizarlas debido a las generalidades que poseen; algunas de ellas se realizan con éxito y otras no. En El Salvador, existe la Ley Especial Contra los Delitos Informáticos y Conexos, que busca proteger los bienes jurídicos de las conductas delictivas cometidas por medio de las tecnologías de la información y la comunicación; como también la Ley Especial contra Actos de Terrorismo que tiene como objeto prevenir, investigar, sancionar y erradicar los delitos que se describen en la misma.

En las compañías comercializadoras de automóviles la recopilación de información financiera se genera por diferentes departamentos; los cuales alimentan al sistema informático en tiempo real, como también son los que hacen uso día con día de los datos resultantes; y es durante estos procesos donde pueden surgir las amenazas; por ejemplo, filtraciones, robo y duplicidad, acceder a campos restringidos, eliminar archivos, destruir documentación, etc.; es por ello que se debe contar con controles eficientes para poder minimizar los riesgos, prevenir y detectar errores, evitar perdida accidental o intencional de activos.

Por su parte, la formación del contador público, generalmente se ha basado en ramas como auditoría, contabilidad, impuestos, etc. Pero a medida la tecnología va innovando, los profesionales de contaduría también deben hacerlo, para estar a la vanguardia de la nueva era; y al referirse a la

seguridad de la información, las grandes compañías de ciberseguridad, consideran que lo más importante es educar a los colaboradores en la materia, hacerles entender la importancia de lo que se comparte y que aquello que es propio de la empresa no debe salir de esta.

Es por ello que los profesionales de la contaduría pública juegan un papel importante, por la vinculación con todas las áreas de la compañía y contar con un plan de seguridad de información es tener una ventaja como herramienta integral de apoyo para la integridad, confidencialidad y disponibilidad de los procesos claves, y que posteriormente es objeto en la toma de decisiones. El departamento de contabilidad es el encargado de generar informes para evaluar la situación financiera y el rumbo de las empresas, sin embargo, al verse afectados con un ataque informático afectaría su ritmo laboral, la razonabilidad de las cifras registradas, subvaluación o sobrevaluación de los inventarios, inflación en la determinación de costos, etc.

1.1.2 Delimitación de la investigación

La investigación se basa en los estándares de mejores prácticas de seguridad de la información y estará sustentada en la normativa legal y técnica aplicable, utilizando como fuente las siguientes:

- La Norma ISO/IEC 27001.
- La Norma ISO/IEC 27002.
- Guías de mejores prácticas Objetivos de control para la información y tecnologías relacionadas (COBIT 2019).
- Ley Especial Contra Delitos Informáticos y Conexos.
- Ley Especial contra Actos de Terrorismo.
- La Biblioteca de Infraestructura de Tecnologías de Información (ITIL 3)

La delimitación temporal se establece en el período comprendido entre los años 2016 a 2019, pues a partir de ese año se generaron aumentos de violaciones a la seguridad de la información, que significaron millones de dólares para muchas empresas afectadas.

Delimitación espacial o geográfica se desarrolla en el municipio de Antiguo Cuscatlán, específicamente en las empresas dedicadas a la comercialización de automóviles, debido a que en esa área geográfica se ha identificado el problema.

1.1.3 Justificación de la investigación.

El desarrollo de la investigación es novedoso, por los efectos que causa la pérdida de activos en las empresas de venta de vehículos, basado en el contenido de los reportes financieros que se manejan, como también los nuevos riesgos de vulnerabilidad de los procesos debido a la evolución que va teniendo la tecnología, por esa razón las entidades deben adoptar un plan proactivo para identificar y proteger a sus activos más importantes. Así mismo, es novedoso para el profesional de la contaduría pública para que tome participación en el área de tecnologías de información, y así cuenta con una herramienta que le ayude a mejorar los procesos clave del área financiera de forma eficiente, segura y exacta.

Se cuenta con material bibliográfico entre ellos normativa legal y técnica, documentos en internet, lo que contribuye al desarrollo de la investigación; se dispone de acceso al personal clave de empresas comercializadoras de automóviles.

Al establecer un plan de seguridad de la información, los principales beneficiarios son los profesionales en contaduría pública, tanto contadores como auditores, puesto que el objetivo del plan es fortalecer los procesos del área financiera, como también serán beneficiadas, las empresas comercializadoras de automóviles del municipio de Antiguo Cuscatlán, debido a que van a contar

con un plan que ayude a la reducción de riesgos y mejorar la integridad de la información financiera, y esto a su vez contribuye a la disminución de los costos que puedan significar la pérdida de información.

1.1.4 Objetivos de la investigación.

1.1.4.1 Objetivo general

Presentar un plan de seguridad de la información enfocado al área financiera de las empresas comercializadoras de automóviles del municipio de Antiguo Cuscatlán, que contribuya al fortalecimiento de los procesos claves y calidad de los reportes generados para la toma de decisiones.

1.1.4.2 Objetivos específicos

- Analizar los conocimientos y deficiencias en materia de seguridad de la información de los recursos humanos del área financiera, de las empresas comercializadoras de automóviles del municipio de Antiguo Cuscatlán.
- Diseñar controles para el resguardo de la información de los procesos claves, que ayuden a la disminución de vulnerabilidad del área financiera.
- Desarrollar un marco de actuación basado en los estándares de mejores prácticas de seguridad de la información, adaptado para el área financiera de las empresas comercializadoras de automóviles.

1.1.5 Hipótesis de la investigación

1.1.5.1 Hipótesis de trabajo.

La presentación de un plan de seguridad de la información enfocado al área financiera de las empresas comercializadoras de automóviles del municipio de Antiguo Cuscatlán, contribuye al fortalecimiento de los procesos claves y calidad de los reportes generados para la toma de decisiones.

1.1.5.2 Determinación de las variables.

Variable independiente: Plan de Seguridad de la Información.

Variable dependiente: Procesos claves y calidad de los reportes generados para la toma de decisiones.

1.1.5.3 Operacionalización de variables

Objetivo General	Hipótesis del Trabajo	Variables	Medición de Variables
Presentar un plan de seguridad de la información enfocado al área financiera de las empresas comercializadoras de automóviles del municipio de Antiguo Cuscatlán, que contribuya al fortalecimiento de los procesos claves y calidad de los reportes generados para la toma de decisiones.	La presentación de un plan de seguridad de la información enfocado al área financiera de las empresas comercializadoras de automóviles del municipio de Antiguo Cuscatlán, contribuye al fortalecimiento de los procesos claves y calidad de los reportes generados para la toma de decisiones.	**Independiente:** Plan de Seguridad de la Información.	• Controles • Procedimientos • Políticas
		Dependiente: Procesos claves y calidad de los reportes generados para la toma de decisiones.	• Minimizar las consecuencias de los riesgos de la seguridad de la información. • Aumentar la solidez en la realización de los procesos del área financiera. • Incrementar la fiabilidad en los reportes financieros que sirven de base para la toma de decisiones.

1.2 MARCO TEÓRICO

1.2.1 Generalidades sobre las empresas dedicadas a la comercialización de automóviles en el municipio de Antiguo Cuscatlán.

El sector automotriz se ha caracterizado como un apoyo a la sociedad salvadoreña en materia de conexión y movilidad, ya que el transporte constituye una necesidad para desarrollar las actividades del diario vivir, es por ello que los distribuidores de automóviles en El Salvador se deben adaptar a las necesidades del usuario, ofrecer un mejor servicio y productos; estos son factores determinantes que han contribuido con el desarrollo de este sector empresarial.

En El Salvador existen distribuidores que tienen la representación de diferentes marcas de vehículos, según cifras de Asociación Salvadoreña de Distribuidores de Vehículos (ASALVE), en el año 2019 se intensificaron las importaciones en el mercado salvadoreño, con un crecimiento entre el 5% y 6% en ventas, en comparación al año anterior. La industria automotriz genera entre más de 3,000 empleos directos e indirectos, siendo un importante sector en aportar a la recaudación fiscal por los derechos arancelarios de importación e impuestos como el IVA.

Entre las principales compañías ubicadas en el Municipio de Antiguo Cuscatlán, están: INCHCAPE El Salvador, S.A. de C.V., Grupo Q El Salvador, S.A. de C.V., Grupo Cofiño, Continental Motores, S.A de C.V; estas diversifican el mercado salvadoreño y su funcionamiento depende de la importación de vehículos de sus marcas representantes.

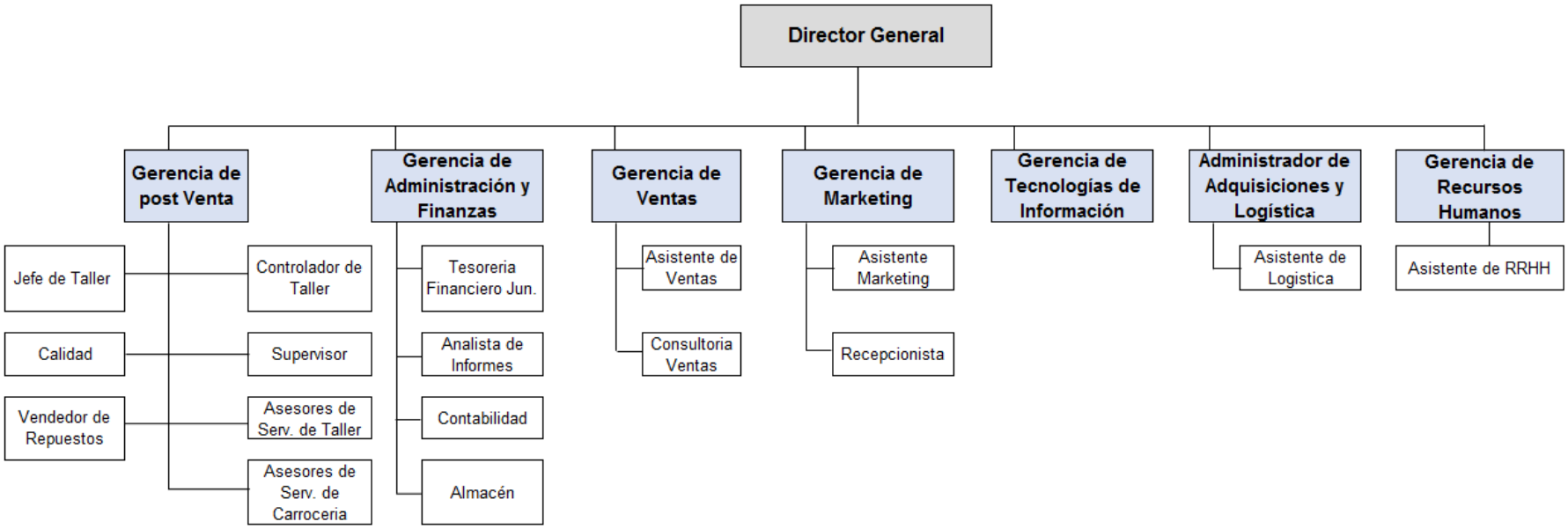


Imagen: *Organigrama NCN, S.A. de C.V.*

El ciclo operativo de estas empresas comienza con la adquisición de los diferentes modelos de vehículos que el fabricante pone a disposición de acuerdo con la demanda del mercado salvadoreño; estos se almacenan en los recintos fiscales, donde se tramita la documentación de importación y posteriormente el pago de impuestos, luego son trasladados a las instalaciones de la empresa comercializadora; lo antes mencionado es realizado por el departamento de logística.

El departamento de logística incorpora al inventario los vehículos nuevos mediante el módulo del sistema de pedido de vehículo, adjuntando el valor de los costos adicionales para la preparación de este y así tener para una medición fiable para las siguientes áreas.

El departamento comercial realiza un costeo interno antes de la exhibición y disponibilidad de los modelos para tener presente un margen de ganancia dicho costeo es trasladado al área de finanzas para su visto bueno, el área comercial también el encargado de facturar y recopilar la información de los clientes y mantenerla bajo estrictas medidas de seguridad.

Proceso de venta: El área comercial realiza la venta al precio establecido en el costeo interno luego el cliente firma la documentación correspondiente a la formalización de la venta; se apertura el expediente del cliente que contiene la información confidencial del mismo, dicho expediente pasa un proceso de validación con el Oficial de Cumplimiento del área financiera, posteriormente se procede a la facturación en el sistema informático, seguido del pago del Impuesto a la Primera Matrícula (IPM) y finalmente se realiza trámite de placas para la entrega del vehículo al cliente.

Los contratos de vehículos al crédito y ventas al contado, se informan al departamento de finanzas para realizar la validación de la información y de los clientes y así tener el fiel cumplimiento de aspectos financieros y tributarios que relacionen estas operaciones.

La información se recopila a través de los procesos que realiza cada departamento y esta se traslada al área financiera para su validación así como para la toma de decisiones y el mejor funcionamiento de la compañía, es ahí donde la seguridad de la información intervine mediante las buenas prácticas de resguardo por parte de los colaboradores cuidando de cada dato a revelar de las operaciones de las entidades.

1.2.2 Generalidades de la seguridad de la información.

Durante los últimos años, los incidentes en seguridad de la información son cada vez más frecuentes. Antiguamente las organizaciones sólo debían preocuparse de que sus oficinas se encuentren protegidas ante robos físicos o incidentes, como inundaciones e incendios, pero actualmente deben implementar procedimientos para proteger y resguardar los datos integrales de una organización, que se encuentran alojados en sistemas informáticos.

Una de las razones fundamentales por los que el avance de la tecnología, se considera que propulsó un cambio en la tendencia de seguridad de la mayoría de empresas, se debe a los virus que surgieron de la mano con la tecnología y que dieron paso al crecimiento para la seguridad de la información a nivel mundial, a causa de las muchas generalidades con las que estos pueden impactar. (Instituto Nacional de Ciberseguridad, 2015)

Se ha llegado a la situación en la que los clientes se preocupan por la mala gestión que se hace de sus datos en las organizaciones por los programas informáticos que utilizan y dan origen a fraudes por robo de identidades.

El fabricante automotriz Honda en 2017 se vio infectado por el virus ransomware en las computadoras en una de sus plantas en Japón, alterando la producción de vehículos; afectando alrededor de 1,000 unidades, las cuales tuvieron fallas en la fábrica cuando WannaCry atacó,

causando que cerraran. El ransomware atacó a las organizaciones que utilizaban tecnología vieja y software obsoleto, y ese parece que fue el caso de la planta de Honda.

En junio de 2018 se expuso en un servidor de acceso al público documentos confidenciales de empresas como Ford, Tesla, Toyota, General Motors, FCA y Volkswagen, la violación de datos fue descubierta por UpGuard Cyber Risk, la brecha expuso 157 gigabytes de datos, un tesoro de 10 años de esquemas de líneas de ensamblaje, planos y diseños de fábrica, configuraciones y documentación robóticas, formularios de solicitud de credencial de identificación, formularios de solicitud de acceso a VPN, detalles personales de algunos empleados, incluidos escaneos de licencias de conducir y pasaportes, y datos comerciales, incluidas facturas, contratos y detalles de cuentas bancarias.

La seguridad de la información envuelve tres características fundamentales: confidencialidad, integridad y disponibilidad, que se denominan "Triangulo de Seguridad de la Información", tal como lo muestra la figura 1. Todos los controles, salvaguardas, amenazas, vulnerabilidades y procedimientos relacionados con la materia se basan en estos tres principios, su definición es la siguiente: (Slideshare, 2016)

Confidencialidad: Mediante este servicio o función de seguridad se busca garantizar que la información contenida o transmitida en algún medio, solo podrá ser accedida por un usuario legítimo, en caso de que esta caiga en manos de otras personas, no podrán tener acceso al contenido del mensaje. "Previene el descubrimiento no autorizado de la misma". (Villela, 2020)

Integridad: Este servicio se encarga de asegurar que no se realicen modificaciones a los datos desde su creación o durante su transmisión, por personas o procesos no autorizados. "Previene una modificación no autorizada". (Villela, 2020)

Disponibilidad: Este servicio es un poco complejo ya que es muy difícil poder garantizarla en su totalidad. La disponibilidad asegura que el acceso a los archivos informáticos se produzca correctamente y en tiempo, es decir, que los sistemas funcionen cuando se les necesite o requiera. “Previene la negación de acceso autorizado”. (Villela, 2020)

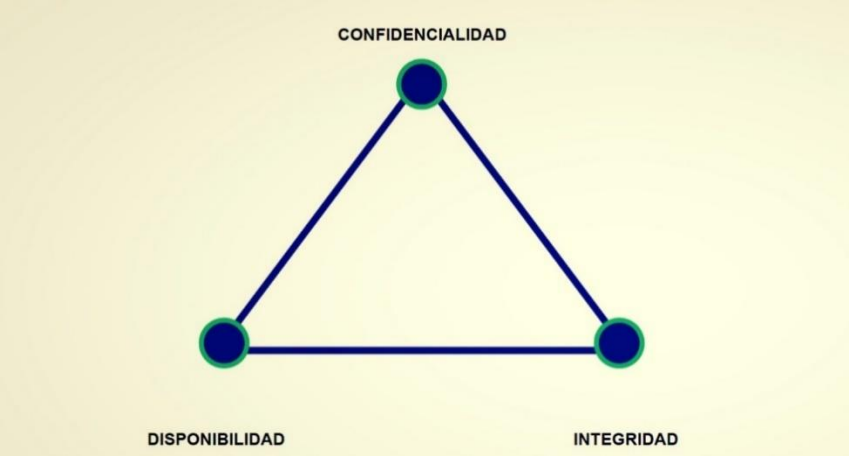


Figura 1: *Triangulo de la Seguridad de la Información.*

Fuente: Blog spot. (2018). Informática 2018. Obtenido de http://adrian-isaac.blogspot.com/

Además, se considera muy importante la integración de otros dos servicios que entrarían en un nuevo esquema denominado "Pirámide de la Seguridad de la Información", tal como lo muestra la figura 2 éstos son: Control de Acceso y Autenticación. Por lo que se considera una parte esencial dentro de las entidades, el poder especializar y preparar profesionalmente a los recursos humanos, con lo que podrán hacer frente a ciberataques y a la era digital.

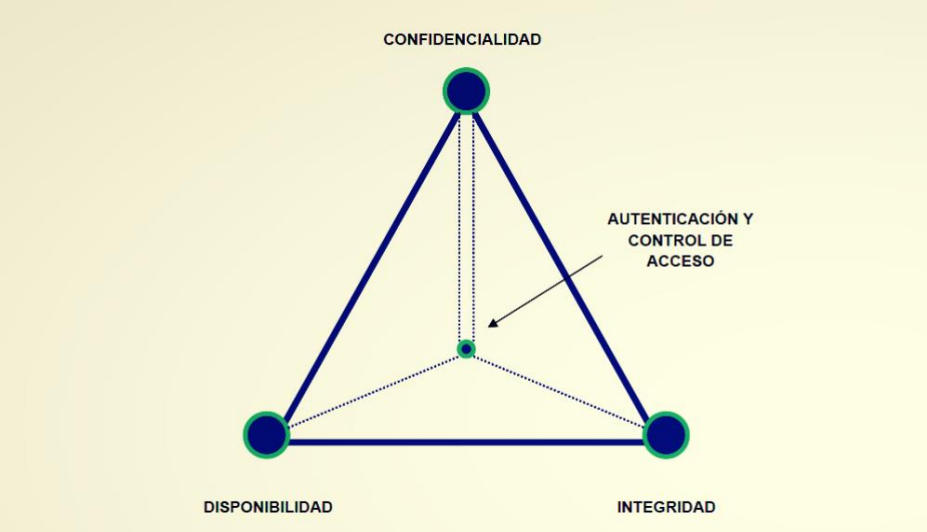


Figura 2: *Pirámide de la Seguridad de la Información.*

Fuente: Villela, E. A. (s.f.). IS IT SKULL. Pirámide de la Seguridad de la Información. Obtenido de https://it-skull.com/content/2-seguridad-de-la-informacion-que-es/9-piramide-de-la-seguridad-de-la-informacion.html

1.2.3 Principales definiciones.

- **Seguridad de la información:** Se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan. (Gestión, 2015)
- **Ciberataque:** Son actos en los cuales se cometen agravios, daños o perjuicios en contra de las personas o grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio de computadoras y a través de la Internet. No necesariamente pueden ser cometidos totalmente por estos medios, sino también a partir de los mismos y puede estar dirigido a los equipos y sistemas de computación que se encuentran operando en la red a nivel mundial, o puede ser orientado hacia la información y los datos que son almacenados en bases de datos. (Net, 2017)

- **Información:** Es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones. (Idalberto, 2006)
- **Ataque cibernético:** Es una acción delictiva y malintencionada que se realiza para acceder a información privada, bien para apropiarse de ella o bien para inutilizarla. (GLOBALFINANZ, 2020)
- **Delito informático:** Se considerará la comisión de este delito, cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información. (Legislativa, Ley Especial Contra Delitos Informáticos y Conexos., 2016)
- **Sistema informático**: Es un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información. (Legislativa, Ley Especial Contra Delitos Informáticos y Conexos., 2016)
- **Ciberseguridad:** Se define como una capa de protección para los archivos de información, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo. (S.L., 2018)
- **Riesgos informáticos:** Son exposiciones tales como atentados y amenazas a los sistemas de información. (Digital, s.f.)

- **Software:** Término informático que hace referencia a un programa o conjunto de programas de cómputo, así como datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático. (Significados, 2020)
- **Autenticación:** Garantiza que la identidad de alguien sea legítima, es decir, que ese alguien es quien dice ser. “Por lo general la autenticación implica una combinación de algo que es, algo que se sabe y algo que se tiene”. (Villela, 2020)
- **Control de acceso:** Después de la identificación y autenticación de un usuario, controlar la manera de acceder a los recursos es indispensable, para ello se definen listas de control de acceso con relación a cada uno de ellos, grupos de personas que tengan acceso al sistema y permisos a los recursos de un sistema o servicio. “Es la capacidad de controlar y conocer quién y cuándo acceden a una zona, servicio o determinada información”. (Villela, 2020)

1.2.4 Marco Técnico.

1.2.4.1 Norma Técnica ISO / IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

La Organización Internacional de Normalización (ISO por sus siglas en inglés) dedicada a la creación de estándares internacionales compuesta por diversas organizaciones de normalización, promueve el uso de estándares como soluciones y procedimientos aplicables a las organizaciones, ha formado varios comités conjuntos con la Comisión Electrotécnica Internacional (IEC) para desarrollar estándares relacionado con áreas de tecnologías que ayuden a la disminución o control de riesgos informáticos. (Organización Internacional para la Estandarización, 2013)

La ISO / IEC 27001 proporciona requisitos para la creación, implementación, supervisión, revisión y mejora de un sistema de gestión de la seguridad de la información, pueden ser aplicables

a cualquier tipo de organizaciones. El principal objetivo de esta ISO es salvaguardar la confidencialidad, la integridad y la disponibilidad de información que posea valor para la empresa. (GCBGlobal, s.f.)

La gestión de la seguridad de la información se realiza por medio de análisis de los riesgos y aplicación de controles para mitigar el riesgo tal cual se muestra en la tabla 1.

Tabla 1: Controles propuestos por la Norma ISO / IEC 27001

OBJETIVO DE CONTROL	ÁREA	CONTROLES
Clasificación de la información	Clasificación de la información	La información se clasificará en términos de requerimientos legales, el valor, la criticidad y sensibilidad a la divulgación o modificación no autorizada.
	Etiquetado de información	Un conjunto apropiado de procedimientos para el etiquetado de información deberá ser desarrollado e implementado de acuerdo con el esquema de clasificación de la información adoptado por la organización.
Manejo de medios	Medios físicos transferencia	Los medios que contienen información estarán protegidos contra usuarios que aún no tienen autorizado acceso, uso indebido o la corrupción durante el transporte.
Control de acceso	Política de control de acceso	Se establecerá una política de acceso, documentado y revisado en base a los requisitos de seguridad.
Gestión de acceso del usuario	El registro de usuarios y cancelación de la matricula	Un proceso de registro de usuarios y de registro formal se llevará a cabo para permitir la asignación de derechos de acceso.
	Gestión de derechos de acceso	La asignación y uso de los derechos de acceso privilegiados serán restringidos y controlados.
	Gestión de información secreta de autentificación de los usuarios.	La asignación de la información secreta de autentificación se controla a través de un proceso de gestión formal.
	Revisión de los derechos acceso de usuarios.	Los propietarios de activos deberán revisar los derechos de acceso de los usuarios a intervalos regulares.

OBJETIVO DE CONTROL	ÁREA	CONTROLES
Responsabilidad de los usuarios	Uso de la información secreta	Los usuarios estarán obligados a seguir las prácticas de la organización en el uso de la información de autenticación secreta.
Controles criptográficos	Política sobre el uso de controles criptográficos	Una política sobre el uso de controles criptográficos para la protección de la información deberá ser desarrollada e implementada.
	La administración de claves	Una política sobre el uso, la protección y la duración de las claves criptográficas se desarrolló e implementó a través de todo su ciclo de vida.
Procedimientos operacionales y responsabilidades	Procedimientos operativos documentados	Procedimientos de operación deberán ser documentados y puestos a disposición de todos los usuarios que lo necesiten.
Copia de seguridad	Copia de seguridad de información	Copias de seguridad de la información, software y del sistema imágenes serán tomadas y analizadas regularmente de acuerdo con una política de copia de seguridad acordado.
Registro y monitoreo	Protección de registro de información	Registro de instalaciones y registrar información estará protegido contra la manipulación y acceso no autorizado.
La transferencia de información	Políticas de transferencia de información procedimientos	Formales de transferencia de políticas, procedimientos y controles deben estar en su lugar para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.

OBJETIVO DE CONTROL	ÁREA	CONTROLES
	Acuerdos sobre la transferencia de información	Acuerdos deberán dirigirse a la transferencia segura de información comercial entre la organización y las partes externas.
	La mensajería electrónica	Información involucrada en la mensajería electrónica se apropiadamente protegida.
	La confidencialidad o acuerdos de no divulgación	Se identificarán los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información, regularmente revisados y documentados.
Requisitos de seguridad de los sistemas de información	Información de análisis de requisitos de seguridad y las especificaciones	Los requisitos relacionados con la seguridad de la información se incluirán en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.
Gestión de incidentes de seguridad de la información y mejoras	Responsabilidades y procedimientos	Se establecerán las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
	Informar sobre los eventos de seguridad de información	Los eventos de seguridad de la información deben ser reportados a través de canales de gestión adecuadas tan pronto como sea posible.

OBJETIVO DE CONTROL	ÁREA	CONTROLES
	Informar sobre las debilidades de la seguridad de la información	Se requiere que los empleados y contratistas que utilizan los sistemas y servicios de información de la organización para observar y reportar cualquier debilidad seguridad de la información que observen o sospechen en los sistemas o servicios.
	Respuesta a incidentes de seguridad de la información	Se debe responder a los eventos de seguridad de la información en concordancia con los procedimientos documentados.

Fuente: ***Anexo A. Norma ISO / IEC 27001: 2013*** (Organización Internacional para la Estandarización, 2013)

1.2.4.2 Norma Técnica ISO / IEC 27002: 2013 Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.

La ISO/IEC 27002 establece un código de mejores prácticas para la implementación de un Sistema de Gestión de Seguridad de la Información en organizaciones. Esta norma describe cómo se pueden establecer controles que deben ser elegidos en base a una evaluación de riesgos de los activos más importantes de las organizaciones. (Organización Internacional para la Estandarización., 2013)

El objetivo principal de la ISO/IEC 27002 es establecer directrices para implementar, mantener y mejorar la seguridad de la información, incluye también la selección, implementación y gestión de los controles teniendo en cuenta los riesgos del entorno de seguridad de información de la organización. Se encuentra distribuida en secciones, que corresponden a controles de seguridad de la información como se muestra en la tabla 2.

Tabla 2: ***Distribución de secciones de la ISO/IEC 27002***

SECCIONES	DESCRIPCIÓN
Políticas de seguridad de la información.	Su objetivo es proporcionar una orientación y apoyo de la dirección para la seguridad de la información de acuerdo con los requisitos de la empresa y con las regulaciones y leyes pertinentes. Deben definirse un conjunto de políticas de seguridad de la información, además de una estructura para establecer los objetivos y formas de control, estas corresponden ser aprobadas por la dirección, publicadas y comunicadas a los empleados y a las partes externas relevantes.
Organización de la seguridad de la información.	El objetivo es establecer un marco de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. Las actividades de seguridad de la información deben ser coordinadas por representantes, que a su vez deben tener responsabilidades bien definidas y proteger la información.
Gestión de activos	Todos los activos relacionados con el procesamiento de información deben ser identificados y mantener un inventario de estos. El objetivo es identificar los activos de la empresa y definir la responsabilidad de protección adecuada.
Seguridad en recursos humanos	Debe realizarse una verificación de antecedentes en todos los candidatos a empleados, de acuerdo con las leyes, regulaciones y normas éticas relevantes. El objetivo es asegurar que los empleados entiendan las responsabilidades asignadas y que sean aptos para los roles para los cuales están siendo contratados.
Seguridad física y del medio ambiente.	Los equipos de procesamiento de información sensibles deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados. El objetivo es evitar accesos físicos y no autorizados, daños e interferencias contra las instalaciones de procesamiento de información.

SECCIONES	DESCRIPCIÓN
Seguridad de las operaciones y comunicaciones.	Los procesamientos de la información deben estar definidos, al igual que las responsabilidades de la gestión y operación de todos los recursos. El objetivo es asegurarse de la operación correcta y segura de las instalaciones de procesamiento de la información; además de asegurarse de la protección de la información en redes.
Control de acceso	Debe garantizarse el acceso de usuario autorizado y prevenir el acceso no autorizado a los sistemas de información, con el fin de evitar daños a documentación y procesamiento de información que estén al alcance de cualquiera. El objetivo es limitar el acceso a la información y a las instalaciones de procesamiento de información.
Adquisición, desarrollo, y mantenimiento de sistemas	Los requisitos de seguridad de los sistemas de información deben ser identificados y acordados antes de su desarrollo o de su implementación.

Fuente: ISO / IEC 27002: 2013 Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (Organización Internacional para la Estandarización., 2013)

1.2.4.3 Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 2019).

COBIT es un marco de referencia para el gobierno y la gestión de la información y la tecnología dirigida a toda la empresa. Son guías de mejores prácticas dirigidas al control y supervisión de las tecnologías de información (TI). En el Marco de referencia COBIT 2019 Objetivos de Gobierno y Gestión, describe objetivos de gestión de seguridad propone dos dominios, que al aplicarse de una manera adecuada ayuda a la seguridad de información. En la tabla 3 se describe el contenido de los dos dominios. (ISACA, 2019)

Tabla 3: Dominios relacionados a la seguridad de la información.

DOMINIO	DESCRIPCIÓN	PRÁCTICA CLAVE DE GESTIÓN
APO13. Gestionar la seguridad	Definir, operar y monitorizar un sistema de gestión de seguridad de la información.	APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI). APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad. APO13.03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI).
DSS05. Gestionar los servicios de seguridad	Proteger la información de la empresa para mantener el nivel de riesgo de la seguridad de la información aceptable para la empresa, conforme con la política de seguridad. Establecer y mantener roles y privilegios de acceso de seguridad de la información. Realizar una monitorización de la seguridad.	DSS05.01 Proteger contra software malicioso DSS05.02 Gestionar la seguridad de la conectividad y de la red. DSS05.03 Gestionar la seguridad de endproint. DSS05.04 Gestionar la identidad del usuario y el acceso lógico. DSS05.05 Gestionar el acceso físico a los activos de Información y Tecnología. DSS05.06 Gestionar documentos sensibles y dispositivos de salida. DSS05.07 Gestionar las vulnerabilidades y monitorizar las infraestructuras para detectar eventos relacionados con la seguridad.

Fuente: ***Marco de referencia COBIT 2019 Objetivos de Gobierno y Gestión.*** (ISACA, 2019)

1.2.4.4 Biblioteca de Infraestructura de Tecnologías de la Información (ITIL V3)

ITIL es un marco de referencia para un conjunto de conceptos y mejores prácticas referentes a la gestión de servicios de Tecnologías de la Información. Se estructura en 5 libros con el objetivo de consolidar el modelo de "Ciclo de vida del Servicio". En uno de sus libros "Diseño del Servicio con ITIL", se menciona la Gestión de la Seguridad de la Información que implica elaborar y mantener políticas de Seguridad de la Información, donde se establezca la integridad, confidencialidad y disponibilidad de la misma. En la tabla 4 se muestran las fases de actuación en materia de seguridad que contiene ITIL V3. (ITIL, 2007)

Tabla 4: Fases de actuación en materia de seguridad

FASES	OBJETIVO
Planificación	Establecer un cronograma y definir unas responsabilidades para la ejecución del Plan de Seguridad y su mantenimiento.
Ejecución	Poner en marcha el plan de seguridad y conseguir los objetivos definidos en él.
Seguimiento	Monitorizar el servicio para conocer si se están cumpliendo los objetivos planteados con respecto a la Seguridad y la evolución de la ejecución del Plan de Seguridad.

Fuente: ITIL V3, Manual integro. (Ríos, 2011)

1.2.4.5 Norma Internacional de Información Financiera para Pequeñas y Medianas Entidades

El profesional debe valerse de un marco normativo aplicable que regule y le permita tener seguridad de los procesos que este aplica para la presentación financiera de sus operaciones contables; las empresas comercializadoras de vehículos preparan y presentan los estados financieros de acuerdo con Norma Internacional de Información Financiera para Pequeñas y Medianas Entidades.

1.2.5 Marco Legal.

La seguridad de la información posee un marco legal que lo regula. En la tabla 5 se mencionan las leyes y artículos relacionados a la seguridad de información y a los procesos de las empresas comercializadores de automóviles.

Tabla 5: Leyes aplicables.

LEYES	ARTÍCULOS	DESCRIPCIÓN
Ley Especial Contra Delitos Informáticos y Conexos.	Art. 1 Objeto de la ley	Tiene como objeto proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley.
	Art. 5 Acceso Indebido a los Programas o Datos Informáticos	La ley establece el que a sabiendas y con intención de usar cualquier dispositivo de la Tecnología de la Información o de la comunicación, accediera parcial o totalmente a cualquier programa o a los datos almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con estos, será sancionado de dos a cuatro años.
	Art. 11 Fraude Informático	El que, por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquier de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercer en perjuicio ajeno, será sancionado con prisión de tres a seis años.
	Art. 12 Espionaje Informático	El que con fines indebidos obtenga datos, información reservada o confidencial contenidas en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus

		componentes, será sancionado con prisión de cinco a ocho años. Si alguna de las conductas descritas en el inciso anterior se cometiere con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas, resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada, confidencial o sujeta a secreto bancario, la sanción será de seis a diez años de prisión.
	Art. 13 Hurto por Medios Informáticos	El que, por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, será sancionado con prisión de dos a cinco años.
	Art. 15 Manipulación de Registros.	Los administradores de las Plataformas Tecnológicas de instituciones públicas o privadas, que deshabiliten, alteren, oculten, destruyan, o inutilicen en todo o en parte cualquier información, dato contenido en registros de acceso, uso de los componentes de estos, será sancionada con prisión de cinco a ocho años. Si las conductas descritas en el inciso anterior, favorecieren la comisión de otro delito, la sanción se agravará hasta en una tercera parte del máximo señalado
	Art. 16 Manipulación Fraudulenta de Tarjetas Inteligentes o Instrumentos Similares	El que intencionalmente y sin la debida autorización por cualquier medio cree, capture, grabe, copie, altere, duplique, clone o elimine datos informáticos contenidos en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; con el objeto de incorporar, modificar usuarios, cuentas, registros, consumos no reconocidos, la configuración actual de

		éstos o de los datos en el sistema, será sancionado con prisión de cinco a ocho años. En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores adquiera, comercialice, posea, distribuya, venda, realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin o de datos informáticos contenidos en ellos o en un sistema.
	Art. 19 Alteración, Daño a la Integridad y Disponibilidad de los Datos.	El que violando la seguridad de un sistema informático destruya, altere, duplique, inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y confidencialidad en cualquier de sus estados de ingreso, procesamiento, transmisión o almacenamiento, será sancionado con prisión de tres a seis años.
	Art. 20 Interferencia de Datos.	El que interfiera, obstruya o interrumpa el uso legítimo de datos o los produzca nocivos e ineficaces, para alterar o destruir los datos de un tercero, será sancionado con prisión de tres a seis años. Si alguna de las conductas descritas en el inciso anterior recae sobre datos, documentos, programas o sistemas informáticos públicos o sobre datos destinados a la prestación de servicios de salud, de comunicaciones, sistemas bancarios, entidades financieras, de provisión y transporte de energía, de medios de transporte u otro servicio público, la sanción de prisión será de cinco a ocho años.
	Art. 21 Interceptación de Trasmisiones entre Sistemas de las Tecnologías de la Información y la Comunicación	La persona que sin justificación intercepte por medios tecnológicos cualquier transmisión hacía, desde o dentro de un sistema informático que no está disponible al público; o las emisiones electromagnéticas que están llevando datos

		de un sistema informático, será sancionado con prisión de siete a diez años.
	Art. 23 Divulgación no autorizada	El que sin autorización da a conocer un código, contraseña de acceso o cualquier otro medio de acceder a un programa o datos almacenados en un equipo o dispositivo tecnológico, con el fin de lucrarse así mismo, a un tercero o para cometer un delito, será sancionado con prisión de cinco a ocho años. Igual sanción tendrá el que sin autorización revele o difunda los datos o información, contenidos en un sistema informático que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, con el fin de obtener algún tipo de beneficio para sí o para otro. Si alguna de las conductas descritas en los incisos anteriores pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado, será sancionado con prisión de seis a doce años.
	Art. 24 Utilización de Datos Personales	El que sin autorización utilice datos personales a través del uso de las Tecnologías de la Información y la Comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando o modificando los datos en perjuicio de un tercero, será sancionado con prisión de cuatro a seis años. La sanción aumentará hasta en una tercera parte del máximo de la pena prevista en el inciso anterior a quien proporcione o revele a otro, información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar.
	Art. 25 Obtención y Transferencia de	El que deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere

	Información de Carácter Confidencial	un sistema o datos informáticos apoyándose en cualquier clase de las Tecnologías de la Información y la Comunicación, incluidas las emisiones electromagnéticas, será sancionado con prisión de cinco a ocho años.
	Art. 26 Revelación indebida de datos o información de carácter personal.	El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años.
	Art. 34 Suplantación en actos de comercialización	El que sin autorización y a nombre de un tercero, mediante el uso de las Tecnologías de la Información y la Comunicación, venda o comercialice bienes o servicios, suplantando la identidad del productor, proveedor o distribuidor autorizado, será sancionado con prisión de tres a cinco años. La conducta descrita en el inciso anterior se agravará con pena de prisión de cuatro a seis años, cuando la venta o comercialización se trate de medicamentos, suplementos o productos alimenticios, bebidas o cualquier producto de consumo humano.
Ley Especial Contra Actos de Terrorismo	Art. 12. Delito Informático	Será sancionado con pena de prisión de diez a quince años, el que para facilitar la comisión de cualquiera de los delitos previstos en la ley: a) Utilizare equipos, medidos, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicación o telemáticos, de servicios públicos,

		sociales, administrativos, de emergencia de seguridad nacional, de entidades nacionales o de otro país; b) Creare, distribuyere, comerciare o tuviere en su poder programas capaces de producir los efectos a que se refiere el literal a), de este artículo.
Ley de Regulación Del Teletrabajo	Art. 1 Objeto	Tiene como objeto promover, armonizar, regular e implementar el Teletrabajo como un instrumento para la generación de empleo y modernización de las instituciones públicas, privadas, autónomas y municipalidades, a través de la utilización de tecnologías de la información y comunicación.
	Art. 2 Objetivos	El aprovechamiento de las tecnologías de la información y comunicación en la prestación de los servicios al público y a la población en general, el aumento y medición de la productividad, mayor eficiencia y transparencia en el uso de los fondos públicos, disminución del gasto, reducción del consumo de energía eléctrica, combustible, alquileres y otros.
	Art. 3 Ámbito de Aplicación	Dentro del ámbito de aplicación de la Ley queda comprendido, las relaciones de trabajo derivadas de cualquier vínculo laboral entre trabajadores, empleadores públicos y privados, cuyos contratos de trabajo se sometan a lo previsto en Ley, demás Leyes laborales vigentes y cualquier otra fuente de derechos y obligaciones laborales.
	Art. 5 Modalidades del Teletrabajo	El Teletrabajo puede realizarse de las siguientes formas: I. De acuerdo al lugar donde desempeñan las labores: - Teletrabajo en domicilio - Teletrabajos en centros de trabajo o telecentros.

		- Teletrabajo móvil o itinerante - Teletrabajo alternado II. De acuerdo a la forma de comunicación pactada en la relación laboral: - Teletrabajo conectado - Teletrabajo desconectado
	Art. 6 Aplicación de la modalidad de teletrabajo	El empleador definirá los puestos de trabajo que de acuerdo a las necesidades de la empresa puedan someterse al Teletrabajo, así como los requisitos que el trabajador debe cumplir. El empleador y el trabajador podrán acordar por escrito aplicar, modificar o revocar la modalidad de Teletrabajo en los términos previstos en la Ley. Las condiciones en las cuales se ejecutará el trabajo bajo la modalidad regulada por la Ley se regirán en sus detalles por el acuerdo entre las partes, observando plenamente no transgredir las Disposiciones del Código de Trabajo y demás normas de carácter laboral.
	Art. 7 La implementación del teletrabajo	La implementación del Teletrabajo es estrictamente voluntaria, tanto para el trabajador como para el patrono y debe existir un acuerdo por escrito entre las partes, donde se establezcan los términos y condiciones; es decir, no debe existir forma coercitiva en la implementación del Teletrabajo por ninguna de las dos partes. Para establecer una relación de Teletrabajo regida por lo dispuesto en la Ley, el empleador y el tele trabajador deberá suscribir un contrato de Teletrabajo, el cual se sujete a esta Ley y a las demás Disposiciones que norman el Código de Trabajo. En el mismo deberá especificarse en forma clara las condiciones en que se ejecutarán las labores, las obligaciones, los derechos y responsabilidades que deben asumir las partes.

	Art. 12 Igualdad de derechos	Las personas empleadas bajo la modalidad del Teletrabajo tienen los mismos derechos individuales y colectivos que los trabajadores presenciales, en cuanto a seguridad social, previsional, prestaciones de Ley, seguridad e higiene ocupacional y libertad sindical.
Ley del Impuesto Especial a la Primera Matrícula de Bienes en el Territorio Nacional	Art. 3 Hecho Generador	Constituye hecho generador del impuesto especial a la matrícula por primera vez de: a) Vehículos automotores, en el Registro Público de Vehículos que regula la Ley de Transporte Terrestre, Tránsito y Seguridad Vial. b) Buques y artefactos navales, en el Registro que para dicho efecto lleve la Autoridad Marítima Portuaria, de acuerdo a la Ley General Marítima Portuaria. c) Aeronaves, en el Registro de Aviación Civil Salvadoreño que lleva la Autoridad de Aviación Civil, de acuerdo a la Ley Orgánica de Aviación Civil.
	Art. 5 Sujetos Pasivos	Son sujetos pasivos del pago del impuesto a que se refiere esta Ley, las personas naturales o jurídicas, sucesiones, fideicomisos o entidades que soliciten la matrícula por primera vez a su nombre de los bienes que trata esta Ley.
	Art. 7 Base imponible del Impuesto	La base imponible para los diferentes hechos generadores del Impuesto será la que a continuación se señala: a) Para los bienes adquiridos en el país, la base imponible será el precio total fijado en la operación, excluyendo el Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios, independientemente de la modalidad contractual. b) Para los bienes importados por el sujeto que solicitará el registro, la base imponible será el valor

		aduanero, más los impuestos o derechos que se hubieren pagado, excluyendo el Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios. c) Para los bienes con matrícula extranjera referidos en el inciso segundo del artículo 3 de esta Ley, la base imponible será equivalente al valor aduanero más los impuestos o derechos que se hubieren pagado si el bien hubiese sido importado excluyendo el Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios.
	Art. 8 Impuesto especial a la primera matrícula de vehículos automotores	El impuesto especial a la primera matrícula de vehículos automotores se determinará aplicando a la base imponible una tasa o alícuota de acuerdo a la categoría del vehículo según lo regulado y la tabla siguiente: **Anexo 1**
	Art. 12 Obligación de información de importadores y fabricante de vehículos	Los importadores, distribuidores, fabricantes de vehículos y sus representantes están obligados a presentar semestralmente a la Dirección General de Impuestos Internos, dentro de los primeros quince días hábiles de los meses de enero y julio de cada año, información en medios magnéticos o electrónicos de: 1) Vehículos nuevos importados: Listado de vehículos según características, indicando por separado, el precio de fábrica de los vehículos importados, valores de seguro, flete, márgenes de utilidad o ganancia y precios de venta al consumidor. 2) Vehículos usados importados: Listado de vehículos según características detalladas de los vehículos importados, precios de adquisición de los proveedores, valores de seguro, flete, márgenes de utilidad o ganancia y precios de venta al consumidor.

		3) Vehículos fabricados en el país: Características detalladas de los vehículos fabricados, precios de venta en el mercado nacional al consumidor, márgenes de utilidad o ganancia otorgados a los distribuidores. Sin perjuicio de lo establecido en el inciso anterior, los importadores, distribuidores, representantes debidamente acreditados en el país y fabricantes, estarán obligados a proporcionar a la Dirección General, la información que les sea requerida, para la administración del impuesto establecido en la Ley, tal como los costos de importación, producción, comercialización, márgenes de ganancia precios de venta al consumidor final y a los distribuidores.
Ley de Regulación de los Servicios de Información sobre el Historial de Crédito de las Personas.	Art. 2 Ámbito de aplicación.	Ley será aplicable a los agentes económicos, personas naturales o jurídicas, públicas o privadas, exceptuando a la Superintendencia del Sistema Financiero, que realicen cualquier actividad económica, financiera, bancaria, comercial, industrial o de servicios, que manejen o tengan acceso a datos sobre el historial de crédito de los consumidores o clientes, por sí mismo, por medio de intermediarios o por un servicio arrendado. También será aplicable a las agencias de información de datos, personas jurídicas, públicas o privadas, exceptuando a la Superintendencia del Sistema Financiero, que tengan autorización para brindar el servicio de almacenamiento, transmisión e información, por cualquier medio tecnológico o manual, de los datos sobre el historial de crédito de los consumidores o clientes.
	Art. 14 Derechos de los consumidores o clientes.	Los consumidores o clientes tendrán los siguientes derechos: a) Acceso a la información: los consumidores o clientes tienen

		derecho a conocer toda la información que de ellos mantengan o manejen los agentes económicos y las agencias de información de datos. Para ello, las agencias de información de datos deberán contar, al menos, con un centro de atención al cliente en cada región, para que las personas interesadas puedan consultar su información. La consulta de esta información no causará costo alguno a los consumidores o clientes. La agencia de información de datos correspondiente deberá proveer de forma escrita, en el momento en que se le solicite, la información al consumidor o cliente, previo requerimiento realizado de forma verbal o escrita, verificando la identidad del consumidor o cliente; así como, darle a conocer qué entidades acreedoras tuvieron acceso a su historial de crédito, y el uso para el que fue requerida.
	Art. 15 Acceso para consulta de información	El agente económico solo podrá tener acceso para consultar información del historial crediticio del consumidor o cliente, con la debida autorización de éste, y únicamente en las condiciones en que la misma haya sido conferida. La autorización a que se refiere este artículo, deberá constar en un documento especial extendido al efecto y no podrá ser parte de cláusulas generales de los contratos que el consumidor suscriba con el agente económico.
Normas para la Importación de Vehículos Automóviles y de otros Medios de Transporte.	Art. 1	En las importaciones de vehículos automóviles nuevos, realizados por distribuidores o representantes debidamente acreditados en el país, el valor aduanero se determinará sobre la base de los precios de venta del fabricante al distribuidor. Dichos precios no incluirán las rebajas que

		otorguen los fabricantes por cantidades compradas o formas de pago. Para los efectos del inciso anterior, la información se obtendrá de la declaración jurada del distribuidor y comprobado en base a los boletines y listas de precios publicados por las empresas fabricantes del país de origen de los vehículos. Dichos boletines y listas deberán estar legalizados por el Consulado de El Salvador en el país de origen de los vehículos y ser aprobados por la Dirección General de la Renta de Aduanas, en lo sucesivo llamada la Dirección General. Los distribuidores y representantes acreditados en el país estarán obligados a presentar semestralmente listas de precios de fábrica. Sin perjuicio que la Dirección General puede solicitar las certificaciones de los precios de exportación emitidos por el fabricante.
	Art. 2	En las importaciones de vehículos nuevos efectuados por particulares, no considerados como distribuidores acreditados, en la determinación del valor aduanero, se tomarán como base los precios a los cuales hace referencia el artículo anterior.
	Art. 3	Para la importación de vehículos usados, el valor aduanero se determinará sobre la base de los precios contenidos en las siguientes publicaciones especializadas en la materia, en su orden obligado y según proceda: - Editions Maclean Hunter Market Reports, Inc. - Ediciones N.A.D.A, guía de carros usados - National Boat Book - Kelley Blue Book
	Art. 4	Para los vehículos usados comprendidos en la partida arancelaria 87.03 y aquellos comprendidos en las Sub-Partidas 87.04.21 y 87.04.31, de peso total con carga máxima inferior o igual a 1.5 toneladas, el valor a

		utilizarse de las publicaciones señaladas en el Artículo anterior, será el precio sugerido del fabricante para el vehículo nuevo (manufacturers suggested retail price when new), rebajado en un 12%. A dichos vehículos, se les aplicará las rebajas en concepto de depreciación definidas en el Art. 5
	Art. 5	Cuando se importen vehículos automóviles comprendidos en la partida arancelaria 87.03 y en las Sub-Partidas 87.04.21 y 87.04.31, de peso total con carga máxima inferior o igual a 1.5 toneladas, se aplicarán sobre el precio base al que hace referencia el primer inciso del artículo anterior, las siguientes rebajas en concepto de depreciación: **Anexo 2.**
	Art. 6	Para obtener el valor aduanero de vehículos sobre el cual se aplicarán los derechos en impuestos, al precio base señalado en los artículos anteriores, según corresponde, y una vez deducida la rebaja por depreciación si procede, se deberán añadir todos los gastos en que se incurra con motivo de la importación, tales como el flete y seguro.
	Art. 7	Para la identificación de los vehículos importados, la Aduana utilizará el VIN (Vehicle Identification Number), que aparece en las fuentes de datos antes expresadas. En los casos que no fuere posible hacerlo por ese medio, se les identificará conforme a sus características especiales del vehículo.
	Art. 8	Todo vehículo que se introduzca al país deberá someterse de inmediato al control de la Aduana de entrada. Cuando proceda la importación definitiva del vehículo, el interesado deberá remitirlo dentro de un plazo de veinticuatro horas hábiles con el documento de tránsito respectivo a la Aduana competente, a efecto que realice los trámites para el pago de los derechos e impuestos aplicables.

Ley de Transporte Terrestre, Transito y Seguridad Vial	Art. 13	Todos los vehículos deberán tener el timón al lado izquierdo de fábrica y cumplir con las normas mínimas para circular por la red vual del país, las cuales serán específicas en el reglamento respectivo. Se exceptúan de esta medida los vehículos de colección cuyo timón es original al lado derecho, los cuales serán regulados en el reglamento respectivo, y deberán atenerse a las normas mínimas de seguridad que el reglamento establezca.
	Art. 17 De su registro o control.	Se establece el registro público de vehículos automotores que puede ser consultado por cualquier persona su organización y funcionamiento estará a cargo del viceministerio de transporte a través de la dirección general de tránsito, contara con un jefe y demás personal administrativo que determine el reglamento y en él se inscribirán los títulos siguientes: a) los testimonios de las escrituras públicas o los documentos debidamente legalizados ante notario, en los que conste, la propiedad, transferencia o tenencia legitima de un vehículo automotor, las resoluciones y modificaciones de dichos documentos; b) en el caso de vehículos automotores importados usados y aun no inscritos, los documentos que acrediten la propiedad en el país de origen; y los de des almacenaje, expedidos por las autoridades aduaneras nacionales; c) los testimonios de escrituras públicas en los que conste cualquier gravamen, o modificación de las características básicas del vehículo; d) las actas de remate o adjudicación en pago; y, e) los demás que la ley o su reglamento establezcan.

		Los títulos sujetos a inscripción deberán presentarse para su correspondiente registro, dentro de los siguientes quince días hábiles que sigan a su otorgamiento en su caso, y surtirá efecto contra terceros a partir de la fecha de presentación del título al registro para su inscripción, incluso para los fines de responsabilidad señalados en la Ley de Procedimientos Especiales sobre Accidentes de Tránsito.

Fuente: (Legislativa, Ley Especial Contra Delitos Informáticos y Conexos., 2016)***;*** (Legislativa, Ley de Regulación de los Servicios de Información sobre el Historial de Crédito de las Personas., 2011)***;*** (Legislativa, Ley de Regulación del Teletrabajo, 2020)***;*** (Legislativa, Ley de Transporte Terrestre, Transito y Seguridad Vial, 1995)***;*** (Legislativa, Ley del Impuesto Especial a la Primera Matrícula de Bienes en el Territorio Nacional, 2009)***;*** (Legislativa, Normas para la Importación de Vehículos Automóviles y de otros Medios de Transporte., 1995)***;*** (Legislativa, Ley Especial Contra Actos de Terrorismo, 2014)

CAPÍTULO II - METODOLOGÍA DE LA INVESTIGACIÓN.

2.1 ENFOQUE Y TIPO DE LA INVESTIGACIÓN.

Para la presente investigación se utiliza un método cualitativo, que permite detallar características del problema en seguridad de la información para los procesos clave del área financiera que ocurren en empresas comercializadoras de automóviles.

2.2 SUJETOS Y OBJETOS DE ESTUDIO.

2.2.1 Unidad de análisis.

Las unidades de análisis para la investigación son los empleados que forman parte de los procesos claves del área financiera de las empresas comercializadoras de automóviles ubicadas en el municipio de Antiguo Cuscatlán; los cuales son: Contador General, Asistente de Contabilidad, Analista Financiero, Gerente Financiero, Gerente de Venta, Analista Comercial y Encargado de Tecnología de la Información.

2.2.2 Universo y muestra.

Para la elaboración de esta investigación se considera a una empresa comercializadora de automóviles del municipio de Antiguo Cuscatlán, con énfasis en el área financiera de esta.

2.2.3 Variables e indicadores.

Las variables dependiente e independiente de la hipótesis se detallan a continuación:

Independiente: Plan de Seguridad de la Información.

Dependiente: Procesos claves y calidad de los reportes generados para la toma de decisiones.

2.3. TÉCNICAS. MATERIALES E INSTRUMENTOS

2.3.1 Técnicas para la recolección de datos.

Se utiliza la entrevista para la recolección de datos en la empresa comercializadora de automóviles, que indique la problemática sobre resguardo de información y de esta manera realizar un estudio cualitativo, mediante el posterior análisis y determinar las posibles soluciones al problema.

2.3.2 Instrumento de medición.

El instrumento de medición utilizado son las entrevistas al personal involucrado en el área financiera de la empresa comercializadora de automóviles, esto con el fin de obtener datos sobre seguridad de información en procesos claves para la toma de decisiones de la entidad. **Anexo 3.**

Los datos que se obtuvieron de la entrevista son ordenados y redactados a través de Microsoft Word, detallando los controles existentes en los aspectos claves, con el propósito de medir el conocimiento acerca de la problemática planteada y concluir si es necesario elaborar un plan de seguridad de la información para mejorar los procesos clave del área financiera.

2.3.3 Cronograma de actividades

Cronograma de Actividades	MES																																							
	FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Inicio de Seminario de Graduación																																											
Capitulo I Marco Teórico																																											
Planteamiento del problema																																											
Delimitación de la investigación																																											
Justificación de la investigación																																											
Objetivos de la Investigación																																											
Primer avance del anteproyecto																																											
Observaciones y correcciones del Capitulo I																																											
Marco teórico, conceptual, técnico legal																																											
Entrega del Anteproyecto																																											
Capitulo I Marco Teórico																																											
correcciones del Capitulo I																																											
Presentación del Capitulo I																																											
Capitulo II Metodología de la Investigación																																											
Investigación de campo																																											
Recolección de datos																																											
Análisis de resultados																																											
Presentación del Capitulo II																																											
Capitulo III Propuestas																																											
Elaboración de propuestas																																											
Verificación de propuestas																																											
Entrega de propuesta final																																											
Capitulo IV Conclusiones y Recomendaciones																																											
Elaboración de conclusiones																																											
Recomendaciones																																											
Presentación del Capitulo IV																																											
Entrega de Trabajo Final																																											
Preparación para la defensa del trabajo																																											
Defensa de trabajo de Grado																																											

2.4 DIAGNOSTICO.

Las entrevistas se llevaron a cabo de manera virtual por la aplicación de Google Meet, esto por motivos de distanciamiento social originados por la Pandemia del Covid-19.

Con la información proporcionada por cada uno de los colaboradores entrevistados se realiza el respectivo análisis correspondiente por cada pregunta, las cuales se agrupan por categorías o áreas de controles de seguridad de acuerdo a la ISO 27001 e ISO 27002, como se desarrolla a continuación:

Recursos Humanos.

Cargo	Preguntas	Respuestas
Encargado de TI	**Pregunta 1**. ¿Cuántas personas conforman el departamento de TI? (Si es más de una persona cuales son las funciones que desempeña cada uno.)	NOTA: Equipo TI Corporativo, no solo para Unidad Automotriz (10 personas) - 1 gerente de TI Corporativo - 1 senior de Infraestructura y DBA - 1 senior de Redes - 1 junior de Infraestructura y Soporte Técnico - 1 junior de Redes y Soporte Técnico - 1 soporte Técnico - 2 consultores de Desarrollo ABAP (SAP) - 1 gestor de Ticket (Incidencias y Requerimientos) - 1 Key User de Sistemas Diversos (entre ellos SAP, Perfil Financiero)
	Pregunta 2. ¿Qué grado académico tiene cada integrante del departamento de TI?	Licenciados en Sistemas e Ingenieros en Sistemas
	Pregunta 3. ¿Recibe capacitaciones o asesorías en temas de seguridad de la información?	Si, al menos una vez por año o en nuevos proyectos
Gerente Financiero	**Pregunta 1.** ¿Qué tipo de actividades son realizadas para concientizar al personal en cuanto a la importancia de la seguridad de la información?	Campañas de correos masivos a las personas que tienen acceso al correo institucional, a las que no, constantes publicaciones y campañas de concientización para dar a conocer medidas de seguridad que no llevan mucho tiempo, pero ganan mucho conocimiento
	Pregunta 2. ¿Cómo se controla la segregación de funciones de los colaboradores del área financiera?	Hay una persona encargada que en nuestro caso se llama controller administrativo, lejos de ser alguien de TI es alguien enfocado en el área administrativa con capacidad de auditor y verifica que los perfiles de cada usuario tengan los accesos de acuerdo al nivel

		jerárquico y las autorizaciones necesarias hasta donde su perfil de su puesto se lo permita.
	Pregunta 3. ¿Qué sanciones existen cuando algún empleado quiere violar los límites de acceso permitido?	Hay sanciones de tipo llamados de atención de jefes inmediatos superiores, también sanciones por medio escrito, acciones de personal, despidos y hasta posibles demandas por el tipo de información que se haya sustraído o el daño que haya causado.
	Pregunta 6. ¿Cuál es la forma en que la entidad informa a los usuarios sobre restricciones de uso de información confidencial?	Hay sanciones de tipo llamados de atención de jefes inmediatos superiores, también sanciones por medio escrito, acciones de personal, despidos y hasta posibles demandas por el tipo de información que se haya sustraído o el daño que haya causado.
Analista Financiero	**Pregunta 1.** ¿Cuántos años tiene de laborar en el rubro de empresas comercializadoras de vehículos?	4 años.
	Pregunta 9. ¿Ha recibido alguna capacitación sobre seguridad de la información?	Si, al menos una vez al mes recibo correos electrónicos de actualizaciones o de amenazas electrónicas como virus o phishing que pueden ocasionar ataques cibernéticos.
Contador General	**Pregunta 1.** ¿Ha recibido capacitaciones acerca de seguridad de la información?	Sí, hace dos semanas aproximadamente se llevó a cabo un curso de ciberseguridad; anteriormente no se le daba mucho seguimiento a nivel de cursos y charlas, pero sí a nivel informativo se recibía correos del corporativo de TI
Asistente Contable	**Pregunta 1.** ¿Cuántos años tiene laborando para la empresa?	2 años.
Gerente de Venta	**Pregunta 1.** ¿Cuántos años tiene de laborar en la empresa?	4 años.
Analista Comercial	**Pregunta 1.** ¿Cuántos años tiene de laborar en el rubro?	7 años.
	Pregunta 6. ¿Ha recibido capacitaciones acerca de seguridad de la información? (si la respuesta es sí, realizar la siguiente pregunta) ¿Cada cuánto tiempo? Y si la respuesta es no realizar la pregunta del porqué.	No, nunca

Análisis: El personal tiene la capacidad requerida para la ejecución de sus puestos de trabajo ya que cuentan con varios años de experiencia, sin embargo, no se capacita constantemente acerca de seguridad de la información, esto conlleva a un riesgo que genera una brecha de vulnerabilidad que atenta contra la seguridad, bien sea por estar desactualizados o por falta de atención. En este sentido, se debe tomar en cuenta que ellos son los que tienen procesos importantes a su cargo, de ahí la importancia de ser capacitados y preparados sobre seguridad de información.

Seguridad Física y Ambiental

Cargo	**Preguntas**	**Respuestas**
Encargado de TI	**Pregunta 14.** ¿Cada cuánto tiempo se les realiza mantenimiento a los equipos de cómputo?	Al menos una vez al año
	Pregunta 17: ¿Se cuenta con controles preventivos para desastres naturales?	Sí, del tipo Proactivos: Con los cuales el área de TI busca impedir o minimizar las consecuencias de una grave interrupción (Centros de Datos en más de un lugar físico, Enlaces redundantes de última milla de servicios de comunicación) Reactivos: Con los cuales el área de TI utiliza para reanudar lo más pronto posible las operaciones (Equipos y Servicios contratados como SAAS, Servicios como IAAS, Equipos de Comunicación Administrados), todos ellos con tiempos cortos de respuestas.

Contador General	**<u>Pregunta 8:</u>** ¿Existe algún protocolo o acceso restringido al departamento físico de contabilidad?	Contabilidad se encuentra en el segundo nivel, para poder ingresar al segundo nivel se necesita de una tarjeta para poder abrir las puertas, ya en el área de contabilidad la oficina es cerrada, pero de las personas que se encuentran en el segundo nivel tiene acceso al área.
Gerente de Venta	**<u>Pregunta 7.</u>** ¿Cuáles son los medios y/ o lugares de almacenamiento para el resguardo de la información de los clientes?	Archiveros y carpetas de computadoras.

Análisis: El mantenimiento de los equipos de trabajo se realiza una vez al año, este tipo de medida no asegura la continuidad y disponibilidad de un activo, debido a que las aplicaciones en su momento requerirán de una actualización de versiones más recientes.

Debido a que los colaboradores del segundo nivel de las oficinas administrativas tienen acceso a todas las áreas estas deben considerar adoptar medidas de restricciones a las oficinas aplicando y diseñando procedimientos para trabajar en áreas seguras y limitantes a todo el personal, esto contribuirá a tener las áreas seguras únicamente permitiendo el acceso al personal autorizado.

Organización de la Seguridad de Información.

Cargo	**Pregunta**	**Respuesta.**
Encargado de TI	**Pregunta 16:** ¿Cuáles son las medidas o controles establecidos para el teletrabajo?	a. Acceso mediante equipo proporcionado por la empresa b. Acceso vía Túnel VPN c. Validación de Credenciales
	Pregunta 11. ¿Los empleados tienen acceso al sistema desde otros dispositivos diferentes de sus ordenadores?	Sí, Solo a ciertos sistemas y aplicaciones.
Contador General	**Pregunta 12:** ¿Cómo se maneja la seguridad de información con el teletrabajo?	En el periodo de la pandemia, por ejemplo, cuando se estuvo trabajando con Office básicamente fue en tema operativos de cierre de cumplimientos.

Análisis: Se realizan actividades por teletrabajo y se posee controles como lo son acceso mediante equipo proporcionado por la empresa, acceso vía túnel VPN y validación de credenciales, no obstante, los controles aplicados son insuficientes para proteger la información accedida, procesada y/o almacenada en los sitios de trabajo remoto.

Operaciones

Cargo	Preguntas	Respuestas
Encargado de TI	**Pregunta 5.** ¿Qué herramientas poseen para asegurar la información digital?	Servidores de aplicación y Bases de Datos en Sitios Seguros (En la Nube y locales (pocos)), en los cuales de almacena toda la data de la empresa., se realizan respaldos diarios de los servidores y Bases de Datos, Backup almacenados en diferentes puntos estratégicos.
	Pregunta 6. ¿Existen planes de contingencia ante un ciberataque?	No claramente.
	Pregunta 7. ¿Cuál es el procedimiento ante un correo sospechoso?	Nivel 1. Filtrado por herramienta de Seguridad Exchange Online Protection (EOP) Nivel 2. Sistema de seguridad de Antivirus Nivel 3. Programas de concientización al usuario en el uso de la información.
	Pregunta 10. ¿Cada cuánto tiempo considera deben ser realizadas copias de seguridad de los archivos que contienen la información más importante de la empresa?	Este proceso es en tiempo real para las estaciones de trabajo y debe ser al menos diario para Servidores de Bases de Datos y Sistemas de Información.
	Pregunta 12. ¿Se realizan análisis y gestión de riesgos informáticos? ¿Cuáles?	Si, al menos una vez al año, la empresa trata de utilizar controles cercanos a los sugeridos por ITIL (pero no certificados). (Análisis del Impacto y Riesgo al Negocio, Evaluación de Mitigación de Riesgo Requerida, Monitorización de Riesgo).
Analista Financiero	**Pregunta 5.** ¿Cuáles son los medios y/o lugares de almacenamiento para el resguardo de la información financiera?	Para la información física se cuenta con bodegas de archivos que están dentro de las instalaciones, no se arrendan ni alquilan para este tipo de información, y para la información virtual se almacena en los

		servidores locales, que en el caso de esta empresa es subarrendado y próximamente será propio.
	Pregunta 7. ¿Con que regularidad realiza copias de seguridad de la información digital que maneja?	Normalmente no, porque se tienen los backup electrónicos que creo se hacen a diario o cada cierto período.
	Pregunta 8. ¿En caso de extravió de información magnética o física que procedimiento realiza para recuperarla o sustituirla?	Hasta el momento no ha ocurrido un hecho así, pero si existen protocolos, por ejemplo, para la información electrónica se realiza un seguimiento de los usuarios que han tenido acceso a esa información, que busquen por donde se ha dado la fuga de información. En la parte física es más complicado, porque por ejemplo en las fotocopias si no se tiene acceso al software de seguridad bajo fotocopias por código de empleado, es bastante difícil controlar quién ha sacado las fotocopias o scanner.
Contador General	**Pregunta 3.** ¿Alguna vez el sistema le ha generado informes con datos erróneos o algún incidente en su puesto de trabajo?	Dentro de sistema actual talvez ocurrió cuando se estaba en la implementación, ya que en marzo de 2020 se migró a una nueva versión del sistema, se tuvieron que hacer pruebas y nuevas configuraciones porque la contabilidad se migró al nuevo sistema (anteriormente se tenía en sistema SAP) ya que la parte operativa ya estaba dentro del sistema. Actualmente no se han generado informes erróneos.
	Pregunta 7. ¿Cuál cree sería el impacto de la generación de reportes financieros erróneos?	El sistema actualmente encuentra todo su soporte en la nube, entonces debe de haber un respaldo de todo ese servidor que se encuentra en Alemania. Con un ámbito malicioso de riesgo económico para la compañía, el sistema como tal no representa mayor fuente de información o extracción de datos.

	Pregunta 9. ¿Según su criterio, al contar con un plan de seguridad de la información, le contribuiría en la ejecución de los procesos de contabilidad? Justifique su respuesta.	De acuerdo a mi punto de vista, un plan mejoraría a reforzar la ejecución de los procesos contables y sobre todo a salvaguardar la información, ya que hay varios procesos que considero tienen vulnerabilidades y al implementar controles mejoraría la situación.
	Pregunta 10. ¿Considera que existen vulnerabilidades en la ejecución de los procesos del área contable?	No, porque está bien definidos los procesos, por ejemplo, la persona que emite cheques solamente tiene acceso esa persona, se imprime y se pasan a firmar, luego regresa a ella y se entrega a caja; caja se encarga de entregarlos a los proveedores o beneficiarios según sea el caso, no se expone la información cuando se traslada algún documento administrativo, se entrega en un sobre sellado.
	Pregunta 11. ¿Cómo respalda la información, se realiza copias de seguridad?	No, ya se almacena automáticamente se hace un backup de la información.
Asistente Contable	**Pregunta 3.** ¿Realiza periódicamente una copia de seguridad de la información que maneja?	Diariamente no, debido a que en las tardes se realiza un backup automático.
	Pregunta 5. ¿Cuál es el procedimiento para anular registros erróneos en el departamento de contabilidad?	Analizar el registro y si no tiene mayor incidencia proceder de lo contrario si el registro que se desee eliminar es de un periodo anterior debe estar autorizado por el jefe inmediato.
	Pregunta 7. ¿Cuáles procesos considera que son vulnerables en el departamento de contabilidad?	- El trámite de elaboración de cheques. - El pago por medio de la banca electrónica. - La recopilación de información de los clientes. - El acceso al sistema mediante los diferentes módulos

	Pregunta 9. ¿Cuáles son los procedimientos para respaldar la documentación fiscal?	Se archiva la documentación física y se guarda en bodegas con acceso solo a contabilidad, luego se hace un backup de la documentación electrónica y esta se guarda en una carpeta compartida en la red al que solo el área financiera tiene el libre acceso
	Pregunta 10. ¿Cómo protegen la información proveniente de los clientes que es considerada confidencial?	Los expedientes de los clientes donde está toda la información se mantienen en una bodega bajo llave.
Gerente de Venta	**Pregunta 2.** ¿Qué tan importante es la seguridad de la información para las operaciones de la empresa?	Es importante porque se maneja datos confidenciales de los clientes, como Estados Financieros, declaraciones de impuestos.
	Pregunta 4. ¿Considera que maneja información de carácter confidencial o importante de los clientes?	Sí, se maneja información de carácter confidencial. Muchas veces respaldan información con depósitos a plazo, acciones, estados bancarios.
	Pregunta 5. ¿Qué tipo de información se solicita a los clientes?	- Estados de cuenta bancarios. - Declaraciones de impuestos. - Constancias salariales. - Si son accionistas. - Escrituras de constitución. - Si es persona jurídica o natural. - Tarjeta del IVA. - Documentación del representante legal.
	Pregunta 8. ¿Cuáles son los procesos de la gerencia de ventas relacionados con el área financiera?	Se tiene una relación cercana, porque cada venta que se hace se verifica el costeo teórico que se tiene versus el costo real de la venta, el área financiera proporciona un archivo donde se compara lo que se tiene presupuestado en el costeo con lo que realmente costó, por ejemplo, cuánto costó hacer mantenimiento al carro, polarizado, impuestos, entre otros. Se trabaja de la mano porque cada venta que se hace se revisa el margen de utilidad

		que realmente dejó, además de eso, el cálculo de la comisión de las vendedoras, y se trabaja de la mano con el cálculo de la primera matrícula, emisiones de cheques, autorizaciones de depósitos.
	Pregunta 9. ¿Considera que sus procesos se realizan de manera segura o necesitan reforzarse?	Existe deficiencia, porque se entregan papeles y en ocasiones no se firma de recibido. Debería de haber más respaldo de la documentación.
Analista Comercial	**Pregunta 5.** ¿Cree usted que los procesos para el manejo de la documentación que realiza son seguros?	No en su totalidad; porque en todos los procesos hay bastante personal involucrado y eso pone en vulnerabilidad a la información.
	Pregunta 10. ¿Considera que, al contar con un plan de seguridad de la información, le garantizaría más confiabilidad en la ejecución de los procesos de su puesto de trabajo? Justificar respuesta.	Sí, porque entre más resguardada esté la información da más seguridad a los clientes de que sus datos estén no estén expuestos.
Gerente Financiero	**Pregunta 5.** ¿La empresa invierte en su planificación financiera temas de ciberseguridad?	Sí, de hecho, el departamento de TI cuenta con un fondo para algún siniestro.
	Pregunta 7. ¿Considera que el software con el que se cuenta actualmente es adecuado para que la información sea integra, atentica y confidencial?	Actualmente no, creería que, trabajando un poco más en el desarrollo en unos 6 meses o 1 año en ciertos módulos, pienso que, si estaría totalmente listo, porque aún está en proceso de implementación. Pero si cuenta con niveles de seguridad bastante buenos.
	Pregunta 8. ¿Por qué considera que el software actual no cumple con los tres aspectos de la seguridad de la información?	Porque si cumple con algunos niveles de seguridad, pero lo íntegro y disponibilidad de la información aún no lo cumple, porque está en el proceso de implementación que aún no se ha terminado pero que el proveedor del sistema si ha ofrecido esos beneficios o bondades, así que se tiene la expectativa que cuando esté terminado se lleguen a concretar, porque se supone

		que el sistema va a poder funcionar solo, sin necesidad de utilizar otro sistema periférico para poder generar información y hasta que se terminen de alinear todos los módulos la información va a fluir mucho más.
	Pregunta 9. Debido a lo anterior, ¿Se ha tenido algún inconveniente o se han generado errores al momento de generar informes?	Sí, de hecho, se dio un problema por la falta de capacitación acerca de la generación de un reporte y sobre cómo se debía generar. Y hasta que se dio el inconveniente nos explicaron cómo se programan estos reportes, pero si se han tenido errores que poco a poco se van corrigiendo.
	Pregunta 10. ¿Considera oportuno que las empresas comercializadoras de automóviles cuenten con políticas de seguridad informática?	La verdad sí, ya que estaríamos protegiendo la información que se maneja de las operaciones de las empresas, clientes y proveedores.

Análisis: Entre los involucrados en el área financiera se puede notar que todos opinan acerca de la importancia al resguardo de la información digital, mas no acerca de la información que se maneja de forma física. Ante los ataques de software maliciosos, no se cuenta con un plan de contingencia por lo tanto no se puede asegurar que la información y las instalaciones de procesamiento de la información estén protegidas. Los entrevistados opinan que el sistema operacional con el que poseen no es completamente íntegro, sin embargo, se realiza un buen procesamiento de la información y los inconvenientes no han sido de mayor afectación, lo cual indica que dentro de las funciones que el sistema contiene, se está realizando una efectiva operatividad.

Control de acceso

Cargo	Preguntas	Respuestas
Encargado de TI	**Pregunta 11**: ¿Los empleados tienen acceso al sistema desde otros dispositivos diferentes de sus ordenadores?	Sí, solo a ciertos sistemas y aplicaciones.
Analista Financiero	**Pregunta 2**. ¿El sistema que tiene la empresa posee niveles de acceso a la información? Si la respuesta es sí, ¿Cuáles?	Sí, posee niveles escalonados dependiendo el nivel jerárquico; se les da a conocer a los empleados dependiendo el área en el que se manejan y se les permite acceso a la información de los módulos que necesitan.
Gerente Financiero	**Pregunta 6:** ¿Cuál es la forma en que la entidad informa a los usuarios sobre restricciones de uso de información confidencial?	Hay varias formas como correos electrónicos a través del correo institucional, publicaciones en las pizarras informativas y también se hacen sesiones como tipo seminarios para dar este tipo de capacitaciones.
Contador General	**Pregunta 5**: ¿El acceso a los módulos de contabilidad está restringidos según las obligaciones que tiene cada colaborador?	Sí, hay una matriz de permisos dependiendo el perfil de cada colaborador así está asignado el permiso para cada área, por ejemplo, dentro del perfil de asistente contable de impuestos no se tiene permiso de crear facturas, afectación de inventarios de almacén, ingresos de cobros en módulo de caja, entre otras operaciones. Lo que se tiene dentro de la matriz es plantillas de grupos por ejemplo en el área de finanzas y contabilidad a los cuales se puede dar acceso a períodos; el acceso a los permisos de funcionalidad de cada módulo le corresponde al área de control interno, solamente ellos tienen acceso a brindar permiso a diferentes módulos y operatividad.

	Pregunta 8: ¿Existe algún protocolo o acceso restringido al departamento físico de contabilidad?	Contabilidad se encuentra en el segundo nivel, para poder ingresar al segundo nivel se necesita de una tarjeta para poder abrir las puertas, ya en el área de contabilidad la oficina es cerrada, pero de las personas que se encuentran en el segundo nivel tiene acceso al área.
Gerente de Venta	**Pregunta 10**. ¿Existe alguna manera de controlar los accesos que se tiene a la información que manejan dentro de la Gerencia de Venta?	Si y no, si se tiene cuidado con la documentación, pero al verificar si los archivos donde se resguarda la información de clientes, lo más probable es que se encuentre sin llave. No existe medidas rigurosas para el resguardo de la información.

Análisis: Según las opiniones de los entrevistados la entidad no cuenta con una política que limite el acceso a los sistemas solo se tiene una matriz de permisos dependiendo el perfil de cada colaborador, pero para el departamento de contabilidad este siempre tiene acceso a los módulos de otras áreas solo en formas de consultas por temas de revisión, aunque esto no garantiza un control de seguridad.

En cuanto al acceso físico al área administrativa los colaboradores tienen tarjetas que permiten entrar al segundo nivel, pero al ingresar no existen perímetros que restrinjan el acceso a la bodega de archivos, estas áreas son las de mayor privilegio ya que en ellas esta recopilada la información confidencial del cliente y reportes financieros un control de entradas permitiría asegurar el acceso al personal autorizado y así aplicar la seguridad física en las oficinas y bodegas.

Comunicaciones

Cargo	Preguntas	Respuestas
Encargado de TI	**Pregunta 8**: ¿La navegación en sitios web de los colaboradores se encuentra limitada?	Si, por medio de políticas Web Rules, aplicadas en Firewall Core
	Pregunta 9: ¿La instalación de otro software inusual por parte de los colaboradores esta monitoreada por el departamento de TI?	Si, por política está prohibido uso de software no evaluado y aprobado por TI., se procede a eliminar.
	Pregunta 11: ¿Los empleados tienen acceso al sistema desde otros dispositivos diferentes de sus ordenadores?	Sí, solo a ciertos sistemas y aplicaciones.
Analista Financiero	**Pregunta 4.** ¿Qué medio utilizan para solicitar requerimientos de información a otras áreas de la empresa?	Normalmente si la información es requerida por instituciones públicas son medios escritos y electrónicos; y si son instituciones bancarias es por medio de correo electrónico, y si son de otra índole (asociaciones, distribuidoras, competencia) es por medio correo electrónico. En el tiempo de pandemia se ha manejado todo por medio electrónico y se considera seguir manejando de esta forma los requerimientos, porque se apuesta mucho por el ahorro del papel.
	Pregunta 6. ¿Maneja algún tipo de información confidencial, y que medidas de seguridad utiliza para su resguardo?	Sí, hay códigos de seguridad de información; actualmente se está en una campaña de divulgación de este código, las medidas de seguridad son bastante fuertes y las sanciones también.

Gerente Financiero	**Pregunta 5:** ¿Cuál es la forma en que la entidad informa a los usuarios sobre restricciones de uso de información confidencial?	Hay varias formas como correos electrónicos a través del correo institucional, publicaciones en las pizarras informativas y también se hacen sesiones como tipo seminarios para dar este tipo de capacitaciones.
	Pregunta 7: ¿Considera que el software con el que se cuenta actualmente es adecuado para que la información sea integra, atentica y confidencial?	Actualmente no, creería que, trabajando un poco más en el desarrollo en unos 6 meses o 1 año en ciertos módulos, pienso que, si estaría totalmente listo, porque aún está en proceso de implementación. Pero si cuenta con niveles de seguridad bastante buenos.
Contador General	**Pregunta 4:** ¿Que medios o dispositivos utiliza para transferir información de forma segura?	Ninguno, excepto por la declaraciones e informes de impuestos cuando se tenía que presentar de forma digital, pero ahora ya todos están en línea, anteriormente por ejemplo el informe 987 (Informe sobre proveedores, Clientes, Acreedores y Deudores) se presentaba en físico, todos esos formularios se pasaban por correo al área de TI y ellos lo guardaban dentro de una USB.
Asistente Contable	**Pregunta 10**: ¿Cómo protegen la información proveniente de los clientes que es considerada confidencial?	Los expedientes de los clientes donde está toda la información se mantienen en una bodega bajo llave.
Gerente de Venta	**Pregunta 6.** ¿Qué medios utilizan para solicitar información personal de los clientes?	Cuando las vendedoras están cerrando una venta ellas tienen un listado de toda la información a solicitar, aquí es donde es importante la carta para compartir información.

Análisis: La seguridad de la red se realiza por medio de Web Rules que limita la navegación en sitios web, además se controla la instalación de software inusual. La transferencia de información se solicita por medios escritos y correos electrónicos, pero el traspaso por medio de dispositivos no se realiza de forma segura, esto representa un riesgo ya que los datos pueden ser interceptados, copiados, modificados y hasta destruidos. Los entrevistados manejan información confidencial, se les informa sobre el uso restringido de está por medio de correos electrónicos, publicaciones en pizarras informativas y también por seminarios; la protección de estos datos se realiza por medio de expedientes almacenados en una bodega bajo llave, sin embargo, los medios de resguardo no son suficientes ni garantizan la integridad y confidencialidad de la información.

CAPITULO III. PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA FINANCIERA DE EMPRESAS COMERCIALIZADORAS DE AUTOMÓVILES.

3.1. DESARROLLO DEL CASO PRÁCTICO.

La propuesta de un plan para la seguridad de la información para empresas dedicadas a la comercialización de vehículos proporciona una herramienta que sirve de directriz más detallada para los recursos humanos, sobre todo para el profesional en contaduría pública que es quien maneja la información más sensible y vulnerable dentro de las entidades y la que influye a la toma de decisiones.

Este plan tiene por finalidad gestionar la integridad, confidencialidad y disponibilidad de la información, en el cual se cuenta con políticas especiales y manuales que detallan sobre cómo llevar a la práctica el cumplimiento de las mismas y la colaboración de los empleados en la materia. Por lo que inicialmente son las empresas, las que deben comprometerse a dar a conocer a todos sus miembros lo establecido en los controles y generar una cultura de buenas prácticas para la protección de la información financiera como de los sistemas de información.

3.2. LIMITANTES.

Las limitaciones en la aplicación del plan de seguridad de la información en las empresas comercializadoras de automóviles son:

- Falta de garantía en la colaboración de todo el personal en aplicar correctamente los controles, lo que conlleva en deficiencias de seguridad de información.
- No seguir un proceso de mejora continua sujeto cambios en la empresa y/o actualizaciones de estándares actuales aplicados.

- Falta de compromiso por la alta gerencia.
- Falta de asignación de un presupuesto o de recursos para la implantación de un plan de seguridad de la información, porque se piensa que es un posible gasto.
- Designación de un responsable sin la preparación y experiencia adecuada.

3.3. OBJETIVO.

Presentar un Plan de Seguridad de la Información, enfocado a generar condiciones de protección de los activos informáticos en su integridad, confidencialidad y disponibilidad en las empresas comercializadoras de automóviles del Municipio de Antiguo Cuscatlán, con el fin de incrementar la seguridad en los procesos clave del área financiera.

3.4. GENERALIDADES DE LA EMPRESA.

En los últimos años el aumento de la demanda vehicular a nivel Centroamericano ha ido de la mano con la eficiencia en que los retailers puedan satisfacer al consumidor final, dejando una huella global, apalancada en toda la cadena de valor para entregar un producto sostenible y de gran valor, seguridad en las transacciones, agilidad en trámites, tiempos de respuesta, entre otros.

Para desarrollar el plan de seguridad de la información fue necesario seleccionar a una de las empresas dedicadas a la comercialización de vehículos ubicadas en el Municipio de Antiguo Cuscatlán, el cual está dirigido para evaluar sus procesos y diseñar controles específicos para el resguardo de la información financiera.

NCN, S.A de C.V es una empresa emergente en el mercado automotriz como distribuidor de vehículos de lujo, tiene presencia en El Salvador desde hace más de 20 años con un trayecto de innovación e introducción de nuevos modelos en sus líneas VIP y comercial todo terreno.

Incorpora en su modelo de negocio la mercadotecnia esto ayuda al proceso de hacer y construir una marca, la línea comercial aporta al desarrollo del país contando con unidades de transporte pesado y el transporte público.

NCN, S.A de C.V busca mejorar continuamente garantizando la satisfacción a los clientes, y poder potenciar la presencia de sus servicios y productos en el mercado salvadoreño desarrollando la venta de vehículos usados, taller de enderezado y pintura para todas las marcas.

a. Misión

Brindar apoyo al desarrollo social ofreciendo calidad y el mejor servicio.

b. Visión

Ser el mayor distribuidor de marcas Premium a nivel mundial.

c. Estrategia

Buscamos incorporar la calidad y excelencia como nuestra mayor prioridad en cada etapa de la cadena de valor, y la confianza en cada proceso.

Figura 3: *Estrategia de NCN, S.A de C.V*

a. Valores

Servicio: La satisfacción del cliente es lo primordial.

Innovación: Ofrecemos las últimas novedades en el mercado automotriz.

Confianza: Brindamos la mayor confiabilidad al cliente en nuestros productos y servicios.

Responsabilidad: Actuamos y nos comprometemos con el cumplimiento de derechos y obligaciones.

Excelencia: Disponemos todo nuestro potencial para obtener los mejores resultados.

Respeto: Valoramos cada cliente, colaborador y proveedor.

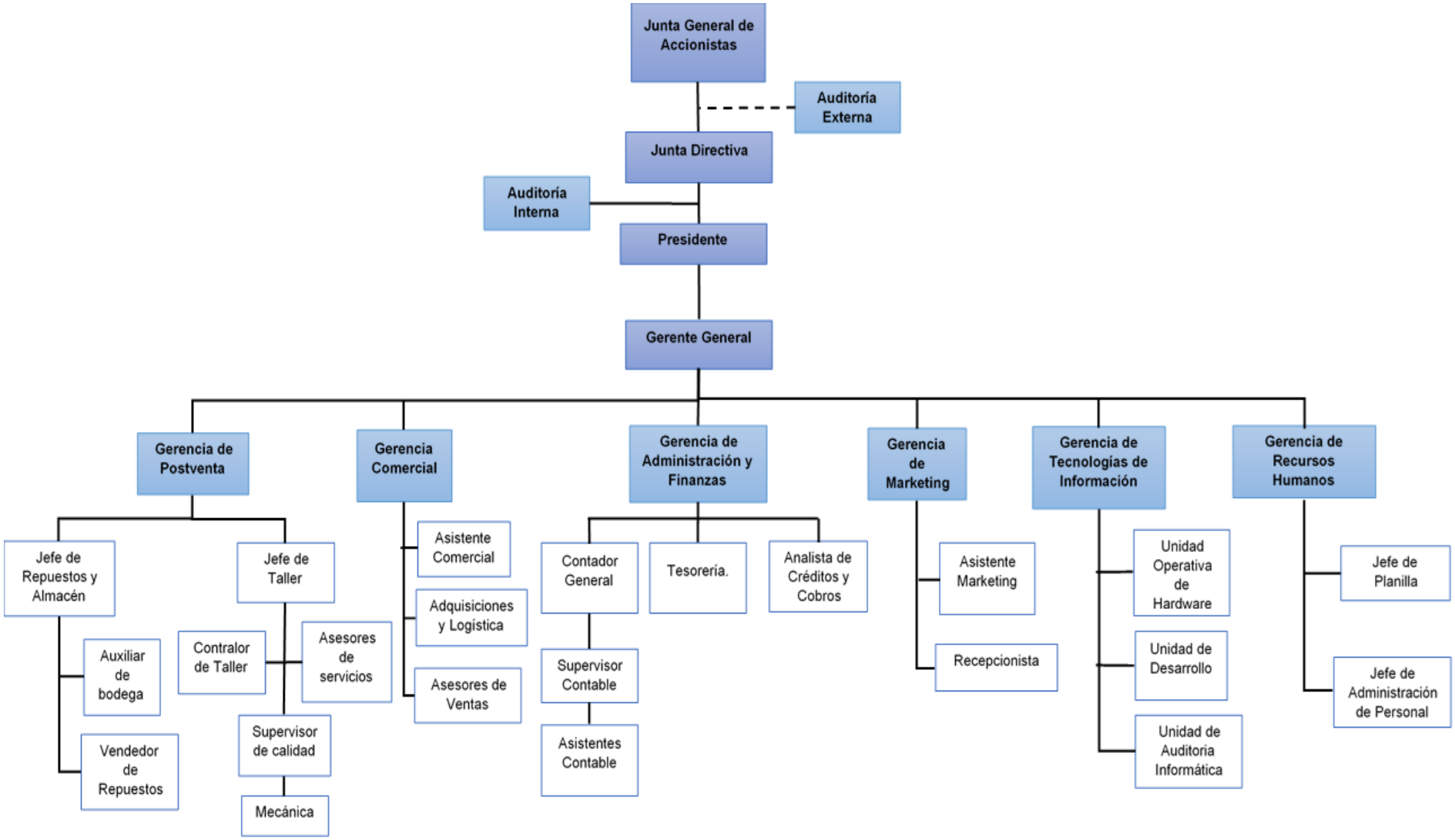
b. Aliados estratégicos

Tenemos asociaciones de larga data con los principales grupos fabricantes de equipos originales de automoción del mundo. Estas valiosas asociaciones permiten una línea de productos consistentemente sólida en toda la empresa.

Hemos representado a Toyota, en el Reino Unido, Hong Kong y Singapur, Mazda en Hong Kong y Mercedes-Benz y Volkswagen en el Reino Unido.

Figura 4: *Aliados estratégicos de NCN, S.A de C.V*

c. Organigrama propuesto.



Hecho por grupo de investigación.

PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA FINANCIERA DE EMPRESAS COMERCIALIZADORAS DE AUTOMÓVILES DEL MUNICIPIO DE ANTIGUO CUSCATLÁN

Índice

Índice de Tabla

A. Introducción.

El objetivo de la seguridad de la información es proteger la información de las empresas, a través de la aplicación de medidas adecuadas, como políticas de seguridad que ayuden a cumplir el objetivo de las empresas, protegiendo sus activos de información, sus sistemas y sus recursos financieros.

El contar con seguridad de la información es fundamental para asegurar la confidencialidad, disponibilidad e integridad de las operaciones de las entidades, con lo que se evita una diversidad de acciones que se pueden cometer; como el uso inadecuado, difundir la información, distorsionarla, realizar modificaciones o hasta eliminarla.

El documento que se presenta como políticas de seguridad de la información, pretende ser el medio por el cual se establezcan controles, procedimientos y normas que prevengan y resguarden los datos contra amenazas y vulnerabilidades. Los controles y políticas, sirven como una referencia y están sujetas a cambios, revisiones y mejoras en cualquier momento, según lo consideren las empresas a quienes va dirigido este documento, siempre y cuando se mantenga presente los objetivos de la seguridad de la información.

B. Objetivo.

El presente plan está diseñado para cumplir con los requisitos de seguridad de información financiera:

1. Disponibilidad: Deberá estar disponible en el momento en que se requiera. (Politica de Seguridad, 2017)
2. Confidencialidad: Sólo podrá ser accedida por los usuarios autorizados. (Politica de Seguridad, 2017)
3. Integridad: Sólo podrá ser modificada por las personas, procedimientos o sistemas informáticos autorizados para hacerlo. (Politica de Seguridad, 2017)

C. Alcance

El Plan de Seguridad de la Información contiene políticas y controles, las cuales deben ser implementadas por los colaboradores que laboran o tengan relación con las empresas comercializadoras de automóviles, para contribuir a la obtención de un nivel razonable de protección en su información.

D. Responsabilidad por funciones.

La responsabilidad por funciones está determinada de la siguiente forma:

Encargado de Tecnología de Información.

El encargado de TI tendrá las responsabilidades siguientes:

- Responsable de velar por la seguridad de información, y mantener el plan actualizado, así como monitorizar los controles que se implementen para asegurar que las estrategias implementadas se están llevando correctamente.
- Coordinar y monitorear el cumplimiento de los controles de seguridad de la información en toda la entidad y en las operaciones o procesos realizados por terceros.
- Participar junto con la Gerencia en el análisis de riesgo de la información de la entidad.
- Participar en la revisión de la documentación relacionada con la operación del Plan de Seguridad en las áreas de la entidad.
- Reportar oportunamente las vulnerabilidades e incidentes de seguridad siguiendo los lineamientos establecidos en el plan de seguridad.
- Contribuir a la divulgación y cumplimiento de las políticas, controles, lineamientos o procedimientos establecidos en el plan.
- Garantizar el soporte de información a los usuarios de los sistemas.

Gerente Financiero.

El Gerente Financiero de la entidad tendrá las responsabilidades siguientes:

- Cumplir y hacer cumplir lo establecido en el plan de seguridad de la información.
- Aprobación de las medidas necesarias para gestionar el riesgo asociado a los sistemas de información.
- Incorporar a las actividades de trabajo los procedimientos de seguridad financiera.

- Evaluar las tendencias en seguridad que afectan el estado financiero de la empresa y planificar nuevas estrategias.
- Supervisar el cumplimiento de implementación de las medidas correctivas y los requisitos señalados en las auditorías.
- Contribuir a la divulgación y cumplimiento de las políticas, controles, lineamientos o procedimientos establecidos en el plan en su área financiera.
- Salvaguardar de forma razonable la confidencialidad, integridad y disponibilidad de la información bajo custodia.
- Trabajar en conjunto con el Gerente de TI en el desempeño de las funciones asignadas.

Gerente Comercial.

El Gerente Comercial de la entidad tendrá las responsabilidades siguientes:

- Velar por la realización del almacenamiento correspondiente, como de la confidencialidad de la información que es brindada por la entidad y como por los clientes.
- Contribuir a la divulgación y cumplimiento de las políticas y controles establecidos en el plan.
- Salvaguardar de forma razonable la confidencialidad, integridad y disponibilidad de la información bajo custodia.
- Garantizar la adecuada realización y registro de los costos y gastos de venta.
- Informar sobre variaciones, realización y registro del inventario de vehículos.

- Garantizar el stock de vehículos en sala de ventas.
- Elaborar informes de ventas semanales, mensuales y trimestrales.
- Realizar exhibiciones especiales y eventos
- Garantizar que los reclamos de los clientes sean atendidos de una manera profesional y eficiente.

Contador General.

El Contador General de la entidad tendrá las responsabilidades siguientes:

- Mantener y cumplir los lineamientos del Plan de Seguridad de la Información dentro del área contable conforme a los principios éticos.
- Reportar a Gerencia de Administración y Finanzas oportunamente las vulnerabilidades e incidentes de seguridad, siguiendo los procedimientos establecidos.
- Dar seguimiento a las actividades de seguridad en los procedimientos de trabajo.
- Colaborar en la realización de las auditorías.
- Verificar la exactitud y cotejar de acuerdo a los parámetros empleados en la generación de reportes contables u otro tipo de reporte relacionado al negocio.
- Asegurarse que los procesos bajo su responsabilidad, incluyan las medidas de seguridad adecuada y consistente con la política de seguridad de la información.
- Salvaguardar de forma razonable la confidencialidad, integridad y disponibilidad de la información bajo custodia.

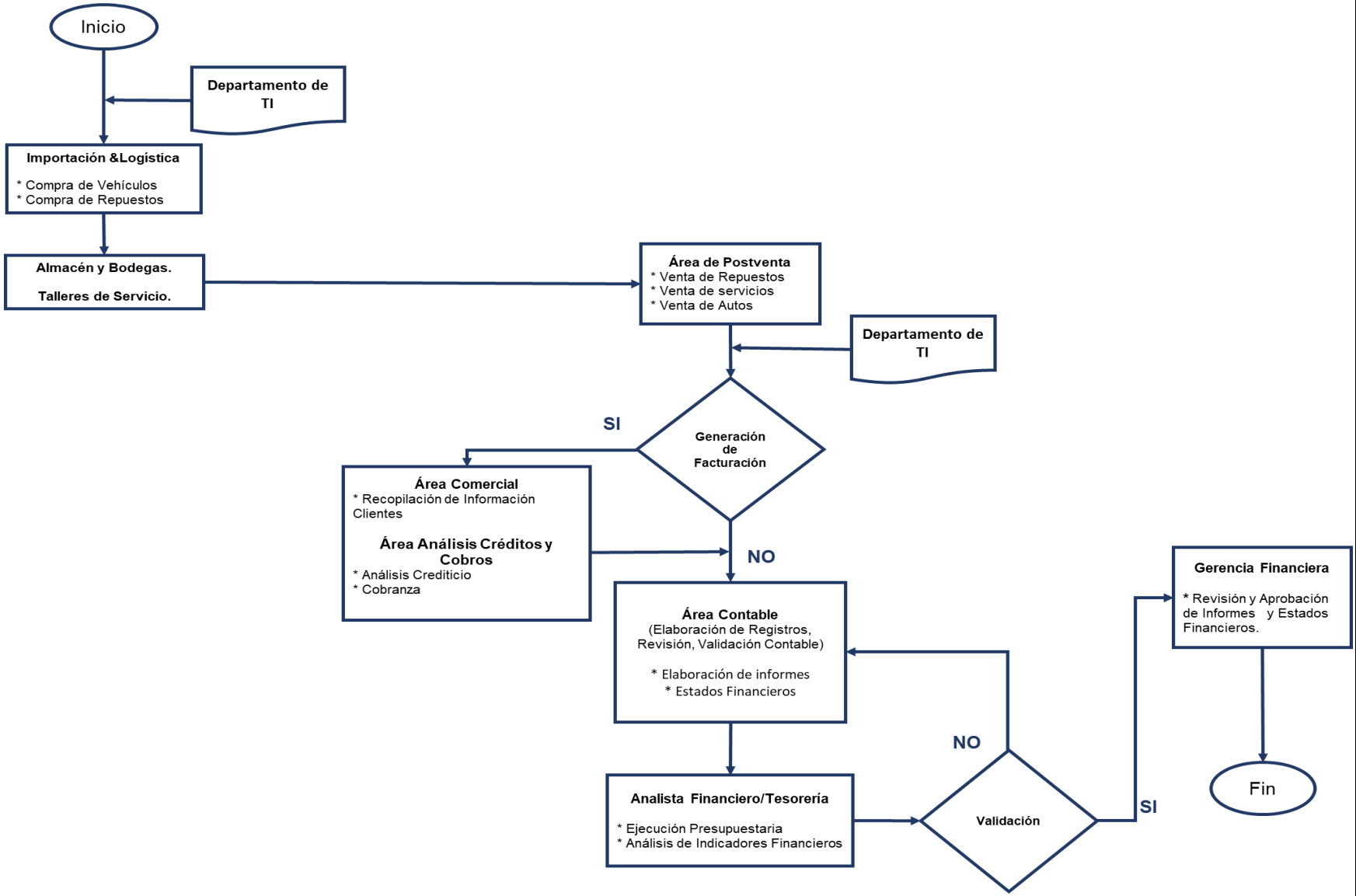
- Asumir responsabilidad por actos de negligencia que resulten de la corrupción, destrucción o divulgación de los datos.

Asistente Contable.

El Asistente Contable de la entidad tendrá las responsabilidades siguientes:

- Aplicación e implantación de la confidencialidad en aspectos contables y financieros del proceso de información gerencial.
- Gestionar con su jefe inmediato los recursos para el tratamiento y aceptación de los riesgos de la información.
- Cumplir los requisitos y ejecutar las mejoras y acciones correctivas señaladas en las auditorias.
- Mantener buenos hábitos como usuario en los sistemas y asegurarse que los procesos bajo su responsabilidad, incluyan las medidas de seguridad adecuada y consistente con la política de seguridad de la información.
- Participar en la identificación de los riesgos de su área de trabajo y en la generación de acciones de mejora para su prevención.

E. Flujograma de Información



Hecho por grupo de investigación.

F. Marco Técnico.

Tabla 1: Marco Técnico

NORMA	DESCRIPCIÓN
ISO/IEC 27001:2013	Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requerimientos
COBIT 2019.	Marco de referencia para el gobierno y la gestión de la información y la tecnología dirigida a toda la empresa. Son guías de mejores prácticas dirigidas al control y supervisión de las tecnologías de información (TI). (ISACA, 2019)
Biblioteca de Infraestructura de Tecnologías de la Información (ITIL V3)	Marco de referencia para un conjunto de conceptos y mejores prácticas referentes a la gestión de servicios de Tecnologías de la Información. (Blog H. , 2019)

G. Responsabilidad.

La aplicación correcta de las políticas y controles establecidos en el presente plan de seguridad de la Información es responsabilidad de cada colaborador de las empresas dedicadas a la comercialización de vehículos, lo que dependerá de la capacitación y concienciación permanente. Pero es exclusivo de la Junta Directiva en conjunto con el Gerente de TI, aprobar las políticas de seguridad de la información, publicarlas y comunicarlas a todos los empleados entidades externas pertinentes, teniendo en cuenta que la seguridad de la información es una cuestión crítica para el negocio.

H. Nivel de actuación

El plan de seguridad de la información propuesto se basa inicialmente en la política general aprobada por la Junta Directiva que se basa en garantizar la credibilidad y apoyar el cumplimiento de las normas o controles para la seguridad de la información; y las políticas especiales o secundarias que se tratan de políticas de carácter más específico y con bastante detalle, son directivas técnicas y reglamentaciones relativas a los elementos de TI y de cualquier aspecto relacionado con la seguridad de la información; y finalmente los manuales o indicaciones prácticas, que son procedimientos comprensibles que buscan aumentar el cumplimiento y la colaboración de los empleados, facilitándoles el trabajo en el ámbito del tratamiento de la información. **Anexo 4**

I. Vigencia.

Los presentes controles entrarán en vigencia cuando sean aprobadas por la Junta Directiva de las empresas comercializadoras de vehículos para su aplicación inmediata. Es recomendable realizar revisión y de ser necesario la actualización, al menos una vez al año o en el momento que se considere necesario.

J. Protocolos de actuación.

J. 1 Políticas especiales

POLÍTICA	**Política de seguridad de la información**
OBJETIVO:	**Establecer una política para la seguridad de la información acorde con el giro, requerimientos técnicos y legales de la entidad que sirva de guía y ejemplo para garantizar las dimensiones de la información.**
CONTROLES	
- Para confirmar el acuerdo de toda la organización con la seguridad de la información, se deberá crear una política general, la cual estará a cargo de la Junta Directiva de la entidad.	
- El Gerente General, Gerencia Administrativa y Financiera en conjunto con el Gerente de TI deberán aprobar las políticas de seguridad de la información, publicarlas y comunicarlas a todos los empleados y entidades externas pertinentes.	
- La principal finalidad de la política de seguridad de la información debe ser el involucramiento de los recursos humanos de toda la organización en la realización de esta tarea.	
- La política de seguridad de la información debe abarcar los procesos clave de la entidad, entre los cuales están: La calidad, disponibilidad y la privacidad, los controles internos, el uso de activos de TI, la ética y los derechos de propiedad intelectual.	
- El Gerente de TI, evaluará y actualizará las políticas, como mínimo anualmente, para encajar en entornos empresariales u operativos cambiantes.	
- La Gerencia General deberá asegurarse que las políticas para la seguridad de la información se adapten a la actividad económica de la empresa.	
- Evaluar la eficacia y el rendimiento de aquellas las partes involucradas a las que se le ha delegado responsabilidad.	
- La Junta Directiva deberá definir los principios fundamentales de la asignación y gestión de recursos y capacidades, de forma que TI pueda satisfacer las necesidades de la empresa conforme a las prioridades acordadas y los límites presupuestarios	
- Entender los requisitos para el alineamiento de la gestión de recursos de TI con la planificación de recursos humanos (RR. HH.) y financieros de la empresa.	

POLÍTICA	**Organización de la seguridad de información**
OBJETIVO:	**Establecer medidas para la implementación y operación de la seguridad de la información dentro de la empresa, así como del teletrabajo.**
CONTROLES	
- La Junta Directiva debe establecer perfiles, definir y asignar todas las responsabilidades de seguridad de la información.	
- El Gerente General junto al Comité Gerencial deben documentar y definir los niveles de autorización.	
- Las personas con las responsabilidades en el área de seguridad de la información, deben ser competentes en el área y les deberán dar oportunidades de estar actualizados con el desarrollo.	
- Las funciones conflictivas y las áreas de responsabilidad deben de separarse para reducir las oportunidades de modificaciones o uso no autorizado o mal intencionado de los activos de la entidad.	
- Tener procedimientos vigentes que especifiquen cuándo y qué autoridades contactar, y como identificar y reportar los incidentes de seguridad de la información en el momento oportuno.	
- La Gerencia General en conjunto con la Gerencia de TI deben de mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	
- La seguridad de la información debe de integrarse en el método de gestión de proyectos de la entidad para garantizar que los riesgos de seguridad sean identificados y tratados como parte de un proyecto.	
- La Gerencia General en conjunto con el Gerente de TI deben establecer condiciones y restricciones para las actividades de teletrabajo.	
- El Gerente de TI debe tomar en cuenta requerimientos de seguridad para el acceso remoto a sistemas internos de la empresa, para la información accedida y que se transmite por enlaces de comunicación.	
- La entidad debe facilitar equipo tecnológico preparado con los estándares de seguridad previamente establecidos por esta.	
- El usuario no deberá compartir información confidencial con familiares.	
- No se deberá usar el equipo asignando para labores externos a la entidad.	
- No se permita el uso de equipo de propiedad privada, que no se encuentre bajo el control de la empresa, además de considerar una adecuada comunicación, incluyendo los métodos para asegurar el acceso remoto.	
- La Gerencia de TI debe suministrar soporte y mantenimiento de hardware y software a todo dispositivo utilizado para teletrabajo.	
- Cuando las actividades de teletrabajo finalicen se debe revocar los derechos de acceso al sistema, y coordinar el regreso de los equipos utilizados en las actividades de trabajo.	
- Al utilizar dispositivos móviles, se debe tener cuidado para garantizar que la información de negocios no se vea comprometida, y protegerse contra robos.	
- En general, para esta política se debe considerar lo siguiente:	

a. Llevar registro de dispositivos móviles. b. Protección física c. Restricción de instalación de softwares. d. Restricción de la conexión a los servicios de información. e. Controles de acceso a los dispositivos. f. Técnicas criptográficas. g. Desactivación, eliminación o bloqueo a distancia. h. Realizarse copias de seguridad de los dispositivos.
- Los dispositivos que lleven información importante, confidencial o critica de la empresa no se deben dejar desatendidos, y cuando sea posible ser físicamente bloqueados o utilizarse bloqueos especiales para asegurar los dispositivos.
- Al personal que utiliza dispositivos móviles se debe proporcionar capacitación sobre riesgos adicionales procedentes de actividades de trabajo.
- La Gerencia de TI debe establecer medidas de seguridad cuando se permita el uso de dispositivos móviles privados, considerando la separación de uso privado y de la empresa.
- El personal que utiliza equipos de tecnología de la información debe de firmar un acuerdo de confidencialidad, comprometidos a la no divulgación de datos críticos de la compañía, clientes y proveedores.
- Toda la información contenido en los equipos de cada colaborador asignado son propiedad de la compañía y esta puede disponer de esta según convenga.

POLÍTICA	**Seguridad de los recursos humanos**
OBJETIVO:	**Asegurarse que los colaboradores desarrollen sus funciones con calidad y conciencia en sus funciones, como en la seguridad de la información desde el inicio hasta el fin de su contrato.**
CONTROLES	
– Realizar indagaciones y verificar las referencias acerca de los antecedentes de los postulantes al empleo, a cargo de la Gerencia de Recursos Humanos, de acuerdo con las leyes, regulaciones y normas de ética correspondientes.	
- Los acuerdos contractuales con empleados y contratistas emitidos por la Gerencia de Recursos Humanos deben establecer las responsabilidades de los colaboradores y de la organización para la seguridad de la información.	
- La Gerencia de Recursos Humanos, se asegurará de verificar que, al darse una nueva contratación, la persona cumpla con el perfil del puesto requerido.	
- La Junta Directiva, mediante la aprobación de la Política de Seguridad de la Información requerirá que los empleados apliquen la seguridad de la información en concordancia con las políticas y controles establecidos por la organización.	
- La Gerencia de Recursos Humanos debe transmitir a los empleados las expectativas de la Junta Directiva sobre cómo deben actuar en materia de seguridad de la información desde una perspectiva de procedimiento.	
- La Gerencia de TI en conjunto con la Gerencia de Recursos Humanos deben definir los modelos de acuerdos de confidencialidad entre la organización y los empleados para articular obligaciones específicas en cuanto a la protección de la información de la entidad, incluyendo compromisos y las penalidades por el incumplimiento de dichos acuerdos.	
- La Gerencia de Recursos Humanos, tiene la obligación de realizar una apropiada concientización, capacitación y actualización periódica y, cuando sea pertinente, de las políticas y procedimientos organizacionales.	
- La Gerencia contratante de un nuevo colaborador, debe realizar la clasificación de la información a la que va a acceder el candidato y los riesgos asociados.	
- Debe existir un proceso disciplinario formal establecido por la Gerencia General y la Gerencia de Recursos Humanos; en actuación en contra de empleados que cometan violación a la seguridad de la información, como también medidas positivas hacia a aquellos empleados con buen desempeño.	
- La Gerencia de Recursos Humanos deberá informar a cada empleado acerca de las sanciones que contraen las violaciones a la seguridad de la información: **Amonestación verbal, amonestación escrita, suspensión de labores y destitución de su trabajo.** Así como también, la clasificación de las faltas cometidas: • **Faltas leves:** El hecho de no aplicar una política de seguridad de la información, que no tenga repercusiones económicas ni un impacto material para la empresa. • **Faltas graves**: El hecho de no aplicar una o varias de las políticas de seguridad de la información, y que las repercusiones afecten la economía en un grado no significativo para la empresa y ocasione cierto impacto a la empresa.	

• **Faltas muy graves:** El hecho de no aplicar una o varias de las políticas de seguridad de la información, y que las repercusiones afecten la economía en un grado muy significativo para la empresa y ocasione grave impacto a la operación e imagen de la empresa.
- La Gerencia General y la Gerencia de Recursos Humanos, deben determinar cuáles serán las responsabilidades y funciones de la seguridad de la información que van a permanecer vigentes en caso de la terminación o cambio de empleo.
- El usuario debe estar informado que es responsabilidad propia realizar periódicamente copia de sus datos y mantenerlas en un lugar suficientemente seguro dentro de la empresa.
– La Gerencia General debe atraer y conservar las habilidades y el personal necesarios para la gestión de riesgos de TI.
– La Gerencia de TI, debe ordenar que los riesgos, oportunidades, problemas o preocupaciones puedan identificarse y comunicarse por cualquier persona a la parte correspondiente en cualquier momento.
– La Gerencia de Recursos Humanos deberá implementar prácticas de supervisión adecuadas, con el fin de asegurar que los roles y responsabilidades se ejerzan adecuadamente, que todo el personal tiene la autoridad y recursos suficientes para ejecutar sus roles y responsabilidades y revisar el rendimiento de cada uno.

POLÍTICA	**Gestión de Activos**
OBJETIVO:	**Identificar los activos y definir las responsabilidades apropiadas de protección, también asegurar que la información recibe el nivel de protección adecuado de acuerdo con su importancia en la organización.**
CONTROLES	
- La Gerencia de TI por medio de la Unidad Operativa de Hardware deberá de identificar y mantener un inventario de activos asociados con información e instalación de procesamiento. La identificación de activos de información puede diferenciarse entre: • Activos primarios: información de la entidad y soporte de la información. • Activos de soporte: Equipos informáticos, software, redes de comunicación, personal, instalaciones y equipos auxiliares. **Anexo 5.**	
- Los activos mantenidos en inventario deben ser asignados y mantener un registro formal de los usuarios autorizados a dichos activos.	
- La protección de los activos será responsabilidad de la Gerencia de TI, sin embargo, cada área y empleado será responsable de los activos que utiliza para desarrollar sus actividades laborales.	
- La Unidad Operativa de Hardware debe cerciorarse que los activos sean inventariados, catalogados y resguardados apropiadamente, además de poseer una clasificación de activos importantes e inspeccionar periódicamente las restricciones de acceso a estos.	
- La Gerencia Administrativa y Financiera en conjunto con el Gerente de TI deben comprobar la existencia de todos los activos adquiridos mediante conciliaciones regulares de inventario físico y lógico.	
- La Gerencia General en conjunto con la Gerencia de TI deberán definir e implementar reglas, documentarlas y establecer el grado de aceptación para el uso de la información y de los activos de información.	
- La Unidad Operativa de Hardware se encargará de determinar regularmente si cada activo continúa proporcionando valor. De ser así, estimar la vida útil esperada durante la que proporcionará valor.	
- Asegurarse que, una vez terminado el contrato, los empleados deben entregar de manera formal todos los activos informáticos asignados propiedad de la empresa.	
- Siempre que sea posible, reasignar los activos cuando ya no se necesiten debido a un cambio de rol del usuario, redundancia en un servicio o retirada de un servicio.	
- La información debe ser catalogada en términos de valor, condiciones legales, susceptibilidad y criticidad a alteraciones o difusiones no autorizadas. El valor de los activos de información se clasifica de acuerdo a su confidencialidad, sea de uso de la empresa o pública.	
- Los procedimientos para el etiquetado de activos de información serán responsabilidad de la Gerencia de TI de acuerdo al modelo de categorización adquirido por la empresa.	
- Se debe clasificar la información física a través del etiquetado o por medio de metadatos. Si se opta por este último, añadir los procesos y la infraestructura para especificar los metadatos sobre los archivos, que contribuya a fomentar y respaldar el intercambio de datos.	

- El etiquetado debe especificar lo siguiente: ▪ Código ▪ Tipo de activo ▪ Clasificación de la información. (si aplica) ▪ Área que lo utiliza. ▪ Descripción del activo. ▪ Responsables del activo.
- La Gerencia de TI debe de verificar, probar y registrar todos los activos de forma controlada, incluyendo etiquetas físicas, cuando se requiera.
- Conservar un inventario de todas las licencias de software obtenidos.
- Ejecutar con regularidad auditorías para identificar la cantidad de softwares con licencia instaladas.
- La Gerencia de TI con autorización de Gerencia General, dispondrá de los activos de forma responsable cuando ya no sean de utilidad debido a la retirada de todos los servicios relacionados, tecnología obsoleta o la falta de usuarios, teniendo en consideración el impacto medioambiental.
- Se debe implementar técnicas de criptografía a todos los correos electrónicos o en su defecto, medios extraíbles para garantizar la confidencialidad e la integridad de la información que se comparte.
- Reemplazar softwares y dispositivos de almacenamiento en un periodo conveniente para prevenir el deterioro de información necesaria e importante.
- Proteger la información almacenada con copias de seguridad en soportes independientes.
- Mantener un registro de dispositivos que han sido dados de baja de forma segura por contener información sensible.
- Establecer un inventario de medios extraíbles de almacenamiento para reducir la viabilidad de pérdida de información.
- La transferencia de datos a medios extraíbles debe ser controlada o restringida de acuerdo a la categorización de valor de la información.
- Los medios que contiene información confidencial deben de almacenarse y eliminarse de forma segura, por ejemplo, mediante la incineración o trituración, o el borrado de datos de uso por otras aplicaciones dentro de la entidad.
- Se debe implementar medidas para prevenir el acceso no autorizado, modificación o corrupción de la información transmitida por medios físicos.
- Para transportar información por medios físicos se debe conservar un registro de transportistas o mensajeros autorizados, además de utilizarse una sobrecubierta para proteger de cualquier daño o manipulación que puede ocasionar durante el trayecto.

POLÍTICA	**Control de Acceso**
OBJETIVO:	**Establecer mecanismos eficientes de controles de accesos a la información**

CONTROLES

- El Gerente General en conjunto al Gerente de TI deberá nombrar un administrador de sistemas quien será responsable de implementar, configurar, mantener, documentar y asegurar el correcto funcionamiento del sistema y controles de accesos.
- El administrador del sistema habilitara la entrada al perfil personal de cada usuario habilitando una contraseña provisional de acceso que dé lugar al cambio posterior de esta.
- La responsabilidad de establecer una contraseña y de alto nivel de seguridad será del usuario final.
- Las contraseñas de usuarios finales y de sistema deberán cumplir las siguientes características:
    - Debe estar conformado por 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales como por ejemplo (*,0 #, @, etc.)
    - No establecer contraseñas las cuales sean fácil de descifrar u obtener basándose en información personal, por ejemplo, nombres de familiares, números telefónicos, fechas de nacimiento, etc.
    - No consistir en palabras que existan en los diccionarios.
    - No tener caracteres consecutivos idénticos, sean de solo caracteres numéricos o de sólo alfabéticos.
- El Gerente de TI deberá contar con una base de datos de contraseñas de los usuarios la cual tendrá acceso el Gerente General.
- Cada gerencia deberá otorgar en conjunto con el departamento de TI los permisos de acceso limitado solamente a la información necesaria para hacer un trabajo, tanto a nivel físico (acceso a instalaciones o soportes de datos), como lógicos (acceso a aplicaciones).
- Se debe contar con un registro de usuarios y de cancelación para permitir la asignación de derechos de acceso, que debería incluir los ID o cuentas de usuarios donde se vincule o identifique el usuario.
- Los ID deben desactivarse automáticamente o de forma inmediata cuando el usuario abandone la entidad. Los ID redundantes nunca pueden ser asignados a otros usuarios y se debe realizar una eliminación periódica de usuarios redundantes.
- El proceso de cancelación debe tomar en cuenta la revocación del ID del usuario y de los permisos.
- Debe de controlarse la asignación de información de autenticación secreta a través de un proceso de gestión formal, el cual debe incluir:
    - Una declaración firmada de cada usuario.
    - Se brindará información de autenticación secreta al inicio de su contrato, en la cual se obligan a cambiarla a partir del primer uso.
    - Comprobar la identidad del usuario antes de facilitar información considerada secreta.
    - Cuando se asigne a los usuarios información de autenticación secreta deberá ser en forma temporal y segura.

- Se deberá revisar periódicamente los accesos de los usuarios y verificar las asignaciones otorgadas.
- Las credenciales de acceso deben ser examinadas y reasignadas cuando se traslade un empleado a otra área de la entidad.
- Los usuarios deben ser advertidos sobre: • Mantener secreto la información de autenticación confidencial, asegurando que no se divulga a otras partes. • Prevenir la suplantación de identidad a través de registros de accesos y contraseñas, a menos que se almacene en lugares y con métodos aprobados como seguros. • Cambiar la información de autenticación secreta siempre que existan indicios de su posible compromiso.

POLÍTICA	**Criptografía**
OBJETIVO:	**Asegurar el fiel cumplimiento de los procedimientos de criptografía con el fin de contribuir a la confidencialidad, autenticidad e integridad de la información que se comparte.**

CONTROLES

- Estará a cargo de la Gerencia de TI la creación y ejecución de una política en la que se determine y explique las funciones de los controles criptográficos.
- La Gerencia de TI es la encargada de ejecutar una política que contenga las condiciones para emplear, resguardar y la permanencia de las claves con criptografía.
- La Gerencia de TI será la responsable de realizar una implementación de cifrado para la protección de información transportada por medios extraíbles, dispositivos móviles o a través de líneas de comunicación.
- Desarrollar un enfoque de administración de claves criptográficas, que trate acerca del proceso de apertura, resguardo, división, y restauración, esta última en el caso de ser estrictamente necesario.
- Se debe seguir el proceso idóneo para la gestión de claves, en el que incluya el ciclo de vida de una clave, siendo es el siguiente:
    - Generación de claves.
    - Pre activación
    - Activación y protección
    - Distribución
    - Custodia
    - Destrucción
- Seleccionar los algoritmos criptográficos, las longitudes de las claves y las prácticas de uso.
- Las claves criptográficas deberán contar con controles que garanticen la protección contra modificación y pérdida de las mismas.
- Las claves secretas y privadas necesitan la protección contra el uso no autorizado, así como contra la divulgación.
- Se debe garantizar la seguridad física del o los equipos que se utilizan para originar, guardar y clasificar las claves criptográficas.
- Para reducir la probabilidad del uso inadecuado, las fechas de activación y desactivación de claves deben ser definidas de modo que solo puedan ser usadas durante un periodo limitado de tiempo.
- La Gerencia de TI deberá llevar un registro del personal a quien se les comparte información confidencial, además de un registro de contraseñas.

POLÍTICA	**Seguridad física y ambiental**
OBJETIVO:	Prevenir el acceso físico no autorizado y garantizar el uso adecuado del equipo de generación de información.
CONTROLES	
- Los colaboradores deberán tener de credenciales de identificación y acceso para apertura y cierre de puertas, entrada y salida a los distintos sectores de la empresa en función de las necesidades derivadas de la actividad profesional.	
- En caso de extravió de tarjeta de acceso o credenciales se repondrá con un costo adicional por parte del empleado	
- Todas las instalaciones incluidas las instalaciones externas a la Administración, debe tener mecanismos de seguridad física que permitan • Controlar la accesibilidad de personas a las instalaciones y restringir el acceso a las áreas donde se procesa o almacene información. • Asegurar la protección de los recursos informáticos.	
- Contar con una bitácora de visitas a las instalaciones, que contenga fecha y hora de entrada y salida de las personas.	
- Sólo se permitirá el acceso por propósitos específicos y autorizados a los cuales se les deberán emitir las instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia.	
- Todos los usuarios empleados, contratistas y terceras personas y todos los visitantes usen de forma visible la identificación de no ser así se deberá notificar inmediatamente al personal de seguridad si se encuentra a un visitante no acompañado y cualquiera que no use una identificación visible.	
- El equipo informático se deberá mantener en concordancia con las medidas de seguridad y especificaciones de servicio recomendados por el proveedor.	
- Disponer de muebles y armarios bajo llave en las salas de equipamiento informático y oficinas administrativas.	
- Los equipos de comunicaciones y servidores, sistemas de audio y vídeo deben de estar instalados en un lugar con acceso restringido y con sistemas de seguridad tanto eléctricos y contra incendios.	
- Los escritorios de oficinas y salas de reuniones deberán mantener los artículos necesarios para laborar.	
- No se permitirá la acumulación de papelería durante la jornada laboral.	
- Se deberá registrar el material que ingresa a bodegas con los procedimientos de gestión de activos a su ingreso al local	
- El equipo informático o software no se retirará de las instalaciones sin previa autorización del jefe inmediato tomando en cuenta los siguientes lineamientos: • Los usuarios empleados y terceras personas que tienen la autoridad para permitir el retiro de los activos fuera del local debieran estar claramente identificados. • Se establecerá límites de tiempo para el retiro del equipo y se debieran realizar un chequeo de la devolución • El equipo deberá ser registrado como retirado del local de igual forma su retorno.	

POLÍTICA	**Seguridad de las operaciones**
OBJETIVO:	Garantizar el correcto acceso a los equipos de comunicaciones, como también a los sistemas de información que utiliza la compañía.
CONTROLES	
- Es obligación de cada colaborador procesar y manejar la información con una estricta confidencialidad.	
- Evaluar periódicamente la eficiencia de los mecanismos para garantizar la precisión y confiabilidad de informes obligatorios.	
- La unidad de Desarrollo deberá elaborar el borrador de una hoja de ruta para la implementación de prácticas y actividades de proceso faltante para ser aprobado por la Gerencia General.	
- Proporcionar las directrices para garantizar la clasificación adecuada y consistente de los elementos de información en el área financiera.	
- El departamento de TI deberá mantener un inventario de información que incluyan una lista de dueños, custodios y clasificaciones.	
- Las jefaturas deberán identificar opciones para mejorar o rediseñar los procesos.	
- Los procedimientos de operación deben documentarse y ponerse a disposición de todos los usuarios que los necesiten; debiendo especificar las instrucciones de funcionamientos que incluyen: • Instalación y configuración de los sistemas. • El procesamiento y manejo de la información, tanto automatizada como manual. • Instrucciones para el manejo de errores u otras situaciones, que pudieran ocurrir durante la realización de la labor. • Soporte y contactos importantes en caso de inesperadas dificultades operacionales o técnicas. • Instrucciones para salida de información y manejo de medios, tales como la utilización de papelería especial o la gestión de salidas confidenciales incluyendo los procedimientos para la disposición segura de la salida de trabajos fallidos. • Procedimientos de reinicio y recuperación del sistema en caso de falla.	
- Cada Gerencia debe de llevar un registro e identificación de cambios significativos en procesos organizacionales.	
- Realizar una evaluación de los impactos potenciales de los cambios en operaciones, incluyendo los impactos en la seguridad.	
- Comunicar los detalles de cambios a todas las personas pertinentes.	
- Se debe identificar e implementar el grado de separación entre los ambientes de desarrollo, prueba y operación que es necesario para prevenir problemas operativos.	
- El personal del área de TI deberá tener las capacitaciones necesarias para que el personal dedicado a la tarea de detección de Software malicioso tenga los conocimientos necesarios.	
- El Gerente de TI establecerá procedimientos para las tareas de mantenimiento y las situaciones de emergencia.	

- La unidad de desarrollo establecerá sistemas de monitoreo de software y las comunicaciones. (datos)
- Se debe hacer backup periódicamente, de los datos más sensibles de la compañía y almacenarlos al menos en un lugar diferente de donde están los servidores, para salvaguardar cualquier daño de un desastre en el sitio principal.
- Cerciorar que las copias de seguridad posean un alcance que envuelva todas las condiciones de respaldo de su información: • Datos e información sensible • Softwares y aplicaciones • Datos de configuración de aplicaciones, sistemas etc. • Datos sobre usuarios, accesos, claves etc. • Registros de actividades, eventos, mensajes o alarmas del sistema.
- Verificar que los documentos de soporte cumplan con las funciones requeridas, garantizando su utilidad cuando sean necesarios.
- La Unidad de Desarrollo deberá implementar medidas de respaldo por medio del cifrado.

POLÍTICA	**Seguridad de las comunicaciones**
OBJETIVO:	**Mantener la seguridad de información en redes y al momento de ser transferida dentro de la compañía y con otras entidades ajenas a la compañía.**
CONTROLES	
- Mantener controles al menos aplicando las mejores prácticas en los sistemas de comunicaciones.	
- Los equipos de comunicación deben estar gestionados y administrados por especialistas internos o subcontratados, para garantizar la seguridad, la consistencia y disponibilidad de las comunicaciones.	
- Las redes deben controlarse y gestionarse adecuadamente para proteger la información de los sistemas y aplicaciones, así mismo garantizar la seguridad en las redes y la protección de los servicios conectados no autorizados.	
- La Gerencia General en conjunto con la Gerencia de TI deberán establecer responsabilidades y procedimientos para la gestión de los equipos remotos.	
- El Gerente de TI deberá revisar los contratos con los proveedores de servicios redes, que estos acuerdos incluyan mecanismos de seguridad, niveles de servicios y otros requisitos que deben identificarse para garantizar la seguridad de la información transmitida.	
- La Gerencia de TI deberá utilizar un método para controlar la seguridad de las redes y dividirlas en dominios de red separadas. La segmentación de redes debe ser de la siguiente manera: ▪ Red VPN (Virtual Private Network o Red Privada Virtual) ▪ Red LAN (Local Area Network o Red de Área Local) ▪ Red WAN (Wide Area Networks o Red de Área Amplia)	
- Admitir que solo dispositivos acreditados adquieran acceso a los sistemas, datos y red de la compañía, además de exigir la introducción de contraseñas para acceder a estos.	
- Los usuarios que ingresen a los sistemas de la organización mediante acceso remoto deben ser identificados antes de obtener acceso, por lo tanto, dicho acceso debe ser controlado por la Gerencia de TI que permita la autenticación al conectarse a la red de datos.	
- Encriptar la conexión (VPN) cuando los colaboradores se conecten desde el internet.	
- La Gerencia de TI deberá llevar a cabo pruebas de penetración al menos una vez al año para determinar la idoneidad de la protección de la red.	
- Establecer y mantener un manejo para la seguridad de la conectividad con base en las evaluaciones de riesgo y los requisitos del negocio.	
- Aplicar protocolos de seguridad aprobados a las conexiones de red.	
- Implementar mecanismos de filtrado de red, como firewalls, web filter, antispam y antivirus.	
- Deben existir acuerdos de intercambios de información para garantizar su uso y los niveles de protección. Los acuerdos deben tratar puntos tales como: ▪ La responsabilidad de las partes en el uso, protección y custodia de la información. ▪ Requisitos de cifrado.	

▪ Responsabilidades en cadena de custodia. ▪ Controles de acceso a la información.
- La Gerencia de TI se encargará de eliminar de forma segura los dispositivos de comunicaciones descartados.
- La Gerencia de TI es la encargada de gestionar el flujo de correos electrónicos con políticas de seguridad (mejores prácticas) en el servidor de correo electrónico, asegurándose que el servicio sea idóneo y seguro para las actividades que requieren el uso de correos electrónicos, respetando los principios de confidencialidad, integridad y disponibilidad.
- La información confidencial transmitida por correo electrónico debe ser controlada, además de solicitar una confirmación de entrega al receptor.

POLÍTICA	**Adquisición, desarrollo y mantenimiento de sistemas**
OBJETIVO:	**Relacionar la seguridad de la información como elemento fundamental de los sistemas de información.**
CONTROLES	
- Los requerimientos que la Gerencia General establezca deben incluirse cuando se adquieran nuevos sistemas de información, o se hagan mejoras a los sistemas existentes, lo que significa que la seguridad es prioridad, además de las funcionalidades requeridas.	
- La Gerencia de TI debe tener en cuenta las posibles fallas que se puedan ocasionar y el impacto que estas ocasionarían a la entidad.	
- Definir los parámetros para los casos de desarrollo de software y sistemas dentro de la entidad, a cargo de la Gerencia General en conjunto con la Gerencia de TI.	
- En la adquisición o desarrollo propio de sistemas, se deben considerar las especificaciones requeridas por la Gerencia General y las demás Gerencias, lo que contribuirá a cumplir con los procesos correctamente y con los pilares de la seguridad de la información.	
- Es responsabilidad de la Gerencia de TI, identificar la información sensible que debe ser reforzada en su resguardo al momento de adquirir, desarrollar o darle mantenimiento al sistema.	
- La Gerencia de TI debe tener en cuenta que antes de implementar o migrar a un sistema, revisar los debidos controles establecidos para garantizar la integridad de la información una vez puestos en marcha.	
- En la transmisión de información a través de redes públicas, la Gerencia de TI debe establecer controles estrictos que mitiguen los riesgos de internet.	
- La Gerencia de TI debe comunicar formal y oportunamente a las diferentes áreas de la compañía sobre la adquisición, desarrollo o cambios del sistema de información.	
- Se debe implementar la validación y verificación de autenticación en toda la cadena de transmisión de información, establecida por la Gerencia de TI junto con la aprobación de la Gerencia General.	
- La Gerencia de TI debe contar con guías en las que se documente sobre la actuación de cualquier cambio que se realice al sistema de información	
- Las Gerencias deben priorizar iniciativas para realizar mejoras continuas al sistema de información, basadas en los beneficios que conllevaría al sistema a constante adaptación de las operaciones.	
- Ante cualquier cambio introducido al sistema de información o la incorporación de nuevas aplicaciones o actualizaciones, es responsabilidad de la Gerencia de TI realizar pruebas y control de calidad.	
- La implementación de cualquier cambio en el sistema de información debe gestionarse mediante procesos de autorización, control de permisos y de planificación.	
- La Gerencia de TI debe llevar un control estricto de las versiones de software con las que cuenta la empresa.	

J.2 Manuales:

	Fecha de elaboración	**Diciembre 2020**
AF-01	Proceso	**Presupuesto**
Objetivo	Contribuir a la realización correcta, ordenada y segura del proceso de preparación, ejecución y administración del presupuesto.	
Campo de aplicación	Área Financiera	
Políticas específicas	La elaboración del presupuesto debe realizarse una vez al año en la fecha que el Gerente General lo establezca.	
	Es responsabilidad de la Gerencia de Administración y Finanzas proporcionar cada año los lineamientos aprobados por la Junta Directiva, estrictamente a los responsables de los centros de costos.	
	Para la elaboración del presupuesto se deben considerar los siguientes aspectos: Inflación, costo de la divisa, electricidad, impuestos, aranceles, tasas de interés activas bancarias, combustibles, cambios de precios, cambios de salarios, prestaciones y otros factores que puedan afectar las finanzas anuales.	
	La elaboración del presupuesto debe realizarse bajo los lineamientos definidos por la Gerencia General de la empresa.	
	La Gerencia de Administración y Finanzas es la responsable de coordinar la elaboración del presupuesto y de presentarlo ante el Gerente General.	
	El presupuesto debe estar autorizado por el comité ejecutivo designado y ratificado por la Junta Directiva.	
	Una vez aprobado el presupuesto, la Gerencia de Administración y Finanzas es la encargada de proporcionar a cada gerente el presupuesto de costos, gastos e inversiones del año.	
	Establecer una jerarquía para las autorizaciones de los gastos presupuestados, de acuerdo al centro de costos correspondiente.	
	Los gastos que no estén considerados dentro del presupuesto anual, deben ser autorizados por el Gerente General.	
	Los encargados de los centros de costos, deben reportar y justificar mensualmente cada variación en los gastos presupuestados	

	Fecha de elaboración	**Diciembre 2020**
AF-02	Proceso	**Cuentas por pagar**
Objetivo	Realizar el pago de las obligaciones adquiridas por la entidad de forma oportuna, cumpliendo con los requerimientos legales y fiscales.	
Campo de aplicación	Área Financiera	
Políticas específicas	Formas de pago: La entidad realizara los pagos mediante trasferencias bancarias y cheques.	
	Cada gerencia es responsable de la autorización de los gastos	
	La documentación para registro y tramite de pagos debe ser la siguiente: Comprobante de Crédito Fiscal o Factura de Consumidor Final o Factura de Sujeto Excluido debidamente firmada y sellada por quien recibió el bien o servicio, además de la autorización del Gerente de Administración y Finanzas.	
	Si el pago es a contratistas de servicio, se debe presentar el contrato que deberá estar firmado y autorizado por el Gerente General, Comprobante de Crédito Fiscal o Factura con sello y firma de recibido de la persona encargada de recibir el servicio.	
	Los pagos por gastos de viaje al exterior deben anexar memorándum autorizado por el gerente del área correspondiente, avalado por el Gerente General, detallando nombre de la persona, lugar de destino, fecha de salida y regreso y la solicitud del cheque.	
	Los pagos de planillas ya sea con abono en cuenta bancaria o emisión de cheques, debe anexar la planilla con detalle de sueldos, comisiones, vacaciones, etc. Y estar autorizado por el Gerente de Administración y Finanzas.	
	Los pagos de los proveedores del exterior se tendrán los siguientes documentos: • Estado de cuenta del Proveedor • Registros contables de lo adeudado al proveedor Se deberá contemplar las retenciones que establecen el Código Tributario y la ley del impuesto a la Transferencia de Bienes Muebles y la Prestación de Servicios.	
	La autorización de los cheques y trasferencias bancarias se harán en forma mancomunada de acuerdo con lo siguiente: Gerente General. A Junta Directiva A Tesorería. B Gerencia Financiera. B Pagos de 1,000.00 a 5,000.00 pueden ser aplicados por dos firmantes BB o bien por una combinación de AB	

	Pagos de 5,000.00 en adelante requieren una combinación de AB o AA
	La entidad dispondrá de fondos de caja chica para pagar compras a proveedores hasta un máximo de $50.00, serán autorizadas por jefes y gerentes por medio de anticipos de caja chica los cuales serán liquidados dentro de los tres días hábiles de haber sido entregado el documento de soporte.
	El encargado del fondo de caja chica deberá solicitar el reintegro cuando el monto del fondo se haya utilizado en un 50%.
	La cajera será la responsable de verificar que los documentos fiscales que reciban cumplan con los requisitos fiscales y legales definidos previo a la entrega del Quedan.
	La Gerencia de Administración y Finanzas junto con la cajera, deben definir el horario para la entrega de Quedan, cheques y pagos electrónicos.
	El plazo para efectuar pagos en la empresa es de 30 días calendario contados a partir de la fecha de emisión del Quedan, si se diera alguna consideración de plazos menores, deberá estar autorizado por el Gerente de Administración y Finanzas.
	Los pagos que se harán de forma inmediata serán algunos como: Los servicios básicos, gastos de viaje, gastos de importación, pagos de impuestos, pagos de taxis, cuotas de crédito, entre otros.
	El controller o auditor interno y el departamento de contabilidad tienen la responsabilidad de realizar aqueo de los fondos de caja chica al menos una vez al mes
	Los cheques de liquidación de empleados serán elaborados por el área contable y se deben entregar directamente a la Gerencia de Recursos Humanos.
	Todos los pagos a proveedores deberán programarse en base al reporte de programación de pagos elaborado por el responsable de cuentas por pagar.
	Los ajustes a la cuenta de un proveedor serán autorizados por la Gerencia de Administración y Finanzas, previa presentación de la nota de crédito o débito firmada por el jefe de compras e importaciones.
	Los pagos por proyectos de inversión deberán especificar el monto a pagar y estar autorizados por el Comité Ejecutivo, anexar copia del contrato de trabajo firmado, Comprobante de Crédito Fiscal con firma y sello de aceptado del encargado del proyecto de inversión. Todo anticipo o garantía relacionado, debe estar revisado por en encargado del proyecto de inversión y autorizado por el Gerente General.

	Los cheques emitidos y no retirados después de 90 días, serán anulados por el departamento de contabilidad y clasificarán el pago como una cuenta por pagar. Si transcurre un año desde la fecha de emisión del cheque se clasificará como Otros Ingresos, debiendo estar autorizado por el Gerente de Administración y Finanzas y el Comité Ejecutivo.
	Cada Gerencia será responsable de autorizar los gastos o inversiones que realicen, lo que conlleva a que también serán responsables de cualquier diferencia o desviación mal efectuada.
	La presentación de documentos a cobro es exclusiva del proveedor en los días establecidos para la entrega de Quedan.
	Toda la documentación antes mencionada, estará en resguardo por el departamento de contabilidad.
	En caso de existir otras situaciones no previstas en esta política deberán ser resueltas por el Gerente de Administración y Finanzas, autorizadas por el Gerente General.

	Fecha de elaboración	**Diciembre 2020**
AF-03	Proceso	**Cuentas por cobrar**
Objetivo	Proporcionar criterios para el otorgamiento y recuperación de créditos a terceras personas naturales y/o jurídicas, con la finalidad de garantizar el cobro de los mismos.	
Campo de aplicación	Área Financiera	
Políticas específicas	La Junta Directiva y el Comité Ejecutivo autorizaran los límites anuales para otorgar créditos en la venta de repuestos, motores y en servicios de post venta.	
	La Junta Directiva establecerá los límites para la cartera de créditos.	
	La cartera de créditos nunca debe reflejar más de un 5% en mora total y 0.5% de incobrabilidad, los limites serán administrados por la Gerencia de Administración y Finanzas.	
	La Gerencia de Administración y Finanzas en coordinación con el Analista de Créditos serán encargados de proponer la provisión y liquidación de cuentas incobrables, y el Comité Ejecutivo debe autorizar la liquidación.	
	Los niveles de cartera y las cuentas incobrables serán revisadas en el mes de junio, por la Gerencia de Administración y Finanzas con la finalidad de garantizar que no sea mayor al 50% de lo provisionado para el año en curso.	
	La empresa podrá autorizar créditos en la venta de repuestos y servicios, para aquellos clientes que cumplan los requisitos establecidos para ser sujeto de créditos.	
	Los requisitos para ser sujetos de créditos son los siguientes: ▪ Completar el formulario de solicitud de crédito. ▪ Aprobar la calificación del Buró de créditos. Además de presentar la siguiente documentación: a. Persona natural: ▪ Carta firmada por el cliente donde autoriza la investigación y el uso de su información. ▪ Fotocopia DUI y NIT. ▪ Dos referencias comerciales. ▪ Dos referencias bancarias. ▪ Constancia de ingresos y detalla de unidades de su propiedad ▪ Fotocopia recibo de agua y energía eléctrica. ▪ En caso de crédito de motores, presentar fotocopia de la tarjeta de circulación del vehículo donde se instalará el motor. b. Persona jurídica: ▪ Fotocopia DUI y NIT del representante legal	

	▪ Fotocopia de escritura de constitución de sociedad. ▪ Dos referencias bancarias. ▪ Fotocopia de registro de IVA
	La información de los clientes será resguarda en caja de seguridad.
	La empresa concederá créditos a clientes previamente clasificados dentro de las siguientes categorías: ▪ Particulares ▪ Propietarios de talleres ▪ Empresarios de transporte colectivo ▪ Cooperativas de autobuses ▪ Instituciones públicas y privadas
	Se podrán conceder créditos a empleados en venta de vehículos, servicios de taller y repuestos con una evaluación previa de RRHH, otorgando un descuento del 20% y un plazo flexible.
	El otorgamiento de créditos a corto plazo a personas naturales o jurídicas en la venta de motores y semi motores, se realizará con un 50% de prima del valor de venta; un porcentaje menor será autorizado por la Junta Directiva y el Gerente General.
	El plazo para otorgar créditos a corto plazo en semi motores y motores será de 6 meses, y en casos especiales hasta 10 meses con previa evaluación del Analista de Créditos y con autorización de la Junta Directiva y Gerente General.
	Para el caso de autos, se podrá otorgar crédito de prima y tres cuotas mensuales sucesivas.
	Se conformará un comité de créditos integrado por: Gerente de Administración y Finanza, Jefe de Repuestos, Gerente de Posventa y Gerente General.
	La autorización de créditos en la venta de repuestos y servicios es la siguiente: ▪ Si el monto es hasta $600.00, el responsable de autorización será el Analista de créditos. ▪ Si el monto es de $600.01 hasta $25,000.00, el responsable de autorización será el Comité de créditos. ▪ Si el monto es mayor a $25,000.00, el responsable de autorización será la Junta Directiva.
	Las modalidades de pago aceptado por la empresa son: efectivo, cheque y transferencias bancarias.
	Todo pago realizado por los clientes en medio distinto al efectivo y sea mayor a $25,000.00 debe ir acompañado del formulario de Transacciones Regulares, de acuerdo a lo establecido en la Ley Contra el Lavado de Dinero y Activos.

	Es responsabilidad del Analista de Créditos y Cobros informar al designado de la UIF sobre aquellos clientes que cancelen de forma anticipada las cuotas pendientes del crédito otorgado.
	La Gerencia de Administración y Finanzas autorizara planes de pago o refinanciamiento a los casos de difícil recuperación, y que dicho plazo no exceda los 12 meses.
	La información de cuentas por cobrar debe estar centralizada en el área de créditos y cobros.
	La responsabilidad sobre la pureza y calidad de información ingresada recae sobre las personas encargadas de su proceso.
	Los vendedores serán responsables de la administración de su cartera de créditos.
	El Analista de Créditos y Cobros es responsable de mantener conciliados, los saldos de cuentas por cobrar, entre los registros contables y los documentos físicos que respalden dichos saldos.
	El Analista de Créditos y Cobros es responsable del seguimiento de la cartera de créditos, generación de información, casos de difícil recuperación y aquellos remitidos a cobro vía jurídica.
	La Gerencia de Administración y Finanzas presentara al Comité Ejecutivo una propuesta anual del cálculo de provisión de cuentas incobrables, esta no podrá exceder al promedio de los últimos cinco años de incobrabilidad con relación a la cartera de más de 120 días con que se cierre cada ejercicio.
	La amortización de la reserva deberá efectuarse en los doce meses posteriores a la autorización o del año en curso.
	En los meses de junio (30) y octubre (30) se deben revisar los niveles de morosidad y definir si la provisión de mantiene o se incrementa.

	Fecha de elaboración	**Diciembre 2020**
AF-04	Proceso	**Tesorería**
Objetivo	Gestionar y canalizar los recursos financieros de manera eficaz para cumplir con las responsabilidades de la empresa.	
Campo de aplicación	Área Financiera	
Políticas específicas	El Gerente de Administración y Finanzas propondrá al Gerente General, las instituciones financieras con las que se trabajará.	
	La captación de fondos se hará por medio de líneas de crédito bancarias.	
	Las cuentas bancarias están a nombre de la empresa, identificadas con el nombre autorizado por el área de tesorería, y cumpliendo las disposiciones legales correspondientes. El número de cuentas se limitará al que sea necesario.	
	Los cheques serán emitidos a nombre del beneficiario ya sea persona natural o jurídica. Y las firmas deberán ser empleadas de forma manual.	
	Cuando se utilicen firmas impresas de cheques, se deberá asegurar que estos cumplan con los requisitos legales y de seguridad establecidos por la ley, en el caso de transferencias vía internet y manual, se deberá de contar con los respectivos comprobantes de respaldo de la transacción.	
	La Junta Directiva validará y aprobará de forma anual las líneas de sobregiro, líneas de créditos rotativos y los créditos decrecientes con las distintas instituciones financieras que realiza operaciones activas, y autorizará al Gerente General para la celebración de contratos.	
	La Gerencia de Administración y Finanzas solicitara al Gerente General la utilización de sobregiros, únicamente cuando las necesidades de fondos sean por plazos menores de 15 días y por montos menores a $150,000.00	
	Las líneas de crédito rotativo se utilizarán para el financiamiento de necesidades de capital de trabajo para plazo menores a 360 días.	
	La captación de fondos por la venta de vehículos, repuestos y taller será efectuada en el área de caja, sean estos en efectivo, cheques, notas de abono o transferencias del exterior.	
	La caja no podrá recibir montos mayores a $4,000.00 en efectivo, sean estos en concepto de prima, reserva, anticipo o pago de cuotas en caso de una venta al crédito.	
	Es responsabilidad de Caja y el Jefe de Tesorería informar al designado por la Unidad de Investigación Financiera, al momento de recibir montos que supere los $25,000.00 o su equivalente en moneda extranjera, sea esta cualquiera forma de pago.	
	No se aceptarán cheques endosados sin tener autorización de la Gerencia de Administración y Finanzas. En el área de caja no	

	se recibirán cheques a nombre de terceros para cancelar cuentas de clientes.
	Tesorería debe monitorear el nivel de endeudamiento de la empresa y presentar informes a la Gerencia de Administración y Finanzas y al Gerente General.
	Cuando se detecte riesgo de quiebra técnica se debe presentar informes extraordinarios al Gerente General, y este debe comunicárselo a la Junta Directiva.
	La empresa distribuirá dividendos siempre que las condiciones financieras lo permitan, y no se distribuirá más del porcentaje establecido en el pacto social.
	La prioridad de pago de dividendos se realizará de acuerdo a lo establecido en el pacto social.

	Fecha de elaboración	**Diciembre 2020**
AF-05	Proceso	**Registros Contables**
Objetivo	Establecer los lineamientos para la presentación de los registros contables mensuales de acuerdo al marco de información aplicable.	
Campo de aplicación	Área Financiera	
Políticas específicas	Inicialmente se debe verificar que la planificación del presupuesto de gastos se ajuste a la estructura del catálogo de cuentas.	
	El responsable del centro de costos debe autorizar la aplicación de los gastos.	
	El Gerente de Administración y Finanzas debe definir el calendario financiero que se utilizará en el sistema informático, y debe detallar los reportes que emitirá el sistema con sus respectivas fechas.	
	En el caso de existir errores por malas aplicaciones contables en gastos, se deberá realizar una solicitud por escrito al Gerente de Administración y Finanzas, que anexe la documentación soporte correspondiente.	
	El departamento de contabilidad es responsable de realizar las correcciones en el sistema informático, siempre y cuando se cumplan los lineamientos anteriores.	
	Si existiera un error por reclasificaciones no contempladas, la responsabilidad de realizar las correcciones es exclusiva de la Gerencia de Administración y Finanzas.	
	Es responsabilidad del departamento de contabilidad mantener actualizado en forma permanente el catálogo de cuentas y el manual de aplicación.	
	Las erogaciones deben ser registradas contablemente en el período en que se realizan.	
	El registro y control de los ingresos se realizará de forma diaria para contribuir a la disponibilidad de la información.	
	Se realizarán las provisiones contables de las erogaciones, provisiones bancarias, de salarios, comisiones y seguros, que se realicen a final de mes, durante el mes en que se realizan.	
	El pago de los impuestos derivados de las operaciones mensuales de la entidad, se efectuarán de acuerdo a las disposiciones legales y fiscales vigentes.	
	Los cierres contables diarios tendrán un lapso máximo de 12 horas.	
	Las demás gerencias excepto Administración y Finanzas deben realizar los cierres de sus módulos al último día hábil del mes.	
	El cierre mensual de los registros contables debe realizarse a más tardar el segundo día hábil del mes siguiente.	

	El jefe del departamento de contabilidad deberá obtener la autorización del Gerente de Administración y Finanzas para efectuar el cierre de fin de año.
	Los reportes que debe emitir el departamento de contabilidad después de cada cierre mensual y anual son: 1. Estado de Situación Financiera 2. Estado de Resultados 3. Estado de Cambios en el Patrimonio 4. Estado de Flujo de Efectivo 5. Libro Diario Mayor 6. Libro Auxiliar 7. Libros Legales de IVA 8. Reporte de Gastos y Variaciones 9. Reporte de Antigüedad de saldos de cuentas por cobrar. 10. Informes y formularios requeridos por la Administración Tributaria. 11. Reporte de Programación de Pago de Proveedores.
	En caso de ser necesario modificar o reabrir periodos contables anteriores, debe realizarse a solicitud del Gerente de Administración y Finanzas.
	Es responsabilidad del departamento de contabilidad verificar que los saldos finales de un período, registrados en el Estado de Situación Financiera, coincidan con los saldos iniciales del siguiente período.
	El jefe de contabilidad tiene la responsabilidad de que los registros contables de la empresa se mantengan actualizados, se efectúen en forma correcta, cumplan con los requerimientos fiscales y legales establecidos y presentar los estados financieros a más tardar el tercer día hábil del mes siguiente.
	Las situaciones no planteadas en esta política, deberán ser resueltas por el Gerente de Administración y Finanzas avalado por el Gerente General.

	Fecha de elaboración	**Diciembre 2020**
AF-06	Proceso	**Seguros**
Objetivo	Gestionar que se realicen de forma correcta, oportuna y eficiente la administración de seguros y reclamos.	
Campo de aplicación	Área Financiera	
Políticas especificas	Las pólizas de seguros de la empresa serán negociadas por la Gerencia de Administración y Finanzas con participación de las diferentes áreas.	
	La Gerencia de Administración y Finanzas será la responsable de presentar y dar seguimiento a los reclamos hechos a la Compañía Aseguradora.	
	Las pólizas de seguros negociadas serán las siguientes: ▪ Automotores ▪ De Fidelidad ▪ Todo Riesgo de Incendio ▪ Todo Riesgo de Equipo Electrónico ▪ De Importaciones ▪ Robo y Hurto ▪ De Personas ▪ Responsabilidad Civil.	
	Las consultas en la plataforma de la compañía aseguradora serán responsabilidad del Administrador de Pólizas y el encargado de reclamos.	
	Mensualmente el encargado de reclamos pedirá a la compañía aseguradora un estado de reclamos presentados.	
	El resguardo de las pólizas de seguro se realizará de la siguiente manera: ▪ El documento original será reproducido de forma escaneada y guardado en un archivo digital. ▪ Las Pólizas originales serán resguardadas en una caja de seguridad.	

	Fecha de elaboración	**Diciembre 2020**
AF-07	Proceso	**Impuestos**
Objetivo	Presentar y administrar oportunamente las obligaciones fiscales de la compañía.	
Campo de aplicación	Área Financiera	
Políticas específicas	La entidad administrara y presentara los impuestos bajo el marco legal vigente de la Republica de El Salvador.	
	Los usuarios, contraseñas y demás servicios en línea estarán autorizados por el Gerente General y compartidos con el encargado del área de impuestos.	
	El encargado de impuestos es el responsable de comunicar a las diferentes áreas que correspondan las fechas de cumplimiento y presentación de informes y formularios fiscales.	
	La emisión de la documentación fiscal tales como: • Comprobantes de crédito fiscal • Facturas de consumidor final • Notas de crédito • Facturas de sujeto excluido • Notas de remisión • Archivos fiscales Estarán bajo la responsabilidad y el resguardo del área de impuestos, quien velara que cumpla los aspectos fiscales requeridos por la ley.	
	Los ingresos ordinarios mensuales que se informan al fisco se validaran en conjunto con el contador general y el encargado de impuestos.	
	Las ventas por facturación de vehículos, servicios y repuestos se trasladarán al área de impuestos quien se asegurará de los cumplimento formales y sustantivos según las leyes correspondientes.	
	La presentación de formularios e informes mensuales estará autorizada por la Gerencia Financiera y esta se realizará con tres días de anticipación de su fecha de vencimiento.	
	Las solicitudes de transferencias bancarias y de cheques por el pago de impuestos fiscales y municipales mayores de $5,000.00 estarán autorizados según los requerimientos de la política de cuentas por pagar.	
	La Gerencia Financiera coordinara con recursos humanos las capacitaciones o asesorías de las actualizaciones del marco legal que correspondan para el buen manejo de la administración de impuestos.	
	Los documentos digitales deberán estar almacenados en discos duros o cualquier otro medio que respalde su seguridad.	

	Fecha de elaboración	**Diciembre 2020**
AF-08	Proceso	**Cuentas Corrientes**
Objetivo	Lograr un control eficiente de registros de las ventas, pago y liquidaciones para la generación de información financiera.	
Campo de aplicación	Área Financiera	
Políticas específicas	El control de las ventas diarias de las diferentes sucursales se manejará por medio de cortes diarios.	
	El documento del corte diario deberá detallar el dinero recibido en: • Cheques • Notas de Abono • Efectivo • Tarjetas de crédito y débito. El encargado de caja remesara el dinero recibido de las diferentes modalidades al banco designado por la compañía.	
	La revisión y validación de las remesas y el arqueo de caja se realizará por el área contable	
	El usuario y contraseña de la banca digital deberá ser autorizado por la Gerencia Financiera quien designará un usuario de acceso al banco.	
	Las liquidaciones de pagos con tarjetas se realizarán a diario para la generación de los flujos de caja	
	Las conciliaciones bancarias se realizarán el primer día de cada mes, y estas serán enviadas al departamento de Tesorería	
	La contabilización de pagarés y reclasificaciones de anticipos de clientes se realizará en forma diaria teniendo un control de la antigüedad de estos.	
	Al final de cada mes se realizará la revisión de los clientes en el sistema de los montos liquidados y así descartar diferencias de faltantes y sobrantes.	
	El acceso a la plataforma del banco se realizará en forma de consulta cualquier cargo o abono a la cuenta bancaria se hará por medio del encargado de cuentas por pagar.	

K. Recursos y personas.

La provisión de recursos es compromiso de la empresa para:

- Establecer, implementar, monitorear, mantener y mejorar el plan de seguridad de la información.
- Asegurar que los procedimientos de seguridad de la información soporten a los requerimientos de la entidad.
- Mantener una apropiada seguridad a través de implementar correctamente los controles.
- Llevar a cabo revisiones y cuando se requiera mejorar la efectividad del plan de seguridad de la información.

La entidad debe garantizar la formación, concientización y competencia del personal para una adecuada ejecución del plan, de la siguiente manera:

- Vela por la competencia del personal, considerando para ellos los perfiles definidos para cada puesto de trabajo.
- Concientiza al personal sobre la importancia de la seguridad de la información en su puesto de trabajo y de su contribución al logro de los objetivos del plan de seguridad de la información.
- Posee registros actualizados del personal, que evidencian la educación, formación, habilidades y experiencia de cada empleado.

L. Herramientas

Algunas de las herramientas que contribuyen a la protección de activos digitales son:

1. **Firewalls o cortafuegos:** Este tipo de herramienta de hardware o un software inspecciona el tráfico de la web protegiendo los equipos individuales, servidores o equipos conectados en red, identifica a los usuarios, bloquea accesos no autorizados y brinda protección incluso contra virus de última generación.

2. **Software de encriptación de unidades de almacenamiento:** Es una herramienta que se basa en la codificación de la información que utiliza un software o un hardware de encriptación, generando algoritmos únicos de cifrado evitando así el acceso no autorizado a información almacenada.

3. **Software antivirus:** Es un conjunto de programas que proporcionan medidas de protección útiles, busca, destruye y advierte las amenazas potenciales de ordenadores y redes; lo ideal es adquirir un software pagado.

4. **Autenticación en dos pasos:** El objetivo radica en la protección de las cuentas de acceso contra accesos no autorizados, protegiendo la información sensible de forma que los usuarios inician sesión utilizando dos elementos: Algo que saben y algo que tienen.

5. **Software de monitoreo a distancia:** Se encarga de otorgar al equipo de TI la función de inspeccionar, determinar y compilar información del uso de la red en diferentes puntos de forma remota.

6. **Red LAN:** Es una red de área local en la que distintos dispositivos pueden comunicarse entre ellos con extensión física limitada, en un mínimo de dos dispositivos finales, pero puede conectar miles.

7. **Red WAN:** Es una red de área amplia que permite la interconexión de equipos terminales u otras redes desde largas distancias.

8. **Proxy:** Es un equipo informático que permite aplicar reglas de filtrado, que hace de intermediario entre las conexiones de un cliente y un servidor de destino, en función de la política de seguridad informática de una empresa escondiendo la dirección IP.

9. **VPN:** Redes privadas virtuales, son redes que se utilizan para conectar una o más computadoras sin que los dispositivos estén conectados entre sí físicamente, a una red privada utilizando internet. Permiten asegurar la confidencialidad e integridad de la información accediendo desde cualquier ubicación geográfica.

10. **Escáner de vulnerabilidades**: Es el software encargado de detectar, evaluar y gestionar las vulnerabilidades en cuestión de seguridad que se tienen en una infraestructura de cómputo, antes de que un hacker o agresor cibernético logre detectarlas.

11. **Plataformas de almacenamiento en la nube:** Es un servicio informático que consiste en el almacenamiento de datos a través de internet a un proveedor externo, siendo una solución comercial de copia de seguridad remota donde la compañía puede transferir y almacenar de forma segura archivos de datos o compartirlos entre ubicaciones.

12. **Webfilter:** Es un software que permite la restricción de los sitios web a los que un usuario puede acceder, funciona con una whitelist o blacklist configurada, bloqueando el acceso a otros recursos que puedan poner en riesgo la seguridad de la conexión y la información.

13. **Antispam:** Es un método que se basa principalmente en el filtrado y bloqueo de los correos electrónicos entrantes y salientes que presenten términos específicos, determinados contenidos, tamaños de archivos, entre otros.

M. Mejora de Seguridad

Mejora continua

La empresa continuamente mejorará la efectividad del plan de seguridad de la información a través de revisión y creación de nuevas políticas y objetivos de seguridad, que se adapten a los estándares actuales, tomando en cuenta los resultados de las auditorias, el análisis de los eventos monitoreados, y las acciones correctivas y preventivas.

Las políticas de seguridad deben ser revisada en intervalos planificados o si ocurren cambios significativos, esto con el fin de mejorar su uso, adecuación y efectividad, las revisiones se harán anualmente dentro del proceso de revisión se recomienda disponer de la siguiente información:

1. Resultados de revisiones independientes (auditorías internas)
2. Tendencias relacionadas con amenazas y vulnerabilidades.
3. Incidentes registrados.
4. Cambios en la empresa.
5. Tecnología
6. Eventos externos
7. Recomendaciones dadas por autoridades
8. Resultados de revisiones anteriores.

Como resultado de la revisión y aprobación por parte de la Junta Directiva y Gerencia General, se debe incluir información acerca de posibles mejoras en el alcance de la organización para gestionar la seguridad de información.

Auditoría.

La auditoría de seguridad es una revisión enfocada a mostrar el estado en que se encuentra la protección de la información dentro de la empresa e involucra la identificación, análisis y evaluación de debilidades en los activos y en los controles aplicados para protegerlos.

La auditoría posee diferentes perspectivas de revisiones, estas evalúan los controles de seguridad física y lógica determinados para el acceso y uso de los sistemas; las revisiones de gestión verifican si se cumple con normas y requisitos legales establecidos para las operaciones.

Las actividades relacionadas con las auditorias deben estar documentadas, para tener evidencia de su aplicación. Las auditorías a las cuales se podrán someter los sistemas, opcionalmente podrán ser internas o externas, ambas buscarán imparcialidad en sus resultados.

CONCLUSIONES

- Las empresas comercializadoras de vehículos no cuentan con planes contra ataques de ciberseguridad, que resguarden su información electrónica permitiendo así una toma de decisiones más confiable.
- Se presentan vulnerabilidades en la seguridad de la información en las empresas comercializadoras de vehículos, debido a que no se cuenta con marco de actuación basado en los estándares internacionales de mejores prácticas; los controles que actualmente poseen derivan de las exigencias de las empresas multinacionales que representan.
- La seguridad de la información les concierne a los profesionales en contaduría pública por todo el tipo de información que manejan, por lo que es importante estén a la vanguardia de los avances tecnológicos como de las mejores prácticas, ya que esto contribuirá a minimizar los riesgos y con ello lo resultados adversos para la empresa.
- Los resultados obtenidos en las entrevistas, son prueba de la falta de conocimiento de seguridad de la información de todo el recurso humano que labora en la empresa tomada como muestra; lo cual indica una de las más grandes vulnerabilidades de la información vital y privada de la misma.

RECOMENDACIONES.

Después de realizada la investigación, se recomienda lo siguiente:

- A los profesionales de contaduría pública, mantenerse a la vanguardia del conocimiento, expandiendo sus áreas de competencia en Tecnologías de la Información, ya que El Consejo de Normas Internacionales de Formación en Contaduría (IAESB) establece en las IES 2, 3 y 4, elementos esenciales que los programas de formación y desarrollo se espera que incluyan y se tenga el potencial para obtener el reconocimiento, aceptación y aplicación internacional.
- A las empresas comercializadoras de vehículos, fortalecer la seguridad de la información implementando un plan de seguridad, combinando los controles, con medidas en las que el factor humano cumpla con un rol activo en coordinación de todas las áreas de la entidad, ya que es un compromiso en todos los niveles jerárquicos.
- A las empresas comercializadoras de vehículos, ejecutar auditorías de sistemas informáticos con la finalidad de conocer las vulnerabilidades de seguridad existentes y los procedimientos que se debe realizar para menguar los riesgos.
- A los encargados de TI de las empresas comercializadoras de vehículos, establecer programas de mejora continua para la seguridad informática y con eso mantener en constante actualización al personal de la empresa, realizar capacitaciones de carácter obligatorio de todo el personal puesto que es un filtro importante de información, la cual debe ser protegida y resguardada.

BIBLIOGRAFÍA.

Blog de Itech Sas . (1 de abril de 2019). *Blog de Itech Sas* . Obtenido de https://www.itechsas.com/blog/ciberseguridad/toyota-pierde-31-millones-de-datos/

Azure, M. (2020). *¿Qué es el almacenamiento en la nube?* Obtenido de https://azure.microsoft.com/es-es/overview/what-is-cloud-storage/#:~:text=El%20almacenamiento%20en%20la%20nube%20es%20un%20servicio%20que%20permite,externo%20que%20mantiene%20un%20tercero

Blog, H. (2019). *ITIL® 4, todas las novedades de ITIL en 2019*. Obtenido de https://www.hiberus.com/crecemos-contigo/novedades-itil-v4/

Blog, T. (2019). *5 Tipos de Herramientas de Seguridad Digital que todo Empresa dede tener*. Obtenido de https://www.gb-advisors.com/es/5-tipos-de-herramientas-de-seguridad-digital-que-toda-empresa-debe-tener/

Digital, C. (s.f.). *Convivencia Digital*. Obtenido de Amenazas y peligros a los que estamos expuestos: https://sites.google.com/site/laconvivenciadigital/riesgos-y-delitos-informaticos

Excel Automotriz. (2020). Obtenido de https://excelautomotriz.com/el-salvador/quienes-somos/historia/

GCBGlobal. (s.f.). *GCBGlobal*. Obtenido de sistema de gestión de seguridad de la información: https://www.gcbglobal.com/copia-de-sast-ohsas

Gestión, B. e. (21 de Mayo de 2015). *ISO 27001: ¿Qué significa la Seguridad de la Información?* Obtenido de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

GLOBALFINANZ. (2020). *GLOBALFINANZ.* Obtenido de ¿Sabes qué es un ataque cibernético y cuales son los más comunes?: https://www.responsabilidadconsejerosydirectivos.com/que-son-los-ataques-ciberneticos/

Idalberto, C. (2006). *Introducción a la Teoría General de la Administración.* McGraw Hill Interamericana.

Instituto Nacional de Ciberseguridad. (11 de marzo de 2015). *Instituto Nacional de Ciberseguridad*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

ISACA. (2019). *COBIT 2019. Marco de Refrencia: Objetivos de gobierno y gestion.* Estados Unidos: ISACA.

ITIL. (2007). *ITIL. Diseño de Servicio V3.*

Legislativa, A. (1995). *Ley de Transporte Terrestre, Transito y Seguridad Vial*. Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/F27F8A6B-0C72-4F8B-AA60-47F95E96141A.pdf

Legislativa, A. (1995). *Normas para la Importación de Vehículos Automóviles y de otros Medios de Transporte.* Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/9F8286E2-CDE7-469A-BA46-1E237EFFD1EE.pdf

Legislativa, A. (2006). *Ley Especial Contra Actos de Terrorismo*. Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073006228_archivo_documento_legislativo.pdf

Legislativa, A. (2009). *Ley del Impuesto Especial a la Primera Matrícula de Bienes en el Territorio Nacional*. Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072945322_archivo_documento_legislativo.pdf

Legislativa, A. (2011). *Ley de Regulación de los Servicios de Información sobre el Historial de Crédito de las Personas.* Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073012044_archivo_documento_legislativo.pdf

Legislativa, A. (2014). *Ley Especial Contra Actos de Terrorismo*. Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073516039_archivo_documento_legislativo.pdf

Legislativa, A. (2016). *Ley Especial Contra Delitos Informáticos y Conexos.* Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073646641_archivo_documento_legislativo.pdf

Legislativa, A. (2020). *Ley de Regulación del Teletrabajo*. Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/384052FA-7820-4835-A5F9-AF8150684D71.pdf

Lizet, A. I. (2016). *Gestión de la ciberseguridad y previsión de los ataques cibérneticos en las PYMES del Perú.* Perú.

Net, C. (27 de Enero de 2017). *Cantabria Net*. Obtenido de Ciberataques en las Pymes: https://www.cantabriared.net/blog-cantabriared/ciberataques-en-las-pymes/

Organización Internacional para la Estandarización. (2013). *ISO 27001. Tecnología de la información. Técnicas de Seguridad. Código de prácticas para controles de la seguridad de la información.* ISO/EC.

Organización Internacional para la Estandarización. (2013). *ISO 27002. Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.* Estados Unidos: ISO/EC.

Politica de Seguridad. (2017). Obtenido de https://repository.udistrital.edu.co/bitstream/handle/11349/8322/Anexo%20C%20-%20Politicas%20de%20seguridad.pdf?sequence=4&isAllowed=y

Q, G. (2012). *GRUPO Q*. Obtenido de https://www.grupoq.com/gt/historia.html

Ríos, S. (2011). *Manual Integro ITIL V3.* Obtenido de https://es.slideshare.net/Biable/manual-itil-integro

S.L., O. (22 de MAyo de 2018). *OpenWebinars S.L.* Obtenido de ¿Qué es la ciberseguridad?: https://openwebinars.net/blog/que-es-la-ciberseguridad/

Significados. (2020). Obtenido de https://www.significados.com/software/

Slideshare. (2016). *5 actividad 5 seguridad de la informacion*. Obtenido de https://www.slideshare.net/elizabethmoreno123456789/5actividad-5-seguridad-de-la-informacion-70187409

Villela, E. A. (2020). *IS IT SKULL*. Obtenido de https://www.it-skull.com/content/2-seguridad-de-la-informacion-que-es/2-seguridad-de-la-informacion-que-es.html

ANEXOS

Anexo 1

Categoría de Vehículo para Impuesto de Primera Matricula.

Categoría	Descripción	Tasa Ad Valorem
Categoría 1	Vehículos automotores para el transporte de personas del tipo autobús o microbús, de motor diesel o gasolina, u otra tecnología.	1.0%
Categoría 2	Vehículos automotores de turismo y demás vehículos automotores concebidos principalmente para el transporte de personas hasta 9 pasajeros incluidos su condutors, de motor diesel o gasolina, u otra tecnología:	
Subcategoría 2.1	Vehículos automotores de 0 a 2000 centímetros cúbicos, del tipo 4x2	4.0%
Subcategoría 2.2	Vehículos automores de más de 2000 centímetros cúbicos, del tipo 4x2	4.0%
Subcategoría 2.3	Vehículos automotores de cualquier cilindrada, del tipo 4x4	6.0%
Subcategoría 2.4	Vehículos automotores de cualquier cilindrada, para transporte especial tales como ambulancias y carros fúnebres.	1.0%
Categoría 3	Vehículos automotores para el transporte de mercancías del tipo pickups, panales, furgonetas, camiones y cabezales, de motor diesel o gasolina, u otra tecnología.	1.0%
Categoría 4	Vehículos automotores del tipo motocicletas, tricimotos y cuadrimotos:	
Subcategoría 4.1	Hasta 250 centímetros cúbicos	1.0%
Subcategoría 4.2	Más de 250 centímetros cúbicos	8.0%
Categoría 5	Vehículos automotores para usos especiales no comprendidos dentro de ninguna de las categorías anteriores, de los utilizados como camión grúa, para sondeo o perforación, de volteo, concreteros, recolectores de basura, camión cisterna, camiones blindados y otros.	2.0%
Categoría 6	Otros vehículos no automotores del tipo remolques y semi remolques para el trnasporte de mercancías y otros usos.	1.0%

Anexo 2.

Rebajas en concepto de depreciación

De 180 días hasta un año	10%
De más de un año hasta a dos años	20%
De más de dos años hasta tres años	40%
De más tres años hasta cuatro años	50%
De más de cuatro años	60%

Anexo 3.

Entrevistas

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Entrevista 1

Dirigida a: Analista Comercial

Tema de Investigación: PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA FINANCIERA DE EMPRESAS COMERCIALIZADORAS DE AUTOMÓVILES DEL MUNICIPIO DE ANTIGUO CUSCATLÁN.

Objetivo: Recopilar información necesaria referente al manejo de la seguridad de la información en las empresas comercializadoras de automóviles, tomando en cuenta la gestión de la integridad, confidencialidad y disponibilidad de la información resultante de los procesos clave del área financiera.

- **Pregunta 1:** ¿Cuántos años tiene de laborar para la empresa?

Objetivo: Valorar la experiencia de los colaboradores que forman parte de los procesos claves del área financiera.

- **Pregunta 2:** En la ejecución de su puesto laboral, ¿Considera que maneja información de carácter confidencial o importante de los clientes?

Objetivo: Evaluar la conciencia que se tiene acerca de la información que se recopila de las operaciones de la entidad.

- **Pregunta 3:** ¿Qué tipo de información se les solicita a los clientes?

Objetivo: Conocer la información que se maneja dentro de la empresa.

- **Pregunta 4:** ¿Qué medios utilizan para solicitar la información personal de los clientes?

Objetivo: Conocer acerca de los medios utilizados para la recopilación de datos de los clientes.

- **Pregunta 5:** ¿Cree usted que los procesos para el manejo de la documentación que realiza son seguros? Justificar la respuesta.

Objetivo: Evaluar la complejidad o simplificación de los procesos del área financiera.

- **Pregunta 6:** ¿Ha recibido capacitaciones acerca de seguridad de la información? (si la respuesta es sí, realizar la siguiente pregunta) ¿Cada cuánto tiempo? Y si la respuesta es no realizar la pregunta del porqué.

Objetivo: Comprender la importancia que la empresa le da al tema de la seguridad de la información.

- **Pregunta 7:** ¿Cada cuánto tiempo renueva su contraseña de acceso al sistema informático?

Objetivo: Conocer acerca de las políticas implementadas para el resguardo de la información.

- **Pregunta 8:** ¿Alguien más aparte de usted tiene su usuario y contraseña de acceso al sistema informático? (si la respuesta es sí, realizar la siguiente pregunta) ¿Quiénes y por qué motivo?

Objetivo: Conocer la existencia del riesgo de que la información sea modificada por personal no autorizado.

- **Pregunta 9:** ¿Alguna vez ha sufrido pérdida de información ya sea física o digital? (si la respuesta es sí, realizar las siguientes preguntas) ¿Cuáles fueron los factores que la originaron? ¿Cómo se solucionó?

Objetivo: Conocer el ambiente que enfrenta la empresa frente a la vulnerabilidad de la información.

- **Pregunta 10:** ¿Considera que, al contar con un plan de seguridad de la información, le garantizaría más confiabilidad en la ejecución de los procesos de su puesto de trabajo? Justificar respuesta.

Objetivo: Verificar la utilidad del plan de seguridad de la información para garantizar la integridad, disponibilidad y confidencialidad de la información propia y de terceros.

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICA

ESCUELA DE CONTADURÍA PÚBLICA

Entrevista 2

Entrevistada: Encargado de Tecnología de Información

Tema de Investigación: PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA FINANCIERA DE EMPRESAS COMERCIALIZADORAS DE AUTOMÓVILES DEL MUNICIPIO DE ANTIGUO CUSCATLÁN.

Objetivo: Recopilar información necesaria referente al manejo de la seguridad de la información en las empresas comercializadoras de automóviles, tomando en cuenta la gestión de la integridad, confidencialidad y disponibilidad de la información resultante de los procesos clave del área financiera.

- **Pregunta 1**: ¿Cuántas personas conforman el departamento de TI? (Si es más de una persona cuales son las funcionen que desempeña cada uno.)

Objetivo: Conocer la segregación de funciones dentro de la entidad.

- **Pregunta 2:** ¿Qué grado académico tiene cada integrante del departamento de TI?

Objetivo: Evaluar el grado de conocimiento en materia de seguridad de información del área de TI.

- **Pregunta 3:** ¿Se recibe capacitaciones o asesorías en temas de seguridad de la información? (Si la respuesta es sí, preguntar cada cuanto tiempo)

Objetivo: Indagar la formación y la importancia en la materia que reciben los colaboradores del departamento de TI.

- **Pregunta 4:** ¿Hay un modelo de concienciación al personal sobre la calidad de la información? (si la respuesta es sí, realizar la siguiente pregunta) ¿Cuál?

Objetivo: Evaluar la importancia que le da la empresa a la seguridad de la información.

- **Pregunta 5:** ¿Qué herramientas poseen para asegurar la información digital?

Objetivo: Comprender las medidas que posee la entidad acerca de la seguridad de la información digital.

- **Pregunta 6:** ¿Existen planes de contingencia ante un ciberataque? (si la respuesta es sí, realizar la siguiente pregunta) ¿Cuáles?

Objetivo: Conocer acerca de los planes actuales que posee la empresa ante las amenazas que se puedan presentar.

- **Pregunta 7:** ¿Cuál es el procedimiento ante un correo sospechoso?

Objetivo: Conocer los controles establecidos por el área de TI ante amenazas de correos sospechosos.

- **Pregunta 8:** ¿La navegación en sitios web de los colaboradores se encuentra limitada?

Objetivo: Investigar acerca de las limitaciones establecidas a los colaboradores

- **Pregunta 9:** ¿La instalación de otro software inusual por parte de los colaboradores esta monitoreada por el departamento de TI?

Objetivo: Verificar el alcance del departamento de TI en la red de la empresa.

- **Pregunta 10:** ¿Cada cuánto tiempo considera deben ser realizadas copias de seguridad de los archivos que contienen la información más importante de la empresa?

Objetivo: Evaluar la frecuencia en la que la información almacenada es resguardada como prevención ante riesgos.

- **Pregunta 11:** ¿Los empleados tienen acceso al sistema desde otros dispositivos diferentes de sus ordenadores?

Objetivo: Verificar los puentes de acceso permitidos al sistema de la entidad.

- **Pregunta 12:** ¿Se realizan análisis y gestión de riesgos informáticos? ¿Cuáles?

Objetivo: Determinar la valoración que se le tiene a los riesgos informáticos que está expuesta la información.

- **Pregunta 13:** ¿Presupuestan los costos que puede incurrir un posible ciberataque?

Objetivo: Analizar la capacidad de afrontar un posible ciberataque en cuanto a los costos que este incurre.

- **Pregunta 14:** ¿Cada cuánto tiempo se les realiza mantenimiento a los equipos de cómputo?

Objetivo: Evaluar el respectivo seguimiento que se les da a los equipos informáticos para su efectivo funcionamiento.

- **Pregunta 15:** ¿Se cuenta con licencias originales de programas informáticos y antivirus?

Objetivo: Verificar la existencia legítima de programas informáticos que se utilizan y protegen

- **Pregunta 16:** ¿Cuáles son las medidas o controles establecidos para el teletrabajo?

Objetivo: Verificar cómo se maneja la seguridad en la modalidad de teletrabajo.

- **Pregunta 17: ¿**Se cuenta con controles preventivos para desastres naturales?

Objetivo: Verificar si la entidad cuenta con controles seguros ante desastres naturales.

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Entrevista 3

Entrevistada: Contador General

Tema de Investigación: PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA FINANCIERA DE EMPRESAS COMERCIALIZADORAS DE AUTOMÓVILES DEL MUNICIPIO DE ANTIGUO CUSCATLÁN.

Objetivo: Recopilar información necesaria referente al manejo de la seguridad de la información en las empresas comercializadoras de automóviles, tomando en cuenta la gestión de la integridad, confidencialidad y disponibilidad de la información resultante de los procesos clave del área financiera.

- **Pregunta 1:** ¿Ha recibido capacitaciones acerca de seguridad de la información?

Objetivo: Indagar la formación y la importancia en la materia que reciben los colaboradores del departamento de contabilidad.

- **Pregunta 2:** ¿Cuáles son los controles y procedimientos que aplican para la protección de los datos con el equipo de trabajo de contabilidad?

Objetivo: Describir los actuales controles que posee el área contable.

- **Pregunta 3:** ¿Alguna vez el sistema le ha generado informes con datos erróneos o algún incidente en su puesto de trabajo?

Objetivo: Identificar las fallas resultantes de los procesos contables en el sistema informático.

- **Pregunta 4:** ¿Que medios o dispositivos utiliza para transferir información de forma segura?

Objetivo: Indagar acerca de los medios que forman parte de los procesos de transferencia de información.

- **Pregunta 5:** ¿El acceso a los módulos de contabilidad están restringidos según las obligaciones que tiene cada colaborador?

Objetivo: Verificar la existencia de restricciones al sistema informático por parte del personal de contabilidad.

- **Pregunta 6**: ¿Cuáles son los métodos utilizados en el departamento de contabilidad para la protección de la documentación física?

Objetivo: Evaluar las medidas que posee la entidad acerca de la seguridad de la información física del departamento de contabilidad, pero no se tiene un control.

- **Pregunta 7:** ¿Cuál cree sería el impacto de la generación de reportes financieros erróneos?

Objetivo: Comprender la dimensión de las fallas en los procesos del área financiera.

- **Pregunta 8:** ¿Existe algún protocolo o acceso restringido al departamento físico de contabilidad?

Objetivo: Verificar la existencia de controles de acceso al departamento de contabilidad.

- **Pregunta 9:** ¿Según su criterio, al contar con un plan de seguridad de la información, le contribuiría en la ejecución de los procesos de contabilidad? Justifique su respuesta.

Objetivo: Estimar el beneficio del plan de seguridad de la información en el departamento de contabilidad.

- **Pregunta 10:** ¿Considera que existen vulnerabilidades en la ejecución de los procesos del área contable?

Objetivo: Identificar los procesos financieros que necesitan reforzar la seguridad.

- **Pregunta 11:** ¿Cómo respalda la información, se realiza copias de seguridad?

Objetivo: Cerciorarse si la información está siendo resguardada de forma oportuna.

- **Pregunta 12:** ¿Cómo se maneja la seguridad de información con el teletrabajo?

Objetivo: Verificar cómo se maneja la seguridad en la modalidad de teletrabajo

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Entrevista 4

Entrevista a: Asistente Contable

Tema de Investigación: PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA FINANCIERA DE EMPRESAS COMERCIALIZADORAS DE AUTOMÓVILES DEL MUNICIPIO DE ANTIGUO CUSCATLÁN.

Objetivo: Recopilar información necesaria referente al manejo de la seguridad de la información en las empresas comercializadoras de automóviles, tomando en cuenta la gestión de la integridad, confidencialidad y disponibilidad de la información resultante de los procesos clave del área financiera.

- **Pregunta 1: ¿**Cuántos años tiene laborando para la empresa?

Objetivo: Valorar la experiencia de los colaboradores que forman parte de los procesos claves del área financiera.

- **Pregunta 2:** ¿Qué instrucciones ha recibido referente a la seguridad de la información que se maneja en el departamento de contabilidad?

Objetivo: Determinar la educación en seguridad de la información que se les brinda a los colaboradores de la empresa.

- **Pregunta 3:** ¿Realiza periódicamente una copia de seguridad de la información que maneja?

Objetivo: Cerciorarse si la información está siendo resguardada de forma oportuna.

- **Pregunta 4:** ¿Existe asesoramiento por parte del departamento de TI sobre la elección y uso de contraseñas?

Objetivo: Comprobar la capacitación de parte del departamento de TI en cuanto a la seguridad lógica del departamento de contabilidad.

- **Pregunta 5:** ¿Cuál es el procedimiento para anular registros erróneos en el departamento de contabilidad?

Objetivo: Analizar la existencia de limitaciones de funciones para cada usuario.

- **Pregunta 6: ¿**Recibió capacitación previa de los procesos que iba a ejecutar en su puesto de trabajo?

Objetivo: Verificar si la entidad capacita a sus empleados para los respectivos procesos.

- **Pregunta 7:** ¿Cuáles procesos considera que son vulnerables en el departamento de contabilidad?

Objetivo: Identificar los procesos financieros que necesitan reforzar la seguridad.

- **Pregunta 8:** ¿Los reportes financieros son de acceso público a todos los empleados o existe alguna restricción? (si la respuesta es sí, realizar la siguiente pregunta) ¿Quiénes son las personas autorizadas?

Objetivo: Determinar si se aplican medidas de acceso a la información.

- **Pregunta 9:** ¿Cuáles son los procedimientos para respaldar la documentación fiscal?

Objetivo: Conocer si existen procedimientos en la gestión de mitigación del riesgo de la pérdida de información.

- **Pregunta 10:** ¿Cómo protegen la información proveniente de los clientes que es considerada confidencial?

Objetivo: Examinar la valoración que se le da a la información vulnerable de los clientes.

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Entrevista 5

Dirigida a: Analista Financiero

Tema de Investigación: PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA FINANCIERA DE EMPRESAS COMERCIALIZADORAS DE AUTOMÓVILES DEL MUNICIPIO DE ANTIGUO CUSCATLÁN.

Objetivo: Recopilar información necesaria referente al manejo de la seguridad de la información en las empresas comercializadoras de automóviles, tomando en cuenta la gestión de la integridad, confidencialidad y disponibilidad de la información resultante de los procesos clave del área financiera.

- **Pregunta 1:** ¿Cuántos años tiene de laborar para la empresa?

Objetivo: Valorar la experiencia de los colaboradores que forman parte de los procesos claves del área financiera.

- **Pregunta 2.** ¿El sistema que tiene la empresa posee niveles de acceso a la información? Si la respuesta es sí, ¿Cuáles?

Objetivo: Determinar si dentro de la empresa aplican medidas de seguridad para acceso a la información.

- **Pregunta 3.** ¿A qué tipo de información y/o documentación tiene acceso?

Objetivo: Identificar los niveles de acceso a la información que poseen dentro de la empresa

- **Pregunta 4.** ¿Qué medio utilizan para solicitar requerimientos de información a otras áreas de la empresa?

Objetivo: Evaluar si poseen controles adecuado para solicitar información financiera para que esta no llegue a personas no autorizadas.

- **Pregunta 5.** ¿Cuáles son los medios y/o lugares de almacenamiento para el resguardo de la información financiera?

Objetivo: Conocer los medios de almacenamiento y respaldo que utilizan la empresa para garantizar el acceso oportuno y fiable de la información.

- **Pregunta 6.** ¿Maneja algún tipo de información confidencial, y que medidas de seguridad utiliza para su resguardo?

Objetivo: Conocer si utilizan medidas de seguridad para el resguardo de información confidencial.

- **Pregunta 7.** ¿Con que regularidad realiza copias de seguridad de la información digital que maneja?

Objetivo: Cerciorarse que la información está siendo resguardada en forma oportuna.

- **Pregunta 8.** ¿En caso de extravió de información magnética o física que procedimiento realiza para recuperarla o sustituirla?

Objetivo: Conocer si existen procedimientos en la gestión de mitigación del riesgo de la pérdida de información cuando este se materializa.

- **Pregunta 9.** ¿Ha recibido alguna capacitación sobre seguridad de la información?

Objetivo: Medir el interés de la gerencia respecto a la seguridad de la información de la empresa.

- **Pregunta 10**. ¿Se cuenta con algún seguro por pérdida o deterioro de la información?

Objetivo: Indagar acerca de los controles preventivos con los que cuenta la entidad.

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Entrevista 6

Dirigida a: Gerente Financiero

Tema de Investigación: PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA FINANCIERA DE EMPRESAS COMERCIALIZADORAS DE AUTOMÓVILES DEL MUNICIPIO DE ANTIGUO CUSCATLÁN.

Objetivo: Recopilar información necesaria referente al manejo de la seguridad de la información en las empresas comercializadoras de automóviles, tomando en cuenta la gestión de la integridad, confidencialidad y disponibilidad de la información resultante de los procesos clave del área financiera.

- **Pregunta 1:** ¿Qué tipo de actividades son realizadas para concientizar al personal en cuanto a la importancia de la seguridad de la información?

Objetivo: Comprender si la seguridad de la información resulta relevante para la entidad y el compromiso que es asignado al personal respecto a esta.

- **Pregunta 2:** ¿Cómo se controla la segregación de funciones de los colaboradores del área financiera?

Objetivo: Conocer la segregación de funciones dentro de la entidad.

- **Pregunta 3:** ¿Qué sanciones existen cuando algún empleado quiere violar los límites de acceso permitido?

Objetivo: Conocer las sanciones que posee la empresa ante una violación de límites de acceso.

- **Pregunta 4:** ¿La empresa invierte en su planificación financiera temas de ciberseguridad?

Objetivo: Medir la importancia que la entidad le da a la información financiera.

- **Pregunta 5:** ¿Cuál es la forma en que la entidad informa a los usuarios sobre restricciones de uso de información confidencial?

Objetivo: Conocer la existencia del riesgo de que la información sea modificada por personal no autorizado**.**

- **Pregunta 6:** ¿Considera que el software con el que se cuenta actualmente es adecuado para que la información sea integra, atentica y confidencial?

Objetivo: Conocer si a los empleados se le provee de las herramientas necesarias el manejo de la información.

- **Pregunta 7:** ¿Por qué considera que el software actual no cumple con los tres aspectos de la seguridad de la información?

Objetivo: Conocer si el software actual de la empresa cumple con los aspectos de seguridad de la información.

- **Pregunta 8:** Debido a lo anterior, ¿Se ha tenido algún inconveniente o se han generado errores al momento de generar informes?
- **Pregunta 9:** ¿Considera oportuno que las empresas comercializadoras de automóviles cuenten con políticas de seguridad informática?

Objetivo: Medir el interés de la gerencia respecto a la seguridad de la información de la empresa.

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Entrevista 7

Dirigida a: Gerente de Ventas

Tema de Investigación: PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA FINANCIERA DE EMPRESAS COMERCIALIZADORAS DE AUTOMÓVILES DEL MUNICIPIO DE ANTIGUO CUSCATLÁN.

Objetivo: Recopilar información necesaria referente al manejo de la seguridad de la información en las empresas comercializadoras de automóviles, tomando en cuenta la gestión de la integridad, confidencialidad y disponibilidad de la información resultante de los procesos clave del área financiera.

- **Pregunta 1.** ¿Cuántos años tiene de laborar en la empresa?

Objetivo: Valorar la experiencia de los colaboradores que forman parte de los procesos claves del área financiera.

- **Pregunta 2.** ¿Qué tan importante es la seguridad de la información para las operaciones de la empresa?

Objetivo: Determinar la importancia que la empresa da al tema de la seguridad de la información.

- **Pregunta 3.** ¿Cómo se controla la segregación de funciones de los colaboradores dentro del área de ventas?

Objetivo: Conocer la segregación de funciones dentro de la entidad.

- **Pregunta 4.** ¿Considera que maneja información de carácter confidencial o importante de los clientes?

Objetivo: Evaluar la conciencia que se tiene acerca de la información que se recopila de las operaciones de la entidad.

- **Pregunta 5.** ¿Qué tipo de información se solicita a los clientes?

Objetivo: Conocer la información que se maneja dentro de la empresa.

- **Pregunta 6.** ¿Qué medios utilizan para solicitar información personal de los clientes?

Objetivo: Conocer acerca de los medios utilizados para la recopilación de datos de clientes.

- **Pregunta 7.** ¿Cuáles son los medios y/ o lugares de almacenamiento para el resguardo de la información de los clientes?

Objetivo: Conocer los medios de almacenamiento y respaldo que se utilizan para garantizar el acceso oportuno y fiable de la información.

- **Pregunta 8.** ¿Cuáles son los procesos de la gerencia de ventas relacionados con el área financiera?

Objetivo: Conocer los procesos en que ambas gerencias están involucrados.

- **Pregunta 9** ¿Considera que sus procesos se realizan de manera segura o necesitan reforzarse?

Objetivo: Determinar si existe seguridad de información en los procesos que se realizan en el área.

- **Pregunta 10.** ¿Existe alguna manera de controlar los accesos que se tiene a la información que manejan dentro de la Gerencia de Venta?

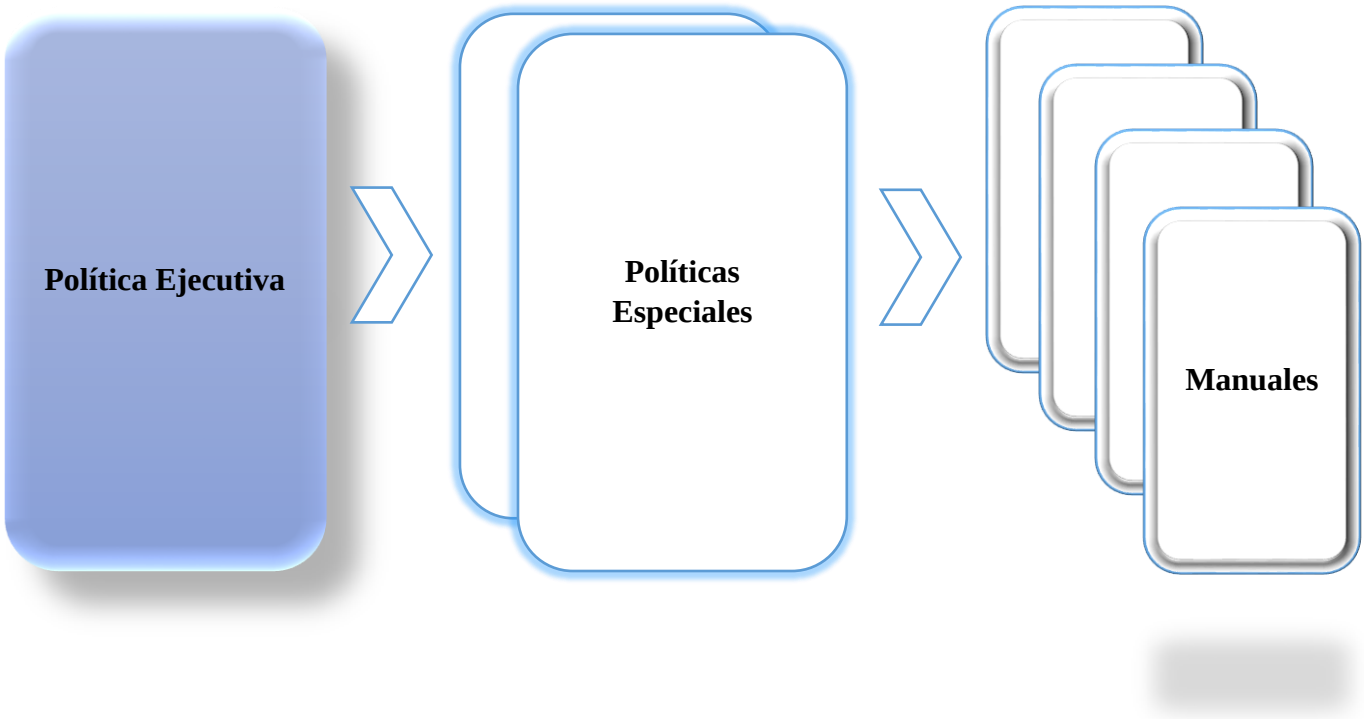
Objetivo: Cerciorarse si existen controles de acceso a la información dentro del área.

- **Pregunta 11.** ¿En algún momento ha sufrido pérdida o robo de información?

Objetivo: Identificar el riesgo a los que está expuesta la entidad en relación a la seguridad de información.

Anexo 4.

Niveles en las políticas de seguridad de la información



Anexo 5.

Clasificación de los activos de información.

Tipo de Activos	Descripción.
Información de la entidad.	Procesos y actividades de la empresa, base de datos de clientes, datos control de acceso y copias de respaldos.
Soporte de Información.	Documentación soporte de las operaciones y actividades, ya sea física o digital.
Equipos informáticos	Dispositivos físicos donde se almacena la información, equipos físicos que procesan los datos de forma directa o indirecta.
Redes de comunicación	Servicios de comunicación contratados a los proveedores.
Software	Todos los programas que contribuyen al funcionamiento de procesamiento de datos.
Instalaciones	Lugares donde están ubicados los activos de información de la empresa.
Personal	Todos los grupos de personas involucradas en el sistema de información.
Equipos auxiliares	Otros equipos que permiten soporte a los sistemas.