TRABAJO DE GRADO
Opción Seminario-Diplomado.

Implementación de Sistema de Control Interno por el Método COSO para la Empresa TRANS-CIA JDN SAS Basado en Tecnologías de la Información.

Corporación Universidad Remington
Facultad de Ciencias Contables
Contaduría Pública

Dayra Soraya Benavides Lopez
Nayely Yeraldin Cuasquer Portilla
Jesús Albeiro García Jaramillo
Robinson Jair Cordoba Cortes
Tutora
Diana Ximena Gallego Marín

Opción de Trabajo de grado Seminario
2025

Dedicatoria

En primer lugar, a Dios por guiar nuestro camino y brindarnos la paciencia suficiente para culminar con éxito nuestros estudios, también a padres, hermanos, hijos y demás familiares que han contribuido en nuestra formación académica y por último y no menos importante a nuestra docente Diana Ximena que con su esfuerzo y dedicación compartió sus conocimientos con nosotros para facilitarnos la realización de nuestro proyecto de grado.

Tabla de contenido

Resumen.

En el siguiente trabajo se abordará el sistema de control interno basado en el método COSO el cual establece parámetros para realizar auditoría interna donde garantice la estabilidad de la organización; así mismo se implementará dicho sistema dentro de la empresa de transporte y logística nacional e internacional TRANS-CIA JDN SAS para visualizar una serie de riesgos y/o amenazas que afecten el buen funcionamiento de la entidad.

Dentro de la empresa fue necesario observar la estructura organizacional, las políticas de buen gobierno, los objetivos misionales, los valores corporativos y los procesos propios de su actividad comercial, con ello se logró identificar riesgos financieros, de mercado y clientes, de talento humano y de TIC´S; dichas amenazas fueron evaluadas y valoradas de acuerdo con la probabilidad y severidad en caso de que ocurran y se anexaron al mapa de calor, el cual visibiliza la capacidad y tolerancia de los riesgos en la empresa; en otras palabras este mapa permite la identificación y priorización de los riesgos para establecer actividades de control y monitoreo, las cuales ayudan a minimizar o eliminar dichos riesgos.

Así mismo se establecen una serie de actividades de monitoreo, que facilita a la empresa la puesta en marcha de un plan de acción, que reduzca las amenazas y garantice la permanencia de la compañía dentro de los mercados nacionales e internacionales.

Palabras clave.

Control interno, COSO, riesgos, mapa de calor y matriz de riesgo, monitoreo.

Objetivos.

Identificar los riesgos que pueda presentar la empresa TRANS-CIA JDN SAS que afecten el funcionamiento de la organización.

Diseñar un protocolo de control interno que contribuya a minimizar o mitigar los riesgos identificados, basados en el modelo COSO.

Aplicar actividades de control y monitoreo que garanticen la eficacia del control interno.

Pregunta orientadora de la búsqueda.

En la actualidad las empresas de transporte de mercancía y logística se encuentran expuestas a diversas amenazas, incluyendo riesgos financieros, de talento humano, de clientes y mercancía, tecnológicos y de información, los cuales pueden comprometer la sostenibilidad de las organizaciones, afectando en si el patrimonio de sus socios e inversionistas, por tal razón es importante que todas las empresas cuenten con un sistema de control interno que ayude a detectar dichas amenazas.

En el siguiente trabajo se busca dar respuesta a la pregunta ¿Qué riesgos enfrenta la empresa TRANS-CIA JDN SAS realizando un control interno por el modelo COSO y cuáles son sus acciones o estrategias para mitigarlos o reducirlos a un nivel mínimo apoyados en las tecnologías de la Información?; es así como se hace necesario conocer un poco más de la empresa para identificar los riesgos y realizar control interno por medio del modelo COSO.

El control interno es una serie de normas y procesos que proporcionan seguridad en cuanto al cumplimiento eficaz y eficiente de los objetivos misionales de la organización, permitiendo reconocer amenazas que afecten el buen funcionamiento, previniendo la pérdida o mal uso de los recursos de la entidad.

De esta manera Barreto (2018) expresa que el control interno es “un proceso que constituye un medio para un fin” es decir, este procedimiento ayuda a proteger los activos de la empresa y es deber de todas las personas colaboradoras en la entidad contribuir con la minimización de los riesgos en la organización. También determina que el control interno se basa en una seguridad

razonable y no absoluta puesto que es imposible evaluar cada movimiento, transacción o actividad en su totalidad (Barreto Vasquez, 2018).

El control interno debe ser integrado en todos los departamentos de la empresa, así mismo debe ayudar a enfrentar los cambios, reducir los riesgos y proporcionar la toma de decisiones, de esta manera se presenta el modelo COSO como un método para facilitar el proceso de controlar la organización y mitigar las amenazas que se puedan presentar.

El modelo COSO es el marco de referencia para la implementación, gestión y control de un adecuado sistema de control interno y fue desarrollado con la finalidad de que las organizaciones establezcan sistemas de control interno efectivo, ayudando a identificar riesgos que se puedan presentar dentro de las empresas y como controlarlos para disminuir sus efectos negativos dentro de las mismas.

El resumen ejecutivo COSO 2013, distingue cinco componentes del control interno: entornos de control, evaluación de riesgos, actividades de control, información y comunicación y actividades de supervisión o monitoreo dichos componentes deben funcionar de manera integrada para obtener resultados concretos, de acuerdo con los objetivos misionales de la organización (COSO, 2013).

Entorno de control.

Es una serie de procesos, estructuras y normas que ayudan a realizar control interno dentro de las empresas, permitiendo establecer una estructura organizacional donde se determinen,

jerarquías, funciones, responsabilidades, políticas administrativas, de integridad y valores institucionales. (Padilla Ayllon Shirley & Sermeño Ortiz Viviana, 2021)

Evaluación de riesgos

"el riesgo se define como la posibilidad de que un acontecimiento ocurra y afecte negativamente a la consecución de los objetivos*"* (COSO, 2013) pág. 4; de esta manera es necesario que las organizaciones identifiquen las amenazas que se puedan presentar dentro de la organización e impidan el cumplimiento de los objetivos, por lo cual es necesario que se establezcan objetivos claros, medibles y alcanzables para cada dependencia de la empresa.

Actividades de control

Padilla & Sermeño (2021) citan a COSO 2013 y mencionan las actividades de control como acciones necesarias para cumplir con la normatividad de la organización logrando así reducir el impacto del riesgo a niveles bajos, facilitando el alcance de los objetivos organizacionales, dichas propuestas pueden ser clasificadas en preventivas cuando se quiere evitar que ocurran estas dificultades y de detección las cuales ayudan a identificar los riesgos inminentes (Padilla Ayllon Shirley & Sermeño Ortiz Viviana, 2021).

Información y comunicación

Al desarrollar los componentes de control interno es necesario brindar una información de calidad, donde se comunique e informe de manera clara los procesos, las actividades, la estructura organizacional, las funciones para cada colaborador y se tengan establecidos

parámetros y rutas de acceso a la información tanto interna como externa, es decir, para el personal colaborador de la empresa, pero también para los clientes y entidades de control.

Actividades de supervisión

Es necesario realizar evaluaciones continuas para verificar el cumplimiento de los componentes de control interno, si dichos determinantes están funcionando de manera eficaz y eficiente en el control de la organización, dichos análisis deben ser constantes y sorpresivos para emitir conceptos sobre los alcances y deficiencias en el control interno de la organización (COSO, 2013).

Según Becerra & Sulca (2017) expresan que el modelo COSO facilita la elaboración de una Matriz de Riesgo, con el objetivo de valorar la administración del riesgo a través de una evaluación del impacto y la probabilidad de ocurrencia, reconociendo los parámetros del Marco de Gestión de Riesgos Empresariales, también conocido como COSO ERM o COSO II, que determina los riesgos empresariales y las normativas actuales en cuanto a riesgos operativos (Becerra Paguay & Sulca Córdova , 2017).

Cabe mencionar que la matriz de riesgo facilita la identificación de las amenazas dentro de las organizaciones su impacto y probabilidad en las mismas, en dicha matriz es posible referenciar los riesgos tanto en severidad como en probabilidad de ocurrencia de manera cuantitativa y cualitativa determinándole un valor de acuerdo con la implicación de cada riesgo, para incluirlos en un mapa de calor el cual identifica la capacidad y tolerancia que tiene la empresa para enfrentar el riesgo.

Metodología de la búsqueda de la información.

El trabajo tendrá un enfoque mixto tanto cualitativo como cuantitativo en el cual se hace un análisis de los procesos y posibles riesgos que comprometen a TRANS-CIA JDN SAS en su buen funcionamiento.

Para ello se hará una revisión documental donde se analizarán las políticas, procedimientos e informes que nos permitan detectar las amenazas financieras, de talento humano, de mercados y clientes y tecnologías de la información, utilizando el modelo COSO como aliado estratégico para evaluar los riesgos con objetividad, su probabilidad de ocurrencia, su severidad y su magnitud.

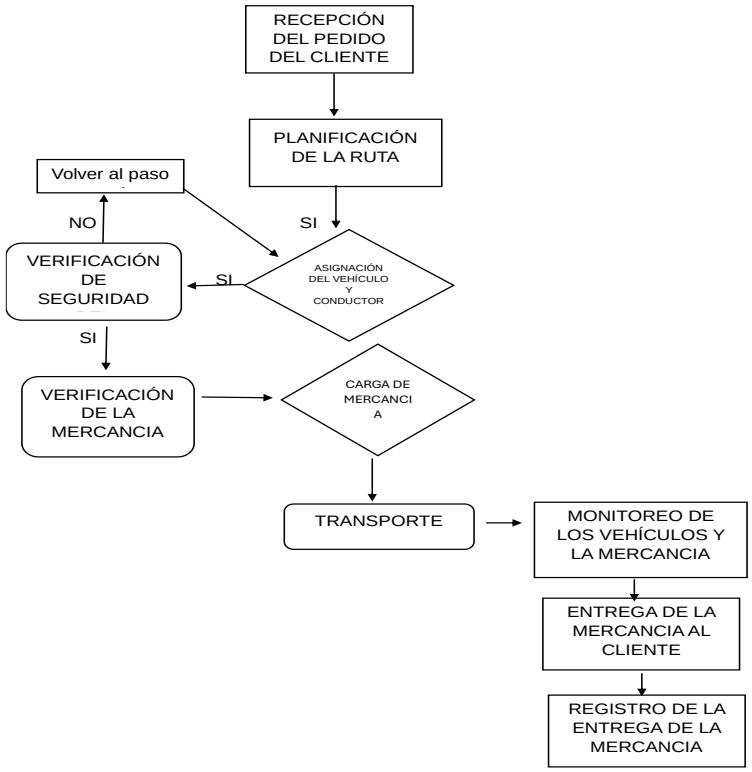
Por lo anterior podemos definir la probabilidad y severidad de manera cualitativa con los valores de riesgo muy bajo, bajo, medio, alto y muy alto y cuantitativamente enumerados del 1 al 5 siendo el 1 muy bajo y el 5 muy alto.

Sustentación teórica de la pregunta.

Flujograma.

En la siguiente representación gráfica podemos observar la presentación visual de los pasos y tareas para el adecuado proceso en el transporte de cargue y descargue de mercancías en la empresa TRANS-CIA JDN SAS.

Ilustración 1 Flujograma. Proceso Trans de Mercancía



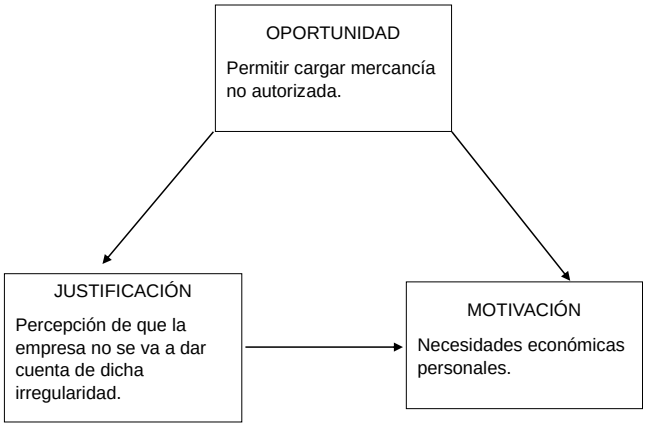
Fuente: elaboración propia

Triángulo del Fraude.

En el triángulo del fraude podemos establecer posibles argumentos que llevan a los colaboradores de una organización a cometer acciones fraudulentas que ponen en riesgo la

organización en cuanto a su estabilidad operativa y financiera, dando como resultado la oportunidad de cometer el fraude, la justificación del por qué y la motivación que tuvo para hacerlo.

Ilustración 2 Triángulo del Fraude



Fuente: elaboración propia

Componentes del control interno modelo coso

Ambientes de control.

La organización establece roles y funciones específicas para cada colaborador.

Puntos de enfoque. Establece manual de funciones para cada uno de los colaboradores de la empresa, dispone de jefe inmediato para cada área, supervisan el desempeño de cada colaborador.

La junta directiva desarrolla políticas administrativas y operativas que faciliten la toma de decisiones para el buen desarrollo de la empresa.

Puntos de enfoque. Cuentan con manual de procedimientos de las operaciones nacionales e internacionales, hacen seguimiento a los objetivos organizacionales para cumplir con la visión de la empresa, realizan encuestas de satisfacción de los clientes, aplicación de mejoras continuas, ejecutan capacitaciones y desarrollo continuo del personal.

La empresa implementa un código de ética sobre el comportamiento de los empleados y la dirección de la empresa.

Puntos de enfoque. Provee de canales seguros para reportar conductas inapropiadas de los empleados sin temer a represalias, aseguran el cumplimiento de todas las leyes y regulaciones aplicables al transporte de carga, seguridad y medio ambiente, establecen procedimientos para reportar violaciones legales.

El personal colaborador conoce y pone en práctica los valores institucionales.

Puntos de enfoque. Cumplen con lo estipulado en el horario de entrega de las mercancías, comunicación clara y efectiva para proporcionar información precisa sobre los servicios.

La empresa adopta un enfoque de calidad en el servicio prestado.

Puntos de enfoque. Aplica innovación en los servicios, adopta nuevas tecnologías que mejoren la seguridad en el transporte de la mercancía.

Valoración del riesgo

- Actividades ilícitas que involucren a la empresa en actividades como: Corrupción, soborno, contrabando, lavado de activos, financiamiento al terrorismo y proliferación de armas de destrucción masiva.

- Control deficiente, al no contar con formatos controlados, que den cuenta de la trazabilidad de las operaciones.

- Retiro de clientes.

- Tramitar documentación adulterada para operaciones de transporte nacional o internacional.

- Contaminación de la carga.

- Corrupción en la inspección de vehículos.

En la siguiente tabla se puede observar la identificación de los riesgos y el impacto que genera a la empresa.

Tabla 1 Valoración del riesgo

IDENTIFICACIÓN DEL RIESGO	IMPACTO
Actividades ilícitas que involucren a la empresa en actividades como: .-Corrupción soborno .-Contrabando, lavado de activos .-Financiamiento al terrorismo y proliferación de armas de destrucción masiva	Baja orientación en los temas de corrupción que involucran tanto a las partes interesadas, así como también, el incumplimiento de la política empresarial donde se prohíbe la realización de actividades ilícitas que atenten contra el buen nombre de la organización.
Control deficiente, al no contar con formatos controlados, que den cuenta de la trazabilidad de las operaciones	No contar con métodos que permitan ejercer un control eficiente para definir la trazabilidad del proceso.
Retiro de clientes.	Insatisfacción por el servicio prestado, nuevos competidores, Tarifas altas.
Tramitar documentación adulterada para operaciones de transporte nacional o internacional.	Falta de capacitación, falta de proceso de inducción, soborno de terceros para conveniencia
Contaminación de la carga.	Aumento de la delincuencia, falta de empleo, delincuencia común y organizada, vinculación insegura de personal y de conductores y unidades de carga
Corrupción en la inspección de vehículos.	Carencias económicas de los empleados, Incumplimiento de los controles establecidos falta de seguimiento en los procesos de vinculación.
Clientes desatendidos.	Falta de programación de visitas comerciales, llamadas telefónicas, invitaciones comerciales.
Incumplimiento de pagos de los clientes.	Falta de seguimiento y análisis de comportamiento de pago, por parte de Comercial. Los acuerdos de pago no fueron evaluados en el proceso de vinculación.
Fallas en el sistema syscar.	La falta de mantenimientos preventivos y actualizaciones del software.

Fuente: elaboración propia

Actividades de control.

1. Verificación de la mercancía cargada.
2. Instalar precinto de seguridad y candado satelital al vehículo.
3. Realizar monitoreo de vehículos en ruta.
4. Implementar un método en donde se evidencien datos con relación a fechas y encargados del proceso de registro de formatos.
5. Visitas periódicas a clientes.
6. Aplicación de encuestas de satisfacción.
7. Contratación del Personal de confianza idóneo y capacitado.
8. Realizar capacitación, proceso de inducción, asignar un tutor por los primeros días.
9. Capacitación del personal en prevención de lavado de activos y financiación del terrorismo.
10. Solicitar un reporte de cartera quincenal.
11. Realizar recordatorio de pagos.
12. Mantenimientos preventivos del software y de los equipos de cómputo.

Información y comunicación.

Existe documentación clara sobre las normas y políticas de la empresa; se encuentran expuestos en carteleras la misión, visión, filosofía, organigrama y valores institucionales de la organización; además, cada área cuenta con los documentos donde se establece el manual de funciones para cada empleado y su jefe inmediato, las actas de responsabilidades de los conductores, de los despachadores, monitores de control de tráfico y del dueño de la mercancía.

La empresa cuenta con página web donde presenta sus datos de ubicación y contacto, sus clientes potenciales, sus servicios y los protocolos a seguir en caso de presentar algún problema

en el transporte de la mercancía como son: robos, bloqueos de vía (paros, movilizaciones y grupos armados), siniestros viales (accidentes de tránsito, derrumbes, etc.), fallas mecánicas, enfermedad de conductor. etc.

Así mismo la empresa cuenta con procesos de capacitación y formación continua para dar cumplimiento a las regulaciones y normativas vigentes sobre el proceso de transporte de carga nacional e internacional (importación y exportación).

Se solicitan informes periódicos de monitoreo y control para evitar riesgos en el cargue y transporte de mercancías.

Monitoreo

1. Reporte de cartera quincenal.
2. Auditorías internas inesperadas.
3. Comparativo de clientes satisfechos por medio de encuestas de satisfacción.
4. Indicador de novedades.
5. Formatos de asignación de precintos.
6. Cronograma de capacitaciones por año.
7. Revisión periódica de los computadores.
8. Supervisión de hojas de vida (filtro de seguridad).
9. Indicador de despachos mensuales.
10. Control de ruta, monitoreo de vehículos.
11. Verificación de antecedentes del vehículo y el conductor.

Matriz de análisis de riesgo o determinación del nivel de riesgo.

En la siguiente tabla se puede observar un análisis de los riesgos la probabilidad de ocurrencia, la severidad, es decir, cuanto puede afectar esta amenaza a la organización y la magnitud del riesgo el cual es el resultado de multiplicar la probabilidad por la severidad, dichas probabilidades y severidades son puntuadas del 1 al 5 donde 1 es muy bajo y 5 muy alto.

Tabla 2 Matriz de análisis de riesgos o determinación del nivel de riesgo

N°	VARIABLES	NOMBRE DEL RIESGO	PROBABILIDAD	SEVERIDAD	MAGNITUD
1	**FINANCIERO**	Inadecuadas proyecciones financieras.	3	3	9
2		Manipulación del aplicativo de las cuentas bancarias por hackers (TI).	3	4	12
3		Falta de liquidez.	2	5	10
4		Gastos imprevistos en operaciones.	4	4	16

5	**CLIENTES Y MERCADO**	Retiro de clientes.	3	5	15
6		Tramitar documentación adulterada para operaciones de transporte nacional o internacional.	2	5	10
7		Actividades ilícitas que involucren a la empresa en actividades como: corrupción soborno. Contrabando, proliferación de armas de destrucción masiva.	2	4	8
8		Control deficiente, al no contar con formatos controlados, que den cuenta de la trazabilidad de las operaciones.	5	3	15
9		Dependencia de plataforma syscar para despacho de vehículos TI	5	5	25

10	**TALENTO HUMANO**	Incumplimiento de requisitos legales asociados a la contratación y gestión de personal.	3	5	15
11		Vinculación de personal, que no cumpla el perfil y requisitos establecidos por la organización.	1	4	4
12		Accesibilidad a la base de datos de clientes sin restricciones, ni políticas de confidencialidad TI.	4	5	20
13		Inasistencia del personal a las capacitaciones programadas.	1	4	4
14		Asignación de nuevas funciones informalmente.	3	4	12
15	**TIC´s**	Fallas en el sistema SYSCAR.	3	4	12

16	Pérdida o alteración de la información producto de un ataque cibernético y/o virus.	1	5	5
17	Accesos no autorizados a aplicativos	1	4	4
18	Alteración de la configuración de seguridad de los sistemas de información.	3	3	9
19	Daño físico de equipos tecnológicos: Impresoras, computadores, celulares.	3	3	9

Fuente: elaboración propia

Matriz de probabilidad por severidad.

Tabla 3 Mapa de calor

Probabilidad	Severidad				
	1. Muy baja	**2.Baja**	**3.Media**	**4.Alta**	**5.Muy alta**
5.Muy alta			8(15)		9(25)
4.Alta				4(16)	12(20)
3.Media			1(9);18(9);19(9)	2(12);14(12);15(12)	5(15);10(15)
2.Baja				7(8)	3(10);6(10)
1.Muy baja				11(4);13(4);17(4)	16(5)

Fuente: elaboración propia

En la anterior tabla se puede observar la matriz de probabilidad por severidad o mapa de calor, el cual por medio de la matriz de análisis de riesgo propicia información relevante del riesgo y el nivel de afectación que puede presentar dentro de la empresa, es por ello que se identifica con colores y muestra la capacidad y tolerancia que la empresa puede soportar estos riesgos.

El color rojo presenta un nivel muy alto del riesgo donde la organización debe tomar medidas preventivas de inmediato para que las amenazas que se encuentren en este nivel se logren disminuir a un nivel mínimo o aceptable para que no ocasione desestabilizar la empresa y el color verde oscuro demuestra que existe un riesgo detectado en la entidad pero que es muy bajo, sin embargo, es necesario prestarle atención para que este riesgo no aumente.

Implementación de controles

A continuación, se estructuran una serie de actividades donde se implementan controles para mitigar y reducir los riesgos identificados en la matriz de análisis de riesgos (ver tabla 2) a un

nivel mínimo donde la empresa pueda soportar estas amenazas; se menciona el número del riesgo y las posibles acciones para minimizarlos.

Riesgo 1. Realizar presupuestos de ingresos y gastos para corto, mediano y largo plazo; presentar alertas sobre movimientos que representen un riesgo financiero.

Riesgo 2. Cambiar con frecuencia las claves de acceso a los aplicativos; acceso restringido a las claves de acceso; solicitar permisos de acceso si van a ingresar de un dispositivo no registrado (TOKENS).

Riesgo 3. Recurrir a préstamos con entidades financieras; ofrecer descuentos por pronto pago; controlar recaudo de cartera informando al cliente con 5 días de anterioridad al vencimiento de su factura.

Riesgo 4. Controlar los gastos de operación, con mantenimientos preventivos a los vehículos; contratar con gasolineras, talleres y parqueaderos que nos ofrezcan precios estándares por un tiempo determinado.

Riesgo 5. Aplicación de encuestas de satisfacción; visitas a clientes; enviar reportes y confirmar recibidos de conformidad con el cliente.

Riesgo 6. contratación del Personal de confianza idóneo y capacitado; establecer controles informáticos para el manejo de las variables que afectan las operaciones y elaboración de documentos; realizar capacitación, proceso de inducción, asignar un tutor por los primeros días.

Riesgo 7. Realizar controles inesperados sobre los procedimientos; monitorear los procesos de cargue y los vehículos en ruta; instalar precinto de seguridad y candado satelital al vehículo.

Riesgo 8. Implementar formatos digitales y físicos en donde se evidencien datos en relación con fechas y encargados del proceso.

Riesgo 9. Contratar plataforma alterna; diseñar plantillas que permitan despachar los vehículos hasta que se solucione el error en la plataforma.

Riesgo 10. Contratar asesoría jurídica y laboral; capacitar al jefe de talento humano en nuevas leyes y regulaciones de contratación; establecer procedimiento de contratación del personal.

Riesgo 11. Realizar un riguroso proceso de selección, contratación y retiro de personal.

Riesgo 12. Hacer firmar actas de compromiso y confidencialidad al iniciar un contrato laboral; restringir el acceso a las bases de datos de los clientes; generar copias de seguridad de las bases de datos y cargarlos a la nube.

Riesgo 13. Asegurar que los temas de capacitación sean de interés para todo el personal; estipular obligatoriedad de asistencia a las capacitaciones; controlar la asistencia a las capacitaciones por el jefe inmediato.

Riesgo 14. Mantener actualizado el manual de funciones.

Riesgo 15. Mantenimiento preventivo del aplicativo; capacitación permanente en el uso del sistema syscar; mantener los equipos de cómputo actualizados y protegidos con antivirus.

Riesgo 16. Establecer e implementar política de seguridad de información; realizar backus de seguridad de la información y cargue a la nube; mantener los antivirus actualizados.

Riesgo 17. Asignar perfiles de acuerdo con el nivel jerárquico, restringiendo el acceso a información.

Riesgo 18. Implementar políticas de uso de recursos informáticos; controlar las cuentas de usuario, actualizarlas y eliminar las de usuarios que ya no pertenezcan a la institución; limitar acciones de acuerdo con las funciones de cada colaborador.

Riesgo 19. Ejecutar programas de mantenimiento de los equipos; renovar equipos tecnológicos de acuerdo con necesidades por obsolescencia o mejorar rendimiento funcional; capacitación al personal de uso adecuado de los medios tecnológicos.

Conclusiones.

Implementar un correcto sistema de control interno dentro de las empresas, facilita la toma de decisiones frente a riesgos inminentes.

El modelo COSO permite detectar riesgos dentro de una organización y establecer actividades de control y monitoreo pertinentes para la minimización o eliminación de estos.

La empresa TRANS-CIA JDN SAS presenta un riesgo muy alto en cuanto a la dependencia del sistema Syscar, pues si este presenta falla la empresa se ve obligada interrumpir sus operaciones, para esto es necesario que la empresa contrate un sistema alterno o construya plantillas para realizar las actividades manuales y cuando el aplicativo vuelva a funcionar, registrar la información del cargue y descargue de vehículos.

También es necesario que la organización establezca políticas de confidencialidad por parte del personal colaborador para evitar perdida de clientes y competencia desleal.

Por último, evidenciamos que ajustar un sistema de control interno de acuerdo con las necesidades de las empresas, garantiza la continuidad de la compañía dentro de los mercados.

Referencias.

Barreto Vasquez, L. H. (2018). Caracterización del control interno en el area de logistica de las empresas del sector servicios del Peru: caso "empresa de servicios santa monica S.R.L.". Obtenido de https://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/4140/ALMACEN_TRANSPORTE_BARRETO_VASQUEZ_LITICIO_HOMAR.pdf?sequence=1&isAllowed=y

Becerra Paguay, E. R., & Sulca Córdova , G. C. (2017). *Control interno. Matriz de riesgo: Aplicación metodología COSO II*. Obtenido de https://revistapublicando.org/revista/index.php/crv/article/view/686/pdf_491

COSO. (2013). *resumen ejecutivo*. Obtenido de https://www.pj.gob.pe/wps/wcm/connect/8ba7cc8040809738ac41ed9515c1560a/3.-+COSO+2013+Resumen+Ejecutivo.pdf?MOD=AJPERES

Padilla Ayllon Shirley & Sermeño Ortiz Viviana. (2021). *propuesta de implementación de un sistema de control interno basado en el modelo coso en el area de logística de una empresa agroindustrial. caso Paprika Perú sac 2019*. Obtenido de https://repositorio.unsa.edu.pe/server/api/core/bitstreams/4d2c5be0-5189-4ebc-8616-c74c51a18a1f/content