PLANTEAMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN APLICANDO LA NORMA NTC ISO/IEC 27001 – 27002 DEL 2013 EN EL PROCESO DE LA REVISIÓN TÉCNICO - MECÁNICA DEL CDA CORPOTRANS

EDNA ROCIO GIRALDO REINA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2019

PLANTEAMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN APLICANDO LA NORMA NTC ISO/IEC 27001 – 27002 DEL 2013 EN EL PROCESO DE LA REVISIÓN TÉCNICO - MECÁNICA DEL CDA CORPOTRANS

EDNA ROCIO GIRALDO REINA

PROYECTO DE GRADO

DIRECTOR

EDGAR ALONSO BOJACA GARAVITO

INGENIERO ELECTRÓNICO ESPECIALISTA EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS E INGENIERIA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2019

Nota de aceptación:

Firma de presidente del jurado

Firma del jurado

Firma del jurado

Ibagué (fecha)

Dedicatoria

A Dios padre celestial por ser mi guía y el motor de vida que brinda habilidad, sabiduría e inteligencia para encaminar los objetivos de vida al éxito y al triunfo con el apoyo de familiares, padres y hermanos quienes han sido el acompañamiento más importante en todos los momentos de vida profesional y laboral.

A las personas que él ha puesto en el ámbito laboral, quienes han sido parte esencial para mi formación profesional y así mismo un camino de aprendizaje y grandes triunfos profesionales, los cuales me permiten aportar grandes ideas en la elaboración y diseño de proyectos.

A mis profesores y tortures quienes dedican su tiempo y esfuerzo para formar grandes profesionales y hacer posible aquellas ideas que nos brindan estabilidad, seguridad y confianza para el entorno.

Edna Rocio Giraldo Reina.

Agradecimientos

Quiero dar gracias a Dios y a los directivos del centro de diagnóstico automotor Corpotrans CDA, quienes han contribuido en este logro como profesional y a su vez han depositado su confianza, permitiendo manejar la documentación confidencial y los aportes para el mejoramiento de la organización.

A su vez quiero agradecer al Ingeniero Edgar Alonso Bojacá Garavito, por su enseñanza, dedicación y acompañamiento, durante el desarrollo y aplicación de las metodologías al diseño e implementación de la norma NTC ISO/IEC 27001 – 27002 DE 2013 en el centro de diagnóstico automotor, el cual es el medio para un gran logro a nivel educativo y en el ámbito laboral.

Así mismo agradezco al tutor Christian Reynaldo Angulo por sus asesorías las cuales contribuyeron en el cumplimiento de los objetivos planteados en las guías para el desarrollo del proyecto de grado.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

ANEXOS

GLOSARIO

SISTEMA DE GESTIÓN: Un sistema de gestión es una manera de trabajar, con el fin de que una organización asegure las necesidades de sus clientes, para lo cual planifica, mantiene y mejora continuamente de sus clientes. Para lo cual planifica de forma continua el desempeño de los procesos, con esto puede generar ventajas competitivas.

MECÁNICA DEL CDA: Es un procedimiento obligatorio que utilizan en Colombia como autoridad para determinar si los vehículos poseen las condiciones mecánicas óptimas para poder circular por las vías públicas y privadas del país.

SEGURIDAD INFORMÁTICA: La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información con la que cuenta una organización, que, por supuesto tiene un sistema informático, sin embargo, existe diferentes formas en las que se puede violentar dicha información.

METODOLOGÍA MAGERIT: Es conocida como un método para el análisis y gestión de riesgos de los sistemas de información elaborada el Consejo Superior de Administración Electrónica para garantizar el buen uso de las TIC y minimizar los riesgos de implantación en las administraciones públicas, y más reciente mente en el sector privado.

RESUMEN

El proyecto tiene como propósito implementar controles, procesos y procedimientos que le permitan conocer al administrador del sistema de gestión y la alta dirección la seguridad a nivel físico, lógico, y recurso humano, el objetivo fue, Plantear un sistema de gestión de seguridad de información que permita establecer políticas, controles y procesos en el Centro De Diagnóstico Automotor basados en la norma NTC ISO/IEC 27001 – 27002 del 2013 para proponer una mejora continua y preservar la confidencialidad, integridad y disponibilidad en los procesos de la revisión técnico - mecánica. La metodología utilizada se basó en el enfoque cuantitativo que permitió verificar el estado del CDA frente a los requisitos de las normas que establecen el cumplimiento para la seguridad informática y de información basándose en la NTC – ISO/IEC 27001, las conclusiones dieron cuenta de la identificación y estado actual tanto de hardware, como del software, aplicaciones web, la transferencia de información en línea y el personal en todo el proceso de revisión técnico – mecánica, es de vital importancia para conocer cuáles son los requisitos de cumplimiento en la prestación de sus servicios y las necesidades de mejora que cada uno de los mismos requiere.

Palabras clave: NTC ISO/IEC 27001 – 27002, MECANICA, GESTION DE CALIDAD, CDA.

INTRODUCCIÓN

El centro de diagnóstico automotor CDA es una empresa dedicada a prestar servicios de revisión técnico - mecánica y de emisiones contaminantes a todo vehículo automotor público o particular que transite a nivel nacional. el organismo de inspección cuenta con la acreditación del organismos nacional de Colombia ONAC frente a la NTC ISO/IEC 17020: 2012, y demás normas que se deriven para garantizar la prestación del servicio, en cumplimiento con las especificaciones del servicio, el CDA debe establecer controles, procesos y procedimientos de seguridad específicos a todo el sistema de información que compone la revisión técnico - mecánica, los cuales garantizan la confidencialidad, integridad y disponibilidad de la información.

Actualmente no se cuenta con los recursos primordiales para la seguridad del software, la información, bitácoras de seguimiento a cada una de las herramientas informáticas, quedando expuesta a los delitos informáticos, de modo que la información se encuentra accesible en formato físico y lógico por medio de la base de datos del software de aplicación, siendo esta vulnerable desde personal interno como externo, por lo anterior se requiere implementar y establecer un sistema de gestión en seguridad de la información e informática que permita conocer el nivel de impacto que tienen los activos como vulnerabilidades, riesgos y amenazas que pueden llegar afectar todas las actividades propias de la empresa.

El proyecto tiene como propósito implementar controles, procesos y procedimientos que le permitan conocer al administrador del sistema de gestión y la alta dirección la seguridad a nivel físico, lógico, y recurso humano, los cuales deben estar alineados con los principios generales de la confidencialidad e imparcialidad de la prestación del servicio.

La delimitación del proyecto se centra en la necesidad de implementar herramientas de detección de intrusiones en la red, el acceso a la información confidencial tanto del software de aplicación como de la empresa, y en la perdida de los datos enviados exitosamente al servidor, encontrado las actividades en estado pendiente y la base de datos sin ningún registro, con el fin de determinar si son fallas derivadas por el estado de la estructura de la red o errores propios del software.

1. TITULO

Planteamiento Del Sistema De Gestión De Seguridad De Información Aplicando La Norma NTC ISO/IEC 27001 – 27002 Del 2013 En El Proceso De La Revisión Técnico - Mecánica Del CDA Corpotrans.

2. PLANTEAMIENTO DEL PROBLEMA

Los centros de diagnóstico automotor son entidades privadas o públicas que tienen como función prestar servicios de inspección mecanizada y de emisiones contaminantes a todo el al parque automotor a nivel nacional y la responsabilidad de emitir un diagnostico a las entidades legales acorde a las condiciones de los vehículos. De acuerdo a la responsabilidad que se tiene frente a estos procesos el ministerio de transporte y la superintendencia de puertos y transporte, a determinado disposiciones de estricto cumplimiento que les permita garantizar que se ha realizado una inspección completa, confiable y segura. Para lo cual ha implementado sistemas de control y vigilancia tanto a las instalaciones físicas – cámara de vigilancia como el resultado de la inspección aplicando auditoria permanente al software de aplicación y monitoreo de las estaciones que se envían los registros.

De acuerdo a la implementación de los sistemas informáticos, los CDA`S deben llevar a cabo mejoras en su infraestructura tecnológica de tal manera que le permita brindar conectividad a la empresa homologada por la entidad legal para ejercer su control y vigilancia solo a los registros de revisión técnico - mecánica y proteger la información que se comparte de los demás sistemas informáticos en red, los cuales presentan vulnerabilidad por falta de controles y permisos solo a los usuarios que jerárquicamente están autorizados como se presenta en el software de aplicación e información administrativa y del sistema de gestión.

La implementación de las NTC ISO/IEC 27001 de 2013, permitirá dar cumplimiento a las especificaciones del servicio, diseño y mejora de los procesos direccionados a garantizar la seguridad informática y de información a nivel de software y de hardware por medio de la guía técnica colombiana GTC-ISO/IEC 27002, en la que

se determinan controles a la seguridad de los sistemas informáticos y se gestionan los recursos tecnológicos a partir de las buenas prácticas para una mejora continua.

De acuerdo al funcionamiento de los CDA y los requisitos de cumplimiento frente a las leyes, resoluciones y normas que los acreditan y habilitan se propone ¿Establecer el sistema de gestión de seguridad informática y de información basado en la NTC ISO/IEC 27001-27002 de 2013, el cual permite alinear los procesos de cumplimiento y gestionar un control frente a las vulnerabilidades de los elementos que conforman el proceso de revisión técnico - mecánica?

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Plantear un sistema de gestión de seguridad de información que permita establecer políticas, controles y procesos en el Centro De Diagnóstico Automotor basados en la norma NTC ISO/IEC 27001 – 27002 del 2013 para proponer una mejora continua y preservar la confidencialidad, integridad y disponibilidad en los procesos de la revisión técnico - mecánica.

3.2. OBJETIVOS ESPECÍFICOS

- ✓ Conocer el estado actual de la seguridad informática, de información en el centro de diagnóstico automotor.

- ✓ Plantear la matriz de los riesgos identificando las vulnerabilidades y amenazas presentadas a todos los activos preservando la confidencialidad, integridad y disponibilidad.

- ✓ Establecer mecanismos de sensibilización de la seguridad y protección a los activos software, redes, y personal que interviene directamente con los procesos y el manejo del software de aplicación para la revisión técnico - mecánica.

4. JUSTIFICACIÓN

Actualmente, los sistemas de información son el activo más importante y soporte central de las organizaciones; en la cual se articulan las prácticas del personal con los procesos y la tecnología. Estas herramientas facilitan las oportunidades de la mejora y la protección de la información fortaleciendo la confidencialidad, la disponibilidad e integridad de los sistemas de información, sin embargo, su aplicación en el sistema organizacional, no ha sido exitoso, lo cual da paso para el acceso a la información desde diferentes equipos informáticos; pasando por alto los parámetros de seguridad en la información establecidos, los cuales están siendo implementados en coyuntura tecnológica. En donde se busca garantizar su confidencialidad, disponibilidad e integridad.

La identificación de las vulnerabilidades, riesgos y amenazas a los que se enfrentan las aplicaciones, los equipos y las personas; permite establecer procesos los cuales proponen la mejora continua para cada uno de los activos y a su vez disminuir el nivel de ocurrencia de las amenazas en la seguridad informática (y de la información) respectivamente. De esta manera los funcionarios deben cumplir con las políticas, normas y medidas preventivas implementadas en la organización como la “cultura de seguridad y control informático” al interior del centro de diagnóstico automotor, se gestiona con el fin de ser usado por los funcionarios, y en ese sentido, creen conciencia sobre la necesidad de proteger el equipamiento informático que se les ha asignado. Así mismo, se protege la información del acceso no autorizado: la manipulación indebida, copia, publicación o alteración accidental o intencional del Software de aplicación, con el fin de garantizar su confiabilidad, disponibilidad e integridad. Por último, el cumplimiento con las normas, políticas, procedimientos y medidas preventivas de seguridad implementadas para el manejo de equipos informáticos e información sistematizada.

5. MARCO TEÓRICO

Los centros de diagnóstico automotor es un ente estatal o privado que nace a partir del código nacional de tránsito – ley 769 de 2002 y las disposiciones que allí se determinan para todo el territorio nacional y regulan la circulación de todo el parque automotor. Por media una serie de pruebas aplicadas a los vehículos que les permita conocer si es apto para transitar. De esta manera los CDA operan en línea con entes legales como el Runt – registro único nacional de tránsito a donde se encuentra toda la información pertinente de los vehículos, propietarios, y el cumplimiento de las disposiciones por parte de los propietarios con el código nacional de tránsito.

Debido a la responsabilidad que tienen los centros de diagnóstico en cuanto a la inspección y registro de resultados, surgen otras disposiciones de cumplimiento que le permite a los entes de control como: ministerio de transporte y superintendencia de puertos y transporte vigilar el cumplimiento del proceso por parte de los CDA y que la información que envían sea la correspondiente al vehículo, para esto todos los establecimientos han tenido que realizar mejoras a su estructura de red y equipos informáticos, de modo que debe existir conectividad en tiempo real.

De acuerdo al cumplimiento la infraestructura de red está en permanente control y supervisión de los procesos que se realizan en las líneas de inspección, por lo tanto, se debe garantizar la confidencialidad, disponibilidad e integridad de los datos que se transmiten y la base de datos del software de aplicación que los contiene. Teniendo en cuenta la implementación de nuevas tecnologías, la exigencia por parte de los entes legales y los costos de operación que esto trae para la organización le permitirá ser competitivo y con un bueno posicionamiento en el mercado a nivel regional. Para lo cual se deben tener claro los conceptos y aplicación de la

seguridad informática y de información que permitan brindar confiabilidad, disponibilidad e integridad de los activos que intervienen en el proceso.

Información En La Organización: Para el centro de diagnóstico automotor la información es fundamental para su funcionamiento a nivel administrativo, financiero, técnico, y operacional, por lo que se debe disponer de herramientas que permitan auditar los procesos informáticos y a partir de sus resultados definir las políticas de seguridad informática e información que garanticen el óptimo funcionamiento.

Prevención de Ataques Informáticos: Es importante para la seguridad de la información la implementación de controles, que permitan prevenir los posibles atentados a la información importante para el CDA por tal motivo se debe asegurar:

- ✓ Protección a los activos.
- ✓ Protección a la información (base de datos del software de aplicación, información sistemática y los registros).
- ✓ Protección de equipos (equipos informáticos, infraestructura de red).
- ✓ Implementar o actualizar las políticas, procesos y procedimientos que conforman la estructura organizacional.

Estándares De Seguridad De La Información: Los estándares como ISO/ IEC 27001 y 27002, promueven las medidas preventivas que permiten proteger la información y con ella mantener la confidencialidad, integridad y disponibilidad, promoviendo la mejora continua del CDA.

Confidencialidad: en la seguridad informática y de información tienen el objetivo de garantizar que la información solo esté disponible para personas autorizadas y almacenada en el sistema informático transmitida por la red, y en base de datos se identifique desde que equipo fue enviada a través de la IP. De manera se evita modificación y alteración en los datos registrados en la base de datos.

Integridad: el software de aplicación reporta los datos a la base de datos identificando desde que equipo fue enviada por medio de la IP, se esta manera se garantiza que los datos no sean modificados desde su creación, permitiendo disponer de una información valida y consistente.

Disponibilidad: el software de aplicación y la información registrada debe estar disponible en todo momento, permitiendo la validar los registros y cada una de plataformas accesibles para realizar el registro de los datos obtenidos.

Metodología De Análisis Y Gestión De Riesgos Magerit: la metodología fue desarrollada por el Consejo Superior de Administración Electrónica, en el que siguen la terminología de la ISO 31000, en la que se implementan los procesos para la gestión de los riesgos generados desde las tecnologías de información, los cuales generan avance en los procesos administrativos y los cumplimientos de los objetivos y el alcance de una organización.

Magerit, se centra en el estudio y la clasificación de los activos de una organización con el propósito de corregir las acciones que generen un riesgo para los procesos, estableciendo acciones de mejora desde el análisis, valoración e implementación de controles que contribuyen a la mitigación del riesgo dentro de centro de diagnóstico automotor. Los cuales se asocian a elementos que permitan la creación,

eliminación, transferencia de información y a su vez se establece el tratamiento de riesgos para mitigarlo y hacer más segura la infraestructura tecnológica.

Con la identificación de los activos se permite clasificar y dar una descripción responsable del proceso y los soportes que se generan a partir de los datos reportados.

Tabla 1. Clasificación de activos

CLASIFICACIÓN DE ACTIVOS	
Tipo de activo	**Descripción**
Datos / información [D]	La información son un activo muy importante, yaqué le permite documentar su sistema de gestión y a partir de los reportes implementar mejoras en la continuidad del negocio.
Claves criptográficas [k]	Uso apropiado de las claves para proteger la confidencialidad, integridad y autenticidad de la información.
Servicios [S]	Están asociados, directamente con los usuarios – clientes y funcionarios.
Software [SW]	Aplicaciones dispuestas para el desarrollo de las funciones de forma automatizada a nivel administrativo y operativo.
Equipamiento informático [HW]	Equipos informáticos dispuestos para realizar sus funciones tanto administrativas como operativas.

Continúa…

CLASIFICACIÓN DE ACTIVOS	
Tipo de activo	**Descripción**
Redes de comunicaciones [COM]	Servicios de comunicaciones e instalaciones propias o de terceros – proveedores y cumple su función de transferencia de información.
Soportes de información [Media]	Son todos aquellos dispositivos físicos con los que cuenta el CDA para almacenar la información de forma permanente o por un tiempo determinado.
Equipamiento auxiliar [AUX]	Son dispositivos o elementos que forman parte del sistema informático, no están directamente relacionados con la información.
Instalaciones [L]	La infraestructura donde se encuentra el sistema informático, información y comunicaciones.
Personas [P]	Funcionarios responsables del sistema informático, información y comunicaciones.

Elaboración: propia.

Con la aplicación de la metodología en el centro de diagnóstico automotor se genera la clasificación de los activos y el análisis con los soportes de la información y los procesos de cada una de las áreas que intervienen en el proceso de revisión técnico - mecánica.

La valoración de los activos permite conocer el nivel de protección y la importancia que tiene frente a los procesos internos, con la identificación de la confidencialidad, integridad y disponibilidad que tiene los sistemas informáticos e información, los cuales se pueden determinar desde el modelo cuantitativo y cualitativo propuesto para el centro de diagnóstico automotor. Desde el modelo cuantitativo el valor del riesgo se clasifica como:

Tabla 2. Valoración de activos

VALORACIÓN DE ACTIVOS	
Criterio	**Concepto**
Muy bajo [MB]	Irrelevante a efectos prácticos
Bajo [B]	El daño puede presentarse rara vez
Medio [M]	El daño puede presentarse en algunas ocasiones
Alto [A]	El daño puede presentarse siempre
Muy alto [MA]	El daño representa peligro para el CDA

Elaboración: propia.

La valoración y análisis de los riesgos permite implementar el diseño del sistema de gestión de seguridad de información – SGSI bajo los requisitos de la NTC ISO/IEC 27001 – 27002 en cada una de las áreas que intervienen en el proceso de revisión técnico - mecánica, el cual tiene como finalidad brindar controles de seguridad a los activos informáticos, y que la responsabilidad y los roles de cada uno de los cargos sean pertinentes, creando conciencia conforme a los avances tecnológicos a los que se enfrenta el centro de diagnóstico actualmente siendo más vulnerable a un ataque de tipo informático, por esta razón es necesario brindar seguridad a la información desde la implementación del SGSI estableciendo e implementando

controles y la inclusión de políticas, procesos, procedimientos dentro de la estructura organizacional y las funciones del software y hardware necesarios para la mejora continua.

Guía Técnica Colombiana GTC ISO /IEC 27002: 2015 – NTC ISO/IEC 27001: La organización internacional de normalización – ISO y la comisión electrónica internacional – IEC forman todo un sistema para la seguridad de la información a través del estándar (ISO/IEC 27001 – GTC - ISO /IEC 27002), las cuales permiten gestionar, controlar y mantener buenas prácticas que orientan a las organizaciones el cumplimiento de sus objetivos.

La guía técnica GTC ISO /IEC 27002 permite diseñar controles de seguridad, para la adecuada administración de la información dentro del proceso de implementación del sistema de seguridad de la información (SGSI - ISO/IEC 27001).

El SGSI le permite al CDA mantener los procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, disponibilidad e integridad de los activos de información y minimizando a la vez los riesgos de seguridad que se presentan en la ejecución de todo proceso, así mismo el SGSI debe seguir siendo eficiente durante el tiempo que se requiera para adaptarse a los cambios internos del CDA, así como los externos del entorno.

El SGSI, minimiza los riesgos informáticos, de cualquier evento extraordinario, como una catástrofe natural, asonada, un incendio, los cuales hacen parte del sistema de seguridad física, perdida de los datos en el tránsito a la base de datos del software de aplicación y alteración o modificación de los archivos que componen la carpeta raíz de las plataformas, lo que le permite definir políticas de seguridad que:

- ✓ Incorporar un marco general de los objetivos de seguridad de la información del centro de diagnóstico automotor.
- ✓ Tener en cuenta los requerimientos legales o contractuales asociados a la seguridad de la información.
- ✓ Esté alineada con el contexto estratégico de la matriz de riesgos del centro de diagnóstico automotor en el que se implemente y sede continuidad al SGSI.
- ✓ Se establecen criterios los cuales van a permitir la evaluación del riesgo.
- ✓ Toda política para ser implementada debe ser aprobada por la alta dirección.

En el centro de diagnóstico automotor se considera la seguridad de los activos como un aspecto y parte de la responsabilidad que tiene el personal que desempeña el cargo que interviene en el proceso de revisión técnico - mecánica. Para algún cargo el grado de responsabilidad es mayor por lo que su compromiso y apropiación del SGSI en el desarrollo de sus actividades es importante.

Para la implementación del SGSI, es importante conocer los procesos internos ya que se encuentran fundamentados a partir de los requisitos de las normas técnicas colombianas que acreditan al centro de diagnóstico automotor como un organismo de inspección de vehículos. La compatibilidad de la NTC 5385 del 2011 permite la integración con la norma NTC ISO/IEC 27001 – 27002 en los procedimientos de seguridad en la información y en la aplicación de controles y políticas desde el diseño del SGSI. El cual será propuesto con la maximización de los recursos donde se hará uso de herramientas existentes, gratuitas o con licencia libre, la disposición de su personal y asesores externos con los que cuente el CDA.

El tiempo para la implementación del SGSI está sujeto a la cooperación de los funcionarios y personal externo con que cuenta el CDA y su vez con la aceptación de la alta dirección una vez se conozcan los costos de implementación durante los 10 meses.

6. MARCO CONCEPTUAL

El centro de diagnóstico automotor CDA ha realizado la restructuración en cuanto a los dispositivos y equipos informáticos mejorando los procesos y el espacio de almacenamiento, y los servicios de internet para hacer más eficientes los procesos que se realizan bajo las diferentes plataformas.

Los equipos informáticos y el servidor son equipos que no tienen acceso a internet, esto se ha establecido como uno de los controles para mitigar el riesgo de personas no autorizadas y virus que pueden llegar afectar el sistema operativo, las aplicaciones y la información de tal manera que puedan perjudicar a la empresa. Por esta razón es necesario identificar y diseñar controles en los sistemas informáticos y en la manipulación de la información física se incluya criterios de seguridad informática y de información, esta debe estar limitada para evitar exponerla a personas ajenas a la utilización de esta.

El diseño de los controles y la matriz de riesgos están dirigidos a los procesos, procedimientos internos, y mecanismos utilizados para garantizar la confidencialidad, integridad, y disponibilidad en los sistemas de procesamiento de datos y en la información que está bajo la responsabilidad de los colaboradores de la empresa, de esta manera es posible detectar las vulnerabilidades y amenazas que puede afectar a la continuidad de la prestación del servicio.

Actualmente, uno de los activos más preciados para una empresa es la información, por esta razón se define la necesidad de establecer controles de seguridad informática y de información a la perdida de los datos cuando se ha realizado una inspección y no llegan los registros a la bases de datos y el acceso a la carpeta raíz de cada una de las plataformas permitiendo garantizar que la información contenida

del software de aplicación sea confiable, siempre esté disponible y mantenga integra, por lo cual se debe diseñar lineamientos de seguridad en los procesos y minimizar los riesgos de fuga de información o el manejo incorrecto de la misma.

Protección Anti – Malware: Son herramientas y aplicaciones que evitan que los malware infecten los equipos informáticos y detienen la proliferación de los posibles ataques brindando seguridad a los correos electrónicos, firewall basado en host, prevención de pérdida de información, bloqueo o advertencias de páginas web infectadas que representa riesgo para la seguridad del equipo informático y los demás que se encuentran en la misma red.

Monitoreo de Red: El monitoreo en la red pretende identificar constantemente componentes defectuosos que puedan causar traumatismo en los procesos y la identificación de intrusiones, de tal manera que las alarmas implementadas ayuden en la administración de la red.

- ✓ Reducción de costos se verifica que herramientas son las necesarias sin ir a dimensiones.
- ✓ Anticipación de problemas por las alertas configuradas.
- ✓ Monitoreo de intrusiones en el tráfico de la red.
- ✓ El monitoreo permite por medio de los análisis adoptar medidas para el rendimiento.

Administrador de Red: Su función es velar por el buen funcionamiento de todos los equipos informáticos que componen la infraestructura de red y quien aplica las herramientas de escaneo y detección de intrusiones, vulnerabilidades e identificación de riesgos, estableciendo para cada uno de ellos medidas de

mitigación o que las pueda mantener estables sin que afecten el normal funcionamiento.

Seguridad de la información: Es el sistema que diseña, establece, e implementa, operaciones monitoreo todos los procesos para mantener promover la mejora continua de los recursos utilizados para la seguridad de la información, determinando:

- ✓ Procesos íntegros, que la información solo sea accesible por personal autorizado.
- ✓ Procesos confiables, donde la información permanece legible a los usuarios autorizados.
- ✓ Procesos disponibles, estables y accesibles.

Seguridad Informática: Son las reglas que se deben diseñar para garantizar la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica teniendo en cuenta el hardware y el software. Las herramientas dispuestas para la seguridad informática con los programas como antivirus, firewalls, procesos de encriptación de información y el uso de contraseñas, las cuales ayudan a provenir las amenazas procedentes de software malicioso.

7. MARCO METODOLÓGICO

7.1. METODOLOGÍA

La metodología cuantitativa permite verificar el estado del CDA frente a los requisitos de las normas que establecen el cumplimiento para la seguridad informática y de información basándose en la NTC – ISO/IEC 27001 DE 2013 así como la inadecuada gestión de los procesos en cuanto al tratamiento de los riesgos presentados en los activos.

Para conocer la organización, los propósitos y la afectación que presentan para el logro de sus objetivos. Se proponen técnicas del método cuantitativo como la entrevista, la encuesta y la observación frente a listas de cumplimiento del sistema de información como requerimiento en la NTC 5385 de 2011 (especificaciones del servicio). De esta manera se busca implementar, establecer o actualizar políticas, procesos y procedimientos que identifiquen los roles de cada uno de los funcionarios, de tal manera que se integren todos los requisitos y se aseguren los recursos necesarios para dar tratamiento, valoración y análisis a los riesgos que se encuentra expuesto el CDA direccionados a la operatividad del servicio y el manejo de la perdida de confidencialidad, integridad y disponibilidad dentro del alcance.

La guía técnica Colombia GTC ISO/IEC 27002 permite establecer controles de cumplimiento dirigidos a las especificaciones del servicio como:

- ✓ Seguridad del software.
- ✓ Seguridad de la información estableciendo medidas de control para:

- ✓ Manejo de contraseñas.
- ✓ Administración de la base de datos del software de aplicación SART.
- ✓ Manejo de información de respaldo.
- ✓ Bitácoras de operación del sistema.
- ✓ Bitácoras de fallas de equipos informáticos.
- ✓ Mantenimiento de equipos informáticos.
- ✓ Controles para software malicioso.

Este proceso busca determinar:

- ✓ Protección apropiada para cada uno de los activos
- ✓ Asegurar la operación correcta de los equipos
- ✓ Proteger la integridad del software, la información y los mecanismos que se deben implementar para prevenir y detectar códigos maliciosos e intrusiones.
- ✓ Proteger la infraestructura de red y con esto la información que transmite.
- ✓ Mantener la integridad, disponibilidad de la información.

De acuerdo a lo establecido para dar solución a la problemática del centro de diagnóstico se definen conceptos que permitirán llevar a cabo el desarrollo de estrategias de seguridad y las actividades.

Activo: Son los recursos del CDA para el manejo de la información y el almacenamiento de la misma, los activos que representan un valor importante, son la base de datos, contratos de prestación de servicios, documentación del sistema de gestión, manuales de usuario, software administrativo, servicio de comunicación en línea con proveedores y entes homologados, equipos informáticos, los

colaboradores y elementos esenciales para el cumplimiento de los objetivos del CDA.

Amenazas: Dentro del CDA se determina a partir de las acciones o elementos que lleguen afectar la seguridad informática, estas se pueden generar por las vulnerabilidades a las que se enfrentan los activos.

- ✓ Las amenazas internas son originadas desde el interior del CDA, para que esto suceda la persona debe tener acceso a la red, conocer el funcionamiento de la red.
- ✓ Las amenazas externas sedan por medio de personas ajenas a la compañía, quienes realizan el ingreso a través de la red, causando un incidente no deseado a todo el sistema.

Vulnerabilidad: Son las debilidades de los activos del CDA, por esta razón se puede llegar a ver afectada la confidencialidad de los datos, el diseño y desarrollo de la prestación del servicio.

Riesgo: Es la probabilidad de amenaza de un activo, el cual puede ocasionar un daño potencial en la compañía generando pérdidas o daños.

Análisis y gestión de riesgos: son los procedimientos que se llevan a cabo para encontrar los riesgos que existen en los sistemas de información, conocer el estado real de la compañía, lo que permite determinar controles y estrategias que minimicen el impacto de las pérdidas de dinero, tiempo en los servicios.

Matriz de riesgos: son controles determinados para mitigar el desarrollo de las vulnerabilidades y que estas sean potenciales amenazas.

La identificación de riesgos y controles anteriormente expuestos pretenden estar alineados con el logro de los objetivos de la empresa de tal manera que se vean reflejados en la prestación del servicio y la seguridad en la información e informática de acuerdo al cumplimiento de los requisitos legales para la inclusión de los sistemas de control y vigilancia de los entes autorizados por entidades legales.

7.2. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Las técnicas de recolección de información permiten realizar el análisis y evidencias de las necesidades del sistema de gestión con el que se cuenta actualmente y que requiere del diseño del sistema de seguridad informática y de información en los cuales se hace uso de herramientas como:

- ✓ Entrevista dirigida al responsable y administrador del sistema de información en la validación de cumplimiento sobre formatos, procesos y procedimientos que se tienen implementados para garantizar el requisito de la NTC 5385.
- ✓ Encuestas al personal, se busca validar los controles con los que cuentan para el manejo de los equipos informáticos e información.
- ✓ Observación frente a listas de cumplimiento del sistema de información como requerimiento en la NTC 5385 de 2011 (especificaciones del servicio), se busca validar el cumplimiento de los requisitos establecidos en la presente norma.

Las técnicas anteriormente seleccionadas permitirán identificar las amenazas, vulnerabilidades y riesgos a los que se expone el CDA frente a la seguridad de los sistemas informáticos y de información.

7.3. METODOLOGÍA DE DESARROLLO

Para el desarrollo de un sistema de gestión de seguridad informática y de información basado en la norma ISO/IEC 27001 y la guía técnica ISO/IEC 27002 versión 2013 que se requiere del apoyo y el conocimiento de todos los colaboradores como una medida primordial para la seguridad de los activos y la funcionalidad del negocio, llevando a cabo el desarrollo de la metodología en tres fases:

Fase 1: Conocer la estructura organizacional para determinar los activos informáticos desde la aplicación de la metodología Magerit

La estructura organizacional del CDA, permite determinar y describir las dependencias que intervienen en el proceso y los responsables que deben garantizar la funcionalidad del servicio con la identificación de activos informáticos y de información. Así mismo se determinarán los controles de la NTC ISO/IEC 27001-27002, los cuales serán aplicados durante la evaluación y tratamiento de riesgos y se tendrá como resultado un conjunto de salvaguardas que permiten la modificación del riesgo desde un valor potencial a un valor residual con la aplicación de características técnicas de los equipos, la estructura de red en la que forman parte. Para esta actividad se proponen recursos como:

- ✓ Entrevista al responsable y administrador del sistema para:

- ✓ Conocer la estructura organizacional (organigrama) y las dependencias que intervienen en el proceso.
- ✓ Conocer el personal, responsabilidades y funciones de acuerdo al manual de funciones frente a los sistemas de información.

- ✓ Realizar visita al establecimiento para el reconocimiento de la estructura de red y sus componentes con el fin de aplicar la metodología Magerit para la identificación, descripción y clasificación de activos.

  - ✓ Datos / información [D]
  - ✓ Claves criptográficas [k]
  - ✓ Servicios [S]
  - ✓ Software [SW]
  - ✓ Equipamiento informático [HW]
  - ✓ Redes de comunicaciones [COM]
  - ✓ Soportes de información [Media]
  - ✓ Equipamiento auxiliar [AUX]
  - ✓ Instalaciones [L]
  - ✓ Personas [P]

Fase 2: plantear la matriz de los riesgos identificando las vulnerabilidades y amenazas presentadas a todos los activos preservando la confidencialidad, integridad y disponibilidad.

La valoración de los activos permite dar inicio a la identificación de las amenazas, vulnerabilidades y riesgos a los que se encuentran expuestos, por medio de la aplicación de la metodología MAGERIT se aplican técnicas para el análisis y gestión de riesgos los cuales permiten aplicar los contrales de la NTC ISO/IEC 27001 del 2013.

- ✓ Implementación de metodología MAGERIT
- ✓ Implementación de controles de NTC ISO/IEC 27001 del 2013

Fase 3: Establecer mecanismos de sensibilización de la seguridad y protección a los activos software, redes, y personal que interviene directamente con los procesos y el manejo del software de aplicación para la revisión técnico - mecánica.

De acuerdo a los controles implementados por la NTC ISO/IEC 27001 del 2013, se planifican métodos de seguimiento, medición y evaluación para asegurar que los resultados son válidos y son los esperados.

- ✓ Se debe contar con toda la información documentada y apropiada como evidencia de los resultados de la implementación de un conjunto de controles, políticas, procesos y procedimientos que forman la estructura del CDA.
- ✓ Se debe documentar la sensibilización al personal que interviene en el proceso en cuanto al manejo de los controles previamente implementados.

8. CENTRO DE DIAGNÓSTICO AUTOMOTOR

Es una entidad privada que centra su actividad económica a la prestación de servicios de revisión técnico - mecánica y emisiones contaminantes a los vehículos que transitan por el territorio nacional, actualmente se encuentra acreditado por el organismo de nacional de Colombia ONAC bajo el número de acreditación 09-OIN-095 y con la habilitación de establecimiento por parte del ministerio de transporte, por esta razón debe cumplir los lineamientos de las normas que acrediten a los organismos de inspección y contar con mecanismos adecuados para garantizar la prestación del servicio y la comunicación permanente con la superintendencia de puertos y transporte quién vigila los procesos a nivel físico y lógico de la revisión técnico - mecánica. Por esta razón se debe tener una mejor seguridad de la información.

Reseña Histórica

La organización Corpotrans CDA, es un organismo Acreditado por ONAC, con código de acreditación 09-OIN-095, dedicada a la evaluación de la conformidad en cuanto a la revisión técnico - mecánica y de emisiones contaminantes en vehículos automotores de tipo pesado, livianos y motocicletas, constituida como sociedad anónima desde el año 2007, con domicilio en el municipio de Ibagué, departamento del Tolima, Colombia.

Para garantía y satisfacción de nuestros usuarios, contamos con tres líneas de inspección; una pista mixta, una pista de livianos y una pista de motos, equipos debidamente calibrados y un personal altamente capacitado, competente y comprometido con la labor.

Misión

En Corpotrans CDA, trabajamos en pro de proteger y salvaguardar la vida y la tranquilidad de las familias colombianas que al volante día tras día las comprometen, prestamos un servicio de calidad y garantizamos que la inspección que realizamos a los vehículos este cumpliendo conforme a los lineamientos y parámetros enmarcados en la normatividad vigente del Ministerio de Puertos y Transporte y el Ministerio del Medio Ambiente para la movilidad segura terrestre.

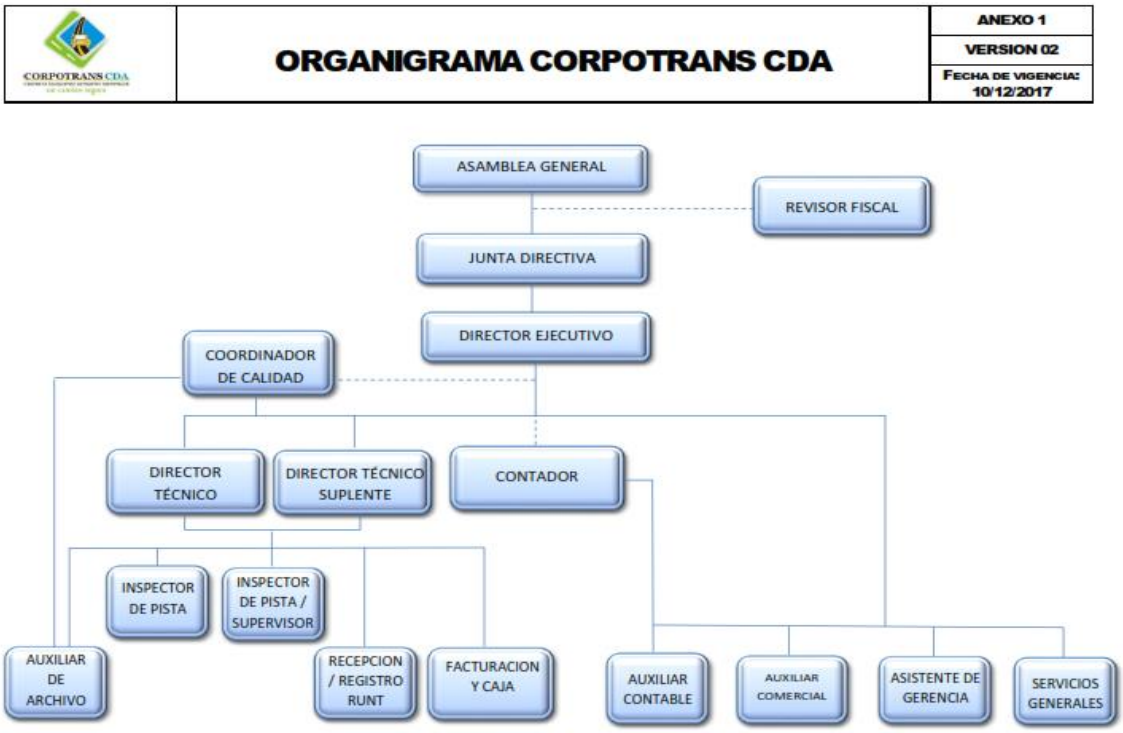
Visión

Para el año 2025 ser el centro de diagnóstico automotor líder a nivel regional, con participación activa en todos los procesos que tiendan a la mejora continua en la prestación de sus servicios y con iniciativa propia en la creación de mecanismos que permitan el desarrollo de este gremio, con altos niveles de innovación, productividad y rentabilidad, con responsabilidad social en el campo de la seguridad vial, al respeto y preservación del medio ambiente.

Diagrama Organizacional

A continuación, se presenta el diseño organización con el cual se rige la empresa, como también las diferentes dependencias que la componen, dentro de ella podemos identificar un despliegue completo que permite el buen funcionamiento de la empresa.

Figura 1. Diagrama organizacional Corpotrans



Fuente. Centro de diagnóstico automotor Corpotrans CDA (2018).

Director Ejecutivo: El objetivo general de cargo se centra en planificar, organizar, controlar y dirigir las actividades administrativas de servicio al cliente, financieras y contables las cuales están encaminadas al cumplimiento de la misión, visión y los objetivos institucionales.

- ✓ Reporta y da a conocer la ejecución de las actividades administrativas y el buen funcionamiento a la junta directiva y asamblea general.
- ✓ Supervisa los procesos y toma de decisiones del área contable, coordinador de calidad, director técnico y director técnico suplente.

Coordinador de calidad: El objetivo general del cargo se centra en la planificación y toma de decisiones frente a los procesos del sistema de gestión y las actividades que de este se derivan para velar por el buen funcionamiento del centro de diagnóstico automotor y la ejecución de las actividades para cada uno de los cargos.

- ✓ Reporta al director ejecutivo y director técnico y suplente todas las actividades que se generen del sistema de gestión como visitas de auditoría externa.
- ✓ Supervisa la ejecución de los procesos de recepción, inspectores, auxiliar de archivo, facturación y caja.

Director técnico: El objetivo general del cargo se centra en supervisar todas las operaciones, procesos y procedimientos de la pista de inspección, recepción y facturación, que estas se encuentren alineadas con las normas técnicas colombianas establecidas para llevar a cabo la revisión técnica mecánica y emisiones contaminantes.

- ✓ Velar por el cumplimiento y adecuado proceso para reportar y emitir los resultados de revisión técnico - mecánica ante el Runt, Superintendencia de puertos y transportes.
- ✓ Reporta al director ejecutivo el cumplimiento de todas las actividades y novedades presentadas.
- ✓ Supervisa todas las actividades de los inspectores, recepción y facturación.

Director técnico suplente: Es la persona que se encarga de llevar a cabo todas las actualizaciones planteadas por el coordinador de calidad en los procedimientos y formatos que conforman el sistema de gestión, así como la ejecución y planificación de capacitaciones en los normas, leyes y resoluciones que determinen condiciones de cumplimiento para la revisión técnico - mecánica.

- ✓ Reporta al director ejecutivo y director técnico suplente las capacitaciones planificadas para el año a todos los funcionarios.
- ✓ Supervisa el correcto diligenciamiento de los formatos propuestos para llevar a cabo el control en las pistas de inspección, recepción, auxiliar de archivo, facturación y caja.

Supervisor – inspector de pista: El supervisor inspector de pista, es una persona con mayor conocimiento en el manejo de equipos para guiar el cumplimiento de los procedimientos de revisión técnico - mecánica en cada una de las estaciones.

- ✓ Reporta al director de técnico, director ejecutivo y coordinador de calidad todas las novedades generadas desde la ejecución de todos los procesos.

Inspector de pista: Es el encargado de realizar la inspección mecanizada y emisiones contaminantes a los vehículos, aplicando los procedimientos, equipos y software para llevar a cabo la inspección completa.

- ✓ Reporta al director de técnico, director ejecutivo y coordinador de calidad todas las novedades generadas con el manejo de equipos tanto mecánicos como informáticos.

Recepción: Es la persona encargada de realizar atención al cliente brindando la adecuada información sobre la revisión técnica mecánica y verificar que el vehículo cumpla con las condiciones para ser inspeccionado.

- ✓ Reporta las novedades del proceso al director técnico.

Facturación y caja: El objetivo general del cargo se centra en la atención al cliente y brindar la información pertinente para realizar la revisión técnico - mecánica y a

su vez reportar los resultados y emitir los certificados con autorización del director técnico.

- ✓ Reporta al director técnico las novedades y los informes de cada una de las plataformas que maneja para llevar a cabo los procesos.

Auxiliar de Archivo: Es el encargado de velar por la organización y custodia de la información que se genera de cada de una de las áreas del centro de diagnóstico automotor, los cuales están bajo su responsabilidad con el propósito de facilitar la consulta y mantener toda la información organizada a disposición de la organización.

- ✓ Reporta las novedades del proceso al coordinador de calidad.

Procesos del área operática del centro de diagnóstico automotor

En el centro de diagnóstico automotor se reconoció nueve áreas fundamentales para llevar a cabo el proceso de revisión técnico - mecánica, las cuales son esenciales para dar cumplimiento a los objetivos propuestos por el CDA y los requisitos de los entes de acreditación y vigilancia.

El área de recepción realiza las siguientes actividades:

- ✓ Genera un registro físico por cada uno de los clientes aceptando el manejo y tratamiento de datos personales.
- ✓ Genera un registro físico y en el software SART de autorización para llevar a cabo el proceso de revisión técnico - mecánica.

El área de archivo realiza las siguientes actividades:

- ✓ Custodia los registros de recepción (formato para autorización de tratamiento de datos personales, registros de autorización para revisión técnico - mecánica).
- ✓ Custodia los soportes de entrega de los certificados de revisión técnico - mecánica.
- ✓ Custodia los formatos diligenciados de alistamiento, control de mantenimientos y bitácora de fallas de los equipos mecánicos e informáticos.

El área de facturación realiza las siguientes actividades:

- ✓ Debe reportar el registro de revisión técnico - mecánica a la plataforma del Runt.
- ✓ Debe reportar el pago de la revisión técnico - mecánica a la plataforma de recaudo autorizada por la Superintendencia De Puertos Y Transporte – Supergiros.
- ✓ Emitir la factura desde el software contable con copia al usuario.
- ✓ En el software de aplicación para la revisión técnico - mecánica debe ingresar la información del vehículo y generar las pruebas que se le practican al mismo.
- ✓ Generar los reportes de aprobación y rechazo de la revisión técnico mecánica esta debe ser suministrada al Runt.

En el área de inspección los inspectores y el supervisor de pista realizan las siguientes actividades:

- ✓ Por medio del software de aplicación se realizan las pruebas tanto mecanizadas, emisiones contaminantes y verificación de intensidad de luz.
- ✓ Se generan registros de mantenimiento de equipos informáticos y mecánicos preventivos y correctivos.
- ✓ Alistamiento diario de equipos informáticos y mecánicos.
- ✓ Reporte de bitácora de fallas de equipos informáticos y mecánicos.

El director técnico realiza las siguientes actividades:

- ✓ Lleva los registros del área operativa determinados desde el sistema de gestión.
- ✓ Verifica el cumplimiento de los procedimientos operativos con los lineamientos de las normas técnicas colombianas.
- ✓ Verifica y validad los resultados de la inspección mecanizada de los vehículos y autoriza la continuidad del proceso desde la plataforma de CI2 autorizada por la Superintendencia De Puertos Y Transporte para vigilar los resultados de la revisión técnico - mecánica.
- ✓ Coordina el cumplimiento de las actividades de recepción, facturación y caja e inspección de pista.
- ✓ Realiza los backup del software de aplicación SART y software contable SIIGO.

El director técnico suplente realiza las siguientes actividades:

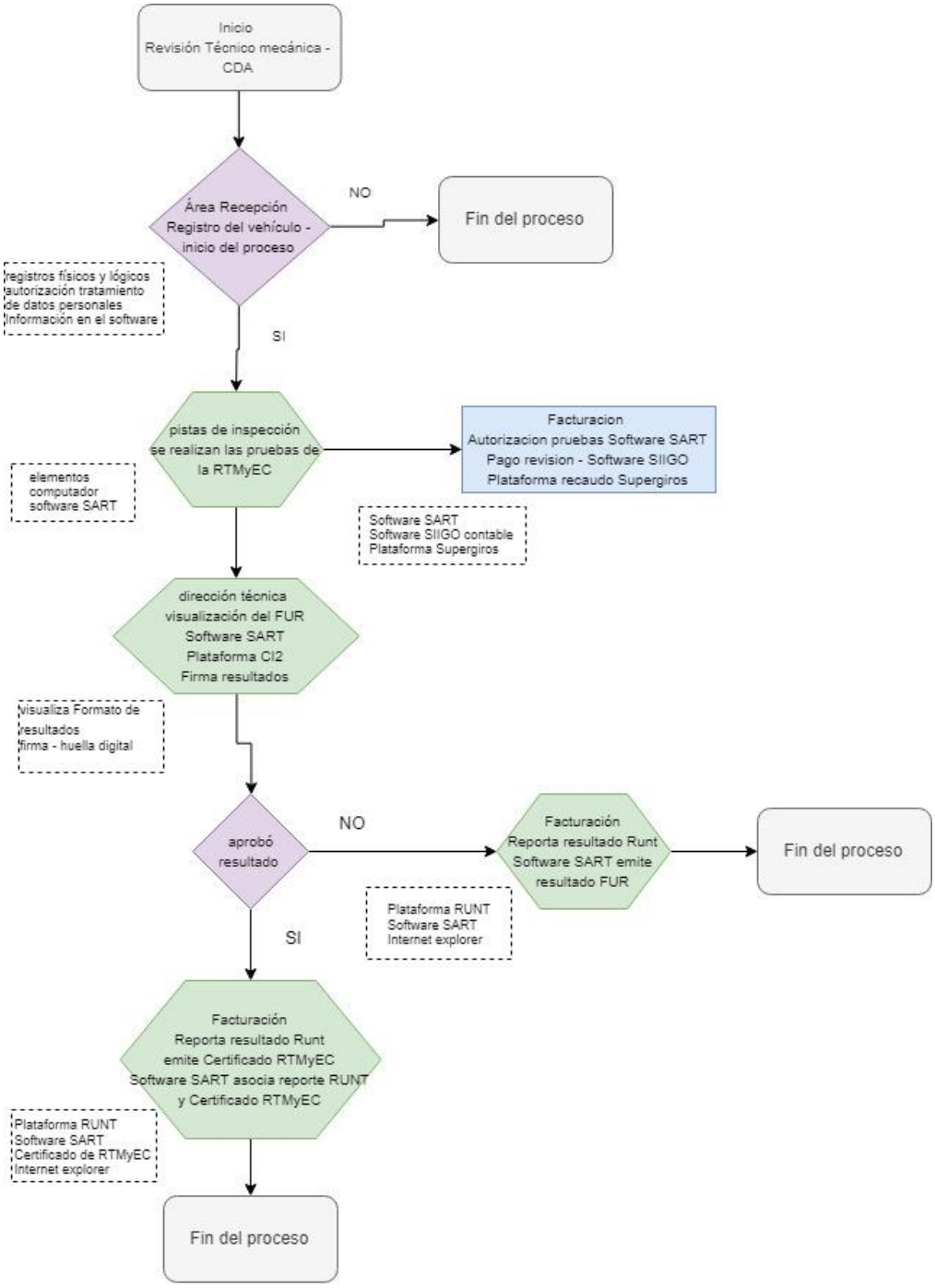
- ✓ Se encarga del manejo de los elementos de protección personal en cada una de las áreas del proceso de la revisión técnico - mecánica.
- ✓ La actualización y gestión de los procesos de calidad, recursos humanos y capacitaciones planificadas desde el sistema de gestión.
- ✓ En ausencia del director técnico principal reporta los resultados a la plataforma de CI2 autorizada por la Superintendencia De Puertos Y Transporte para vigilar los resultados de la revisión técnico - mecánica.
- ✓ En ausencia del director técnico principal realiza los backup del software de aplicación SART.

El coordinador de calidad realiza las siguientes actividades:

- ✓ Velar por el cumplimiento de los requisitos de las normas, leyes y resoluciones que actualicen y/o modifiquen el proceso de revisión técnico - mecánica con la generación de procesos y procedimientos que garanticen el cumplimiento.
- ✓ Es el responsable de atender las auditorias de seguimiento en acompañamiento del director técnico, las cuales son programadas por el organismo de acreditación de Colombia – ONAC.

A continuación, encontraremos el diagrama de flujo de la organización, el cual representa los procesos con los cuales se da vía a la revisión de los automotores para la respectiva revisión técnico-mecánica, también se muestra el macro y micro proceso llevado por la empresa para garantizar la aplicación de las normas establecidas.

Figura 2. Diagrama de proceso de revisión técnico - mecánica



Elaboración: propia.

9. RECURSOS E IMPLEMENTACIÓN PARA EL DESARROLLO DEL SGSI EN CORPOTRANS CDA

Para la implementación y diseño del sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 y la guía técnica 27002, se determinan los activos como el recursos humanos, físicos, tecnológicos con los que cuenta el CDA, y a partir de estos identificar los riesgos que permitirán implementar controles para la seguridad informática y la mejora continua de los procesos internos por medio del mantenimiento y monitoreo del SGSI.

Recursos Humanos

Para el CDA es un activo de vital importancia yaqué hacen parte de los procesos que se deben llevar a cabo dentro de la revisión técnico - mecánica, por lo tanto, el personal está capacitado y certificado para el desempeño de sus funciones y el manejo de los equipos informáticos. Por esta razón es de vital importancia la concientización del manejo de los sistemas informáticos y la información. Esto permitirá mitigar el riesgo y mejorar el desarrollo de sus funciones.

- ✓ De acuerdo con el organigrama del CDA se identifica el recurso humano.

Tabla 3. Recurso humano del CDA

Recurso humano	Cantidad	Descripción
Director técnico Director técnico suplente	4 colaboradores	En el área de inspección cuenta con el personal calificado para llevar a cabo los procesos de inspección sin embargo requieren de conocimiento sobre la seguridad informática y de información.

Continúa…

Recurso humano	Cantidad	Descripción
Coordinador de calidad Director técnico Director técnico suplente	3 colaboradores	Cuento con el conocimiento para el desarrollo de sus funciones conocen la importancia de la seguridad informática y la información, son los responsables de los procesos en línea con los entes homologados sin embargo no se realizan prácticas y controles de seguridad adecuados para el cumplimiento de los requisitos de la NTC 5385 en cuanto a los sistemas de información.
Recepción Facturación y caja Auxiliar de archivo	3 colaboradores	Desarrollan funciones administrativas y de atención al cliente con el manejo de plataformas que requieren de un conocimiento adecuado en la seguridad informática y de información.

Elaboración: propia.

Recursos físicos

Son elementos esenciales para la seguridad informática y de la información, por esta razón se debe concientizar al personal del cuidado, mantenimiento y protección por lo cual es importante que el departamento de sistemas mantenga su inventario actualizado para evitar la adquisición de equipos con características y funciones similares a los que hacen parte de los activos informáticos.

- ✓ De acuerdo con el organigrama del CDA se identificarán los recursos físicos.

Tabla 4. Recursos físicos

Recurso físico	Cantidad	Descripción
Administrativo	4 PC	Manejan procesos administrativos y contables, para el desarrollo de sus funciones cuentan con Software contable en los 4 equipos.
Recepción Inspección de pista	11 PC	Se realizan los procesos de revisión técnico - mecánica y conjunto con equipos mecanizados de medición.
Ingenieros responsables de proceso de inspección.	3 PC	Se realizan los procesos de confirmación de los resultados de la RTMyEC y las actividades del sistema de gestión como organismo de inspección.
Área de equipo servidor	Servidor SART, Servidor contable, Switch, Router.	Los computadores están identificados con una IP fija a un grupo de trabajo en una red LAN. En el servidor se encuentran instalados: ✓ El software de aplicación de revisión técnico - mecánica – SART. ✓ El software contable – SIIGO. ✓ Información general del sistema de gestión como organismo de inspección.
Impresoras	4	Las impresoras se encuentran configuradas en la red LAN.

Continúa…

Recurso físico	Cantidad	Descripción
Huella digital	3 hulleros de Idéntica	Son elementos de confirmación de las actividades de inspección frente a los resultados con los entes homologados para certificar y autorizar la generación de resultados de los vehículos en la plataforma de CI2 y el Runt.

Elaboración: propia.

Recursos técnicos y tecnológicos

Se deben definir los sistemas informáticos con los que cuenta el CDA como activos dentro del sistema de gestión de seguridad informática y de información, con el fin de avaluar las vulnerabilidad y amenazas a los que se enfrentan por falta de controles de acceso a la información, a los archivos de diseño y configuración, esto con el propósito de garantizar la protección total al sistema.

Los controles que se determinen como mejora o innovación deben estar de sujetos a la planificación de capacitación y formación a las adaptaciones de una infraestructura tecnológica que responda a las necesidades de la entidad por parte de los colaboradores

- ✓ De acuerdo al organigrama del CDA se identificarán los recursos tecnológicos.

Tabla 5. Recursos técnicos y tecnológicos

Recurso técnico y tecnológicos	Cantidad	Descripción
Energía eléctrica UPS	18 UPS.	Los equipos informáticos cuentan con UPS independiente, como protección a los picos de energía que se presenten y tiempo mínimo para guardar la información en caso de interrupción en la energía.
Protección contra incendios	10 extintores	El CDA cuenta con 10 extintores multipropósito distribuidos en toda el área.
Sistema operativo	15 PC	Los equipos están configurados con Windows 7, 8 y 10 tanto en el área administrativa como de inspección de vehículos, directores técnicos y coordinación de calidad, no cuentan con licencia.
Licencia del SO del servidor	1 PC	El equipo está configurado con Windows server foundation 2012 configuración RAID 2. Si tiene licencia.
Herramientas de Microsoft Office	11 PC	Los equipos tienen configurado Microsoft Office para el desarrollo de sus actividades el cual no cuenta con licencia en ninguno de los equipos, y se manejan diferentes versiones como 2007, 2010 y 2013.
Licencia software contable – SIIGO	4 PC	Está configurado en los 4 equipos informáticos administrativos con una licencia anual para 4 equipos.

Continúa…

Recurso técnico y tecnológicos	Cantidad	Descripción
Antivirus	21 PC	Los equipos cuentan con antivirus de Avast, y kaspersky sin licencia para su funcionamiento.
Licencia de software de aplicación RTMyEC – SART	14 PC	El software de aplicación para la RTMyEC SART se encuentra licenciado y solo está instalado en los equipos informáticos de inspección de pista, director técnico y suplente, servidor y facturación.
Plataforma de sistema de recaudo – Supergiros	1PC	Es el Sistema en línea del ente homologado por la superintendencia de puertos y transporte para controlar el valor de la revisión técnico - mecánica.
Plataforma de CI2	3 PC	Es el Sistema en línea del ente homologado por la superintendencia de puertos y transporte para auditar los registros y el resultado final de las inspecciones de revisión técnico - mecánica.
Plataforma Runt	1 PC	Es el Sistema en línea por medio del cual se cargan los resultados de aprobado y rechazado de los vehículos automotores.

Elaboración: propia.

10. APLICACIÓN DE LA METODOLOGÍA MAGERIT

10.1. INVENTARIO DE ACTIVOS

Con la identificación de los activos como recurso humano, físico y tecnológico con los que cuenta el CDA, se define la importancia que tienen frente al ciclo de vida de la seguridad informática frente al procesamiento, almacenamiento, transmisión, eliminación y destrucción, con el propósito de mantener los activos seguros frente a los controles que se determinen.

Para llevar a cabo este proceso desde el departamento de sistemas se identifican los activos que están directamente enfocados con el área de sistemas, donde se llevara el tratamiento para cada uno de los activos ya sea con el personal de la organización u outsourcing que realicen el análisis, identificación, implementación, pruebas de escritorio.

- ✓ Para cada uno de los activos se definen los criterios y se clasifican permitiendo encontrar el manejo por parte de los administradores de red.

- ✓ Se determina el manejo que se le quiere llegar a dar a la información para que se garantice la confidencialidad, integridad y disponibilidad.

Tabla 6. Inventario de activos

IDENTIFICACIÓN DE ACTIVOS	
Nombre del activo	**Clasificación de activo**
Base de datos del software de aplicación - SART	
Base de datos del software de aplicación - SIIGO	
Backup del sistema de gestión 17020 versión 2012, Software SART y SIIGO	Datos / información [D]
Microsoft Windows 7	
Microsoft Windows 8	
Microsoft Windows 10	
Windows server foundation 2012 configuración RAID 2	
herramientas de Microsoft office	Software [SW]
Plataforma RUNT	
Plataforma CI2	
Plataforma Supergiros	
Software SIIGO contable	
Software de aplicación SART	
Antivirus Avast	
Antivirus Kaspersky	
Navegador Internet Explorer	
Computadores de escritorio directores técnicos y calidad	
Computadores de escritorio inspección de pista	
Computador de escritorio administrativo	Equipamiento
Computador Servidor SART	informático [HW]

Continúa…

IDENTIFICACIÓN DE ACTIVOS	
Nombre del activo	**Clasificación de activo**
Router Switch Cableado estructurado - red LAN Instalaciones Eléctricas Internet de claro por fibra optica16 megas	Redes de comunicaciones [COM]
dispositivo de identificación de huella digital Energía eléctrica UPS	Equipamiento auxiliar [AUX]
proveedor de mantenimiento instalaciones físicas y eléctricas proveedor de mantenimiento de equipos informáticos	Personas [P]

Elaboración: propia.

Con la determinación y clasificación de los activos se permite identificar el área responsable de los procesos y los soportes de información permitirán establecer la valoración de los activos y tratamiento de los riesgos con la aplicación de la metodología Magerit, a su vez se asignarán los posibles controles de la NTC ISO/IEC 27002 que contribuyan a la mitigación del riesgo.

Durante la evaluación de los riesgos se aplicarán dominios de la NTC ISO/IEC 27001 en cuanto a:

- ✓ **Política de seguridad de la información:** Debe orientar y dar soporte a los requisitos implementados a nivel interno y externo.

- ✓ **Organización de la seguridad de la información:** Determina los lineamientos para dar inicio a la implementación del SGSI, de roles, tareas, seguridad y dispositivos móviles.

- ✓ **Seguridad de los recursos humanos:** Responsabilidades y asignación de roles, formación frente a la importante de la información frente al desarrollo de las actividades.

- ✓ **Gestión de activos:** Identificación de la información como un activo y en las medidas de seguridad adoptadas pata la seguridad.

- ✓ **Control de acceso:** Limitar el acceso a las instalaciones y la información de acuerdo a las funciones y roles.

- ✓ **Criptografía:** protege la confidencialidad, integridad y autenticidad en la información.
- ✓ **Seguridad física y del entorno:** Garantizar el acceso no autorizado a nivel físico, aporta eficiencia en la gestión de seguridad.

- ✓ **Seguridad de las operaciones:** Garantizar la ejecución de las operaciones y procesamiento de información frente a las copias de seguridad, software malicioso, control de software y gestión de vulnerabilidades.

- ✓ **Seguridad de las comunicaciones:** Garantizar la protección de la información en redes y equipos dispuestos para el procesamiento de información, y los diferentes medios utilizados con las TIC (redes sociales).

- ✓ **Adquisición, desarrollo y mantenimiento de sistemas de información:** determinar la seguridad de la información a nivel interno y externo y en todos los requisitos implementados en el SG.

- ✓ **Relaciones con los proveedores:** Comunicar las medidas de seguridad de los activos a los proveedores.

- ✓ **Gestión de incidentes de seguridad de la información:** Comunicar los incidentes, debilidades de seguridad y debilidades dando un enfoque coherente.

- ✓ **Aspectos de la seguridad de la información que se relacionan con la gestión de continuidad de negocio:** Garantizar la continuidad de la seguridad de la información y mitigar el riesgo de poner en peligro la continuidad del negocio que satisface los requisitos y expectativas del CDA.

- ✓ **Cumplimiento:** Evitar incumplimientos legales y políticas, a cada de estos se le dar cumplimiento desde la implementación de cualquier sistema de gestión - SG.

10.2. VALORACIÓN DE LOS ACTIVOS

La valoración de los activos permite conocer en el centro de diagnóstico automotor el nivel de protección y la importancia que tiene frente a los procesos internos, con la identificación de la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad que tiene los sistemas informáticos y la información que se maneja

durante el proceso de revisión técnico - mecánica, por lo tanto, se valora desde las siguientes dimensiones.

- ✓ Valoración de la Confidencialidad. Qué tan confidencial debe ser el activo que se está evaluando y que solo este a disposición por el personal o entidades, proveedores autorizados.
- ✓ Valoración de la Integridad. Qué tan íntegro es el contenido del activo que se está evaluando y que este no presente alteración sin autorización.
- ✓ Valoración de la Disponibilidad. Qué tan disponible debe ser para el público en general el activo que se está evaluando, y si frente a este se tiene acceso cuando se requiere.
- ✓ Valoración de la autenticidad. Que tan auténticos son los datos frente a las fuentes por las que se obtiene.
- ✓ Valoración de la trazabilidad. permite identificar el origen de los datos y los procesos que la tratan / modifican.

Valoración cuantitativa: Para la valoración de los activos se contemplan las opciones de la metodología Magerit cualitativa y cuantitativa, en donde el método cualitativo permite valorar a los activos por medio de una escala en la que se determina el impacto que puede causar en el centro de diagnóstico automotor con respecto al daño o pérdida generada.

Probabilidad: es el grado de exposición al que se encuentran los activos frente a una amenaza y la magnitud de un evento determinado, por esta razón se deben clasificar de acuerdo con la siguiente escala:

Tabla 7. Escala de valor cualitativa para activos

VALORACIÓN DE ACTICOS		
Valor	**Criterio**	**Concepto**
0	Muy bajo [MB]	Irrelevante a efectos prácticos
1 - 2	Bajo [B]	El daño puede presentarse rara vez
3 - 5	Medio [M]	El daño puede presentarse en algunas ocasiones
6 - 8	Alto [A]	El daño puede presentarse siempre
9	Muy alto [MA]	El daño representa peligro para el CDA
10	Extremo [E]	Daño extremadamente grave

Elaboración: propia.

- ✓ La metodología Magerit dispone de escalas estándar:

Tabla 8. Escala de valoración de criterios

ESCALA DE VALORACIÓN DE CRITERIOS		
Valor	**Justificación**	**Criterio**
10	10.si	**[si] Seguridad:** Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.

Continúa…

ESCALA DE VALORACIÓN DE CRITERIOS		
Valor	**Justificación**	**Criterio**
10	10.olm	**[olm] Operaciones:** Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.
	10.lbl	**[lbl.nat] Información clasificada (nacional):** Secreto.
9	9.lro	**[lpo] Obligaciones legales:** probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación.
	9.si	**[si] Seguridad:** probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.
	9.cei.d	**[cei] Intereses comerciales o económicos:** causa de pérdidas económicas excepcionalmente elevadas.
	9.cei.d	**[cei] Intereses comerciales o económicos:** causa de muy significativas ganancias o ventajas para individuos u organizaciones.
	9.da	**[da] Interrupción del servicio:** Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.
	9.olm	**[olm] Operaciones:** Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística.

Continúa…

ESCALA DE VALORACIÓN DE CRITERIOS		
Valor	**Justificación**	**Criterio**
9	9.lg. b	**[lg] Pérdida de confianza (reputación):** Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general.
	9.lbl	**[lbl.nat] Información clasificada (nacional):** Reservado.
8	8.lbl	**[lbl.nat] Información clasificada (nacional):** Confidencial.
7	7.si	**[si] Seguridad:** probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
	7.cei.c	**[cei] Intereses comerciales o económicos:** causa de graves pérdidas económicas.
	7.da	**[da] Interrupción del servicio:** Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.
	7.lg. b	**[lg] Pérdida de confianza (reputación):** Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general.

Continúa…

ESCALA DE VALORACIÓN DE CRITERIOS		
Valor	**Justificación**	**Criterio**
	7.olm	**[olm] Operaciones:** Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
	7.lbl	**[lbl.nat] Información clasificada (nacional):** Confidencial.
6	6.pi1	**[pi] Información de carácter personal:** probablemente afecte gravemente a un grupo de individuos.
	6.lbl	**[lbl.nat] Información clasificada (nacional):** Difusión limitada.
5	5.pi1	**[pi] Información de carácter personal:** probablemente afecte gravemente a un individuo.
	5.da	**[da] Interrupción del servicio:** Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones.
	5.lbl	**[lbl.nat] Información clasificada (nacional):** Difusión limitada.
	5.adm	**[adm] Administración y gestión:** probablemente impediría la operación efectiva de más de una parte de la Organización.
4	4.pi1	**[pi] Información de carácter personal:** probablemente afecte a un grupo de individuos.
	4.lbl	**[lbl.nat] Información clasificada (nacional):** Difusión limitada.

Continúa…

ESCALA DE VALORACIÓN DE CRITERIOS		
Valor	**Justificación**	**Criterio**
3	3.pi1	**[pi] Información de carácter personal:** probablemente afecte a un individuo.
	3.si	**[si] Seguridad:** probablemente sea causa de una disminución en la seguridad o dificulte la investigación de un incidente.
	3.cei.e	**[cei] Intereses comerciales o económicos:** constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros.
	3.da	**[da] Interrupción del servicio:** Probablemente cause la interrupción de actividades propias de la Organización.
	3.olm	**[olm] Operaciones:** Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).
	3.lg	**[lg] Pérdida de confianza (reputación):** Probablemente afecte negativamente a las relaciones internas de la Organización.
	3.lbl	**[lbl.nat] Información clasificada (nacional):** Difusión limitada.

Continúa…

ESCALA DE VALORACIÓN DE CRITERIOS		
Valor	**Justificación**	**Criterio**
2	2.pi1	**[pi] Información de carácter personal:** pudiera causar molestias a un individuo.
	2.cei.b	**[cei] Intereses comerciales o económicos:** de bajo valor comercial.
	2.lg	**[lg] Pérdida de confianza (reputación):** Probablemente cause una pérdida menor de la confianza dentro de la Organización.
1	1.pi1	**[pi] Información de carácter personal:** pudiera causar molestias a un individuo.
	1.si	**[si] Seguridad:** pudiera causar una disminución en la seguridad o dificultar la investigación de un incidente.
	1.cei.b	**[cei] Intereses comerciales o económicos:** de pequeño valor comercial.
	1.da	**[da] Interrupción del servicio:** Pudiera causar la interrupción de actividades propias de la Organización.
	1.olm	**[olm] Operaciones:** Pudiera disminuir la eficacia o seguridad de la misión operativa o logística (alcance local).
	1.lg	**[lg] Pérdida de confianza (reputación):** Pudiera causar una pérdida menor de la confianza dentro de la Organización.
0	1	No afecta la seguridad de las personas.

Continúa…

ESCALA DE VALORACIÓN DE CRITERIOS		
Valor	**Justificación**	**Criterio**
0	2	Sería causa de inconvenientes mínimos a las partes afectadas.
	3	Supondría pérdidas económicas mínimas.
	4	No supondría daño a la reputación de la organización.

Fuente. (Electrónica, 2012, pág. 19)

Tabla 9. Valoración de criterios a los activos

CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

Identificación de activos		**Valoración de activos de acuerdo a la escala de criterios**										
		Confidencialidad		**Integridad**		**Disponibilidad**		**Autenticidad**		**Trazabilidad**		**Criticidad**
Clasificación de activo	**Nombre del activo**	Valor	Justificación	Valor	Justificación	Valor	Justificación	Valor	Justificación	Valor	Justificación	**Valor Total**
Datos / información [D]	Base de datos del software de aplicación – SART	10	10.olm	10	10.si	10	10.lbl	9	9.da	9	9.si	10
	Base de datos del software de aplicación – SIIGO	10	10.olm	10	10.olm	9	9.si	9	9.olm	9	9.lg. b	9
	Backup del sistema de gestión 17020 versión 2012, Software SART y SIIGO	8	8.lbl	9	9.olm	7	7.olm	7	7.olm	6	6.lbl	7

Continúa…

CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

Identificación de activos		Valoración de activos de acuerdo a la escala de criterios										
		Confidencialidad		Integridad		Disponibilidad		Autenticidad		Trazabilidad		Criticidad
Clasificación de activo	Nombre del activo	Valor	Justificación	Valor	Justificación	Valor	Justificación	Valor	Justificación	Valor	Justificación	Valor Total
Software [SW]	Microsoft Windows 7	9	9.da	9	9.olm	7	7.da	8	8.lbl	7	7.olm	9
	Microsoft Windows 8	9	9.da	9	9.olm	7	7.da	8	8.lbl	7	7.olm	9
	Microsoft Windows 10	9	9.da	9	9.olm	7	7.da	8	8.lbl	7	7.olm	9
	Windows server foundation 2012 configuración RAID 2	9	9.da	9	9.olm	7	7.da	8	8.lbl	7	7.olm	9
	herramientas de Microsoft office	9	9.da	9	9.olm	7	7.da	8	8.lbl	7	7.olm	9
	Plataforma RUNT	10	10.si	10	10.olm	10	10.lbl	9	9.lro	10	10.olm	10
	Plataforma CI2	10	10.si	10	10.olm	10	10.lbl	9	9.lro	10	10.olm	10
	Plataforma Supergiros	10	10.si	10	10.olm	10	10.lbl	9	9.lro	10	10.olm	10
	Software SIIGO contable	8	8.lbl	9	9.olm	9	9.lbl	9	9.olm	9	9.olm	9
	Software de aplicación SART	10	10.si	9	9.olm	9	9.lbl	10	10.olm	10	10.olm	10
	Antivirus Avast	8	8.lbl	9	9.olm	9	9.da	8	8.lbl	9	9.olm	9
	Antivirus Kaspersky	8	8.lbl	9	9.olm	9	9.da	8	8.lbl	9	9.olm	9
	Navegador Internet Explorer	7	7.da	7	7.olm	5	5.lbl	5	5.pi1	7	7.cei.c	7
Equipamiento informático [HW]	Computadores de escritorio directores técnicos y calidad	7	7.da	7	7.olm	5	5.lbl	5	5.pi1	7	7.cei.c	7
	Computadores de escritorio inspección de pista	7	7.da	7	7.olm	5	5.adm	5	5.da	7	7.cei.c	7
	Computador de escritorio facturación – administrativo	7	7.da	7	7.olm	5	5.adm	5	5.da	7	7.cei.c	7
	Computador Servidor SART	7	7.da	7	7.olm	5	5.lbl	5	5.pi1	7	7.cei.c	7
Redes de comunicaciones [COM]	Router	5	5.da	7	7.olm	6	6.pi1	5	5.da	6	6.lbl	5
	Switch	5	5.da	7	7.olm	6	6.pi1	5	5.da	6	6.lbl	5
	Cableado estructurado - red LAN	7	7.da	9	9.da	9	9.olm	9	9.si	9	9.cei.d	9

Continúa…

CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

Identificación de activos		Valoración de activos de acuerdo a la escala de criterios										
		Confidencialidad		Integridad		Disponibilidad		Autenticidad		Trazabilidad		Criticidad
Clasificación de activo	**Nombre del activo**	Valor	Justificación	Valor	Justificación	Valor	Justificación	Valor	Justificación	Valor	Justificación	**Valor Total**
Equipamiento auxiliar [AUX]	Instalaciones Eléctricas	9	9.lg. b	7	7.cei.c	7	7.da	7	7.cei.c	3	3.cei.e	7
	Internet de claro por fibra optica16 megas	9	9.lg. b	7	7.cei.c	7	7.da	9	9.cei.d	3	3.cei.e	9
	dispositivo de identificación de huella digital	7	7.da	7	7.cei.c	7	7.da	9	9.cei.d	3	3.cei.e	7
	Energía eléctrica	7	7.olm	7	7.cei.c	7	7.da	7	7.cei.c	3	3.cei.e	7
Personas [P]	UPS proveedor de mantenimiento instalaciones físicas y eléctricas	7	7.olm	4	4.pi1	5	5.da	3	3.cei.e	3	3.da	3
	proveedor de mantenimiento de equipos informáticos	7	7.olm	4	4.pi1	5	5.da	3	3.cei.e	3	3.da	3

Elaboración: propia.

Valoración cuantitativa: La valoración de los activos desde el modelo cuantitativo permite especificar a los activos sobre una escala de valores con números reales por medio del cual se estiman valores de costo sobre el mantenimiento de los activos. Cuando los activos se enfrentan a una amenaza existe un porcentaje de degradación en el que puede ser el 0% y un 100%. A continuación, se especifica la escala de valores cuantitativos para el centro de diagnóstico automotor:

Tabla 10. Escala de valor cuantitativa para los activos

ESCALA DE VALORACIÓN CUANTITATIVA			
Valor	**Criterio**	**Concepto**	**Descripción**
0	Muy bajo [MB]	Irrelevante a efectos prácticos	$0 a $ 500.000
1 - 2	Bajo [B]	El daño ocurrirá raras veces	$501.000 a $ 1`000.000
3 - 5	Medio [M]	El daño ocurrirá en algunas ocasiones	$1`01.000 a $ 2`000.000
6 - 8	Alto [A]	El daño ocurrirá siempre	$2`001.000 a $ 4`000.000
9	Muy alto [MA]	El daño representa peligro para el CDA	$4`001.000 a $ 5`000.000
10	Extremo [E]	Daño extremadamente grave	$5`001.000 a mas

Elaboración: propia.

Tabla 11. Valoración cuantitativa de los activos

ESCALA DE VALORACIÓN CUANTITATIVA			
Criterio de la escala cuantitativa	**Activo**	**Identificación de la escala del valor cuantitativo**	**Descripción expresada en valor contable**
Extremo [E]	Base de datos del software de aplicación - SART Plataforma RUNT Plataforma CI2 Plataforma Supergiros Software de aplicación SART	10	$5`001.000 a mas
Muy alto [MA]	Base de datos del software de aplicación - SIIGO Microsoft Windows 7 Microsoft Windows 8 Microsoft Windows 10 Windows server foundation 2012 configuración RAID 2 herramientas de Microsoft office Software SIIGO - contable Antivirus Avast Antivirus Kaspersky Cableado estructurado - red LAN Internet de claro por fibra optica16 megas	9	$4`001.000 a $ 5`000.000

Continúa…

ESCALA DE VALORACIÓN CUANTITATIVA			
Criterio de la escala cuantitativa	**Activo**	**Identificación de la escala del valor cuantitativo**	**Descripción expresada en valor contable**
Alto [A]	Backup del sistema de gestión 17020 versión 2012, Software SART y SIIGO Navegador Internet Explorer Computadores de escritorio directores técnicos y calidad Computadores de escritorio inspección de pista Computador de escritorio facturación - administrativo Computador Servidor SART Instalaciones Eléctricas dispositivo de identificación de huella digital Energía eléctrica UPS	7	$2`001.000 a $ 4`000.000
Medio [M]	Router Switch	5	$1`01.000 a $ 2`000.000
Medio [M]	proveedor de mantenimiento instalaciones físicas y eléctricas proveedor de mantenimiento de equipos informáticos	3	$1`01.000 a $ 2`000.000

Elaboración: propia.

10.3. IDENTIFICACIÓN DE AMENAZA

Una vez se han identificado los activos, la descripción y los responsables del proceso en el centro de diagnóstico automotor, se definen las amenazas que se puedan llegar a generar y materializar en pérdidas a los activos, para lo cual se propone el catálogo de amenazas por Magerit, estas se encuentran clasificadas en cuatro grupos de acuerdo a los lineamientos de (MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012).

- ✓ Desastres naturales [N]
- ✓ De origen industrial [I]
- ✓ Errores y fallos no intencionados [E]
- ✓ Ataques intencionados [A]

Este grupo de amenazas admite caracterizar de los activos en el entorno en que se encuentra el sistema informático, las consecuencias y la probabilidad que sucedan (pág. 25).

Tabla 12. Identificación de amenazas

Identificación de amenazas	
Clasificación	**Descripción de la amenaza**
Desastres naturales [N]	Fuego Daños por agua Desastres naturales
De origen industrial [I]	Fuego Daños por agua Desastres industriales Contaminación electromagnética Avería de origen físico o lógico Corte del suministro eléctrico Condiciones inadecuadas de temperatura o humedad Fallo de servicios de comunicaciones Interrupción de otros servicios o suministros esenciales Degradación de los soportes de almacenamiento de la información
Errores y fallos no intencionados [E]	Errores de los usuarios Errores del administrador Errores de monitorización (log) Errores de configuración Deficiencias en la organización Difusión de software dañino Errores de (re) encaminamiento Errores de secuencia Escapes de información Alteración accidental de la información Destrucción de la información Fugas de información Vulnerabilidades de los programas (software) Errores de mantenimiento / actualización de programas (software) Errores de mantenimiento / actualización de equipos (hardware) Caída del sistema por agotamiento de recursos Pérdida de equipos Indisponibilidad del personal

Continúa…

Identificación de amenazas	
Clasificación	**Descripción de la amenaza**
Ataques intencionados [A]	Manipulación de los registros de actividad (log) Manipulación de la configuración Suplantación de la identidad del usuario Abuso de privilegios de acceso Uso no previsto Difusión de software dañino (re) encaminamiento de mensajes Alteración de secuencia Acceso no autorizado Análisis de tráfico Repudio Interceptación de información (escucha) Modificación de información deliberada Destrucción de la información Divulgación de información Manipulación de programas Manipulación de los equipos Denegación de servicio Robo de equipos Ataque destructivo Ocupación enemiga Indisponibilidad del personal Extorsión Ingeniería social (picaresca)

Fuente. (Electrónica, 2012, pág. 25)

Tabla 13. Valoración de amenazas por tipo de activo identificado en el CDA

IDENTIFICACIÓN DE AMENAZAS A LOS ACTIVOS DEL CDA	
Clasificación	**Descripción de la amenaza por tipo de activo identificado en el CDA**
Datos / información [D]	Errores de los usuarios [E] Errores del administrador [E] Escapes de información [E] Alteración accidental de la información [E] Destrucción de la información [E] Fugas de información [E] Suplantación de la identidad del usuario [A] Abuso de privilegios de acceso [A] Acceso no autorizado [A] Modificación deliberada de la información [A] Destrucción de la información [A] Divulgación de información [A]
Software [SW]	Avería de origen físico o lógico [I] Errores de los usuarios [E] Errores del administrador [E] Errores de monitorización (log) [E] Errores de configuración [E] Difusión de software dañino [E] Errores de (re) encaminamiento [E] Errores de secuencia [E] Alteración accidental de la información [E] Destrucción de la información [E] Fugas de información [E] Vulnerabilidades de los programas (software) [E] Errores de mantenimiento / actualización de programas (software) [E] Manipulación de los registros de actividad (log) [A] Manipulación de la configuración [A] Suplantación de la identidad del usuario [A] Abuso de privilegios de acceso [A] Uso no previsto [A] Difusión de software dañino [A] (re) encaminamiento de mensajes [A] Alteración de secuencia [A] Acceso no autorizado [A] Repudio [A] Modificación deliberada de la información [A] Destrucción de la información [A] Divulgación de información [A] Manipulación de programas [A]

Continúa…

IDENTIFICACIÓN DE AMENAZAS A LOS ACTIVOS DEL CDA	
Clasificación	**Descripción de la amenaza por tipo de activo identificado en el CDA**
Equipamiento informático [HW]	Fuego [N] Daños por agua [N] Desastres naturales [N] Fuego [I] Daño por agua [I] Desastres industriales [I] Contaminación mecánica [I] Contaminación electromagnética [I] Avería de origen físico o lógico [I] Corte del suministro eléctrico [I] Condiciones inadecuadas de temperatura o humedad [I] Emanaciones electromagnéticas [I] Errores del administrador [E] Errores de mantenimiento / actualización de equipos (hardware) [E] Caída del sistema por agotamiento de recursos [E] Pérdida de equipos [E] Abuso de privilegios de acceso [A] Uso no previsto [A] Acceso no autorizado [A] Modificación deliberada de la información [A] Interceptación de información (escucha) Manipulación de los equipos [A] Denegación de servicio [A] Robo [A] Ataque destructivo [A]
Redes de comunicaciones [COM]	Fallo de servicios de comunicaciones [I] Errores del administrador [E] Errores de (re) encaminamiento [E] Errores de secuencia [E] Alteración accidental de la información [E] Destrucción de la información [E] Fugas de información [E] Caída del sistema por agotamiento de recursos [E] Suplantación de la identidad del usuario [A] Abuso de privilegios de acceso [A] Uso no previsto [A]

Continúa…

IDENTIFICACIÓN DE AMENAZAS A LOS ACTIVOS DEL CDA	
Clasificación	**Descripción de la amenaza por tipo de activo identificado en el CDA**
	Alteración de secuencia [A]
	Acceso no autorizado [A]
	Análisis de tráfico [A]
	Interceptación de información (escucha) [A]
	Modificación deliberada de la información [A]
	Divulgación de información [A]
	Denegación de servicio [A]
	Fuego [N]
	Daños por agua [N]
	Desastres naturales [N]
	Fuego [I]
	Daño por agua [I]
	Desastres industriales [I]
	Contaminación mecánica [I]
	Contaminación electromagnética [I]
	Avería de origen físico o lógico [I]
	Corte del suministro eléctrico [I]
	Condiciones inadecuadas de temperatura o humedad [I]
	Interrupción de otros servicios o suministros esenciales [I]
	Emanaciones electromagnéticas [I]
Equipamiento auxiliar [AUX]	Errores de mantenimiento / actualización de equipos (hardware) [E]
	Pérdida de equipos [E]
	Uso no previsto [A]
	Acceso no autorizado [A]
	Manipulación de los equipos [A]
	Robo [A]
	Ataque destructivo [A]
	Deficiencias en la organización [E]
	Fugas de información [E]
Personas [P]	Indisponibilidad del personal [E]
	Indisponibilidad del personal [A]
	Extorsión [A]
	Ingeniería social (picaresca) [A]

Fuente. (Electrónica, 2012, pág. 25)

10.4. VALORACIÓN DEL RIESGO

La valoración de los riesgos se determina a partir de los valores de la probabilidad, los cuales permiten determinar qué tan crítico se presenta y tomar medidas específicas de prevención corrección e intervención y evitar la materialización de la amenaza, por medio de la estimación del impacto y aplicación de controles de la NTC ISO/IEC 27001-27002.

Estimación de la probabilidad: se determina desde la escala cualitativa para cada una de las amenazas.

Tabla 14. Estimación de la probabilidad

Valor	Criterio	Concepto
1	Muy bajo [MB]	amenaza irrelevante a efectos prácticos, sucede al menos una vez al año
2	Bajo [B]	El daño de la amenaza ocurre rara vez, con una frecuencia de 6 meses.
3	Medio [M]	El daño de la amenaza ocurre en algunas ocasiones, con una frecuencia de un mes.
4	Alto [A]	El daño de la amenaza ocurre siempre, cada semana.
5	Muy alto [MA]	El daño de la amenaza es muy grave para el CDA, ocurre a diario.

Elaboración: propia.

Estimación del impacto: se aprecian según el potencial de gravedad de los activos y son independiente de la probabilidad de ocurrencia del riesgo. Se clasifican en:

Tabla 15. Estimación del impacto

Valor	Criterio	Concepto
1	Muy bajo [MB]	Los daños causados son muy poco frecuentes y no tiene incidencia.
2	Bajo [B]	Son de poca gravedad, causan impactos menores, no es frecuente.
3	Medio [M]	Causan un impacto en la operatividad dejando consecuencias en el macroproceso.
4	Alto [A]	Impactan la operatividad de los procesos dejando consecuencias graves.
5	Muy alto [MA]	Impacto de pérdida prácticamente seguro en la operatividad de los procesos, dejando consecuencias muy graves.

Elaboración: propia.

Estimación Del Riesgo: la estimación del riesgo se determina de acuerdo con el cálculo matemático entre la probabilidad y el impacto, estimada para los activos, las cuales cambian frente al estado del centro de diagnóstico automotor, la estimación se toma a partir de la valoración de los riesgos en cuanto a la confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad.

Tabla 16. Estimación del riesgo

$$riesgo = probabilidad$$

Impacto						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5

Probabilidad

Nivel de Riego	
4	ALTO
3	MEDIO
2	BAJO
1	MUY BAJO

Elaboración: propia

El nivel del riesgo establece la valoración para los activos con un nivel de eficacia y de aplicación de controles de la NTC ISO/IEC 27001-27002:

Tabla 17. Eficacia del control

Criterio	Valor
Alto	4
Medio	3
Bajo	2
Inexistente	1

Elaboración: propia

.

La categorización de los riesgos permite ser tratados a partir de los controles que se seleccionan con la identificación de amenazas encontradas durante la aplicación de la de Metodología Magerit se establece el método sistemático para analizar y gestionar a cada uno de los activos genera un valor de riesgo residual y se reduce la posibilidad de materialización a un nivel aceptado por la dirección.

La ecuación para determinar el grado de exposición del riesgo es la división entre el valor del riesgo inherente y el valor de eficacia del control que en efecto está asociado al riesgo.

$$\textbf{Riesgo Residual} = \frac{\textbf{valor del riesgo inherente}}{\textbf{valor eficacia del control}}$$

Escala definida para determinar el Riesgo Residual en el Centro De Diagnóstico Automotor:

Tabla 18. Valoración del riesgo residual

Valoración del riesgo residual	
Nivel del riesgo residual	**Calificación**
Inaceptable	> 16
Importante	11 a 15
Moderado	6 a 10
Tolerable	2 a 5
Aceptable	< 2

Ejemplo:

Nivel de riesgo inherente: Moderado (6)

Valor de eficacia del control: Medio (3)

$$Riesgo\ Residual\ \ 6 \div 3 = 2$$

este valor corresponde a un nivel de riesgo residual es **Aceptable**

Elaboración: propia.

Tabla 19. Matriz de riesgos centro de diagnóstico automotor Corpotrans CDA

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control									
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual					
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Base de datos del software de aplicación - SIIGO	Escapes de información [E]	Conocimiento de la información por personas sin autorización, sin embargo, esta no es alterada	2	4	5	5			8	10	10	0	0	A9.2.3-Gestión de derechos de acceso privilegiado	4	2,0	2,5	2,5	0,0	0,0
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	4	4	4		5	12	12	12	0	15	A12.4.2-Protección de la información de registro	4	3,0	3,0	3,0	0,0	3,8
		Destrucción de la información [E]	Amenaza identificada sobre los datos en general.	2	5	5	4		4	10	10	8	0	8	A12.3.1-Respaldo de la información	4	2,5	2,5	2,0	0,0	2,0
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	3	4	5	4	4	9	12	15	12	12	A9.4.2-Procedimiento de ingreso seguro	4	2,3	3,0	3,8	3,0	3,0
		Divulgación de información [A]	Revelación de información.	2	5	5	4		4	10	10				A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	2,5	2,5	0,0	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Base de datos del software de aplicación - SIIGO	Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	3	3	3	4			9	9	12	0	0	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0	0,0	0,0
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	4	3	4		3	12	9	12	0	9	A12.4.2-Protección de la información de registro	4	3,0	2,3	3,0	0,0	2,3
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	3	3	4			9	9	12	0	0	A9.2.3-Gestión de derechos de acceso privilegiado	4	2,3	2,3	3,0	0,0	0,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	4	3	4	12	12	12	9	12	A9.4.1-Restricción de acceso a la información	4	3,0	3,0	3,0	2,3	3,0
		Fugas de información [E]	Incontinencia verbal, medios electrónicos, soporte papel.	3	5		4		4	15	0	12	0	12	A9.2.6-Retiro o ajuste de los derechos de acceso	4	3,8	0,0	3,0	0,0	3,0
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	2	5	4	4	5	4	10	8	8	10	8	A8.3.2-Disposición de los medios	4	2,5	2,0	2,0	2,5	2,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Base de datos del software de aplicación - SIIGO	Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	4	5	4	5		4	20	16	20	0	16	A9.4.2-Procedimiento de ingreso seguro	4	5,0	4,0	5,0	0,0	4,0
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	4	5	4		4	12	15	12	0	12	A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,8	3,0	0,0	3,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	5	5	4	4	3	15	15	12	12	9	A9.1.1-Política de control de acceso	4	3,8	3,8	3,0	3,0	2,3
		Divulgación de información [A]	Revelación de información.	2	5	4	5			10	8	10	0	0	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	2,5	2,0	2,5	0,0	0,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	5	4	4			15	12	12	0	0	A12.2.1-Controles contra códigos maliciosos	4	3,8	3,0	3,0	0,0	0,0
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	2	4	4	4		4	8	8	8	0	8	A9.2.3-Gestión de derechos de acceso privilegiado	4	2,0	2,0	2,0	0,0	2,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Base de datos del software de aplicación - SIIGO	Errores de mantenimiento / actualización de programas (software) [E]	Defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	4		3	4		4	0	12	16	0	16	A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	0,0	3,0	4,0	0,0	4,0
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	4	5	4		4		20	16	0	16	0	A8.3.2-Disposición de los medios	4	5,0	4,0	0,0	4,0	0,0
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	4	5	4	5			20	16	20	0	0	A9.4.2-Procedimiento de ingreso seguro	4	5,0	4,0	5,0	0,0	0,0
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	4	4	5			12	12	15	0	0	A12.2.1-Controles contra códigos maliciosos	4	3,0	3,0	3,8	0,0	0,0
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	5	4				15	12	0	0	0	A9.2.3-Gestión de derechos de acceso privilegiado	4	3,8	3,0	0,0	0,0	0,0
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	4	5	5	4	4	3	20	20	16	16	12	A9.4.4-Uso de programas utilitarios privilegiados	4	5,0	5,0	4,0	4,0	3,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Base de datos del software de aplicación - SIIGO	Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	4	4	3		3	12	12	9	0	9	A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,0	2,3	0,0	2,3
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	4	5	4				20	16	0	0	0	A9.2.6-Retiro o ajuste de los derechos de acceso	4	5,0	4,0	0,0	0,0	0,0
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	4	5	5	5			20	20	20	0	0	A8.1.3-Uso aceptable de los activos	4	5,0	5,0	5,0	0,0	0,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	4		5			8	0	10	0	0	A12.3.1-Respaldo de la información	4	2,0	0,0	2,5	0,0	0,0
		Divulgación de información [A]	Revelación de información.	3	5	4	4			15	12	12	0	0	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,8	3,0	3,0	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control						
					Frecuencia			Valor del impacto potencial									Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Base de datos del software de aplicación - SIIGO	Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	3	3	3				9	9	0	0	0	A13.2.1-Políticas y procedimientos de transferencia de acción	4	2,3	2,3	0,0	0,0	0,0
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	3	3	3	4		3	9	9	12	0	9	A9.4.1-Restricción de acceso a la información	4	2,3	2,3	3,0	0,0	2,3
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	5	4				15	12	0	0	0	A9.2.3-Gestión de derechos de acceso privilegiado	4	3,8	3,0	0,0	0,0	0,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	3	3	4	12	12	9	9	12	A9.1.1-Política de control de acceso	4	3,0	3,0	2,3	2,3	3,0
		Divulgación de información [A]	Revelación de información.	3	4	4	4			12	12	12	0	0	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,0	3,0	3,0	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Base de datos del software de aplicación - SIIGO	Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	4	4	4	3	4	3	16	16	12	16	12	A9.4.4-Uso de programas utilitarios privilegiados	4	4,0	4,0	3,0	4,0	3,0
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	5	5	5		4	15	15	15	0	12	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,8	3,8	3,8	0,0	3,0
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	2	5	4	5		4	10	8	10	0	8	A9.2.5-Revisión de los derechos de acceso de usuarios	4	2,5	2,0	2,5	0,0	2,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	2	4	4	5			8	8	10	0	0	A12.2.1-Controles contra códigos maliciosos	4	2,0	2,0	2,5	0,0	0,0
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	2	4	4	5			8	8	10	0	0	A12.2.1-Controles contra códigos maliciosos	4	2,0	2,0	2,5	0,0	0,0
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	5	4				10	8	0	0	0	A9.2.3-Gestión de derechos de acceso privilegiado	4	2,5	2,0	0,0	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Base de datos del software de aplicación - SIIGO	Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	5	5	4	4	4	10	10	8	8	8	A9.1.1-Política de control de acceso	4	2,5	2,5	2,0	2,0	2,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	5		5			10	0	10	0	0	A12.3.1-Respaldo de la información	4	2,5	0,0	2,5	0,0	0,0
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	2	5	4	5	4	4	10	8	10	8	8	A9.4.4-Uso de programas utilitarios privilegiados	4	2,5	2,0	2,5	2,0	2,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	4	4	3	4			16	12	16	0	0	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	4,0	3,0	4,0	0,0	0,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	4	3	4			12	9	12	0	0	A12.2.1-Controles contra códigos maliciosos	4	3,0	2,3	3,0	0,0	0,0
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	4	4	4	4			16	16	16	0	0	A9.4.1-Restricción de acceso a la información	4	4,0	4,0	4,0	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Base de datos del software de aplicación - SIIGO	Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	3	4	3	3		3	12	9	9	0	9	A9.2.6-Retiro o ajuste de los derechos de acceso	4	3,0	2,3	2,3	0,0	2,3
		Vulnerabilidades de los programas (software) [E]	Defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	4	3	3	5			12	12	20	0	0	A12.6.1-Gestión de las vulnerabilidades técnicas	4	3,0	3,0	5,0	0,0	0,0
		Errores de mantenimiento / actualización de programas (software) [E]	Defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	4	3	3	5			12	12	20	0	0	A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	3,0	3,0	5,0	0,0	0,0
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	4	3	3	3			12	12	12	0	0	A8.1.3-Uso aceptable de los activos	4	3,0	3,0	3,0	0,0	0,0
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	4	3	4			12	9	12	0	0	A12.2.1-Controles contra códigos maliciosos	4	3,0	2,3	3,0	0,0	0,0
		Divulgación de información [A]	Revelación de información.	3	4	4	3		3	12	12	9	0	9	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,0	3,0	2,3	0,0	2,3

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Plataforma RUNT	Avería de origen físico o lógico [I]	Fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	4	3	4	5		3	12	16	20	0	12	A11.2.4-Mantenimiento de los equipos.	4	3,0	4,0	5,0	0,0	3,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	2	5	4	4		4	10	8	8	0	8	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,5	2,0	2,0	0,0	2,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	4	4	5			12	12	15	0	0	A12.2.1-Controles contra códigos maliciosos	4	3,0	3,0	3,8	0,0	0,0
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	4	4	5			12	12	15	0	0	A12.2.1-Controles contra códigos maliciosos	4	3,0	3,0	3,8	0,0	0,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	2	4	4	5			8	8	10	0	0	A12.2.1-Controles contra códigos maliciosos	4	2,0	2,0	2,5	0,0	0,0
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	2	4	4	5			8	8	10	0	0	A12.2.1-Controles contra códigos maliciosos	4	2,0	2,0	2,5	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Plataforma RUNT	Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	4	4	5		4	8	8	10	0	8	A12.3.1-Respaldo de la información	4	2,0	2,0	2,5	0,0	2,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	3	3	3	4		4	9	9	12	0	12	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0	0,0	3,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	3	3	5			9	9	15	0	0	A12.2.1-Controles contra códigos maliciosos	4	2,3	2,3	3,8	0,0	0,0
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	4	4	3		4	12	12	9	0	12	A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,0	2,3	0,0	3,0
		Vulnerabilidades de los programas (software) [E]	Defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	3	3	5			9	9	15	0	0	A12.6.1-Gestión de las vulnerabilidades técnicas	4	2,3	2,3	3,8	0,0	0,0
		Errores de mantenimiento / actualización de programas (software) [E]	Defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3	3	3	5			9	9	15	0	0	A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	2,3	2,3	3,8	0,0	0,0
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	3	4	4	4		9	12	12	12	0	A8.3.2-Disposición de los medios	4	2,3	3,0	3,0	3,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Plataforma RUNT	Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	3	3	5			9	9	15	0	0	A12.2.1-Controles contra códigos maliciosos	4	2,3	2,3	3,8	0,0	0,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	4	4	4	12	12	12	12	12	A9.1.1-Política de control de acceso	4	3,0	3,0	3,0	3,0	3,0
		Divulgación de información [A]	Revelación de información.	3	4	3			4	12	9	0	0	12	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,0	2,3	0,0	0,0	3,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	3	4	3	3		3	12	9	9	0	9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,0	2,3	2,3	0,0	2,3
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	3	3	4			9	9	12	0	0	A12.2.1-Controles contra códigos maliciosos	4	2,3	2,3	3,0	0,0	0,0
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	4	4	3			12	12	9	0	0	A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,0	2,3	0,0	0,0
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	3	3	3	4		3	9	9	12	0	9	A9.4.1-Restricción de acceso a la información	4	2,3	2,3	3,0	0,0	2,3
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	3	3	3				9	9	0	0	0	A9.2.6-Retiro o ajuste de los derechos de acceso	4	2,3	2,3	0,0	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control						
					Valor del impacto potencial			Valor del riesgo potencial								Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Plataforma RUNT	Vulnerabilidades de los programas (software) [E]	Defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	3	3	3			9	9	9	0	0	A12.6.1-Gestión de las vulnerabilidades técnicas	4	2,3	2,3	2,3	0,0	0,0
		Errores de mantenimiento / actualización de programas (software) [E]	Defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3		4	4			0	12	12	0	0	A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	0,0	3,0	3,0	0,0	0,0
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	5	5		4		15	15	0	12	0	A8.3.2-Disposición de los medios	4	3,8	3,8	0,0	3,0	0,0
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	4	4	4			12	12	12	0	0	A9.4.2-Procedimiento de ingreso seguro	4	3,0	3,0	3,0	0,0	0,0
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	3	3	4		3	9	9	12	0	9	A12.2.1-Controles contra códigos maliciosos	4	2,3	2,3	3,0	0,0	2,3
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	4	4	4			12	12	12	0	0	A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,0	3,0	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	3		4	12	12	9	0	12	A9.1.1-Política de control de acceso	4	3,0	3,0	2,3	0,0	3,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	3	4	4	5		4	12	12	15	0	12	A12.3.1-Respaldo de la información	4	3,0	3,0	3,8	0,0	3,0
		Divulgación de información [A]	Revelación de información.	4	4	4	4		4	16	16	16	0	16	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	4,0	4,0	4,0	0,0	4,0
		Avería de origen físico o lógico [I]	Fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	3	4	4	5		4	12	12	15	0	12	A11.2.4-Mantenimiento de los equipos.	4	3,0	3,0	3,8	0,0	3,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	3	3	3	3		3	9	9	9	0	9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	2,3	0,0	2,3
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	3	3	4		3	9	9	12	0	9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0	0,0	2,3

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	4	4	5			12	12	15	0	0	A12.2.1-Controles contra códigos maliciosos	4	3,0	3,0	3,8	0,0	0,0
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	2	5	5	4		4	10	10	8	0	8	A9.4.1-Restricción de acceso a la información	4	2,5	2,5	2,0	0,0	2,0
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	2	4	4				8	8	0	0	0	A9.2.6-Retiro o ajuste de los derechos de acceso	4	2,0	2,0	0,0	0,0	0,0
		Errores de mantenimiento / actualización de programas (software) [E]	Defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3	4	4	5			12	12	15	0	0	A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	3,0	3,0	3,8	0,0	0,0
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	2	4	4	5			8	8	10	0	0	A6.1.2-Separación de deberes	4	2,0	2,0	2,5	0,0	0,0
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	4	4	3	3	4	12	12	9	9	12	A8.3.2-Disposición de los medios	4	3,0	3,0	2,3	2,3	3,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	4	4	5			12	12	15	0	0	A12.2.1-Controles contra códigos maliciosos	4	3,0	3,0	3,8	0,0	0,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	4	4	5	5	4	8	8	10	10	8	A9.1.1-Política de control de acceso	4	2,0	2,0	2,5	2,5	2,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	4	4	5			8	8	10	0	0	A12.3.1-Respaldo de la información	4	2,0	2,0	2,5	0,0	0,0
		Divulgación de información [A]	Revelación de información.	2	4	4			4	8	8	0	0	8	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	2,0	2,0	0,0	0,0	2,0
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	3	4	4	5	4	4	12	12	15	12	12	A9.4.4-Uso de programas utilitarios privilegiados	4	3,0	3,0	3,8	3,0	3,0
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	5	5	3		3	15	15	9	0	9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,8	3,8	2,3	0,0	2,3
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	3	4	4			4	12	12	0	0	12	A9.2.5-Revisión de los derechos de acceso de usuarios	4	3,0	3,0	0,0	0,0	3,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	4	5	5	5			20	20	20	0	0	A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0	0,0	0,0
		Vulnerabilidades de los programas (software) [E]	Defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	4	5	4	4			20	16	16	0	0	A12.6.1-Gestión de las vulnerabilidades técnicas	4	5,0	4,0	4,0	0,0	0,0
		Errores de mantenimiento / actualización de programas (software) [E]	Defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	4	3	3	4			12	12	16	0	0	A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	3,0	3,0	4,0	0,0	0,0
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	4	5	5	5			20	20	20	0	0	A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0	0,0	0,0
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	3	3	3	4	3	4	9	9	12	9	12	A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	3,0	2,3	3,0
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	3	4	4			3	12	12	0	0	9	A9.2.5-Revisión de los derechos de acceso de usuarios	4	3,0	3,0	0,0	0,0	2,3
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	4	5	5	5			20	20	20	0	0	A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Vulnerabilidades de los programas (software) [E]	Defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	4	5	4	4			20	16	16	0	0	A12.6.1-Gestión de las vulnerabilidades técnicas	4	5,0	4,0	4,0	0,0	0,0
		Errores de mantenimiento / actualización de programas (software) [E]	Defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	4		4	4			0	16	16	0	0	A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	0,0	4,0	4,0	0,0	0,0
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	4	5	5	5			20	20	20	0	0	A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0	0,0	0,0
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	3	3	3	4	3	4	9	9	12	9	12	A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	3,0	2,3	3,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	3	3	3	4			9	9	12	0	0	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0	0,0	0,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	4	5	4	4			20	16	16	0	0	A12.2.1-Controles contra códigos maliciosos	4	5,0	4,0	4,0	0,0	0,0
		Vulnerabilidades de los programas (software) [E]	Defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	3	3	4			9	9	12	0	0	A12.6.1-Gestión de las vulnerabilidades técnicas	4	2,3	2,3	3,0	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Errores de mantenimiento / actualización de programas (software) [E]	Defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3		3	3			0	9	9	0	0	A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	0,0	2,3	2,3	0,0	0,0
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	4	4		4		12	12	0	12	0	A8.3.2-Disposición de los medios	4	3,0	3,0	0,0	3,0	0,0
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	4	5	4	4			20	16	16	0	0	A12.2.1-Controles contra códigos maliciosos	4	5,0	4,0	4,0	0,0	0,0
		Divulgación de información [A]	Revelación de información.	3	4	4	3		3	12	12	9	0	9	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,0	3,0	2,3	0,0	2,3
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	3	3	3	5	4	4	9	9	15	12	12	A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	3,8	3,0	3,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	3	3	4	4	3	9	9	12	12	9	A9.1.1-Política de control de acceso	4	2,3	2,3	3,0	3,0	2,3
		Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en si misma se vea alterada.	3	4	4	3			12	12	9	0	0	A9.1.2-Acceso a redes y a servicios en red	4	3,0	3,0	2,3	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	**Amenazas**	**Descripción de la Amenaza**	**Frecuencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**	**Controles NTC ISO/IEC 27001-27002**	**Eficacia del control**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
	Software de aplicación SART	Manipulación de los equipos [A]	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	3	4		4	3	3	12	0	12	9	9	A9.4.4-Uso de programas utilitarios privilegiados	4	3,0	0,0	3,0	2,3	2,3
		Denegación de servicio [A]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	3	4	4	5			12	12	15	0	0	A13.1.2-Seguridad de los servicios de red	4	3,0	3,0	3,8	0,0	0,0
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	4	4	3			12	12	9	0	0	A9.4.2-Procedimiento de ingreso seguro	4	3,0	3,0	2,3	0,0	0,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	4	3	3	12	12	12	9	9	A9.1.1-Política de control de acceso	4	3,0	3,0	3,0	2,3	2,3
		Manipulación de los equipos [A]	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	3	4	3	4	3	4	12	9	12	9	12	A9.4.4-Uso de programas utilitarios privilegiados	4	3,0	2,3	3,0	2,3	3,0
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	3	3	4		3	9	9	12	0	9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0	0,0	2,3

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control							
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Errores de mantenimiento / actualización de equipos (hardware) [E]	Defectos en los procedimientos o controles de actualización de los equipos que se utilizan más allá del tiempo de uso	3	3	3	4			9	9	12	0	0	A.14.2.2-Procedimientos de control de cambios en sistemas	4	2,3	2,3	3,0	0,0	0,0
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	4	4	5			12	12	15	0	0	A9.4.2-Procedimiento de ingreso seguro	4	3,0	3,0	3,8	0,0	0,0
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	4	5	4	4			20	16	16	0	0	A8.1.3-Uso aceptable de los activos	4	5,0	4,0	4,0	0,0	0,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	3	4	4	3	4	9	12	12	9	12	A9.1.1-Política de control de acceso	4	2,3	3,0	3,0	2,3	3,0
		Manipulación de los equipos [A]	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	3	3	3	3	4	3	9	9	9	12	9	A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	2,3	3,0	2,3
		Denegación de servicio [A]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	3	3	3	3			9	9	9	0	0	A13.1.2-Seguridad de los servicios de red	4	2,3	2,3	2,3	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Avería de origen físico o lógico [I]	Fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	2	4	4	5			8	8	10	0	0	A11.2.4-Mantenimiento de los equipos.	4	2,0	2,0	2,5	0,0	0,0
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	4	4	5	4	4	12	12	15	12	12	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,0	3,0	3,8	3,0	3,0
		Errores de mantenimiento / actualización de equipos (hardware) [E]	Defectos en los procedimientos o controles de actualización de los equipos que se utilizan más allá del tiempo de uso	3		4	5		4	0	12	15	0	12	A.14.2.2-Procedimientos de control de cambios en sistemas	4	0,0	3,0	3,8	0,0	3,0
		Pérdida de equipos [E]	La pérdida de equipos provoca directamente la carencia de un medio para prestar el servicio, es decir indisponibilidad.	2		4	5		4	0	8	10	0	8	A11.2.4-Mantenimiento de los equipos.	4	0,0	2,0	2,5	0,0	2,0
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	4	4	3		4	12	12	9	0	12	A9.4.2-Procedimiento de ingreso seguro	4	3,0	3,0	2,3	0,0	3,0
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	2	4	4	4		4	8	8	8	0	8	A8.1.3-Uso aceptable de los activos	4	2,0	2,0	2,0	0,0	2,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	4	4	5	5	4	8	8	10	10	8	A9.1.1-Política de control de acceso	4	2,0	2,0	2,5	2,5	2,0
		Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en si misma se vea alterada.	3	4	4			4	12	12	0	0	12	A9.1.2-Acceso a redes y a servicios en red	4	3,0	3,0	0,0	0,0	3,0
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	4	4	3	4		12	12	9	12	0	A8.3.2-Disposición de los medios	4	3,0	3,0	2,3	3,0	0,0
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	3	3	4			9	9	12	0	0	A9.4.2-Procedimiento de ingreso seguro	4	2,3	2,3	3,0	0,0	0,0
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	3	3	3	3			9	9	9	0	0	A8.1.3-Uso aceptable de los activos	4	2,3	2,3	2,3	0,0	0,0
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	4	4				8	8	0	0	0	A9.2.3-Gestión de derechos de acceso privilegiado	4	2,0	2,0	0,0	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Análisis de tráfico [A]	El atacante sin análisis de comunicaciones, extrae análisis de origen, destino, volumen y frecuencia de los intercambios	2	4	4			4	8	8	0	0	8	A13.2.1-Políticas y procedimientos de transferencia de acción	4	2,0	2,0	0,0	0,0	2,0
		Interceptación de información (escucha) [A]	El atacante llega a tener acceso a información que no le corresponde, sin que la información en si misma se vea alterada.	2	4	4			4	8	8	0	0	8	A9.1.2-Acceso a redes y a servicios en red	4	2,0	2,0	0,0	0,0	2,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	5	4	4	12	12	15	12	12	A9.1.1-Política de control de acceso	4	3,0	3,0	3,8	3,0	3,0
		Denegación de servicio [A]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2	4	4	4			8	8	8	0	0	A13.1.2-Seguridad de los servicios de red	4	2,0	2,0	2,0	0,0	0,0
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	3	3	4	3	3	9	9	12	9	9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0	2,3	2,3
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	4	4	5	4	4	8	8	10	8	8	A9.1.1-Política de control de acceso	4	2,0	2,0	2,5	2,0	2,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Avería de origen físico o lógico [I]	Fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	2	4	4	4		4	8	8	8	0	8	A11.2.4-Mantenimiento de los equipos.	4	2,0	2,0	2,0	0,0	2,0
		Pérdida de equipos [E]	La pérdida de equipos provoca directamente la carencia de un medio para prestar el servicio, es decir indisponibilidad.	4	3	3	5		4	12	12	20	0	16	A11.2.4-Mantenimiento de los equipos.	4	3,0	3,0	5,0	0,0	4,0
		Robo [A]	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar servicios, es decir indisponibilidad	4	3	3	5	4	4	12	12	20	16	16	A11.1.3-Seguridad de oficinas, recintos e instalaciones.	4	3,0	3,0	5,0	4,0	4,0
		Ataque destructivo [A]	Vandalismo, terrorismo, acción militar, la amenaza puede ser perpetrada por personal interno, externo o contratadas.	4	3	3	5	4	4	12	12	20	16	16	A12.3.1-Respaldo de la información	4	3,0	3,0	5,0	4,0	4,0
		Indisponibilidad del personal [E]	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones de orden público.	3	3	3	4			9	9	12	0	0	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0	0,0	0,0
		Indisponibilidad del personal [E]	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones de orden público.	3	3	3	3			9	9	9	0	0	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	2,3	0,0	0,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA																						
IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros														Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual						
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Ingeniería social (picaresca) [A]	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	3	4	4	4			12	12	12	0	0	A8.1.3-Uso aceptable de los activos	4	3,0	3,0	3,0	0,0	0,0

Fuente. (Internacional, 2013, pág. 19)

11. CONTROLES NTC ISO/IEC 27001 DE 2013. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Con la implementación y establecimiento del sistema de gestión de seguridad de información – SGSI en el centro de diagnóstico automotor, se permite no solo identificar aspectos tecnológicos si no también aspectos organizacionales de la gestión de seguridad, el análisis implica comprender los riesgos en los sistemas de información y a su vez la identificación de controles a las posibles amenazas que pueden estar expuestos. Cada control lo conforma un conjunto de acciones, políticas, documentos, en los que se busca cumplir con los objetivos del CDA y la seguridad de la organización.

La definición de estos controles debe estar alineados con las determinaciones del alcance de implementación del sistema en el CDA, de este modo se basan en los principios de aceptación de los riesgos, las medidas adoptadas para el tratamiento de riesgos, la asignación de responsabilidades y autoridad para la implementación en la que se asume un punto de vista de múltiples interacciones y la coordinación de los riesgos de seguridad de información.

La aplicación de la metodóloga Magerit en el proceso de revisión técnico - mecánica del CDA, permitió la identificación y análisis de los activos informáticos que forman parte de su actividad principal y así mismo la determinación de los controles en los cuales se tuvo en cuenta los procesos, procedimientos, responsabilidades y políticas que se deben adoptar para brindar mayor seguridad a la estructura organizacional, las funciones del hardware y del software como soporte fundamental para la prestación de servicios.

El sistema de información de la revisión técnico - mecánica y emisiones contaminantes lo conforma un conjunto de activos clasificados como:

- ✓ Datos / información [D]
- ✓ Software [SW]
- ✓ Equipamiento informático [HW]
- ✓ Redes de comunicaciones [COM]
- ✓ Equipamiento auxiliar [AUX]
- ✓ Personas [P]

Conformados por 29 activos a los cuales se les determinaron 33 controles en los siguientes dominios:

- ✓ A.6. Organización de la seguridad de la información
- ✓ A.7. Seguridad de los derechos humanos
- ✓ A.8. Gestión de activos
- ✓ A.9. Control de acceso
- ✓ A.11. Seguridad física y del entorno
- ✓ A.12. Seguridad de las operaciones
- ✓ A.13. Seguridad de las comunicaciones
- ✓ A.14. Adquisición, desarrollo y mantenimiento de sistemas
- ✓ A.16. Gestión de incidentes de seguridad de la información

Tabla 20. Controles NTC ISO/IEC 27001-27002 de 2013

CONTROLES NTC ISO/IEC 27001 -27002	
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
A.6.1 organización interna	**Objetivo:** Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1-Roles y responsabilidades para la seguridad de la información	**Control:** Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2-Separación de deberes	**Control:** Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización
A.6.1.3-Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.
A.7. SEGURIDAD DE LOS DERECHOS HUMANOS	
A.7.2. durante la ejecución del empleo	**Objetivo:** Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	**Control:** Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.

Continúa…

CONTROLES NTC ISO/IEC 27001 -27002	
A.8. GESTIÓN DE ACTIVOS	
A.8.1. responsabilidad por los activos	**Objetivo:** Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.3-Uso aceptable de los activos	**Control:** Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.3. manejo de medios	**Objetivo:** Evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada.
A.8.3.2-Disposición de los medios	**Control:** Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.9. CONTROL DE ACCESO	
A.9.1. requisitos del negocio para el control de acceso	**Objetivo:** Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1-Política de control de acceso	**Control:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.
A.9.1.2-Acceso a redes y a servicios en red	**Control:** Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

Continúa…

CONTROLES NTC ISO/IEC 27001 -27002	
A.9.2. gestión de acceso de usuarios	**Objetivo:** Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.3-Gestión de derechos de acceso privilegiado	**Control:** Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
A.9.2.5-Revisión de los derechos de acceso de usuarios	**Control:** Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6-Retiro o ajuste de los derechos de acceso	**Control:** Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A.9.4. Control de acceso a sistemas y aplicaciones	**Objetivo:** Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1-Restricción de acceso a la información	**Control:** El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A.9.4.2-Procedimiento de ingreso seguro	**Control:** Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A.9.4.4-Uso de programas utilitarios privilegiados	**Control:** Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

Continúa…

CONTROLES NTC ISO/IEC 27001 -27002	
A.11. SEGURIDAD FÍSICA Y DEL ENTORNO	
A.11.1. áreas seguras	**Objetivo:** Prevenir el acceso físico no autorizado, el daño y la interferencia la información y a las instalaciones de procesamiento de información de la organización.
A.11.1.1-Perímetro de seguridad física	**Control:** Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.
A.11.1.3-Seguridad de oficinas, recintos e instalaciones.	**Control:** Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.
A.11.1.4-Protección contra amenazas externas y ambientales.	**Control:** Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.2. equipos	**Objetivo:** Prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.
A.11.2.2-Servicios de suministro	**Control:** Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.4-Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Continúa…

CONTROLES NTC ISO/IEC 27001 -27002	
A.12. SEGURIDAD DE LAS OPERACIONES	
A.12.2. protección contra código malicioso	**Objetivo:** Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1-Controles contra códigos maliciosos	**Control:** Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3. copias de respaldo	**Objetivo:** Proteger contra la perdía de datos.
A12.3.1-Respaldo de la información	**Control:** Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
A.12.4. registro y seguimiento	**Objetivo:** Registrar eventos y generar evidencia.
A.12.4.2-Protección de la información de registro	**Control:** Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.12.4.3-Registros del administrador y del operador	**Control:** Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A.12.6. gestión de las vulnerabilidades técnicas	**Objetivo:** Gestión de las vulnerabilidades técnicas.
A.12.6.1-Gestión de las vulnerabilidades técnicas	**Control:** Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

Continúa…

CONTROLES NTC ISO/IEC 27001 -27002	
A.13. SEGURIDAD DE LAS COMUNICACIONES	
A.13.1. gestión de la seguridad de las redes	**Objetivo:** Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte.
A13.1.2-Seguridad de los servicios de red	**Control:** Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.2. transferencia de información	**Objetivo:** Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
A.13.2.1-Políticas y procedimientos de transferencia de acción	**Control:** Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
A.13.2.2-Acuerdos sobre transferencia de información	**Control:** Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.4-Acuerdos de confidencialidad o de no divulgación	**Control:** Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Continúa…

CONTROLES NTC ISO/IEC 27001 -27002	
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
A.14.1. Requisitos de seguridad de los sistemas de información	**Objetivo:** Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que presta servicios sobre redes públicas.
A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	**Control:** La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2. seguridad en los procesos de desarrollo y de soporte	**Objetivo:** Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A.14.2.2-Procedimientos de control de cambios en sistemas	**Control:** Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.5-Principio de Construcción de los Sistemas Seguros.	**Control:** Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

Continúa…

CONTROLES NTC ISO/IEC 27001 -27002	
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
A.16.1. gestión de incidentes y mejoras en la seguridad de la información	**Objetivo:** Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información incluida la comunicación sobre eventos de seguridad y debilidades.
A.16.1.2-Reporte de eventos de seguridad de la información	**Control:** Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3. Reporte de debilidades de seguridad de la información	**Control:** Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

Fuente. (Internacional, 2013, pág. 13)

12. ALCANCE DEL SGSI EN EL CDA

Para la implementación del SGSI se deben seguir los requisitos de la norma NTC ISO/IEC 27001 - Sistemas De Gestión De La Seguridad De La Información, con el propósito de demostrar la capacidad de proporcionar consistentemente servicios confiables, íntegros y disponibles en cumplimiento de los requisitos de los usuarios, así como para asegurar de manera permanente la calidad de cumplimiento con los objetivos establecidos. Por consiguiente, el contexto externo e interno está relacionado con el alcance de la gestión de los riesgos:

Los parámetros del contexto externo abarcan:

- ✓ Los requisitos legales y reglamentarios.
- ✓ El nivel competitivo ya sea a nivel nacional, regional o local, así mismo se definen en lo financiero y tecnológico.

Los parámetros del contexto interno abarcan:

- ✓ Los procesos.
- ✓ La estructura organizativa como las funciones y responsabilidades, políticas y recursos como capital, tiempo, personas, procesos, sistemas y tecnología.
- ✓ Normas y modelos adoptados por la organización.

Estos factores son pertinentes para asegurar el enfoque de conformidad con la NTC ISO/IEC 27001: 2013 y los servicios de revisión técnico - mecánica, con el propósito de aumentar la seguridad de información en base a los controles identificados durante el análisis se deben documentar, implementar, operar y monitorear de acuerdo al modelo en la norma.

13. PLAN DE TRATAMIENTO DE RIESGOS

La categorización de los riesgos permite ser tratados a partir de los controles que se seleccionan con la identificación de las amenazas encontradas durante la aplicación de la metodología Magerit se establece el método sistemático para analizar y gestionar a cada uno de los activos. Los controles seleccionados para la implementación se tomaron en base a medidas administrativas y herramientas gratuitas o de bajo costo en la medida de lo posible para hacer frente a los riesgos. Así mismo se verifico que procesos, procedimientos, del sistema de gestión actual abarcan las directrices de los controles y cuáles no, de esta manera se da cumplimiento a las condiciones específicas del servicio para centros de diagnóstico automotor en la norma NTC 5385 del 2011.

En el plan de tratamiento de riesgos se da a conocer las acciones correctivas, los responsables que deben velar por el cumplimiento de los controles propuestos y el monitoreo permanente por el personal asignado de acuerdo a rol y responsabilidad que tiene frente a la eficacia de los procesos de revisión técnico - mecánica, la mejora continua y eficacia del sistema de gestión documentado.

- ✓ En el análisis y evaluación de los riesgos, se definen los controles conforme al nivel de riesgo, los objetivos del control y la necesidad de implementación frente a las condiciones de cumplimiento de la norma NTC 5385 del 2011.

Tabla 21. Plan de tratamiento de riesgos

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control									Plan De Tratamiento De Riesgos			
				Valor del riesgo residual										
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
Datos / información [D]	Base de datos del software de aplicación - SART	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	2,0	1,5	0,0	1,3	Aceptable	SI	El programa de formación debe incluir capacitaciones sobre el buen uso del software, los módulos de administración y operación para el desarrollo de las actividades de los servicios prestados	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.2.3-Gestión de derechos de acceso privilegiado	3	3,0	3,0	4,0	4,0	0,0	2,8	Tolerable	SI	El software cuenta con un mecanismo de autenticación de usuario y contraseña diferente para cada uno de los usuarios, esto permite verificar las actividades realizadas	Dirección Técnica	
		A12.3.1-Respaldo de la información	3	2,7	2,7	2,0	2,7	0,0	2,0	Tolerable	SI	Se debe solicitar al director técnico estrategias que garanticen los respaldos de información con una frecuencia diaria para el software de aplicación manejados dentro del proceso de revisión técnico - mecánica.	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual							Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
Datos / información [D]	Backup del sistema de gestión 17020 versión 2012, Software SART y SIIGO	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,0	1,0	1,3	0,0	0,0	0,7	Aceptable	SI	El programa de formación debe incluir todos los sistemas de gestión con los que cuenta la organización, así como los requisitos legales y contractuales para la prestación de los servicios	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A8.3.2-Disposición de los medios	4	2,5	2,0	2,0	2,5	2,0	2,2	Tolerable	SI	Tanto para la información como para el manejo de versiones del software y aplicaciones se maneja un tiempo de retención mínimo de 3 años como lo establece las obligaciones contractuales para estos organismos, sin embargo, no existe un mecanismo para la eliminación o destrucción de información	Coordinador de calidad	12 de diciembre de 2018
		A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,8	3,0	0,0	3,0	2,6	Tolerable	SI	Se deben incluir mecanismo de autenticación para el acceso a los backup, actualmente solo se encuentran comprimidos lo que facilita el acceso a la información por personal no autorizado	Dirección Técnica	12 de diciembre de 2018
		A9.1.1-Política de control de acceso	4	3,8	3,8	3,0	3,0	2,3	3,2	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico y físico solo para el personal que tiene asignado los roles y responsabilidades para el manejo de dispositivos e información que contiene	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual								Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
Datos / información [D]	Backup del sistema de gestión 17020 versión 2012, Software SART y SIIGO	A12.3.1-Respaldo de la información	3	2,0	2,7	2,7	0,0	2,7	2,0	Tolerable	SI	Se debe solicitar al director técnico estrategias que garanticen los respaldos de información sé que lleva a cabo para el proceso de revisión técnico - mecánica.	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.2.5-Revisión de los derechos de acceso de usuarios	3	4,0	4,0	3,0	0,0	4,0	3,0	Tolerable	SI	Dentro del programa de mantenimiento se debe incluir formatos para la verificación de cambio de contraseñas en tiempos regulares de 30 días	Dirección Técnica	12 de diciembre de 2018
		A12.6.1-Gestión de las vulnerabilidades técnicas	3	6,7	6,7	5,3	0,0	5,3	4,8	Tolerable	SI	Definir, documentar e implementar formatos y procedimiento en el que se permita llevar a cabo inventario de los activos y se relacionen las vulnerabilidades a las que se enfrenta.	Dirección Técnica Director Ejecutivo	12 de diciembre de 2018
		A8.3.2-Disposición de los medios	4	5,0	4,0	0,0	4,0	0,0	2,6	Tolerable	SI	En el plan de mantenimiento se debe incluir el tratamiento y destrucción de las imágenes de los sistemas operativos cuando ya no sea funcional por parte del proveedor o se requiera cambios de compatibilidad por actualización de los softwares para la revisión técnico - mecánica	Coordinador de calidad	12 de diciembre de 2018
		A9.1.2-Acceso a redes y a servicios en red	3	4,0	4,0	0,0	0,0	4,0	2,4	Tolerable	SI	Definir comunicar y documentar la divulgación del acceso y uso de la red de acuerdo a los permisos y autorización para la transferencia de información	Coordinador de Calidad Director Técnica director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual								Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A9.4.4-Uso de programas utilitarios privilegiados	4	5,0	5,0	4,0	4,0	3,0	4,2	Tolerable	SI	Se debe incluir en el programa de mantenimiento reglas para denegar permisos de instalación de programas utilitarios, con el fin de evitar bloqueos en las aplicaciones SART, CI2, Supergiros y actualizaciones en el navegador que afecte el correcto funcionamiento de la plataforma Runt	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A12.6.1-Gestión de las vulnerabilidades técnicas	3	3,0	3,0	4,0	0,0	0,0	2,0	Tolerable	SI	Definir, documentar e implementar formatos y procedimiento en el que se permita llevar a cabo inventario de los activos y se relacionen las vulnerabilidades a las que se enfrenta.	Dirección Técnica Director Ejecutivo	12 de diciembre de 2018
		A12.6.1-Gestión de las vulnerabilidades técnicas	3	4,0	3,0	4,0	0,0	0,0	2,2	Tolerable	SI	Definir, documentar e implementar formatos y procedimiento en el que se permita llevar a cabo inventario de los activos y se relacionen las vulnerabilidades a las que se enfrenta.	Dirección Técnica Director Ejecutivo	12 de diciembre de 2018
		A9.1.1-Política de control de acceso	4	3,0	3,0	2,3	2,3	3,0	2,7	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico solo para el personal que tiene asignado los roles y responsabilidades desde la alta dirección	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA														
IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control									Plan De Tratamiento De Riesgos			
				Valor del riesgo residual										
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A12.3.1-Respaldo de la información	3	5,0	4,0	5,0	0,0	0,0	2,8	Tolerable	SI	Se debe solicitar al director técnico estrategias que garanticen los respaldos de las imágenes de los sistemas operativos, el software y las actualizaciones como mejoras o cambios de cumplimiento.	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	4	4,0	4,0	3,0	4,0	3,0	3,6	Tolerable	SI	Se debe incluir en el programa de mantenimiento reglas para denegar permisos de instalación de programas utilitarios, con el fin de evitar bloqueos en las aplicaciones SART, CI2, Supergiros y actualizaciones en el navegador que afecte el correcto funcionamiento de la plataforma Runt	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,8	3,8	3,8	0,0	3,0	2,9	Tolerable	SI	El programa de formación debe incluir el buen uso de los equipos informáticos y el manejo de herramientas y programa utilitarios	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A12.6.1-Gestión de las vulnerabilidades técnicas	3	3,3	3,3	3,3	0,0	0,0	2,0	Tolerable	SI	Definir, documentar e implementar formatos y procedimiento en el que se permita llevar a cabo inventario de los activos y se relacionen las vulnerabilidades a las que se enfrenta.	Dirección Técnica Director Ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual							Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A9.1.1-Política de control de acceso	4	2,5	2,5	2,0	2,0	2,0	2,2	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico solo para el personal que tiene asignado los roles y responsabilidades desde la alta dirección	Coordinador de Calidad Director ejecutivo	12 de diciembre de 2018
		A13.2.4-Acuerdos de confidencialidad o de no divulgación	3	3,3	2,7	2,7	0,0	2,7	2,3	Tolerable	SI	Desde la alta dirección se deben establecer acuerdos de confidencialidad frente al manejo de información obtenida durante el desarrollo de las actividades de sus servicios, estos reportes no deben estas expuestos a fugas de información y ser divulgados	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	4	2,5	2,0	2,5	2,0	2,0	2,2	Tolerable	SI	Se debe incluir en el programa de mantenimiento reglas para denegar permisos de instalación de programas utilitarios, con el fin de evitar bloqueos en las aplicaciones SART, CI2, Supergiros y actualizaciones en el navegador que afecte el correcto funcionamiento de la plataforma Runt	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A12.6.1-Gestión de las vulnerabilidades técnicas	4	3,0	3,0	5,0	0,0	0,0	2,2	Tolerable	SI	Definir, documentar e implementar formatos y procedimiento en el que se permita llevar a cabo inventario de los activos y se relacionen las vulnerabilidades a las que se enfrenta.	Dirección Técnica Director Ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control									Plan De Tratamiento De Riesgos			
				Valor del riesgo residual										
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,0	3,0	2,3	0,0	2,3	2,1	Tolerable	SI	Desde la alta dirección se deben establecer acuerdos de confidencialidad frente al manejo de información del sistema de gestión y la que se derive de la prestación de los servicios, estos reportes no deben estas expuestos a fugas de información y ser divulgados	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.1.2-Acceso a redes y a servicios en red	1	4,0	4,0	0,0	0,0	4,0	2,4	Tolerable	SI	Definir comunicar y documentar la divulgación del acceso y uso de la red de acuerdo a los permisos y autorización para la transferencia de información y el uso de medios	Coordinador de Calidad Director Técnica director ejecutivo	12 de diciembre de 2018
		A13.2.4-Acuerdos de confidencialidad o de no divulgación	1	4,0	4,0	3,0	0,0	4,0	3,0	Tolerable	SI	Desde la alta dirección se deben establecer acuerdos de confidencialidad frente al manejo de información obtenida durante el desarrollo de las actividades de sus servicios, y sus reportes a entidades legales	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	1	4,0	4,0	5,0	5,0	4,0	4,4	Tolerable	SI	No se debe realizar la actualización de complementos mientras el proveedor no emita la actualización del aplicativo	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A9.2.6-Retiro o ajuste de los derechos de acceso	2	4,0	4,0	4,0	0,0	0,0	2,4	Tolerable	SI	Al formato de registro de cambio o eliminación de los accesos de un usuario esto aplica para los usuarios que finalizan su contratación laboral o existe cambio de funciones, se debe incluir la eliminación formal con el proveedor	Coordinador de Calidad Dirección Técnica Director Ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control									Plan De Tratamiento De Riesgos				
				Valor del riesgo residual											
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A9.1.2-Acceso a redes y a servicios en red	2	5,0	5,0	0,0	0,0	4,0	2,8	Tolerable	SI	Definir comunicar y documentar la divulgación del acceso y uso de la red de acuerdo a los permisos y autorización para la transferencia de información y el uso de medios	Coordinador de Calidad Director Técnica director ejecutivo	12 de diciembre de 2018
		A13.2.4-Acuerdos de confidencialidad o de no divulgación	2	5,0	4,0	0,0	0,0	4,0	2,6	Tolerable	SI	Desde la alta dirección se deben establecer acuerdos de confidencialidad frente al manejo de información obtenida durante el desarrollo de las actividades de sus servicios, y sus reportes a entidades legales	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	2	3,0	3,0	5,0	4,0	4,0	3,8	Tolerable	SI	No se debe realizar la actualización de complementos mientras el proveedor no emita la actualización del aplicativo	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0	0,0	3,0	2,1	Tolerable	SI	El programa de formación debe incluir la capacitación dentro de la formación de inducción para los cargos que manejan este tipo de herramientas	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A9.1.2-Acceso a redes y a servicios en red	2	4,0	4,0	0,0	0,0	4,0	2,4	Tolerable	SI	Definir comunicar y documentar la divulgación del acceso y uso de la red de acuerdo a los permisos y autorización para la transferencia de información y el uso de servicios de red	Coordinador de Calidad Director Técnica director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual							Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A9.1.1-Política de control de acceso	4	3,0	3,0	3,0	3,0	3,0	3,0	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico solo para el personal que tiene asignado los roles y responsabilidades desde la alta dirección	Coordinador de Calidad Director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	3	2,0	2,0	2,7	2,7	2,7	2,4	Tolerable	SI	No se debe realizar la actualización de complementos mientras el proveedor no emita la actualización del aplicativo	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A9.1.1-Política de control de acceso	4	3,0	3,0	2,3	0,0	3,0	2,3	Tolerable	SI	Se incluye la política de acceso físico y lógico en el que se incluye reglas de cumplimiento para todos los activos de la organización	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	4,0	4,0	4,0	0,0	4,0	3,2	Tolerable	SI	Desde la alta dirección se deben establecer acuerdos de confidencialidad frente al manejo de información obtenida durante el desarrollo de las actividades de sus servicios, estos reportes no deben estas expuestos a fugas de información y ser divulgados	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	3	2,0	2,0	3,3	2,7	2,0	2,4	Tolerable	SI	No se debe realizar la actualización de complementos mientras el proveedor no emita la actualización del aplicativo	Dirección Técnica director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual								Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A8.3.2-Disposición de los medios	4	3,0	3,0	2,3	2,3	3,0	2,7	Tolerable	SI	Tanto para la información como para el manejo de versiones del software y aplicaciones se maneja un tiempo de retención mínimo de 3 años como lo establece las obligaciones contractuales para estos organismos, sin embargo, no existe un mecanismo para la eliminación o destrucción de información	Coordinador de calidad	12 de diciembre de 2018
		A9.1.2-Acceso a redes y a servicios en red	3	4,0	4,0	0,0	0,0	4,0	2,4	Tolerable	SI	Definir comunicar y documentar la divulgación del acceso y uso de la red de acuerdo a los permisos y autorización para la transferencia de información y el uso de medios	Coordinador de Calidad Director Técnica director ejecutivo	12 de diciembre de 2018
		A9.1.1-Política de control de acceso	4	2,0	2,0	2,5	2,5	2,0	2,2	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico de la carpeta raíz del software de aplicación, el cual debe contar con niveles de seguridad de acuerdo a los roles y responsabilidades definidas por la alta dirección	Coordinador de Calidad Director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	4	3,0	3,0	3,8	3,0	3,0	3,2	Tolerable	SI	No se debe realizar la actualización de complementos mientras el proveedor no emita la actualización del aplicativo	Dirección Técnica director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA																
IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual								Plan De Tratamiento De Riesgos				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva		
		A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,8	3,8	2,3	0,0	2,3	2,4	Tolerable	SI	El programa de formación debe incluir para todos los funcionarios el manejo de programas utilitarios	Dirección Técnica director ejecutivo	12 de diciembre de 2018		
		A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0	0,0	0,0	3,0	Tolerable	SI	Evitar el uso no autorizado de software, la instalación y bajar aplicaciones desde los diferentes canales de comunicación	Coordinador de calidad Dirección técnica director ejecutivo	12 de diciembre de 2018		
		A12.6.1-Gestión de las vulnerabilidades técnicas	4	5,0	4,0	4,0	0,0	0,0	2,6	Tolerable	SI	Definir, documentar e implementar formatos y procedimiento en el que se permita llevar a cabo inventario de los activos y se relacionen las vulnerabilidades a las que se enfrenta.	Dirección Técnica Director Ejecutivo	12 de diciembre de 2018		
		A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0	0,0	0,0	3,0	Tolerable	SI	Evitar el uso no autorizado de software, la instalación y bajar aplicaciones desde los diferentes canales de comunicación	Coordinador de calidad Dirección técnica director ejecutivo	12 de diciembre de 2018		
		A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	3,0	2,3	3,0	2,6	Tolerable	SI	Se debe incluir en el programa de mantenimiento reglas para la instalación y actualización solo por personal con privilegios especiales, esto para evitar otras descargas	Dirección Técnica director ejecutivo	12 de diciembre de 2018		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual								Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	3	5,0	5,0	3,0	0,0	0,0	2,6	Tolerable	SI	El programa de formación debe incluir para todos los funcionarios el manejo de programas utilitarios	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0	0,0	0,0	3,0	Tolerable	SI	Evitar el uso no autorizado de software, la instalación y bajar aplicaciones desde los diferentes canales de comunicación	Coordinador de calidad Dirección técnica Director ejecutivo	12 de diciembre de 2018
		A12.6.1-Gestión de las vulnerabilidades técnicas	4	5,0	4,0	4,0	0,0	0,0	2,6	Tolerable	SI	Definir, documentar e implementar formatos y procedimiento en el que se permita llevar a cabo inventario de los activos y se relacionen las vulnerabilidades a las que se enfrenta.	Dirección Técnica Director Ejecutivo	12 de diciembre de 2018
		A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0	0,0	0,0	3,0	Tolerable	SI	Evitar el uso no autorizado de software, la instalación y bajar aplicaciones desde los diferentes canales de comunicación	Coordinador de calidad Dirección técnica director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	3,0	2,3	3,0	2,6	Tolerable	SI	Se debe incluir en el programa de mantenimiento reglas para la instalación y actualización solo por personal con privilegios especiales, esto para evitar otras descargas	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A12.2.1-Controles contra códigos maliciosos	4	5,0	4,0	4,0	0,0	0,0	2,6	Tolerable	SI	Evitar el uso no autorizado de software, la instalación y bajar aplicaciones desde los diferentes canales de comunicación	Coordinador de calidad Dirección técnica director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual								Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A12.2.1-Controles contra códigos maliciosos	4	5,0	4,0	4,0	0,0	0,0	2,6	Tolerable	SI	Evitar el uso no autorizado de software, la instalación y bajar aplicaciones desde los diferentes canales de comunicación	Coordinador de calidad Dirección técnica director ejecutivo	12 de diciembre de 2018
		A9.1.2-Acceso a redes y a servicios en red	2	4,0	4,0	0,0	0,0	4,0	2,4	Tolerable	SI	Definir comunicar y documentar la divulgación del acceso y uso de la red de acuerdo a los permisos y autorización para la transferencia de información a los sitios web	Coordinador de Calidad Director Técnica director ejecutivo	12 de diciembre de 2018
		A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,0	3,0	2,3	0,0	2,3	2,1	Tolerable	SI	Desde la alta dirección se deben establecer acuerdos de confidencialidad frente al manejo de información y los reportes que se envían a las entidades legales por medio de sitios web	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	3,8	3,0	3,0	2,9	Tolerable	SI	se debe incluir en el programa de mantenimiento reglas para denegar permisos de instalación de programas utilitarios, con el fin de evitar bloqueos en las aplicaciones SART, CI2, Supergiros y actualizaciones en el navegador que afecte el correcto funcionamiento de la plataforma Runt	Dirección Técnica director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control									Plan De Tratamiento De Riesgos			
				Valor del riesgo residual										
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A11.2.2-Servicios de suministro	2	3,0	4,0	4,0	0,0	0,0	2,2	Tolerable	SI	El CDA cuenta con instalaciones eléctricas regulada y no regulada, y para cada uno de sus equipos UPS pequeña de 8 minutos para que los procesos se finalicen correctamente, deben ser incluidas en el plan de mantenimiento de las instalaciones físicas no se especifican estas condiciones para garantizar la continuidad del negocio.	Dirección Técnica Director Ejecutivo	12 de diciembre de 2018
		A9.1.1-Política de control de acceso	4	2,3	2,3	3,0	3,0	2,3	2,6	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico y físico los cuales esta definidos con la asignación de roles y responsabilidades establecidos por la alta dirección	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	4	3,0	0,0	3,0	2,3	2,3	2,1	Tolerable	SI	Se debe incluir en el programa de mantenimiento reglas para denegar permisos de instalación de programas utilitarios, con el fin de evitar bloqueos en las aplicaciones SART, CI2, Supergiros y actualizaciones en el navegador que afecte el correcto funcionamiento de la plataforma Runt	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A11.2.4-Mantenimiento de los equipos.	3	3,0	4,0	4,0	0,0	0,0	2,2	Tolerable	SI	Actualmente se cuenta con la planificación y formatos de reportes de mantenimiento sin embargo no existe un instructivo que le permita al personal o proveedor conocer los requerimientos para asegurar la disponibilidad	Dirección Técnica director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA															
IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual							Plan De Tratamiento De Riesgos				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva	
		A9.1.1-Política de control de acceso	4	3,0	3,0	3,0	2,3	2,3	2,7	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico y físico los cuales esta definidos con la asignación de roles y responsabilidades establecidos por la alta dirección	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018	
		A9.1.2-Acceso a redes y a servicios en red	3	2,7	2,7	2,7	0,0	2,7	2,1	Tolerable	SI	Definir comunicar y documentar la divulgación del acceso y uso de la red de acuerdo a los permisos y autorización para la transferencia de información	Coordinador de Calidad Director Técnica director ejecutivo	12 de diciembre de 2018	
		A9.4.4-Uso de programas utilitarios privilegiados	4	3,0	2,3	3,0	2,3	3,0	2,7	Tolerable	SI	Se debe incluir en el programa de mantenimiento reglas para denegar permisos de instalación de programas utilitarios, con el fin de evitar bloqueos en las aplicaciones SART, CI2, Supergiros y actualizaciones en el navegador que afecte el correcto funcionamiento de la plataforma Runt	Dirección Técnica director ejecutivo	12 de diciembre de 2018	
		A9.1.1-Política de control de acceso	4	2,3	3,0	3,0	2,3	3,0	2,7	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico y físico los cuales esta definidos con la asignación de roles y responsabilidades establecidos por la alta dirección	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018	

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual							Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A9.1.2-Acceso a redes y a servicios en red	3	4,0	4,0	0,0	3,0	0,0	2,2	Tolerable	SI	Definir comunicar y documentar la divulgación del acceso y uso de la red de acuerdo a los permisos y autorización para la transferencia de información	Coordinador de Calidad Director Técnica director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	2,3	3,0	2,3	2,4	Tolerable	SI	Se debe incluir en el programa de mantenimiento reglas para denegar permisos de instalación de programas utilitarios, con el fin de evitar bloqueos en las aplicaciones SART, CI2, Supergiros y actualizaciones en el navegador que afecte el correcto funcionamiento de la plataforma Runt	Dirección Técnica Director ejecutivo	12 de diciembre de 2018
		A11.2.2-Servicios de suministro	2	3,0	3,0	5,0	0,0	4,0	3,0	Tolerable	SI	De acuerdo al equipamiento en el espacio del servidor se cuenta con UPS que garantiza el funcionamiento de los equipos por 2 horas para que los procesos se finalicen correctamente, deben ser incluidas en el plan de mantenimiento de las instalaciones físicas no se especifican estas condiciones para garantizar la continuidad del negocio.	Dirección Técnica Director Ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual								Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
		A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,0	3,0	3,8	3,0	3,0	3,2	Tolerable	SI	El programa de formación debe incluir toda la documentación de los sistemas de gestión para garantizar el compromiso y la concientización sobre el manejo de información, equipos informáticos, dispositivos periféricos dispuestos por el CDA para la prestación de los servicios	Dirección Técnica Proveedor de Mantenimiento director ejecutivo	12 de diciembre de 2018
		A9.1.1-Política de control de acceso	4	2,0	2,0	2,5	2,5	2,0	2,2	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico y físico los cuales esta definidos con la asignación de roles y responsabilidades establecidos por la alta dirección	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A9.4.4-Uso de programas utilitarios privilegiados	3	3,3	3,3	3,3	2,7	2,7	3,1	Tolerable	SI	Se debe incluir en el programa de mantenimiento reglas para denegar permisos de instalación de programas utilitarios, con el fin de evitar bloqueos en las aplicaciones SART, CI2, Supergiros y actualizaciones en el navegador que afecte el correcto funcionamiento de la plataforma Runt	Dirección Técnica director ejecutivo	12 de diciembre de 2018
		A9.1.1-Política de control de acceso	4	3,0	3,0	3,8	3,0	3,0	3,2	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico y físico para el manejo de dispositivos que proporcionan conectividad a nivel de red de datos.	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		Evaluación Del Control		Valor del riesgo residual							Plan De Tratamiento De Riesgos			
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Promedio	Valoración del riesgo residual	Requiere Plan de Mejoramiento	Acción Correctiva	Responsable	Fecha limite documentación de acción Correctiva
Elaboración: propia.	Cableado estructurado - red LAN	A12.6.1-Gestión de las vulnerabilidades técnicas	3	2,0	0,0	2,7	2,7	2,7	2,0	Tolerable	SI	El procedimiento debe definir las directrices para la instalación de aplicaciones dispositivos de controles de acceso como el firewall	Dirección Técnica Director Ejecutivo	12 de diciembre de 2018
		A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0	2,3	2,3	2,4	Tolerable	SI	El programa de formación debe incluir toda la documentación de los sistemas de gestión para garantizar el compromiso y la concientización sobre el manejo de información, equipos informáticos, dispositivos periféricos dispuestos por el CDA para la prestación de los servicios	Dirección Técnica Proveedor de Mantenimiento director ejecutivo	12 de diciembre de 2018
		A9.1.1-Política de control de acceso	4	2,0	2,0	2,5	2,0	2,0	2,1	Tolerable	SI	Definir comunicar y documentar la divulgación de los controles de acceso lógico y físico los cuales esta definidos con la asignación de roles y responsabilidades establecidos por la alta dirección	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018
		A13.2.4-Acuerdos de confidencialidad o de no divulgación	3	3,3	3,3	2,7	0,0	2,7	2,4	Tolerable	SI	Desde la alta dirección se deben establecer acuerdos de confidencialidad frente al manejo de información obtenida durante el desarrollo de las actividades de sus servicios, y la transferencia de datos a nivel interno y externo.	Coordinador de Calidad director ejecutivo	12 de diciembre de 2018

Elaboración: propia.

En la tabla de plan de tratamiento de riesgos se asocian 17 controles para todos los activos los cuales conforman la estructura del sistema de gestión de seguridad de información y a su vez del sistema de gestión para organismos de inspección actual. Estos deben ser agregados por personal externo competente puesto que los funcionarios deben recibir socialización y capacitación para la debida inclusión. Una vez sede su aplicación estas herramientas permiten obtener mejores resultados para el tratamiento y manejo de los sistemas informáticos e información.

Los controles seleccionados deben ser informados al director ejecutivo y al coordinador de calidad para el estudio de implementación teniendo en cuenta el bajo costo que le implica al Centro de Diagnóstico Automotor ponerlos en funcionamiento con herramientas que no generan grandes inversiones y no requieren de contratación del personal permanente.

14. POLÍTICAS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN E INFORMÁTICA

14.1. POLÍTICA DE SEGURIDAD EN LA INFORMACION

Objetivo: Determinar la estrategia y reglamentación para la seguridad de la información conforme a los aspectos de confidencialidad, integridad y disponibilidad desde la gestión de recursos humanos sobre las bunas prácticas con los activos de la organización.

Directriz

La Organización Corpotrans CDA S.A.S., Comprometida con sus actividades de revisión técnico - mecánica, promueve el bienestar integral de sus trabajadores, proveedores, contratistas, subcontratistas, visitantes, gobierno, comunidad, demás grupos de interés involucrados y partes interesadas con la operación, garantizando la satisfacción de sus clientes y accionistas, así como con la mitigación de los posibles impactos socio–ambientales, tecnológicos, éticos, comerciales y legales o reguladores a nivel nacional y en sus áreas de influencia, proporcionando los controles necesarios a la propiedad intelectual y manejo de la información confidencial de los usuarios con el ánimo de mitigar los riesgos asociados al servicio.

El compromiso se fundamenta en los siguientes aspectos:

Confidencialidad: la alta dirección lidera la responsabilidad del Sistema de Gestión de seguridad en la información (SGSI), aportando sus experiencias, competencia técnica, asignando el talento humano, materiales y un amplio respaldo económico al SGSI, mantendrá la información cada cliente disponible para él, estableciendo acuerdos de confidencialidad y controles de acceso a la información en todo lo relacionado con procedimientos, estrategias, documentación legal y confidencial del negocio, métodos y datos, asegurando contractualmente la confidencialidad, como valor de ética profesional, no suministrando información a terceras personas, organizaciones, entidades o procesos no autorizados por el mismo cliente sin previo aviso, Igualmente la alta dirección se compromete a informar, cuando expresamente por orden proveniente de una autoridad legal competente, se requiera brindar información de la empresa o de nuestros clientes, esto involucra las quejas o apelaciones.

Integridad e imparcialidad: Corpotrans CDA S.A.S., desarrolla sus actividades con independencia, e imparcialidad con el fin de minimizar conflictos de intereses y la aplicación de matriz de riesgos tecnológicos para el manejo de la información en el que ha identificado los riesgos a los que está expuesto en materia de Independencia, Imparcialidad, conflicto de intereses, disponibilidad, autenticidad y trazabilidad, según los riesgos procedentes del desarrollo de sus actividades, o de sus relaciones (ver matriz de riesgos) y un Convenio de confidencialidad, independencia y conflicto de intereses, suscrito por los empleados, proveedores, contratistas y clientes.

Disponibilidad de la Información: Todos los funcionarios de Corpotrans CDA S.A.S., tienen acceso sólo a la información fundamental para el desarrollo de sus actividades. En el caso de personal no autorizado deben solicitar autorización formal al director ejecutivo o al director técnico y ellos darán sólo el acceso indispensable de acuerdo con el trabajo realizado por cada funcionario o proveedor contratado. El

acceso a la información se encuentra delimitado de acuerdo a los procedimientos definidos su actividad.

Proveedores, auditorías externas y terceras personas solo cuentan con privilegios durante el periodo del tiempo en el que se llevan a cabo las funciones, auditorias aprobadas y por ningún caso podrán llevar información de ningún cliente.

Autenticidad: La alta dirección y sus funcionarios deben identificar los requerimientos para asegurar la autenticidad, integridad de la información de los usuarios a través de medios y controles establecidos en la matriz de riesgos.

Mediante los backup de la información, se pretende minimizar el riesgo de pérdida disponibilidad e integridad de la información. En caso que se presente una eventualidad que ponga en riesgo la consistencia de la información se debe documentar dentro del sistema y tomar las acciones pertinentes para una solución.

Para tal efecto y como política se debe realizar periódicamente la validación de los backup y el restablecimiento de los mismos aplicando políticas de restauración, gestión de roles o perfiles de usuarios o multiusuarios en red, para asegurar que todo se pueda recuperar tras un desastre o un fallo de los soportes.

No-Repudio: la organización Corpotrans CDA S.A.S., ha establecido como mecanismo de control a la recepción y la entrega de la información de cada cliente mediante medios extraíbles y no manejo por correos electrónicos para evitar la manipulación mal intencionada por terceros, alteración o modificación injustificada de la información manteniendo estos archivos encriptados y sus claves protegidas a través de los convenios firmados entre las partes.

Confiablidad: la satisfacción del servicio de revisión técnico - mecánica está enfocado en el cumplimiento de requisitos legales y reglamentarios. Realizado por personal productivo y competente, en el cual busca asegurar la seguridad de la información de quienes participan en el proceso.

Todo cambio (creación y modificación de documentación) que afecte los recursos informáticos, o el sistema de seguridad en la información no se podrá realizar sin la intervención del director ejecutivo o del coordinador de calidad el cual realizara las modificaciones a los documentos.

Mejora continua: Estimular el mantenimiento de los procesos a partir de estrategias de seguimiento, medición y monitoreo en el que le permita a Corpotrans CDA S.A.S, cumplir con los objetivos gerenciales desde la implementación del sistema de gestión de seguridad de información. La custodia del sistema se gestiona a través de auditorías internas, análisis de riesgos, acciones correctivas y revisiones gerenciales programadas.

Seguridad Contractual: Corpotrans CDA S.A.S, tiene como compromiso establecer y revisar los objetivos propuestos dentro del Sistema de seguridad en la información (SGSI), con el propósito de identificar el cumplimiento y requisitos legales obligatorios, los cuales deben incluidos en Matriz para dar inicio a su adecuada implementación y justificación dentro de la organización.

Los métodos para evaluar el cumplimiento legal en Corpotrans CDA S.A.S. son:

- ✓ Auditorías internas, frecuencia anual.
- ✓ Auditorías Externas, cuando se requiera o en los ciclos, frecuencia anual.

- ✓ Matriz de Riesgos, frecuencia permanentemente.
- ✓ Verificación por la ARL o por parte de las partes interesadas, frecuencia semestral o a solicitud.

Adicionalmente la evaluación del cumplimiento legal contractual es realizada por el director ejecutivo y un ingeniero de soporte, dejando registro de los resultados de la misma en la matriz en cuanto a su revisión y verificación del cumplimiento.

Responsables: El cumplimiento de esta política integra al director ejecutivo, la participación de todos los funcionarios, contratistas que forma parte de la organización.

Nota: La presente política será revisada, divulgada, publicada y de estricto cumplimiento para todo el personal.

Sanciones:

- ✓ El incumplimiento de la política una vez comunicada y publicada genera llamados de atención con copia a la hoja de vida, los cuales dan lugar a una suspensión o finalización del contrato.

14.2. POLÍTICA DE FORMACIÓN

Objetivo: Definir los lineamientos de cumplimiento y procedimientos necesarios para la planificación y toma de conciencia frente al manejo y aseguración de los activos de información que intervienen en la prestación de los servicios.

Directriz

Corpotrans CDA S.A.S., está comprometida con la seguridad de la información en toda la organización, sus trabajadores y partes interesadas Uno de los principios de la política de seguridad en la información, consiste en potenciar la formación continua a través de un Cronograma Anual de Capacitación y/o Formación personalizado que incluye la inducción, reinducción, entrenamiento y evaluación para funcionarios, proveedores, contratistas y partes interesadas. Conscientes que el recurso más importante de la organización son las personas, su conocimiento y su implicación en la estrategia de la organización; imprescindibles para alcanzar el completo desarrollo de todo su potencial y sus cualidades personales y profesionales.

La formación en Corpotrans CDA S.A.S., está dirigida a la consecución de los siguientes objetivos:

- ✓ Alcanzar el mayor nivel técnico de todos los funcionarios dedicados a la implementación de los sistemas de seguridad en la información.
- ✓ Optimizar la comunicación, gestión de equipos y liderazgo entre funcionarios y la expectativa frente a los proveedores, contratistas y partes interesadas.
- ✓ Alcanzar altos índices de satisfacción en el lugar de trabajo a través de la formación destinada al desarrollo profesional y humano de todo el personal.
- ✓ Evitar la obsolescencia y actualizarse en nuevas tecnologías en controles de seguridad en la información.
- ✓ Establecer lineamientos para la rendición de cuentas por parte de todo el personal en caso de omisiones propias o generales.

Tanto el procedimiento de gestión, como el cronograma Anual de Capacitación y/o Formación se somete a las correspondientes auditorías internas y externas, hecho que garantiza el más alto nivel de rendimiento, como la mejora continua de esta línea estratégica de Corpotrans CDA S.A.S.

Responsables: El cumplimiento de esta política involucra el liderazgo gerencial, así como la participación de todos los funcionarios, contratistas y demás partes interesadas.

Nota: La presente política será revisada, divulgada, publicada y de estricto cumplimiento para todo el personal.

Sanciones

- ✓ El incumplimiento de la política una vez comunicada y publicada genera llamados de atención con copia a la hoja de vida, los cuales dan lugar a una suspensión o finalización del contrato.
- ✓ Para los proveedores y contratistas que no sigan los lineamientos de la política se genera la cancelación del contrato y se activan las pólizas de incumplimiento.

14.3. POLÍTICA DE CONTROL DE ACCESO

Objetivo: Establecer los derechos de acceso y permisos para el manejo adecuado de los activos de información (equipos, aplicaciones, procedimientos, espacio físico) que requieren los usuarios desde la asignación de las funciones y responsabilidades de cada uno de los cargos.

Directriz

Corpotrans CDA ha establecido los requisitos de cumplimiento para llevar a cabo los procedimientos para la ejecución del procesos internos y en cumplimiento con los roles y responsabilidades frente a los activos lógicos y físicos los cuales son importantes para organización desde el entorno económico, Por lo tanto se debe tener en cuenta la responsabilidad por la adecuada manipulación desde los funcionarios, proveedores y contratistas quienes deben garantizar la confiabilidad de la información, la integridad y autenticidad sobre los equipos informáticos. Así mismo se determinan la verificación y autenticación de acceso para cada una de las herramientas de tecnológicas de información y comunicación con el fin de llevar los registros de los usuarios en las actividades de dicho proceso.

Los roles y las responsabilidades están sujetos a los procesos que desarrollan en el sistema de información y el líder que verifique y valide que el nivel de acceso es el adecuado con los parámetros de seguridad de información.

La seguridad en el software propone medidas para evitar poner en riesgo de código malicioso afectar la integridad y la autenticidad tomando provecho de las vulnerabilidades del mismo, es por esto que el proveedor del software de garantizar la seguridad del ciclo de vida y establecer lineamientos de cumplimiento por parte de la organización.

La seguridad en el hardware propone medidas de protección para evitar el daño del entorno en el que se encuentra y su vez permite hacer énfasis en los dispositivos de que funcionan como escáner en el tráfico de red y que a partir de los mismos se facilita la inclusión de mecanismos criptográficos.

La seguridad en la red propone medidas de protección en la red garantizando la integridad y seguridad de los datos que se transmiten de amenazas como malware, interceptación de código malicioso, ataques de denegación de servicios, suplantación y robo de identidad, en donde es posible a través de herramientas físicas y lógicas como software de detección de código malicioso, el cual debe permanecer actualizado y con licencia vigente esto permite que trabajen en conjunto para la mejora de seguridad y mantenimiento de los componentes de la red.

Los controles de acceso se rigen por los siguientes principios y actividades:

- ✓ La Restricción a los programas e información permite en la organización:
- ✓ Garantizar que los funcionarios trabajen sin la supervisión permanente y el riesgo presente de modificación ante los datos de programas e información confidencial.
- ✓ Se segura que el acceso a la información y programas es adecuado a sus roles y responsabilidades sobre el programa apropiado.
- ✓ Se asegura la transmisión de los datos entre el emisor y del destinatario a nivel de red interna.

Que en caso de fallas se establezcan canales de comunicación para la transferencia de información.

Responsables: El cumplimiento de esta política involucra el liderazgo gerencial, así como la participación de todos los funcionarios, contratistas y demás partes interesadas.

Nota: La presente política será revisada, divulgada, publicada y de estricto cumplimiento para todo el personal.

Sanciones

- ✓ El incumplimiento de la política una vez comunicada y publicada genera llamados de atención con copia a la hoja de vida, los cuales dan lugar a una suspensión o finalización del contrato.
- ✓ Para los proveedores y contratistas que no sigan los lineamientos de la política se genera la cancelación del contrato y se activan las pólizas de incumplimiento.

14.4. POLÍTICA DE ACCESO A REDES Y A SERVICIOS DE RED

Objetivo: Definir los requisitos de autenticación y el manejo apropiado de estos elementos por parte de cada de los usuarios frente a los servicios de red interna y externa.

Directriz

La Organización Corpotrans CDA S.A.S. en su compromiso con la seguridad y el logro de la aplicación de controles eficientes en su estructura de red establece la política de acceso a redes y a servicios de red, garantizando la conectividad de la intranet por medio de componentes que faciliten el estudio y análisis de posibles riesgos y amenazas, el uso de la red y la responsabilidad de cada uno de los funcionarios, proveedores y contratistas por hacer buen uso de este recurso.

Los recursos de acceso y canales de comunicación intranet e internet son el servicio principal para el negocio de la organización desde diferentes puntos de acceso del sistema de información en el que intervienen equipos informáticos para dicha comunicación con sistemas externos los cuales son esenciales para prestar los

servicios y así mismo se encuentran asociados con los objetivos misionales de la empresa.

Estos servicios se encuentran a disposición de funcionarios, proveedores y contratistas con el único objetivo de facilitar el desarrollo de sus labores para los que fueron contratados, es por esto que no está permitido el uso desmesurado para la ejecución de actividades propias y que a su vez no estén alineadas con los objetivos de la entidad.

Toda información que se maneje al interior de la organización es confidencial y por lo tanto funcionarios, proveedores y contratistas cuentan con medidas de autenticación y de acceso en donde:

- ✓ El funcionario de acuerdo al rol y sus funciones maneja su propia autenticación para el acceso a los servicios y aplicaciones que hacen uso de la intranet e internet.
- ✓ La organización cuenta con el responsable que supervisa y verifica el cumplimiento de los procesos y de la autonomía que se les ha otorgado a los funcionarios tenga uso prudente sobre el servicio.
- ✓ Los servicios en línea cuentan con plataformas autorizadas por entidades legales en donde se debe contar con el navegador instalado en equipos específicos dentro del proceso.
- ✓ Los funcionarios cuentan con medidas de autenticación como usuario y contraseña, firma digital, lector de huella, las cuales con otorgadas desde la dirección ejecutiva y los responsables del proceso.
- ✓ El acceso a los servicios de los sitios web se realiza por las páginas web directamente de las entidades delegadas por las leyes colombianas.
- ✓ Las cuentas de usuario, firma digital y huella anteriormente registrada no se encuentren en permanente uso, se genera el bloqueo automático y solo los

responsables del proceso autorizados para realizar actualización y/o modificaciones de información sobre su personal podrá llevar a cabo estos cambios o reactivación.

Responsables: El cumplimiento de esta política involucra el liderazgo gerencial, así como la participación de todos los funcionarios, contratistas y demás partes interesadas.

Nota: La presente política será revisada, divulgada, publicada y de estricto cumplimiento para todo el personal.

Sanciones

- ✓ El incumplimiento de la política una vez comunicada y publicada genera llamados de atención con copia a la hoja de vida, los cuales dan lugar a una suspensión o finalización del contrato.

14.5. POLÍTICA USO DE SOFTWARE NO AUTORIZADO

Objetivo: Definir las buenas prácticas frente al manejo de equipos y aplicaciones dispuestos para el desarrollo de los procesos y funcionalidad permanente y controlada de los mismos.

Directriz

Corpotrans CDA S.A.S., está comprometida con la seguridad de su información y en el manejo de datos y de los activos que tiene a disposición para las actividades

propuestas de prestación de los servicios, por consiguiente fomenta la capacitación y formación de los funcionarios, contratistas y proveedores en el buen uso del hardware y software como uno de los recursos importantes de los procesos de la organización, a su vez realiza énfasis en la prohibición de la utilización de software sin licencia, el uso de los canales de comunicación de internet con fines personales generando descargas e sitios web no autorizados en los equipos y dispositivos tecnológicos. Causando traumatismos en los sistemas de información exponiendo la seguridad a riesgos y amenazas como perdida de información, filtración de código malicioso, interrupción en los servicios de red, daño en los sistemas, robo y suplantación de identidad.

Se regirán por los siguientes principios y actividades:

- ✓ Se debe contar con sistemas que en conjunto se permita asegurar la integridad de los sistemas de información y del software.
- ✓ Se debe tomar conciencia frente a las posibles amenazas y los peligros que origina el software malicioso y no autorizado para su uso por los responsables del proceso.
- ✓ El uso adecuado del canal de comunicación y solo con fines pertinentes a las labores que fueron asignadas promoviendo el uso responsable de la misma.
- ✓ los funcionarios responsables, contratistas y proveedores designados por la alta dirección deben velar por el cumplimiento de restricción de instalación de aplicaciones.
- ✓ Se debe mantener todas las aplicaciones como el antivirus actualizado en cada uno de las fuentes de trabajo en los que se cuentan con equipos informáticos.

- ✓ Todos los programas deben ser instalados por personal autorizado desde la dirección y a su vez deben proporcionar las actualizaciones directamente del proveedor.

El personal para el cumplimiento de las medidas de seguridad adoptadas debe monitorear y supervisar por medio de la planificación periódica de mantenimiento a los equipos, la actualización y configuración versiones funcionales para el software de análisis de detección, plataformas en línea, y software propio para la prestación de los servicios en la organización.

Responsables: El cumplimiento de esta política involucra el liderazgo gerencial, así como la participación de todos los funcionarios, contratistas y demás partes interesadas.

Nota: La presente política será revisada, divulgada, publicada y de estricto cumplimiento para todo el personal.

Sanciones

- ✓ El incumplimiento de la política una vez comunicada y publicada genera llamados de atención con copia a la hoja de vida, los cuales dan lugar a una suspensión o finalización del contrato.
- ✓ Para los proveedores y contratistas que no sigan los lineamientos de la política se genera la cancelación del contrato y se activan las pólizas de incumplimiento.

14.6. POLÍTICA DE RESPALDO DE INFORMACIÓN

Objetivo: Establecer las reglas y procedimientos para la integridad y disponibilidad de la información confidencial de la revisión técnico mecánica y responsabilidad de la gestión para los cargos con responsabilidades y privilegios especiales.

Directriz

La organización ha establecido procedimientos específicos para realizar copias de seguridad de la información contenida en los discos duros de los servidores. A la hora de hacer una copia de seguridad, lo primero que hay que tener en cuenta es la integridad de los datos que se estén guardando. Cuando los contenidos de una base de datos se modifican, la integridad de los datos almacenados puede perderse, para esto se requiere que la información sólo pueda ser modificada por personal autorizado o en su defecto si el cliente lo autoriza. La modificación incluye escritura, cambio, borrado, creación y modificación de los datos. El software posee las condiciones de seguridad, encriptación y manejo de base de datos y archivos diseñada para garantizar la confiabilidad de la información, además tiene el procedimiento para las copias de seguridad, y para los requerimientos establecidos según la prestación del servicio.

Se regirán por los siguientes principios y actividades:

- ✓ **Aspectos que influyen directamente con la seguridad de la información vital para el negocio:** optimización de la actualización de datos, comprobación de la integridad de la base de datos, realización de un plan de copia de seguridad de la base de datos, realización de un plan de copia de

seguridad del registro de transacciones y descripción de los informes para generar

- ✓ **Almacenamiento:** almacenar un nivel mínimo de información de respaldo, junto a los registros exactos y completos de las copias de seguridad y a procedimientos documentados de recuperación, a una distancia suficiente para evitar todo daño por desastres en el local principal. La información de respaldo debe almacenar por un tiempo mínimo.

- ✓ **Tiempos de conservación de la información:** Se debe dar a la información de respaldo un nivel adecuado de protección física y del entorno, un nivel consistente con las normas aplicados a los soportes en el local, para cubrir el lugar de respaldo.

- ✓ Es necesario hacer también una copia de seguridad manualmente y guardarla en un medio óptico y conservarlo fuera de la organización en un lugar seguro y confiable guardando su confidencialidad, para asegurar que esta información se pueda recuperar tras un desastre o un fallo del sistema y de los soportes que se tienen dentro del servidor. El medio óptico debe estar identificado con los siguientes datos, nombre de quien realizo la copia, nombre de la base de datos a la que se le creo la copia y fecha a la cual se restaurara la base de datos con dicha copia.

- ✓ Las copias de seguridad se deben almacenar en condiciones ambientales que favorezcan la conservación de estas y no permitan su deterioro.

- ✓ **comprobación de los soportes de respaldo:** Los soportes de respaldo se deben probar regularmente, donde sea factible, para asegurar que son fiables cuando sea preciso su uso en caso de emergencia, esto se debe realizar en un equipo informático ajeno a la organización con el fin de garantizar su correcto funcionamiento. Se deben comprobar y probar regularmente los procedimientos de recuperación, para asegurar que son eficaces y que pueden cumplirse en el tiempo establecimiento los procedimientos de recuperación.

Responsable del proceso: La mejor forma de controlar los procesos que se desarrollan en el sistema de información, aunque estos estén desarrollados en una parte importante por el propio sistema, es que exista un responsable de la supervisión de la seguridad de esta copias de seguridad, para ello se debe designar a una persona que incluya entre sus funciones la supervisión del proceso de copias de seguridad, el almacenamiento de los soportes empleados en un lugar designado a tal fin e incluso de la verificación de que las copias se han realizado correctamente.

Responsables: El cumplimiento de esta política involucra el liderazgo gerencial, así como la participación de todos los funcionarios, contratistas y demás partes interesadas.

Nota: La presente política será revisada, divulgada, publicada y de estricto cumplimiento para todo el personal.

Sanciones

- ✓ El incumplimiento de la política una vez comunicada y publicada genera llamados de atención con copia a la hoja de vida, los cuales dan lugar a una suspensión o finalización del contrato.

14.7. POLÍTICA DE TRANSFERENCIA DE LA INFORMACIÓN

Objetivo: Definir los lineamientos de cumplimiento entre el CDA y las partes externas que por requisitos legal deben tener acceso permanente a la transferencia de información por medio de equipos y aplicaciones.

Directriz

La Organización Corpotrans CDA S.A.S., Comprometida con la seguridad en la información y en el manejo de datos estable la política de transferencia, para tal efecto se establece los siguientes lineamientos:

- ✓ El hardware y software sólo puede utilizarse para los fines de la compañía o para aquellos expresamente autorizados por ésta. La utilización de software sin licencia queda terminantemente prohibida. El personal no puede utilizar los equipos, sistemas y dispositivos tecnológicos para otros fines que los autorizados por la empresa.

- ✓ El uso de software ajeno a los estándares oficiales no está permitido, salvo con autorización escrita de las áreas técnicas respectivas. El personal debe abstenerse de introducir en los ambientes tecnológicos de la empresa copias ilegales de software.

- ✓ Los empleados que operen recursos tecnológicos serán informados sobre las restricciones de uso y deberán actuar de modo de no violar los acuerdos de licencia ni ejecutar actos que comprometan la responsabilidad de la empresa. El manejo de los recursos tecnológicos debe efectuarse siguiendo

las normas y los procedimientos de operación definidos por las áreas responsables del tema.

- ✓ Se prohíbe la instalación de Aplicaciones o Software diferente al autorizado por la organización. Al instalar Aplicaciones o Software no autorizados la responsabilidad e implicaciones legales serán asumidas por el usuario que tiene en su custodia el equipo informático. Por seguridad e integridad del software instalado en cada equipo, por ningún motivo se debe compartir las unidades de disco (ejemplo SISTEMA (C:), ARCHIVOS (D:)) en su totalidad, solo las carpetas o directorios que realmente se requieren ser vistos en la red para evitar fallos en la transferencia de datos.

  Al momento de compartir una carpeta o directorio se debe tener en cuenta que cualquier usuario que navegue en la intranet de la organización podrá acceder a los archivos, leerlos, modificarlos, borrarlos, es necesario asignar los permisos adecuados al momento de compartir (Completo o Solo Lectura) con precaución y analizando las consecuencias de mostrar él o los archivos en la red, las instrucciones para realizar el procedimiento de compartir información se deberá ser solicitada a un funcionario del Área de Sistemas.

Es necesario verificar cualquier medio que contenga información, que vaya a ser leído en el equipo de cómputo a cargo, sea disquete o información de Internet. Por lo tanto, se debe verificar los archivos o carpetas desconocidos o de usuarios externos con la aplicación Antivirus instalada en cada uno de los equipos de cómputo mediante los siguientes pasos:

- ✓ Antes de realizar el procedimiento, es preferible cerrar los programas que esté ejecutando en el momento, hasta que finalice el proceso, con el fin de

evitar problemas, tales como bloqueo de la máquina durante la exploración en búsqueda de virus. La aplicación para consultar, recibir, enviar y guardar los correos electrónicos UNICAMENTE INSTITUCIONALES, se puede acceder a la plataforma de correos institucionales o Microsoft Office Outlook.

Es importante no abrir correos recibidos de remitentes desconocidos, ni los archivos adjuntos que puedan contener, se debe realizar un mantenimiento constante de las bandejas de entrada, enviados y papelera, eliminando los correos que ya no sea importante conservar, ya que estos archivos ocupan espacio en disco duro y ocasionan lentitud al momento de la carga de la aplicación.

El uso de Internet debe ser racional ya que hace parte de las herramientas tecnológicas suministradas por la organización para realizar nuestras funciones, por tal razón no se deben instalar aplicaciones o programas no autorizados, bajar música, videos, etc., los cuales ocasionan el daño del Sistema Operativo, lentitud para realizar los procesos propios del sistema, saturación del espacio en disco, infección de virus entre otros problemas.

Responsables: El cumplimiento de esta política involucra el liderazgo gerencial, así como la participación de todos los trabajadores, contratistas y demás partes interesadas.

Nota: La presente política será revisada, divulgada, publicada y de estricto cumplimiento para todo el personal.

Sanciones

- ✓ El incumplimiento de la política una vez comunicada y publicada genera llamados de atención con copia a la hoja de vida, los cuales dan lugar a una suspensión o finalización del contrato.

- ✓ Para los proveedores y contratistas que no sigan los lineamientos de la política se genera la cancelación del contrato y se activan las pólizas de incumplimiento.

14.8. POLÍTICA DE CONFIDENCIALIDAD

Objetivo: Establecer un marco de compromiso para la adecuada gestión de la información obtenida y generada durante el desarrollo de las actividades de la prestación de los servicios del CDA.

Directriz

Corpotrans CDA asume un compromiso de reserva y confidencialidad sobre la información de (bases de datos de clientes, procedimientos, estrategias, documentación legal y confidencial del negocio, métodos y datos del sistema de gestión documentado, información financiera y contratos) a la cual la ORGANIZACION le permita el acceso. El compromiso que a través del presente documento asume el INTERESADO incluye además la obligación que asiste a los socios, ejecutivos, funcionarios, consejeros, asesores, abogados, contratistas, proveedores, representantes o cualquier otra persona que actúe o intervenga en el proceso de información en nombre o en beneficio del INTERESADO, compromiso que tiene el alcance que le es propio a la naturaleza y propósitos propios de la

confidencialidad de la información, incluyendo las siguientes obligaciones específicas:

Se compromete a mantener la información en reserva o secreto, brindarle a la misma el carácter de estrictamente confidencial, y mantenerla debidamente protegida del acceso de terceros, con el fin de no permitir su conocimiento o manejo por parte de personas no autorizadas.

Se compromete a no utilizar la información de (bases de datos de clientes, procedimientos, estrategias, documentación legal y confidencial del negocio, métodos y datos del sistema de gestión documentado, información financiera y contratos), para fines diferentes al estudio y-o cumplimiento de su objeto contractual.

Se compromete a no permitir la copia o reproducción total o parcial de los documentos e información obtenidos en (bases de datos de clientes, procedimientos, estrategias, documentación legal y confidencial del negocio, métodos y datos del sistema de gestión documentado, información financiera y contratos) sin previo consentimiento expreso y escrito de la ORGANIZACION.

Se compromete a guardar estricta confidencialidad, discreción y cuidado respecto de los documentos e información que le sean entregados o a los que tenga acceso a (bases de datos de clientes, procedimientos, estrategias, documentación legal y confidencial del negocio, métodos y datos del sistema de gestión documentado, información financiera y contratos).

Cumplir y acatar las exigencias formuladas por la ORGANIZACION cuando se evidencie que la información o los documentos confidenciales han sido suministrados a terceros no autorizados, sin perjuicio de la responsabilidad que el uso indebido le genere a la ORGANIZACION o a terceros o involucrados directos o

subsecuentes en la información mencionada, en virtud del presente compromiso y/o de las normas legales que eventualmente puedan ser violadas.

Responsables: El cumplimiento de esta política involucra el liderazgo gerencial, así como la participación de todos los trabajadores, contratistas y demás partes interesadas.

Nota: La presente política será revisada, divulgada, publicada y de estricto cumplimiento para todo el personal.

Sanciones

- ✓ El incumplimiento de la política una vez comunicada y publicada genera llamados de atención con copia a la hoja de vida, los cuales dan lugar a una suspensión o finalización del contrato.

- ✓ Para los proveedores y contratistas que no sigan los lineamientos de la política se genera la cancelación del contrato y se activan las pólizas de incumplimiento.

15. PLAN DE CONTINUIDAD DEL NEGOCIO

Propósito

En el Centro De Diagnóstico Automotor se establece el plan de continuidad del negocio aplicando la norma internacional ISO 22301, con el propósito de proteger a los activos de la organización de un imprevisto de seguridad que puedan afectar e impactar sus servicios. Por esta razón es fundamental proteger el principal proceso de revisión técnico - mecánica a partir de acciones que permiten al CDA restablecerse tras un incidente de seguridad en un periodo de tiempo que no afecte la continuidad del negocio. De esta forma se gestionan respuestas planificadas, esto genera mayor confianza a los usuarios y se mantiene la imagen y reputación organizacional.

Objetivos

Definir los criterios en los que se establezcan reglas y procedimientos necesarios para la recuperación del servicio frente a un incidente de desastre que coloque en riesgo la prestación de los servicios.

- ✓ Contar con respaldo de información (bases de Datos) en caso desastres naturales, o causados con el fin de evitar pérdida de datos del CDA.

- ✓ Contar con el personal y los procedimientos internos para restablecer los sistemas de información que intervienen en el proceso.

Alcance

El alcance del PCN está orientado a cubrir los procesos de la revisión técnico - mecánica en caso de presentar algún tipo de interrupción, pérdida o crisis al funcionamiento de los servicios que brinda el CDA causados por factores como desastres naturales, incidentes ocasionados y ataques informáticos.

Responsables del PCN

Desde la alta dirección se definen roles y responsabilidades con el recurso humano activo en la organización, por lo tanto, es asignado a los ingenieros que cubren el proceso de revisión técnico - mecánica.

- ✓ Coordinador de calidad
- ✓ Director técnico
- ✓ Director técnico suplente

Tabla 22. Líderes del plan de continuidad del negocio

líderes del PCN	
Rol	**Responsabilidades**
Coordinador de calidad	administrador: ✓ Establece el PCN y coordina los procesos para la adecuada implementación ✓ Verifica y monitorea, el cumplimiento, documentación de las proposiciones del PCN
Director técnico	diseña y planifica estrategias para el restablecimiento de los servicios como: ✓ El estado de la red y sistemas informáticos software SART.

Continúa…

líderes del PCN	
Rol	**Responsabilidades**
	✓ Restablecimiento de comunicaciones - internet ✓ Comunicación en línea con las plataformas Runt, CI2, Supergiros.
Director técnico suplente	Diseña y planifica estrategias para el restablecimiento de los servicios ante incidentes o desastres naturales como: ✓ Huelga Laboral ✓ Inundación ✓ Daño grave en el fluido eléctrico

Elaboración: propia.

15.1. POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Objetivo: Establecer los lineamientos y procedimientos de gestión frente a la recuperación de las instalaciones y procesamiento de información como equipos, aplicaciones y recintos expuestos a incidentes intencionados o de origen que coloquen en riesgo la prestación de los servicios.

Directriz

La política de continuidad del negocio propone fortalecer y actualizar los lineamientos relativos a la salvaguarda del recurso humano, documental y equipamiento informático necesario para asegurar la sostenibilidad del servicio, es por esto que se definen principios de vital importancia:

- ✓ La integridad del personal es prioridad en la toma de decisiones.
- ✓ El restablecimiento de servicio una vez se tomen y se ejecuten acciones correctivas sobre los posibles incidentes o ataques intencionados.

Se definen compromisos como:

- ✓ Velar por las buenas prácticas en la prestación del servicio y una buena imagen ante los usuarios.
- ✓ El plan de continuidad proteja las áreas indispensables y servicios críticos para la prestación del servicio.
- ✓ Verificar y validar el cumplimiento del PCN que propicie la mejora continua.
- ✓ Contar con recursos informáticos disponibles en caso de presentar una falla y que los usuarios no resulten afectados por la interrupción de tiempo en el servicio.
- ✓ Cumplir con las políticas internas del CDA con el fin de fomentar el desarrollo adecuado de los planes de contingencia propuestos.

Responsables: El cumplimiento de esta política involucra el liderazgo gerencial, así como la participación de todos los funcionarios, contratistas y demás partes interesadas.

Nota: La presente política será revisada, divulgada, publicada y de estricto cumplimiento para todo el personal.

Sanciones

- ✓ El incumplimiento de la política una vez comunicada y publicada genera llamados de atención con copia a la hoja de vida, los cuales dan lugar a una suspensión o finalización del contrato.

- ✓ Para los proveedores y contratistas que no sigan los lineamientos de la política se genera la cancelación del contrato y se activan las pólizas de incumplimiento.

Tabla 23. Acciones y recursos del plan de continuidad del negocio

Acciones y recursos del plan de continuidad del negocio			
Ítem	**Falla**	**Actividad**	**Responsable**
1	ausencia de personal	✓ Facturación y Caja: mercadeo. ✓ Inspector: Inspector -Jefe de Pista. ✓ Director técnico: director técnico suplente y/o Coordinador de calidad. ✓ Técnico de sistemas: persona delegada por el Administrador.	Director Ejecutivo
2	Falla de equipos informáticos. (software y hardware)	✓ Se ha implementado un programa de mantenimiento preventivo y correctivo para mantener en óptimo estado los equipos. ✓ En caso de que ocurran fallas en los equipos se debe llamar de inmediato al proveedor de sistemas para que dé solución a las fallas presentadas. ✓ Si el proveedor de Sistemas no puede presentarse en el CDA deberá prestar asistencia telefónica o remota. ✓ En caso de que el proveedor de sistemas no pueda presentarse ni asistir telefónicamente se procederá a llamar un segundo proveedor de sistemas bajo la autorización del director ejecutivo.	Director técnico Proveedor

Continúa…

Acciones y recursos del plan de continuidad del negocio			
Ítem	**Falla**	**Actividad**	**Responsable**
2	Falla de equipos informáticos. (software y hardware)	✓ En el caso que la falla requiera un cambio menor (daño de Mouse, teclado etc.) el Director Técnico procederá a realizar este cambio con los elementos disponibles del inventario de equipos. Se debe proceder a realizar el registro del daño de equipo no conforme.	Director técnico Proveedor
3	Falla Fluido Eléctrico	✓ El CDA cuenta con UPS para el respaldo de energía en los equipos informáticos de las oficinas y de las líneas de inspección que permiten el tiempo necesario para guardar la información. ✓ Se debe instalar y poner el funcionamiento la planta eléctrica para normalizar el servicio.	Director técnico Director Ejecutivo
4	Daño en el Software de la línea	Se llama de inmediato al proveedor de software SART la línea de asistencia telefónica o remota al Director Técnico	Director técnico Director técnico suplente
5	Fallas de comunicación	El Director Técnico reporta y solicita atención inmediata a las líneas de asistencia de cada una de las plataformas Runt, CI2, Supergiros.	Director técnico Director técnico suplente
6	Caída de servicio de Internet	Reportar al proveedor de internet y cambiar el canal de comunicación al Router del proveedor de contingencia.	Director técnico Director técnico suplente

Continúa…

Acciones y recursos del plan de continuidad del negocio			
Ítem	**Falla**	**Actividad**	**Responsable**
7	Pérdida de datos esenciales del CDA	Se debe recuperar la información realizada en medios ópticos que se guardan en la caja de seguridad y/o los que se encuentran en un lugar seguro fuera del CDA y guiarse por el instructivo copias de soporte y restauración establecido por el proveedor de software.	director técnico proveedor de software SART
8	Vandalismo (robo de certificados y/o equipos)	✓ En caso de robo mantener la situación controlada de peligro o de pánico. ✓ Se informa a la Aseguradora que suministró la póliza. ✓ Se informa a las autoridades competentes. ✓ En el caso de robo de los certificados se informa al Ministerio de Transporte.	Director técnico Director Ejecutivo
9	Inundaciones	✓ Como método preventivo el CDA realiza limpieza a los drenajes de agua ✓ Se cuenta con una caja contenedora de aguas lluvias con un cheque que no permite que las aguas rebocen hacia las líneas de inspección. ✓ Se informa a la Aseguradora que suministro la póliza. ✓ En caso de inundación todos los equipos se deben apagar de inmediato. ✓ En caso de inundación se bajan los breakeres de la caja del control de mando.	Todo el personal

Continúa…

Acciones y recursos del plan de continuidad del negocio			
Ítem	**Falla**	**Actividad**	**Responsable**
10	Incendio	Inicialmente se debe llamar a bomberos como **acciones preventivas para evitar el incendio** ✓ contar con extintores ABC multipropósito ubicados estratégicamente y en cumplimiento con el sistema de seguridad y salud en el trabajo. ✓ Tener siempre en lugares visibles los números de emergencias, bomberos, organismos de socorro, entidades legales. ✓ Los extintores deben recibir mantenimiento periódico en el que garantice el tiempo de vigencia y presión adecuada. ✓ Las reparaciones de las instalaciones eléctricas se deben realizar por personal competente. ✓ No generar una sobre carga con equipo de mayor voltaje al permitido en la certificación. ✓ No usar elementos que propicien los incendios como velas, pinturas, y materiales inflamables en el inventario de herramientas. **acciones a tomar durante el incendio** ✓ Hacer uso de las líneas de emergencia bomberos y organismos de socorro.	

Continúa…

Acciones y recursos del plan de continuidad del negocio			
Ítem	**Falla**	**Actividad**	**Responsable**
		✓ De acuerdo a las brigadas conformadas por el sistema de gestión de seguridad y salud en trabajo, acudir a los puntos de encuentro, seguir la señalización de evacuación. ✓ Mantener el control propio, de los compañeros de trabajo y usuarios del CDA. **Recomendaciones** ✓ Activar alarma de incendio y poner en práctica lo aprendido en las brigadas contraincendios. ✓ Los extintores solo pueden ser manipulados por personas experto. ✓ Antes de propagarse el incendio y generar las alertas de socorro. ✓ Interrumpir el fluido eléctrico en los equipos en cada una de las áreas del CDA. ✓ Hacer uso de las pólizas con los que cuenta el CDA como obligación contractual para el funcionamiento del establecimiento.	
Elaboración: propia.			

Programa de inducción, reinducción, formación, capacitación, conocimiento técnico del SGSI

El programa de formación y toma de conciencia para la protección y aseguramiento de la información confidencial que se obtiene y se genera a partir de los procesos de revisión técnico - mecánica están determinados por el ciclo de planificar, hacer,

verificar, y actuar, con el propósito de mantener la mejora continua desde el plan de continuidad del negocio y los lineamientos de cumplimiento propuestos con la política de formación permiten la consistencia del objetivo del control (toma de conciencia, educación y formación de la seguridad de información) propuesto desde el sistema de gestión de seguridad de información NTC-ISO/IEC 27001 de 2013.

- ✓ **Planificar:** se establecen las actividades formación anualmente, las cuales están sujetas a modificación y/o actualización de acuerdos a los cambios que se presente durante la gestión y desarrollo de los procesos de la organización.

- ✓ **Hacer:** se establecen los responsables y los recursos por áreas para la formación a partir de técnicas como conferencias y estudio autónomo.

- ✓ **Verificar:** desde el monitoreo y verificación de los controles propuestos se toman acciones de mejora o se continua con lo establecido.

- ✓ **Actuar:** se toman acciones de mejora planificadas o inmediatas de acuerdo a la toma de decisiones que la alta dirección realice a partir de los registros de monitoreo.

Tabla 24. Programa de formación del SGSI

	PROGRAMA DE INDUCCIÓN, REINDUCCIÓN, FORMACIÓN, CAPACITACIÓN, CONOCIMIENTO TÉCNICO DEL SGSI	CODIGO:
		VERSION:
		Fecha:
OBJETIVO	Garantizar que todo el personal, contratistas y proveedores de Corpotrans CDA. Tenga la formación y el entrenamiento técnico, del sistema de gestión de seguridad informática y de información (SGSI), en cuanto a los requisitos de la normatividad legal y reglamentaria sobre la prestación del servicio.	
ALCANCE	el alcance está alineado con los propósitos de la política de formación, permitiendo realizar capacitaciones o inducciones para todo el personal que intervenga en los procesos de revisión técnico - mecánica y así fortalecer los canales comunicativos para hacer una buena apropiación de los requisitos internos de la organización, sus políticas, objetivos y procedimientos, cubre a proveedores, contratistas y demás partes interesadas.	
JUSTIFICACIÓN	El personal debe tener la formación y competencias requeridas y específicas para cada uno de los cargos, en cuanto a la implementación del Sistema de gestión de seguridad informática e información (SGSI).	

	ACTIVIDAD	2018																						FRECUENCIA	RESPONSABLE	RECURSOS	AREA	REQUERIMIENTO	OBSERVACIONES
		ENE		FEB		MAR		ABR		MAY		JUN		JUL		AGO		SEP		OCT		NOV		DIC							
		P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E						
PLANEAR																															
HACER																															
VERIFICAR																															
ACTUAR																															

Elaboración: propia.

16. PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁICA CORPOTRANS CDA

El establecimiento y planificación del sistema de gestión informática esta dado a partir de tres fases en las que se determina el cumplimiento de los objetivos propuestos y que su vez se encuentran alineados con los objetivos misionales de la organización y la perspectiva en general frente al aseguramiento de los activos de información que son indispensables para la funcionalidad del negocio, permitiendo manejar en materia de seguridad aspectos que no se encuentran determinados y aquellos que su cumplimiento es parcial. En consecuencia, se lleva acabo el análisis y valoración de los riesgos como método de identificación de estado actual en cuanto a los posibles incidentes derivados de la actividad, es por esto que se han propuesto controles que se fundamentan bajo medidas preventivas en función de mitigar la materialización de los riesgos.

Los controles anteriormente identificados están enfocados al cumplimiento y adecuada gestión del manejo de los activos por medio de políticas, procesos y procedimientos que requieren de habilidades y destrezas que se toman a partir de plan de formación y capacitación a todo el personal de la organización. Las fases están fundamentas con requisitos que permiten la factible puesta en marcha del SGSI.

Los requerimientos de cada una de las fases esta dado, bajo los criterios de cumplimiento para asegurar la seguridad de la información obtenida y generada del servicio como los requisitos específicos de las normas técnicas colombianas vigentes NTC 5385 del 2011, por lo cual los criterios que hacen referencia en cada una de las fases son:

Fase 1: Conocer la estructura organizacional para determinar los activos informáticos desde la aplicación de la metodología Magerit

De acuerdo a la puesta en funcionamiento del SGSI en Corpotrans CDA enfocado al proceso de revisión técnico - mecánica, en el cual intervienen activos de información que requieren de seguridad y controles para su adecuada gestión y funcionalidad, se analizan los controles propuestos desde la norma NTC ISO/IEC 27001-27002 de 2013, como un conjunto de salvaguardas que proponen medidas preventivas a las instalaciones de procesamiento de información como equipos, software, aplicaciones e instalaciones que el personal necesita para la realización de sus actividades.

Con el análisis de los controles propuestos desde el plan de tratamiento de riesgos, se identifican medidas de protección de la información y que a su vez estas sean las necesarias y no se encuentre redundancia, es por esto que las políticas, procesos, procedimientos e instructivos deben ser claros y que los objetivos del control se encuentre de manera implícita y por medio del cual se expresan las decisiones de cumplimiento desde la alta dirección ya sea por requerimiento u obligación contractual y legal o por requisitos de la prestación del servicio y del resultado del análisis de riesgo.

Tabla 25. Análisis de controles en la organización Corpotrans CDA

Análisis de controles en la organización Corpotrans CDA						
Tipo de control	**Objetivo**	**Aplica**	**Responsable**	**Razón para la selección / Justificación**	**Justificación de inclusión**	**Controles Implementados**
A5.1.1-Políticas para la seguridad de la información	Brindar orientación y dar soporte, por parte de la dirección para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	SI	Director Ejecutivo Coordinador de Calidad Director Técnico Personal Operativo Partes externas	Definir los criterios para las políticas de seguridad de información, aprobadas por la alta dirección, esta debe ser aprobada y comunicada a todos los empleados y partes externas como contratistas, proveedores y socios para su apropiado cumplimiento.	Corpotrans CDA, cuenta con un sistema de gestión con directrices establecidas por el director ejecutivo que funcionan como base del sistema de gestión.	Sin implementar
A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	SI	Dirección Técnica Director ejecutivo	El personal que interviene en el proceso de revisión técnico - mecánica como empleados, contratistas, proveedores, deben contar con la formación apropiada y estar en permanente actualización de conocimientos frente a las políticas, procedimientos propuestos desde la alta dirección.	Para la organización es necesario realiza la sensibilización y divulgación que el fin de proponer la adecuada implementación del SGSI.	Sin implementar
A8.3.2-Disposición de los medios	Evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada.	SI	Coordinador de calidad	De acuerdo al manejo de equipos informáticos y los constantes cambios deben establecer un procedimiento para disponer de forma segura cuando sean dados de baja por daño u actualización de tecnología.	Los procedimientos se encuentran parcialmente implementados de modo que deben ser actualizados.	Implementado
A9.1.1-Política de control de acceso	Limitar el acceso a información y a instalaciones de procesamiento de información.	SI	Coordinador de Calidad Director ejecutivo	Se debe establecer una política de control de acceso de acuerdo a los requisitos de la seguridad de información, responsabilidades y funciones de cada uno de los cargos.	se debe disponer de una política que ayude al adecuado acceso a la información por parte de todo el personal en cada uno de los procesos	Sin implementar

Continúa…

Análisis de controles en la organización Corpotrans CDA						
Tipo de control	**Objetivo**	**Aplica**	**Responsable**	**Razón para la selección / Justificación**	**Justificación de inclusión**	**Controles Implementados**
A9.1.2-Acceso a redes y a servicios en red	Limitar el acceso a información y a instalaciones de procesamiento de información.	SI	Coordinador de Calidad Director Técnica Director ejecutivo	Se debe establecer una política de acceso a los usuarios en la red y servicios solamente para los que se les ha asignado.	Como parte requisito del negocio se requiere de la funcionalidad y manejo adecuado de operaciones tecnológicas que hacen parte del proceso.	Sin implementar
A9.2.3-Gestión de derechos de acceso privilegiado	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	SI	Dirección Técnica	Se debe establecer métodos para restringir el acceso y que este solo sea posible con privilegios especiales y controlados.	De adecuado control de creación, modificación y eliminación de usuarios de acuerdo a las políticas establecidas.	Sin implementar
A9.2.5-Revisión de los derechos de acceso de usuarios	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	SI	Dirección Técnica	Se debe establecer un responsable sobre el manejo de los activos como medida de prevención para el monitoreo a intervalos planificados los permisos de acceso de los usuarios.	De acuerdo al sistema de gestión se tiene implementado la ejecución de auditoria internas sin embargo estas esta enfocadas al cumplimiento del proceso, se deben definir directrices para los derechos de acceso.	Implementado
A9.2.6-Retiro o ajuste de los derechos de acceso	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	SI	Coordinador de Calidad Dirección Técnica Director Ejecutivo	Se deben establecer procedimientos y formatos de registro y control para el retiro y/o modificación de los derechos acceso alineados con el contrato laboral.	Se encuentra parcialmente implementado de modo que existe el formato para la autorización del cargo, pero este no tiene en cuenta el manejo con los activos de información.	Implementado

Continúa…

Análisis de controles en la organización Corpotrans CDA						
Tipo de control	**Objetivo**	**Aplica**	**Responsable**	**Razón para la selección / Justificación**	**Justificación de inclusión**	**Controles Implementados**
A9.4.4-Uso de programas utilitarios privilegiados	Evitar el acceso no autorizado a sistemas y aplicaciones.	SI	Dirección Técnica Director ejecutivo	Se debe restringir el uso y manejo de programas utilitarios con el fin de garantizar la funcionalidad del software de aplicación y los demás sistemas propuestos. Las herramientas administrativas permiten conceder o denegar permisos lo que ayuda a mantener el sistema de información controlado.	Se deben implementar medidas que garanticen la seguridad de información, la funcionalidad y la instalación de programas utilitarios por parte del personal.	Sin implementar
A11.2.2-Servicios de suministro	Prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.	SI	Dirección Técnica Director Ejecutivo	Los equipos se deben estar protegidos contra fallas de energía e interrupciones causadas por el proveedor de servicios.	como parte requisito del negocio se requiere de la funcionalidad de las operaciones	Implementado
A11.2.4-Mantenimiento de los equipos.	Prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.	SI	Dirección Técnica Director ejecutivo	Se debe garantizar la funcionalidad de los equipos, el software y las aplicaciones para asegurar la disponibilidad e integridad.	Se tiene implementado el cronograma de mantenimiento y que siempre se encuentran en condiciones óptimas para poder cumplir con las actividades del negocio, sin embargo, este no cumple con las fechas propuestas.	Implementado
A12.2.1-Controles contra códigos maliciosos	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	SI	Coordinador de calidad Dirección técnica Director ejecutivo	Se debe establecer una política para el control y detección, prevención y recuperación de información, esta debe estar alineada con el plan de formación para todo el personal.	Como parte requisito del negocio se requiere de la funcionalidad y manejo adecuado de operaciones tecnológicas que hacen parte del proceso.	Sin implementar

Continúa…

Análisis de controles en la organización Corpotrans CDA						
Tipo de control	**Objetivo**	**Aplica**	**Responsable**	**Razón para la selección / Justificación**	**Justificación de inclusión**	**Controles Implementados**
A12.3.1-Respaldo de la información	Proteger contra la perdía de datos.	SI	Coordinador de Calidad Director ejecutivo	Se debe establecer una política para copias de respaldo de información, software SART e imágenes de los sistemas operativos y verificar su funcionamiento a intervalos planificados.	Como parte requisito del negocio se requiere de la funcionalidad y manejo adecuado de operaciones tecnológicas que hacen parte del proceso.	Sin implementar
A12.4.3-Registros del administrador y del operador	Registrar eventos y generar evidencia.	SI	Dirección Técnica Director ejecutivo	Se deben separar las responsabilidades del administrados del sistema con el responsable del proceso con el fin de mitigar irregularidades y establecer monitoreo permanente.	Estas garantizan la trazabilidad de las operaciones realizadas con los activos de información.	Sin implementar
A12.6.1-Gestión de las vulnerabilidades técnicas	Gestión de las vulnerabilidades técnicas.	SI	Dirección Técnica Director Ejecutivo	Se debe llevar registro de las vulnerabilidades técnicas de los sistemas de información, en donde se permita la evaluación y establecimiento de controles a partir de acciones preventivas y correctivas.	Esto segura el adecuado desempeño tanto del recurso humano como de los activos informáticos y de información destinados para la prestación del servicio.	Sin implementar
A13.1.2-Seguridad de los servicios de red	Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte.	SI	Dirección Técnica Director Ejecutivo	Se deben establecer mecanismos de seguridad, niveles y requisitos para los servicios en red tanto internamente como externamente.	Como parte requisito del negocio se requiere de la funcionalidad y manejo adecuado de operaciones tecnológicas que hacen parte del proceso.	Sin implementar
A13.2.1-Políticas y procedimientos de transferencia de acción	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	SI	Coordinador de calidad Dirección técnica Director ejecutivo	Se debe establecer una política para la transferencia formal de información, por medio de dispositivos que ayuden a proteger los canales de comunicación.	En las operaciones del proceso de revisión técnico - mecánica la transferencia de información es una de las actividades indispensables para la prestación del servicio.	Sin implementar

Continúa…

Análisis de controles en la organización Corpotrans CDA						
Tipo de control	**Objetivo**	**Aplica**	**Responsable**	**Razón para la selección / Justificación**	**Justificación de inclusión**	**Controles Implementados**
A13.2.4-Acuerdos de confidencialidad o de no divulgación	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	SI	Coordinador de Calidad Director ejecutivo	Se debe establecer una política confidencialidad en la que se permita la verificación periódica de los acuerdos de confidencialidad y la no divulgación de la información obtenida y generada de la realización de las actividades.	Todo el personal tanto empleados como proveedores, contratistas, asociados deben cumplir con las determinaciones de dicha política en cumplimiento con las condiciones contractuales con las responsabilidades sobre el uso de la información.	Sin implementar

Fuente. (Internacional, 2013, pág. 19)

La determinación de los 18 controles está orientada para la puesta en marcha con el personal de la organización y en acompañamiento de un asesor externo o empresa certificada experta en sistemas de gestión de seguridad informática y de información que promuevan la apropiada aplicación de todas las etapas, el desarrollo y cambios de los sistemas que actualicen o mejoren la seguridad.

Fase 2: plantear la matriz de los riesgos identificando las vulnerabilidades y amenazas presentadas a todos los activos preservando la confidencialidad, integridad y disponibilidad.

Con el empleo de la metodología Magerit para el análisis de los sistemas de la organización, se contribuye en el reconocimiento de los riesgos que pueden presentarse para los activos informáticos y de información que hacen parte del proceso, de igual forma estos deben estar alineados con los requisitos legales y los avances tecnológicos que se deben cumplir para la correcta funcionalidad del proceso de revisión técnico - mecánica, la formación para el personal actual que asegure un grado de conciencia y acciones a tomar para dar respuesta ante los incidentes de seguridad y como mitigarlos.

El modelo de Magerit permitió:

- ✓ Planificar la identificación de los activos desde un marco global.
- ✓ Determinar en el análisis de los riesgos que tan protegidos se encuentran y el nivel del riesgo al que se enfrentan los activos.
- ✓ Con la gestión del riesgo se seleccionaron salvaguardas que permiten conocer, prevenir, reducir y controlar los riesgos hallados.

Estas herramientas ayudan en la compresión de exposición de amenazas que se enfrentan los activos y los daños significativos para las actividades de Corpotrans CDA por la falta de salvaguardas de seguridad que promuevan la gestión de buenas

prácticas, en consecuencia, con las determinaciones de la matriz se riesgos se define:

- ✓ El establecimiento de controles de la norma NTC ISO/IEC 27001 - 27002 del 2013
- ✓ El alcance que se espera con la implementación del SGSI
- ✓ La aplicación del plan de tratamiento de riesgos para definir los controles aplicar de acuerdo a la valoración del riesgo residual.

Los 18 controles aplicados le permiten a la compañía evaluar la complejidad y evaluar el progreso de las actividades frente al cumplimiento de los requisitos actuales de la NTC 5385 de 2011, en cuanto a:

Tabla 26. Sistema de Información Corpotrans CDA

Corpotrans CDA: sistema de información de la revisión técnico - mecánica y de emisiones contaminantes	
requisitos de NTC 5385 de 2011	**Evidencias**
seguridad del software de aplicación SART	✓ Se deben definir parámetros de control para garantizar la funcionalidad del software, evitar la manipulación, evitar la instalación de programas utilitarios que generen incidentes de funcionamiento, políticas que garanticen los controles de acceso solo por el personal autorizado y la transferencia de los registros solo a los entes legales y que cumplimiento contractual se debe gestionar.

Continúa…

Corpotrans CDA: sistema de información de la revisión técnico - mecánica y de emisiones contaminantes	
requisitos de NTC 5385 de 2011	**Evidencias**
seguridad de la información	✓ No se evidencia que se encuentren claramente definidos los parámetros para brindar seguridad a la información confidencial, se evidencia obsolescencia sobre el manejo de los activos informáticos.
uso de contraseñas	✓ Desde el sistema de gestión implementado se lleva formato de registro del cambio de contraseñas, sin embargo, se debe implementar en la formación la importancia del cambio de contraseñas, la protección de no divulgación, las pautas para cread las contraseñas y que estas sean intransferibles.
Administración de la base de datos	✓ Los responsables del proceso no tienen claramente definidos las buenas prácticas para la administración de la base de datos a partir de políticas, procesos, procedimientos y herramientas que gestionen el seguimiento del sistema.
información de respaldo	✓ A nivel de procesos se tiene implementado un procedimiento para llevar acabo las copias de respaldo sin embargo el responsable del proceso no lo realiza con la frecuencia establecida y se tiene claro la importancia de verificación en intervalos planificados procedimientos de restauración.

Continúa…

Corpotrans CDA: sistema de información de la revisión técnico - mecánica y de emisiones contaminantes	
requisitos de NTC 5385 de 2011	**Evidencias**
información de respaldo	✓ No se cuenta con un equipo informático independiente que facilite los procedimientos de restauración y poder conservar la confiabilidad e integridad de la información en el equipo informático (Servidor) central.
bitácora de operación del sistema	✓ No se evidencia registro de las actividades del administrador y operario que permite la validación y verificación de los sistemas de información.
bitácora de fallas de los equipos de computo	✓ El programa de mantenimiento cuenta con formatos que le permiten llevar el control y asegurar la disponibilidad de los activos informáticos sin embargo este no se lleva adecuadamente.
mantenimiento de equipos de computo	✓ Se tiene implementado un cronograma de mantenimiento, sin embargo, este no se realiza en las fechas propuestas. ✓ No se evidencia los registros de todos los mantenimientos ejecutados.
controles contra software malicioso	✓ EL software antivirus, no se encuentra licenciado y de acuerdo al sistema operativo no es compatible con todos manejan dos antivirus. ✓ No se evidencia registros de actualizaciones periódicas que permita el correcto análisis y detección de archivos entrantes y salientes de la red interna y externa.

Continúa…

Corpotrans CDA: sistema de información de la revisión técnico - mecánica y de emisiones contaminantes	
requisitos de NTC 5385 de 2011	**Evidencias**
controles contra software malicioso	✓ No se evidencia control sobre la instalación de software no autorizado.

Elaboración: propia.

De acuerdo al cumplimiento de los requisitos de la NTC 5385 de 20011, se encaminan los controles al aseguramiento de los procesos de tal manera que se garantice la continuidad de la ejecución de los mismos, es decir estos no afectan las labores operativas por parte del personal que realiza la revisión técnica mecánica.

- ✓ Las salvaguardas técnicas enfocadas a las aplicaciones, comunicaciones y equipos.
- ✓ Las salvaguardas físicas enfocadas a las instalaciones de trabajo del recurso humano y equipos.
- ✓ Las medidas de prevención y de gestión de incidentes.
- ✓ Políticas están orientadas a las decisiones de cumplimiento de todas las partes tanto interno como externo.

Esto indica que el personal que forma parte de los procesos operativos debe recibir formación y capacitación sobre la implementación del sistema de gestión de seguridad informática como la toma de conciencia y el manejo apropiado del recurso que dispone para la ejecución de las actividades.

Implementación de controles

Es un aspecto fundamental del diseño y establecimiento del sistema de gestión, en el cual se busca asegurar el mantenimiento al sistema y la mejora continua de los procesos con la intervención de la alta dirección, los directores técnicos y el coordinador de calidad, quienes participan en la planificación y ejecución de la puesta en marcha en unión con entes certificadores o asesores expertos quienes por medio de la evaluación objetiva y auditorías internas ayudan a la evolución de la organización.

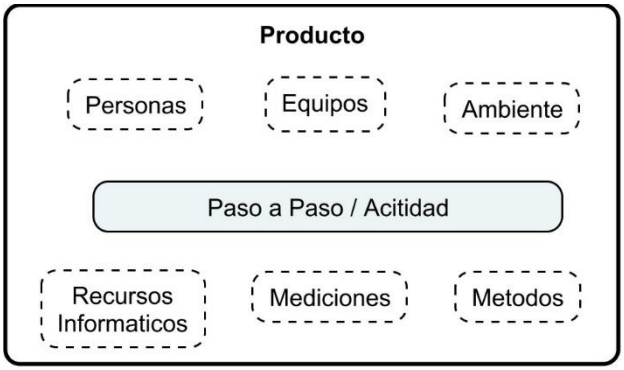
La auditoría se compone de dos fases:

- ✓ **La fase 1:** se inicia el proceso con la verificación de la documentación que se tienen implementados como soportes de registro para operar, monitorear y muestra de evidencias de mejoramiento documentado.

- ✓ **La fase 2:** se valida el cumplimiento de los procesos y la documentación de lo planificado y realizado dentro del conjunto de actividades conformadas por recursos como informáticos y personas.

Esto indica que la inclusión de los controles permite la transformación de los procesos, siendo estos más seguros en el momento que operen y en que intervienen factores como:

Figura 3. Proceso Corpotrans CDA



Elaboración: propia.

Cada proceso que forma parte del sistema de gestión de seguridad informática y de información en Corpotrans CDA, genera transformación dentro del alcance como un modelo que optimiza las actividades y las interacciones bajo un método de gestión conforme al enfoque de la norma NTC 27001 – 27002 de 2013, en el cual se mide la eficacia del desempeño y partir de ahí se generan acciones correctivas tratadas desde la aplicación de Magerit en el cual se redefinen los controles a partir de los riesgos encontrados.

Fase 3: Establecer mecanismos de sensibilización de la seguridad y protección a los activos software, redes, y personal que interviene directamente con los procesos y el manejo del software de aplicación para la revisión técnico - mecánica.

Desde los controles propuestos del plan de tratamiento de riesgos se propone un cronograma de formación y capacitación en el cual inicialmente estaría orientado a la toma de conciencia del cumplimiento de las determinaciones desde las políticas:

- ✓ Política de seguridad en la información
- ✓ Política de formación
- ✓ Política de control de acceso
- ✓ Política de acceso a redes y a servicios de red
- ✓ Política de uso de software no autorizado
- ✓ Política de transferencia
- ✓ Política de confidencialidad

El plan de formación debe abarcar las proposiciones del SGSI en el que deje registro de supervisión periódica del cumplimiento de las responsabilidades frente a las establecidas en el manual funciones así como evaluación de competencia laboral para el personal responsable de la ejecución y cumplimiento de los procesos en el que se identifique las capacidades necesarias que un nivel técnico alto frente a los aspectos técnicos y administrativos, en el que se identifique que el personal operativo este tomando formación eficaz para el manejo de los recursos informáticos.

El plan de formación hace parte del plan de continuidad del negocio como un programa para garantizar la seguridad de la información, el uso adecuado y asignación de responsabilidades para el personal.

El plan de continuidad del negocio

El plan de continuidad del negocio dentro del sistema de gestión de seguridad informática tiene como propósito establecer medidas contingencia a las acciones y recursos de todos los elementos dispuestos para el desarrollo de las actividades de

la revisión técnico - mecánica con la finalidad de garantizar la funcionalidad del servicio:

- ✓ Con la disponibilidad de todos los procesos tanto para empleados, clientes, proveedores, contratistas.
- ✓ Gestionar la continuidad de todas las actividades que se llevan a diario con el propósito de mantener el trabajo y facilitar la restauración.

En conformidad con el plan de continuidad y los requisitos de cumplimiento se propone la certificación como un aliado que le permitirá garantizar la seguridad de la información siendo esta confiable integra y disponible solo para la ejecución de las actividades de inspección y los resultados que de estos se genere par los entes legales. Es por esto que la certificación permite:

- ✓ Mejorar la gestión de seguridad en la información.
- ✓ la información que se dispone es confidencial, disponible e integra.
- ✓ La disminución y control sobre los posibles riesgos.
- ✓ Confiabilidad como imagen empresarial en el sector.
- ✓ Reducción de costos destinados para los incidentes causados por la seguridad de la información.
- ✓ A nivel de personal toma de conciencia por adoptar las medidas de seguridad en la información.
- ✓ Cumplimiento contractual por brindar seguridad a la información con el tratamiento de datos personales y el tiempo de retención.

Auditoría interna

La planificación de las auditorías internas debe estar alineadas con el periodo de certificación el cual está acompañado de auditoria de seguimiento semestrales o anuales, es por esto se debe mantener seguimiento periódico por parte del representante de la dirección y el asesor experto quien se encarga de demostrar que el sistema de gestión es conforme con los requisitos de la norma y las directrices implementadas por la organización. Las auditorias se planifican y se llevan a cabo teniendo en cuenta los siguientes factores:

- ✓ Criticidad
- ✓ La madurez o experiencia
- ✓ El desempeño previo
- ✓ Cambios en la organización
- ✓ Cambios en los procedimientos

El resultado de las mismas debe permitir:

- ✓ Inspeccionar los registros, procesos y procedimientos que se llevan en la práctica.
- ✓ Reunión con el personal que interviene en los procesos.
- ✓ El informe de auditorías preliminares.
- ✓ La ejecución en el tiempo establecido para las tareas derivadas de las acciones correctivas y preventivas en las que se debe incluir verificación de informes de resultados por la alta dirección.

Seguimiento y medición de los procesos

Los procesos son seguidos y medidos a través de los objetivos de los controles propuestos, los cuales son analizados en el comité conformado por el asesor experto y los responsables del proceso, allí se toman las acciones correctivas y preventivas que dan solución a la mejora continua del servicio.

- ✓ **Acciones correctivas:** son las medidas necesarias para suprimir las causas de las no conformidades, estas deben ser pertinentes a las consecuencias de los problemas encontrados de acuerdo a lo definido en los controles de la norma NTC ISO/IEC 27001-27002 de 2013.
- ✓ **Acciones preventivas:** son las medidas que ayudan a mitigar el riesgo de acciones correctivas potenciales.

Tabla 27. Formato programa auditoria

	Programa de Auditoria Interna de SGSI		**Código:**
			Versión:
			Fecha de vigencia:
Fecha:			
Objetivo:			
Alcance:			
Proceso Auditado:			
Recursos:			
Nombre del Auditor:		Criterios de Auditoría:	
Tipo De Auditoria	**Procesos / Actividades AUDITAR**	**Requisitos**	**Responsable**
Observaciones:			
Aprobado:			**Elaborado por:**
Elaboración: propia.			

17. IMPACTO Y RESULTADO

La adopción del SGSI en Corpotrans CDA, permitió aplicar las diferentes herramientas como la Metodología Magerit, el Plan de continuidad del negocio de ISO 22301, las cuales se direccionaron al cumplimiento de los requisitos de implementación y mantenimiento del sistema de gestión de seguridad información bajo la norma NTC ISO/IEC 27001- 27002 de 2013, con la determinación de controles que causan un impacto positivo en los resultados como:

- ✓ La necesidad de implementar directrices a través de políticas que promuevan el comportamiento, el desempeño y el manejo adecuado sobre los procedimientos y los recursos para el procesamiento de información.

- ✓ Se evidencia la necesidad de adquirir herramientas de hardware o de software que ayuden a la administración de la base de datos, el software y las aplicaciones de las cuales se genera información tanto entrante como saliente.

- ✓ La toma de conciencia por el manejo adecuado de las contraseñas, los parámetros que se deben seguir para la creación y cambio de las mismas en las frecuencias establecidas.

- ✓ La importancia de los respaldos de la información y como esta de ser verificada en cuestiones de funcionalidad y restablecimientos que no generen retrocesos en la prestación del servicio.

- ✓ La necesidad de actualizar y ejercer monitoreo sobre el programa de mantenimiento de equipos garantizando la disponibilidad de los mismos, así como el software, las aplicaciones y las instalaciones físicas en las que se encuentran ubicados.

- ✓ Toma de consciencia tanto para la ata dirección como para los directores técnicos responsables del proceso sobre la adquisición y uso de software con licencia, las actualizaciones periódicas dado a que estas permiten el análisis de todo el sistema.

- ✓ Toma de conciencia al personal con el propósito de evitar el manejo de programas utilitarios en los equipos informáticos de la organización, así como los incidentes que estos causan al software de aplicación y aplicaciones web que forman parte del proceso.

- ✓ Exponer a la alta dirección la necesidad de implementar el sistema de gestión y las garantías que trae consigo la certificación con un ente certificador en cuanto a la reducción de costos para incidentes y mayor posicionamiento en el sector por la confiabilidad de los procesos.

18. RECOMENDACIONES

Recomendaciones para Corpotrans CDA: De acuerdo con los resultados de la aplicación de la metodología Magerit, el plan de tratamiento de riesgos y el plan de continuidad del negocio se recomienda:

Des de la alta dirección restructurar la responsabilidad del director técnico principal yaqué actualmente se encuentra desempeñando funciones como la construcción de los procesos y procedimientos del área de sistemas y de inspección conforme a las actividades de revisión técnico - mecánica, lo que conlleva a una no conformidad en el cumplimiento de los programas establecidos. Viéndose afectado:

- ✓ El cumplimiento del cronograma de mantenimiento de equipos informáticos.
- ✓ La ejecución de las copias de respaldo a diario y en las fechas establecidas.
- ✓ La extracción de las copias de respaldo en un dispositivo externo el cual se encuentre fuera de las instalaciones.
- ✓ La verificación de funcionalidad y restauración de las copias de respaldo.
- ✓ El cumplimiento por parte del personal con el cambio de contraseñas.
- ✓ Velar por el cumplimiento de las fechas programadas para la formación de los funcionarios y que cumplan con las directrices de la organización.

Desde el área de sistemas implementar herramientas administrativas con el propósito de monitorear el tráfico entrante y saliente de información, el cual debe ser expuesto ante la dirección como una inversión de mejora, en donde se llevará la trazabilidad de la seguridad de la información y la identificación de vulnerabilidades a los que se encuentra expuesta:

- ✓ Controlar el acceso de sitios web por parte de funcionarios con propósitos personales.
- ✓ Establecer acuerdos de seguridad con el proveedor del software de aplicación con el propósito de evitar que programas utilitarios o la alteración de archivos afecten su funcionalidad.

La implementación del sistema de gestión de seguridad informática por parte de asesores calificados le permite a la organización desde la coordinación de calidad, establecer programas de formación de acuerdo a las responsabilidades del personal por área, el cual permite:

- ✓ Realizar auditorías internas planificadas
- ✓ Identificar un responsable por cada uno de los procesos, permitiendo el fácil cumplimiento.

19. CONCLUSIONES

La propuesta de implementación del sistema de gestión de seguridad informática y de información esta direccionada como un sistema aplicable a todo tipo de organización que promueva la confidencialidad, integridad y disponibilidad de sus servicios. Es por esto que Corpotrans CDA cumple con los lineamientos de modo que tiene como visión de ser reconocido a nivel regional y nacional en el sector transporte como el centro de diagnóstico automotor que brinda seguridad a sus clientes con el manejo de su vehículo automotor y la información confidencial que es puesta a su disposición. Es por esto que en cada uno de los procesos son identificados el con propósito de establecer controles que ayuden a mitigar la manipulación o alteración de la información por terceros viéndose de esta manera comprometida de la seguridad de la información.

- ✓ La identificación y estado actual tanto de hardware, como del software, aplicaciones web, la trasferencia de información en línea y el personal en todo el proceso de revisión técnico – mecánica, es de vital importancia para conocer cuáles son los requisitos de cumplimiento en la prestación de sus servicios y las necesidades de mejora que cada uno de los mismos requiere. Es por esto que se ve la necesidad de implementar el SGSI como mecanismo de análisis y valoración de posibles riesgos y amenazas desde la aplicación de la Metodología Magerit, la cual permite conocer a que se encuentra expuesta la información de sus clientes y por ende la calidad de su servicio. Estos deben estar alineados con lo establecido en las leyes, resoluciones y normas técnicas colombianas que regulan su proceso.

- ✓ La identificación de los riesgos, las vulnerabilidades y amenazas presentadas para cada uno de los activos, se generaron desde la aplicación de la metodología Magerit en donde se evidencia el nivel de riesgo a los que se encuentran expuestos y la probabilidad que pueden llegar a suceder, siendo estos como un incidente de nivel bajo, medio y alto en donde siempre se va a ver afectada la continuidad y prestación del servicio en cuanto a las demoras causadas durante el proceso. Desde este punto de vista se aplicaron contrales de la norma NTC ISO/EC 27001 -27002 de 2013 como mecanismos para mitigar cualquier tipo de nivel de incidente en el cual siempre se va a ver afectado el tiempo del servicio y la satisfacción del cliente.

- ✓ Con la implementación del SGSI se proponen controles para el manejo de los recursos de personal y de medios de procesamiento de información actuales en los que intervienen la formación y toma de conciencia apropiada frente a las políticas, procedimientos propuestos en la organización desde la alta dirección.

  La inclusión de nuevos procesos y la mejora de los existentes no afectan el principio de las actividades y aspectos que regulan el correcto funcionamiento del sistema en la organización, estos están determinados desde la toma de conciencia frente a la seguridad y protección de cada uno de los activos.

BIBLIOGRAFÍA

17020, N. T.-I.-I. (2012). *evaluacion de la conformidad. requisitos para el funcionamiento de los diferentes tipos de organismos que realizan la inspeccion.* Recuperado el 11 de 09 de 2018.

5385, N. T. (2011). Centros de diagnostico Automotor. Especificaciones del Servicio. En Icontec, *Centros de diagnostico Automotor. Especificaciones del Servicio* (pág. 9 item 4.16.2. seguridad de la informacion). Recuperado el 15 de 09 de 2018.

COMUNICACIÓN, I. I. (24 de 11 de 2018). Implantación de un SGSI en la empresa. Recuperado el 24 de 11 de 2018, de Implantación de un SGSI en la empresa: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ELECTRÓNICA, P. d. (2012). MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Vol. Libro II: Catálogo de Elementos). Madrid: Ministerio de Hacienda y Administraciones Públicas. Recuperado el 15 de 10 de 2018, de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W8eNEGgzbIU

GARAVITO, E. A. (2016). *Diseño de un sistema de gestion de seguridad informatica basado en la norma ISO/IEC 27001 - 27002 para el area administrativa y de historias clinicas del Hospital San Francisco de Gacheta.* Gacheta Cundinamarca. Recuperado el 30 de 09 de 2018.

ICONTEC - Instituto Colombiano de Normas Técnicas. (2012). CONTINUIDAD DEL NEGOCIO. SISTEMAS DE GESTIÓN DE CONTINUIDAD DE NEGOCIO. REQUISITOS. Bogotá D.C: Instituto colombiano de normas técnicas y certificación. Recuperado el 04 de 11 de 2018, de http://bibliotecavirtual.unad.edu.co:3101/pdfview/viewer.aspx?locale=es-419&Q=C5EC0CABB074B242D71EB7E1C99D45B796DF3D9C2A164539&Req=

INFORMACION, S. I. (12 de 10 de 2018). *ST2*. Obtenido de ST2: https://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

INTERNACIONAL, I. (2013). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos (Vol. Primera actualización). Bogotá D.C: Instituto Colombiano de Normas Técnicas y Certificación. Recuperado el 15 de 10 de 2018, de http://bibliotecavirtual.unad.edu.co:3101/pdfview/viewer.aspx?locale=es-419&Q=1775CD1AFBC53D942B1D63945F22285F96DF3D9C2A164539&Req=

INTERNACIONAL, I. (2013). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos (Vol. Primera actualización). Bogotá D.C: Instituto Colombiano de Normas Técnicas y Certificación. Recuperado el 15 de 10 de 2018, de http://bibliotecavirtual.unad.edu.co:3101/pdfview/viewer.aspx?locale=es-419&Q=1775CD1AFBC53D942B1D63945F22285F96DF3D9C2A164539&Req=

ISO: 27001, I. e. (04 de septiembre de 2014). ISACA Confianza y valor en sistemas informáticos. Recuperado el 25 de 11 de 2018, de ISACA Confianza y valor en sistemas informáticos:

http://m.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

LEWIS, D. A. (s.f.). Proceso de Implementación de los Sistemas de Gestión ISO 27001 E ISO 22301. Obtenido de Proceso de Implementación de los Sistemas de Gestión ISO 27001 E ISO 22301: https://www.isecauditors.com/sites/default/isecauditors.com/files//files/20171130_Proceso-Implementacion-SGSI-SGCN-dagonzalez.pdf

MORALES, G. G. (15 de mayo de 2017). Método para implementar un SGSI según el ISO/IEC 27001:2013. Recuperado el 25 de 11 de 2018, de Método para implementar un SGSI según el ISO/IEC 27001:2013: https://www.linkedin.com/pulse/m%C3%A9todo-para-implementar-un-sgsi-seg%C3%BAn-el-isoiec-g%C3%B3mez-morales

OLAVE, M. L. (20178). *Diseño de un lan estrategico de seguridad de informcion (PESI) para una compañia del sector asegurador.* Institucion Universitaria POLITECNICO GRANCOLOMBIANO .

PERALTA, J. M. (s.f.). Administración Electrónica Gestión de Riesgos Magerit. Recuperado el 22 de 11 de 2018, de Administración Electrónica Gestión de Riesgos Magerit: https://www.tithink.com/publicacion/MAGERIT.pdf

PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. (2012). MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado el 15 de 10 de 2018, de Portal de Administración Electrónica:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W9qE6pMzbIV

POVEDA, J. M. (20 de 11 de 2018). *Modulo 8: Analisis y Valoracion de los Riesgos. Metodologias*. Obtenido de Modulo 8: Analisis y Valoracion de los Riesgos. Metodologias: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

TRANSPORTE, M. d. (2013). por el cual se establecen las condiciones que deben cumplir los centros de diagnostico automotor para su habilitacion, funcionamiento y se adicionan otras disposiciones. En *Resolucion 3768* (pág. Articulo 6 Numeral f). Recuperado el 11 de 09 de 2018.

VULNERABILIDADES, A. y. (18 de 10 de 2018). *Gestion del Riesgo en la Seguridad Informatica*. Obtenido de Gestion del Riesgo en la Seguridad Informatica: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

ANEXO: resumen analítico RAE

Anexo 1. Resumen RAE

Título:	**PLANTEAMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN APLICANDO LA NORMA NTC ISO/IEC 27001 – 27002 DEL 2013 EN EL PROCESO DE LA REVISIÓN TÉCNICO - MECÁNICA DEL CDA CORPOTRANS**
Autores:	Giraldo Reina Edna Rocio
Nombre de editorial:	instituto colombiano de normas técnicas y certificación - ICONTEC
Fecha:	09 de diciembre 2018
Palabras claves:	Centro de diagnóstico automotor, Sistema de gestión de seguridad de información, Activos informáticos, Confidencialidad, Integridad, Disponibilidad, Metodología Magerit, Riesgo, Amenaza, Políticas, Programa de formación.
Descripción:	El proyecto aplicado de la universidad nacional abierta a ya distancia en el diseño e implementación del sistema de gestión de seguridad informática y de información en todo el proceso de la revisión técnico - mecánica en el que intervienen sistemas informáticos, los cuales deben permitir la disponibilidad, integridad y confidencialidad ante la ejecución de los procesos y la mejora continua de la organización a partir de la inclusión en el sistema de gestión existente para organismos de inspección desde la norma NTC ISO/IEC 17020:2012.
Fuentes bibliográficas:	La implementación del sistema de gestión de seguridad informática y de información está conformado por 10 fuentes bibliográficas, a continuación, se indican las más representativas para el desarrollo del proyecto aplicado.

Continúa…

Fuentes bibliográficas:

Electrónica, P. d. (2012). MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Vol. Libro II: Catálogo de Elementos). Madrid: Ministerio de Hacienda y Administraciones Públicas. Recuperado el 15 de 10 de 2018, de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W8eNEGgzbIU

ICONTEC - Instituto Colombiano de Normas Técnicas. (2012). CONTINUIDAD DEL NEGOCIO. SISTEMAS DE GESTIÓN DE CONTINUIDAD DE NEGOCIO. REQUISITOS. Bogotá D.C: Instituto colombiano de normas técnicas y certificación. Recuperado el 04 de 11 de 2018, de http://bibliotecavirtual.unad.edu.co:3101/pdfview/viewer.aspx?locale=es-419&Q=C5EC0CABB074B242D71EB7E1C99D45B796DF3D9C2A164539&Req=

Internacional, I. (2013). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos (Vol. Primera actualización). Bogotá D.C: Instituto Colombiano de Normas Técnicas y Certificación. Recuperado el 15 de 10 de 2018, de http://bibliotecavirtual.unad.edu.co:3101/pdfview/viewer.aspx?locale=es-419&Q=1775CD1AFBC53D942B1D63945F22285F96DF3D9C2A164539&Req=

Continúa…

Contenido:	El centro de diagnóstico automotor Corpotrans CDA, es una media empresa que lleva a cabo la inspección vehicular a partir de sistemas de información y comunicación de resultados en línea, es por esto que se identifica la necesidad de diseñar e implementar el sistema de gestión se seguridad informática y de información por medio de la norma NTC ISO/IEC 27001 -27002, la cal permitirá incluir controles y medidas de seguridad lógica y física y si no también a su entorno con la intensión de preservar la disponibilidad de la prestación del servicio, el cumplimiento con los requisitos normativos y legales que deben cumplir a partir de los objetivos de la revisión técnico - mecánica y emisiones contaminantes. Así mismo se identifica la falta de control y administración los sistemas de información lo cual causa posibles amenazas y riesgos en los activos informáticos y la seguridad de la información que se maneja y se obtiene desde los procesos realizados. NTC ISO/IEC 27001 -27002 de 2013: es una norma técnica colombiana que le permite a las empresas aplicar en su estructura organizacional un alto nivel de seguridad de la información resguardando siempre la confidencialidad, integridad y disponibilidad de la información a partir de procesos. Plan de continuidad del negocio: está basado en la norma ISO 22301, el cual busca disminuir el nivel de incidente en los procesos a partir de requisitos que mantiene la mejora continua y el tiempo de reacción ante posibles amenazas y riesgos actuales y futuros en una empresa. Información de respaldo: es un procedimiento de copia de información en el cual debe estar establecido con un periodo y nivel de acceso a la misma solo por parte de personal autorizado.

Continúa…

	Bitácora de operación del sistema: los sistemas de información deben contar con un registro LOG de las actividades del sistema en el que se permite verificar la interacción de todos los usuarios con la información que se maneja así se verifica la correcta asignación de permisos y si estos se mantienen confirme a las funciones y responsabilidades establecidas desde la alta dirección.
Objetivos	OBJETIVOS ESPECÍFICOS
	Conocer el estado actual de la seguridad informática, de información en el centro de diagnóstico automotor. Plantear la matriz de los riesgos identificando las vulnerabilidades y amenazas presentadas a todos los activos preservando la confidencialidad, integridad y disponibilidad. Establecer mecanismos de sensibilización de la seguridad y protección a los activos software, redes, y personal que interviene directamente con los procesos y el manejo del software de aplicación para la revisión técnico - mecánica.
Metodología:	La metodología cuantitativa permite verificar los requisitos de la norma y establecer un cumplimiento para la seguridad informática y de información basada en los controles de la norma NTC – ISO/IEC 27001 – 27002 DE 2013 y a su vez determinar que procesos no son satisfactorios para el debido cumplimiento en cuanto al tratamiento de los riesgos presentados en los activos. De esta manera se busca implementar, establecer o actualizar políticas, procesos y procedimientos que identifiquen los roles de cada uno de los funcionarios, de tal manera que se integren todos los requisitos y se aseguren los recursos necesarios para dar tratamiento, valoración y análisis a los riesgos que se encuentra expuesto el CDA direccionados a la operatividad del servicio y el manejo de la perdida de confidencialidad, integridad y disponibilidad dentro del alcance.

Continúa…

Conclusiones:	La propuesta de implementación del sistema de gestión de seguridad informática tiene como propósito promover la confidencialidad, integridad y disponibilidad todos los procesos de la revisión técnico - mecánica en el que intervienen sistemas de información como hardware, software, aplicaciones web y la trasferencia de información en línea, los cuales son requisitos de cumplimiento para la prestación de sus servicios, es por esto que desde el sistema de gestión se realiza el de análisis y valoración de posibles riesgos y amenazas a los que se encuentra expuesta la información de sus cliente y por ende la calidad de su servicio y cumplimiento con lo establecido en las leyes, resoluciones y normas técnicas colombianas que regulan su proceso. Por otra parte, el diseño de implementación esta propuesto desde el manejo de los recursos de personal y de medios de procesamiento de información actuales, para que desde la alta dirección determinen la implementación como una mejora yaqué el costo de inversión no es alto y la inclusión de nuevos procesos y las mejora de los existentes no afectan el principio de las actividades y aspectos que regulan el correcto funcionamiento del sistema de la organización.
Autor RAE:	Edna Rocio Giraldo Reina

Elaboración: propia

Anexo 2. Matriz de Riesgos Corpotrans CDA

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
Datos / información [D]	Base de datos del software de aplicación - SART	Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	2	3	3	4	3		6	6	8	6		A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	2,0	1,5	
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	2	4	4	4	3	4	8	8	8	6	8	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,0	2,0	2,0	1,5	2,0
		Escapes de información [E]	conocimiento de la información por personas sin autorización, sin embargo, esta no es alterada	2	4	5	5			8	10	10			A9.2.3-Gestión de derechos de acceso privilegiado	4	2,0	2,5	2,5		
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	4	4	4		5	12	12	12		15	A12.4.2-Protección de la información de registro	4	3,0	3,0	3,0		3,8
		Destrucción de la información [E]	Amenaza identificada sobre los datos en general.	2	5	5	4		4	10	10	8		8	A12.3.1-Respaldo de la información	4	2,5	2,5	2,0		2,0
		Fugas de información [E]	Incontinencia verbal, medios electrónicos, soporte papel.	1	4	4	3	4		4	4	3	4		A8.3.2-Disposición de los medios	3	1,3	1,3	1,0	1,3	
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	3	4	5	4	4	9	12	15	12	12	A9.4.2-Procedimiento de ingreso seguro	4	2,3	3,0	3,8	3,0	3,0
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	3	3	4	4		9	9	12	12		A9.2.3-Gestión de derechos de acceso privilegiado	3	3,0	3,0	4,0	4,0	

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros														Evaluación del control									
					Valor del impacto potencial					Valor del riesgo potencial								Valor del riesgo residual									
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad					
	Base de datos del software de aplicación - SIIGO	Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	4	4	3	4		8	8	6	8		A12.3.1-Respaldo de la información	3	2,7	2,7	2,0	2,7					
		Divulgación de información [A]	Revelación de información.	2	5	5	4		4	10	10				A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	2,5	2,5							
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	3	3	3	4			9	9	12			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0						
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	1	3	3	4		4	3	3	4		4	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	0,8	0,8	1,0		1,0				
		Escapes de información [E]	conocimiento de la información por personas sin autorización, sin embargo, esta no es alterada	2	4	3	3			8	6	6			A9.2.3-Gestión de derechos de acceso privilegiado	3	2,7	2,0	2,0						
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	4	3	4		3	12	9	12		9	A12.4.2-Protección de la información de registro	4	3,0	2,3	3,0		2,3				
		Destrucción de la información [E]	Amenaza identificada sobre los datos en general.	1	4	4	4		3	4	4	4		3	A12.3.1-Respaldo de la información	4	1,0	1,0	1,0		0,8				
		Fugas de información [E]	Incontinencia verbal, medios electrónicos, soporte papel.	1	4	2	2			4	2	2			A8.3.2-Disposición de los medios	4	1,0	0,5	0,5						
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	4	4	2	4		12	12	6	12		A9.4.2-Procedimiento de ingreso seguro	4	3,0	3,0	1,5	3,0					

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual							
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad		
	Backup del sistema de gestión 17020 versión 2012, Software SART y SIIGO	Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	3	3	4			9	9	12			A9.2.3-Gestión de derechos de acceso privilegiado	4	2,3	2,3	3,0				
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	4	3	3	4		8	6	6	8		A9.1.1-Política de control de acceso	4	2,0	1,5	1,5	2,0			
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	4	3	4	12	12	12	9	12	A9.4.1-Restricción de acceso a la información	4	3,0	3,0	3,0	2,3	3,0		
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	3	3	3		3	6	6	6		6	A12.3.1-Respaldo de la información	3	2,0	2,0	2,0		2,0		
		Divulgación de información [A]	Revelación de información.	1	4	4	3		3	4	4	3		3	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	1,0	1,0	0,8		0,8		
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	1	4	4	5			4	4	5			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,0	1,0	1,3				
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	1	5	5	5		3	5	5	5		3	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,3	1,3	1,3		0,8		
		Escapes de información [E]	conocimiento de la información por personas sin autorización, sin embargo, esta no es alterada	2	4	4	3			8	8	6			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,0	2,0	1,5				

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control									
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual					
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	1	4	4	3		4	4	4	3		4	A9.2.3-Gestión de derechos de acceso privilegiado	4	1,0	1,0	0,8		1,0
		Destrucción de la información [E]	Amenaza identificada sobre los datos en general.	1	5	5	4		3	5	5	4		3	A12.3.1-Respaldo de la información	4	1,3	1,3	1,0		0,8
		Fugas de información [E]	Incontinencia verbal, medios electrónicos, soporte papel.	3	5		4		4	15		12		12	A9.2.6-Retiro o ajuste de los derechos de acceso	4	3,8		3,0		3,0
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	2	5	4	4	5	4	10	8	8	10	8	A8.3.2-Disposición de los medios	4	2,5	2,0	2,0	2,5	2,0
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	4	5	4	5		4	20	16	20		16	A9.4.2-Procedimiento de ingreso seguro	4	5,0	4,0	5,0		4,0
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	4	5	4		4	12	15	12		12	A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,8	3,0		3,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	5	5	4	4	3	15	15	12	12	9	A9.1.1-Política de control de acceso	4	3,8	3,8	3,0	3,0	2,3
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	3	4	4		4	6	8	8		8	A12.3.1-Respaldo de la información	3	2,0	2,7	2,7		2,7

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
Software [SW]	Microsoft Windows 7	Divulgación de información [A]	Revelación de información.	2	5	4	5			10	8	10			A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	2,5	2,0	2,5		
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	2	3	3	4			6	6	8			A11.2.4-Mantenimiento de los equipos.	3	2,0	2,0	2,7		
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	1	3	3	4		3	3	3	4		3	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	0,8	0,8	1,0		0,8
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	1	4	4	5			4	4	5			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,0	1,0	1,3		
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	5	5			3	5	5			3	A9.4.2-Procedimiento de ingreso seguro	4	1,3	1,3			0,8
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	3	4	4	3		4	12	12	9		12	A9.2.5-Revisión de los derechos de acceso de usuarios	3	4,0	4,0	3,0		4,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	5	4	4			15	12	12			A12.2.1-Controles contra códigos maliciosos	4	3,8	3,0	3,0		
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	1	4	4			3	4	4			3	A13.2.1-Políticas y procedimientos de transferencia de acción	3	1,3	1,3			1,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	1	3	4				3	4				A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	1,0	1,3			
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	2	4	4	4		4	8	8	8		8	A9.2.3-Gestión de derechos de acceso privilegiado	4	2,0	2,0	2,0		2,0
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	1	4	4	5		3	4	4	5		3	A9.4.1-Restricción de acceso a la información	2	2,0	2,0	2,5		1,5
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	1	5	5	4			5	5	4			A9.2.6-Retiro o ajuste de los derechos de acceso	3	1,7	1,7	1,3		
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	4	5	5	4		4	20	20	16		16	A12.6.1-Gestión de las vulnerabilidades técnicas	3	6,7	6,7	5,3		5,3
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	4		3	4		4		12	16		16	A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4		3,0	4,0		4,0
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	2	4	4			4	8	8			8	A12.4.3-Registros del administrador y del operador	3	2,7	2,7			2,7
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	3	4	4	5			12	12	15			A6.1.2-Separación de deberes	3	4,0	4,0	5,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	4	5	4		4		20	16		16		A8.3.2-Disposición de los medios	4	5,0	4,0		4,0	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	4	5	4	5			20	16	20			A9.4.2-Procedimiento de ingreso seguro	4	5,0	4,0	5,0		
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	3	4	4	5			12	12	15			A8.1.3-Uso aceptable de los activos	3	4,0	4,0	5,0		
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	4	4	5			12	12	15			A12.2.1-Controles contra códigos maliciosos	4	3,0	3,0	3,8		
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	2	4	3			3	8	6			6	A13.2.1-Políticas y procedimientos de transferencia de acción	3	2,7	2,0			2,0
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1	3	4				3	4				A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	1,0	1,3			
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	5	4				15	12				A9.2.3-Gestión de derechos de acceso privilegiado	4	3,8	3,0			

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control							
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual						
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Microsoft Windows 8	Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	4	4	3	4	4	8	8	6	8	8	A9.1.1-Política de control de acceso	4	2,0	2,0	1,5	2,0	2,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	3	4	4			6	8	8			A12.3.1-Respaldo de la información	3	2,0	2,7	2,7		
		Divulgación de información [A]	Revelación de información.	1	4	4	3		3	4	4	3		3	A13.2.4-Acuerdos de confidencialidad o de no divulgación	3	1,3	1,3	1,0		1,0
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	4	5	5	4	4	3	20	20	16	16	12	A9.4.4-Uso de programas utilitarios privilegiados	4	5,0	5,0	4,0	4,0	3,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	1	3	3	3			3	3	3			A11.2.4-Mantenimiento de los equipos.	2	1,5	1,5	1,5		
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	1	5	4	4			5	4	4			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,3	1,0	1,0		
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	1	4	3	4		3	4	3	4		3	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,0	0,8	1,0		0,8
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	3	3				3	3				A9.4.2-Procedimiento de ingreso seguro	2	1,5	1,5			

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros				Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	1	3	3	4		3	3	3	4		3	A9.2.5-Revisión de los derechos de acceso de usuarios	2	1,5	1,5	2,0		1,5
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	2	4	3	4			8	6	8			A12.2.1-Controles contra códigos maliciosos	4	2,0	1,5	2,0		
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	1	3	3				3	3				A13.2.1-Políticas y procedimientos de transferencia de acción	4	0,8	0,8			
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	1	3	3				3	3				A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	1,5	1,5			
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	4	4	3		3	12	12	9		9	A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,0	2,3		2,3
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	3	5	4	4		3	15	12	12		9	A9.4.1-Restricción de acceso a la información	3	5,0	4,0	4,0		3,0
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	4	5	4				20	16				A9.2.6-Retiro o ajuste de los derechos de acceso	4	5,0	4,0			
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	3	3	4			9	9	12			A12.6.1-Gestión de las vulnerabilidades técnicas	3	3,0	3,0	4,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3		3	3				9	9			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	3		3,0	3,0		
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	1	3	3			3	3	3			3	A12.4.3-Registros del administrador y del operador	2	1,5	1,5			1,5
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	1	4	3	4			4	3	4			A6.1.2-Separación de deberes	2	2,0	1,5	2,0		
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	2	5	4			4	10	8			8	A8.3.2-Disposición de los medios	3	3,3	2,7			2,7
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	2	4	4	5			8	8	10			A9.4.2-Procedimiento de ingreso seguro	3	2,7	2,7	3,3		
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	4	5	5	5			20	20	20			A8.1.3-Uso aceptable de los activos	4	5,0	5,0	5,0		
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	2	4	3	4			8	6	8			A12.2.1-Controles contra códigos maliciosos	4	2,0	1,5	2,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control							
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Microsoft Windows 10	Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1	4	4	3		3	4	4	3		3	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	2,0	2,0	1,5		1,5
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	4	5				8	10				A9.2.3-Gestión de derechos de acceso privilegiado	3	2,7	3,3			
		Repudio [A]	negación de origen, recepción y entrega de mensajes	1	3	3			3	3	3			3	A9.1.2-Acceso a redes y a servicios en red	2	1,5	1,5			1,5
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	4	4	3	3	4	8	8	6	6	8	A9.1.1-Política de control de acceso	4	2,0	2,0	1,5	1,5	2,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	4		5			8		10			A12.3.1-Respaldo de la información	4	2,0		2,5		
		Divulgación de información [A]	Revelación de información.	3	5	4	4			15	12	12			A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,8	3,0	3,0		
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	2	3	4	4	3	3	6	8	8	6	6	A9.4.4-Uso de programas utilitarios privilegiados	4	1,5	2,0	2,0	1,5	1,5
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	1	3	3	3			3	3	3			A11.2.4-Mantenimiento de los equipos.	3	1,0	1,0	1,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual					
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	2	4	4	3			8	8	6			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,0	2,0	1,5		
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	1	3	3	5			3	3	5			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	0,8	0,8	1,3		
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	3	3				3	3				A9.4.2-Procedimiento de ingreso seguro	3	1,0	1,0			
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	1	3	3	4		3	3	3	4		3	A9.2.5-Revisión de los derechos de acceso de usuarios	2	1,5	1,5	2,0		1,5
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	2	3	3	4			6	6	8			A12.2.1-Controles contra códigos maliciosos	4	1,5	1,5	2,0		
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	3	3	3				9	9				A13.2.1-Políticas y procedimientos de transferencia de acción	4	2,3	2,3			
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	3	3	3	3			9	9	9			A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	3,0	3,0	3,0		
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	1	4	4	3		3	4	4	3		3	A9.2.3-Gestión de derechos de acceso privilegiado	3	1,3	1,3	1,0		1,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	3	3	3	4		3	9	9	12		9	A9.4.1-Restricción de acceso a la información	4	2,3	2,3	3,0		2,3
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	1	3		2			3		2			A9.2.6-Retiro o ajuste de los derechos de acceso	3	1,0		0,7		
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	4	3	4			12	9	12			A12.6.1-Gestión de las vulnerabilidades técnicas	3	4,0	3,0	4,0		
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3		4	4				12	12			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	3		4,0	4,0		
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	1	3	3			3	3	3			3	A12.4.3-Registros del administrador y del operador	2	1,5	1,5			1,5
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	2	3	3	4			6	6	8			A6.1.2-Separación de deberes	4	1,5	1,5	2,0		
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	5	2		5		15	6		15		A8.3.2-Disposición de los medios	3	5,0	2,0		5,0	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	3	3	5			9	9	15			A9.4.2-Procedimiento de ingreso seguro	3	3,0	3,0	5,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	1	4	4	4			4	4	4			A8.1.3-Uso aceptable de los activos	2	2,0	2,0	2,0		
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	2	3	3	4			6	6	8			A12.2.1-Controles contra códigos maliciosos	4	1,5	1,5	2,0		
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	3	3	3				9	9				A13.2.1-Políticas y procedimientos de transferencia de acción	3	3,0	3,0			
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	2	3	3				6	6				A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	2,0	2,0			
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	5	4				15	12				A9.2.3-Gestión de derechos de acceso privilegiado	4	3,8	3,0			
		Repudio [A]	negación de origen, recepción y entrega de mensajes	1	3	3			3	3	3			3	A9.1.2-Acceso a redes y a servicios en red	2	1,5	1,5			1,5
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	3	3	4	12	12	9	9	12	A9.1.1-Política de control de acceso	4	3,0	3,0	2,3	2,3	3,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual							
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Windows server foundation 2012 configuration RAID 2	Divulgación de información [A]	Revelación de información.	3	4	4	4			12	12	12			A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,0	3,0	3,0		
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	4	4	4	3	4	3	16	16	12	16	12	A9.4.4-Uso de programas utilitarios privilegiados	4	4,0	4,0	3,0	4,0	3,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	1	4	4	5		4	4	4	5		4	A11.2.4-Mantenimiento de los equipos.	4	1,0	1,0	1,3		1,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	1	5	4	5		4	5	4	5		4	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,3	1,0	1,3		1,0
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	5	5	5		4	15	15	15		12	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,8	3,8	3,8		3,0
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	4	4				8	8				A9.4.2-Procedimiento de ingreso seguro	3	2,7	2,7			
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	2	5	4	5		4	10	8	10		8	A9.2.5-Revisión de los derechos de acceso de usuarios	4	2,5	2,0	2,5		2,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	2	4	4	5			8	8	10			A12.2.1-Controles contra códigos maliciosos	4	2,0	2,0	2,5		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros				Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	1	5	4			4	5	4			4	A13.2.1-Políticas y procedimientos de transferencia de acción	4	1,3	1,0			1,0
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	2	4	4			4	8	8			8	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	4,0	4,0			4,0
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	2	4	5	5		4	8	10	10		8	A9.2.3-Gestión de derechos de acceso privilegiado	3	2,7	3,3	3,3		2,7
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	2	4	4	5		4	8	8	10		8	A9.4.1-Restricción de acceso a la información	3	2,7	2,7	3,3		2,7
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	2	4	4			4	8	8			8	A9.2.6-Retiro o ajuste de los derechos de acceso	3	2,7	2,7			2,7
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	2	5	5	5			10	10	10			A12.6.1-Gestión de las vulnerabilidades técnicas	3	3,3	3,3	3,3		
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	1		5	5				5	5			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4		1,3	1,3		
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	1	5	5			4	5	5			4	A12.4.3-Registros del administrador y del operador	3	1,7	1,7			1,3

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	1	4	4	5			4	4	5			A6.1.2-Separación de deberes	3	1,3	1,3	1,7		
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	2	5	4		4		10	8		8		A8.3.2-Disposición de los medios	3	3,3	2,7		2,7	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	2	5	4	5			10	8	10			A9.4.2-Procedimiento de ingreso seguro	3	3,3	2,7	3,3		
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	1	4	4	5			4	4	5			A8.1.3-Uso aceptable de los activos	2	2,0	2,0	2,5		
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	2	4	4	5			8	8	10			A12.2.1-Controles contra códigos maliciosos	4	2,0	2,0	2,5		
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	1	5	4			4	5	4			4	A13.2.1-Políticas y procedimientos de transferencia de acción	3	1,7	1,3			1,3
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1	4	4			4	4	4			4	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	1,3	1,3			1,3

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control							
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual						
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	herramientas de Microsoft office	Repudio [A]	negación de origen, recepción y entrega de mensajes	1	4	5			4	4	5			4	A9.1.2-Acceso a redes y a servicios en red	3	1,3	1,7			1,3
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	5	5	4	4	4	10	10	8	8	8	A9.1.1-Política de control de acceso	4	2,5	2,5	2,0	2,0	2,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	5		5			10		10			A12.3.1-Respaldo de la información	4	2,5		2,5		
		Divulgación de información [A]	Revelación de información.	2	5	4	4		4	10	8	8		8	A13.2.4-Acuerdos de confidencialidad o de no divulgación	3	3,3	2,7	2,7		2,7
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	2	5	4	5	4	4	10	8	10	8	8	A9.4.4-Uso de programas utilitarios privilegiados	4	2,5	2,0	2,5	2,0	2,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	3	3	3	4			9	9	12			A11.2.4-Mantenimiento de los equipos.	3	3,0	3,0	4,0		
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	4	4	3	4			16	12	16			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	4,0	3,0	4,0		
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	1	4	4	5		4	4	4	5		4	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,0	1,0	1,3		1,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	3	3				3	3				A9.4.2-Procedimiento de ingreso seguro	2	1,5	1,5			
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	1	3	3	4		3	3	3	4		3	A9.2.5-Revisión de los derechos de acceso de usuarios	2	1,5	1,5	2,0		1,5
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	4	3	4			12	9	12			A12.2.1-Controles contra códigos maliciosos	4	3,0	2,3	3,0		
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	1	3	3	3		3	3	3	3		3	A13.2.1-Políticas y procedimientos de transferencia de acción	4	0,8	0,8	0,8		0,8
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	1	4	4	3		3	4	4	3		3	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	2,0	2,0	1,5		1,5
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	3	3	4		3	9	9	12		9	A9.2.3-Gestión de derechos de acceso privilegiado	3	3,0	3,0	4,0		3,0
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	4	4	4	4			16	16	16			A9.4.1-Restricción de acceso a la información	4	4,0	4,0	4,0		
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	3	4	3	3		3	12	9	9		9	A9.2.6-Retiro o ajuste de los derechos de acceso	4	3,0	2,3	2,3		2,3

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	4	3	3	5			12	12	20			A12.6.1-Gestión de las vulnerabilidades técnicas	4	3,0	3,0	5,0		
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	4	3	3	5			12	12	20			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	3,0	3,0	5,0		
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	1	3	3			3	3	3			3	A12.4.3-Registros del administrador y del operador	2	1,5	1,5			1,5
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	1	3	3	4			3	3	4			A6.1.2-Separación de deberes	3	1,0	1,0	1,3		
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	2	4	3		3		8	6		6		A8.3.2-Disposición de los medios	3	2,7	2,0		2,0	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	1	3	3	4			3	3	4			A9.4.2-Procedimiento de ingreso seguro	2	1,5	1,5	2,0		
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	4	3	3	3			12	12	12			A8.1.3-Uso aceptable de los activos	4	3,0	3,0	3,0		
		Difusión de software dañiino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	4	3	4			12	9	12			A12.2.1-Controles contra códigos maliciosos	4	3,0	2,3	3,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	1	3	3	3			3	3	3			A13.2.1-Políticas y procedimientos de transferencia de acción	3	1,0	1,0	1,0		
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1	3	3	3		3	3	3	3		3	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	1,0	1,0	1,0		1,0
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	3	3	3			9	9	9			A9.2.3-Gestión de derechos de acceso privilegiado	3	3,0	3,0	3,0		
		Repudio [A]	negación de origen, recepción y entrega de mensajes	2	3	3			3	6	6			6	A9.1.2-Acceso a redes y a servicios en red	2	3,0	3,0			3,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	4	4	4	3	4	8	8	8	6	8	A9.1.1-Política de control de acceso	4	2,0	2,0	2,0	1,5	2,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	3		3	3				9	9			A12.3.1-Respaldo de la información	3		3,0	3,0		
		Divulgación de información [A]	Revelación de información.	3	4	4	3		3	12	12	9		9	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,0	3,0	2,3		2,3
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	2	3	3	4	3	3	6	6	8	6	6	A9.4.4-Uso de programas utilitarios privilegiados	4	1,5	1,5	2,0	1,5	1,5

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Plataforma RUNT	Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	4	3	4	5		3	12	16	20		12	A11.2.4-Mantenimiento de los equipos.	4	3,0	4,0	5,0		3,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	2	5	4	4		4	10	8	8		8	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,5	2,0	2,0		2,0
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	2	3	3	5			6	6	10			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	2,5		
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	4	4				8	8				A9.4.2-Procedimiento de ingreso seguro	2	4,0	4,0			
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	2	3	4			3	6	8			6	A9.2.5-Revisión de los derechos de acceso de usuarios	2	3,0	4,0			3,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	4	4	5			12	12	15			A12.2.1-Controles contra códigos maliciosos	4	3,0	3,0	3,8		
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	1	4	4				4	4				A13.2.1-Políticas y procedimientos de transferencia de acción	3	1,3	1,3			

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	2	5	5	4		4	10	10	8		8	A9.2.3-Gestión de derechos de acceso privilegiado	2	5,0	5,0	4,0		4,0
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	1	4	4	3		3	4	4	3		3	A9.4.1-Restricción de acceso a la información	1	4,0	4,0	3,0		3,0
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	3	5	4				15	12				A9.2.6-Retiro o ajuste de los derechos de acceso	3	5,0	4,0			
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	4	4	5		4	12	12	15		12	A12.6.1-Gestión de las vulnerabilidades técnicas	3	4,0	4,0	5,0		4,0
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3		4	5				12	15			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	3		4,0	5,0		
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	1	4	4			4	4	4			4	A12.4.3-Registros del administrador y del operador	1	4,0	4,0			4,0
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	1	4	4	5			4	4	5			A6.1.2-Separación de deberes	1	4,0	4,0	5,0		
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	2	3	3			3	6	6			6	A8.3.2-Disposición de los medios	2	3,0	3,0			3,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	1	3	3	4			3	3	4			A9.4.2-Procedimiento de ingreso seguro	1	3,0	3,0	4,0		
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	1	2	2	3			2	2	3			A8.1.3-Uso aceptable de los activos	1	2,0	2,0	3,0		
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	4	4	5			12	12	15			A12.2.1-Controles contra códigos maliciosos	4	3,0	3,0	3,8		
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	1	4	3			3	4	3			3	A13.2.1-Políticas y procedimientos de transferencia de acción	4	1,0	0,8			0,8
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1	4	4				4	4				A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	1	4,0	4,0			
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	4	4			3	4	4			3	A9.2.3-Gestión de derechos de acceso privilegiado	1	4,0	4,0			3,0
		Repudio [A]	negación de origen, recepción y entrega de mensajes	1	4	4			4	4	4			4	A9.1.2-Acceso a redes y a servicios en red	1	4,0	4,0			4,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual					
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Plataforma CI2	Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	1	4	4	5			4	4	5			A12.3.1-Respaldo de la información	3	1,3	1,3	1,7		
		Divulgación de información [A]	Revelación de información.	1	4	4	3		4	4	4	3		4	A13.2.4-Acuerdos de confidencialidad o de no divulgación	1	4,0	4,0	3,0		4,0
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	1	4	4	5	5	4	4	4	5	5	4	A9.4.4-Uso de programas utilitarios privilegiados	1	4,0	4,0	5,0	5,0	4,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	2	3	3	5		3	6	6	10		6	A11.2.4-Mantenimiento de los equipos.	2	3,0	3,0	5,0		3,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	1	3	3	4		4	3	3	4		4	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	0,8	0,8	1,0		1,0
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	2	3	3	4			6	6	8			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	2,0		
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	3	3				6	6				A9.4.2-Procedimiento de ingreso seguro	2	3,0	3,0			
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	2	4	5	5		4	8	10	10		8	A9.2.5-Revisión de los derechos de acceso de usuarios	2	4,0	5,0	5,0		4,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	2	4	4	5			8	8	10			A12.2.1-Controles contra códigos maliciosos	4	2,0	2,0	2,5		
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	1	5	4	3		3	5	4	3		3	A13.2.1-Políticas y procedimientos de transferencia de acción	3	1,7	1,3	1,0		1,0
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	2	4	4				8	8				A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	4,0	4,0			
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	1	3	4	4		3	3	4	4		3	A9.2.3-Gestión de derechos de acceso privilegiado	1	3,0	4,0	4,0		3,0
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	2	4	4	4		3	8	8	8		6	A9.4.1-Restricción de acceso a la información	2	4,0	4,0	4,0		3,0
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	2	4	4	4			8	8	8			A9.2.6-Retiro o ajuste de los derechos de acceso	2	4,0	4,0	4,0		
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	4	4	5			12	12	15			A12.6.1-Gestión de las vulnerabilidades técnicas	3	4,0	4,0	5,0		
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3	4	4	5			12	12	15			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	3	4,0	4,0	5,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	1	4	4	3		4	4	4	3		4	A12.4.3-Registros del administrador y del operador	1	4,0	4,0	3,0		4,0
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	1	4	4	4			4	4	4			A6.1.2-Separación de deberes	1	4,0	4,0	4,0		
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	3	3		4		9	9		12		A8.3.2-Disposición de los medios	3	3,0	3,0		4,0	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	2	3	3	4		3	6	6	8		6	A9.4.2-Procedimiento de ingreso seguro	2	3,0	3,0	4,0		3,0
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	1	2	2	3			2	2	3			A8.1.3-Uso aceptable de los activos	1	2,0	2,0	3,0		
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	2	4	4	5			8	8	10			A12.2.1-Controles contra códigos maliciosos	4	2,0	2,0	2,5		
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	1	4	4	3		3	4	4	3		3	A13.2.1-Políticas y procedimientos de transferencia de acción	4	1,0	1,0	0,8		0,8

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Plataforma Supergiros	Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	4	4				8	8				A9.2.3-Gestión de derechos de acceso privilegiado	2	4,0	4,0			
		Repudio [A]	negación de origen, recepción y entrega de mensajes	2	5	5			4	10	10			8	A9.1.2-Acceso a redes y a servicios en red	2	5,0	5,0			4,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	1	4	4	5	5	4	4	4	5	5	4	A9.1.1-Política de control de acceso	4	1,0	1,0	1,3	1,3	1,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	4	4	5		4	8	8	10		8	A12.3.1-Respaldo de la información	4	2,0	2,0	2,5		2,0
		Divulgación de información [A]	Revelación de información.	2	5	4			4	10	8			8	A13.2.4-Acuerdos de confidencialidad o de no divulgación	2	5,0	4,0			4,0
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	2	3	3	5	4	4	6	6	10	8	8	A9.4.4-Uso de programas utilitarios privilegiados	2	3,0	3,0	5,0	4,0	4,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	3	4	4	5		4	12	12	15		12	A11.2.4-Mantenimiento de los equipos.	3	4,0	4,0	5,0		4,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	3	3	3	4		4	9	9	12		12	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0		3,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros														Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual								
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad			
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	2	3	3	5		3	6	6	10		6	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	2,5		1,5			
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	3	3				6	6				A9.4.2-Procedimiento de ingreso seguro	2	3,0	3,0						
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	2	4	4	5		4	8	8	10		8	A9.2.5-Revisión de los derechos de acceso de usuarios	2	4,0	4,0	5,0		4,0			
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	3	3	5			9	9	15			A12.2.1-Controles contra códigos maliciosos	4	2,3	2,3	3,8					
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	2	3	3				6	6				A13.2.1-Políticas y procedimientos de transferencia de acción	3	2,0	2,0						
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	2	4	4			4	8	8			8	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	4,0	4,0			4,0			
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	4	4	3		4	12	12	9		12	A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,0	2,3		3,0			
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	1	4	4	3		4	4	4	3		4	A9.4.1-Restricción de acceso a la información	3	1,3	1,3	1,0		1,3			

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros														Evaluación del control									
					Valor del impacto potencial					Valor del riesgo potencial								Valor del riesgo residual							
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad				
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	1	3	3				3	3				A9.2.6-Retiro o ajuste de los derechos de acceso	3	1,0	1,0							
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	3	3	5			9	9	15			A12.6.1-Gestión de las vulnerabilidades técnicas	4	2,3	2,3	3,8						
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3	3	3	5			9	9	15			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	2,3	2,3	3,8						
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	1	3	3	4		3	3	3	4		3	A12.4.3-Registros del administrador y del operador	2	1,5	1,5	2,0		1,5				
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	1	4	4	4			4	4	4			A6.1.2-Separación de deberes	2	2,0	2,0	2,0						
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	3	4	4	4		9	12	12	12		A8.3.2-Disposición de los medios	4	2,3	3,0	3,0	3,0					
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	2	3	3	3			6	6	6			A9.4.2-Procedimiento de ingreso seguro	3	2,0	2,0	2,0						
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	2	3	3	2			6	6	4			A8.1.3-Uso aceptable de los activos	2	3,0	3,0	2,0						

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Difusión de software dañiino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	3	3	5			9	9	15			A12.2.1-Controles contra códigos maliciosos	4	2,3	2,3	3,8		
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	2	3	3				6	6				A13.2.1-Políticas y procedimientos de transferencia de acción	4	1,5	1,5			
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	2	3	3	4			6	6	8			A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	3,0	3,0	4,0		
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	4	4				4	4				A9.2.3-Gestión de derechos de acceso privilegiado	3	1,3	1,3			
		Repudio [A]	negación de origen, recepción y entrega de mensajes	2	4	4			4	8	8			8	A9.1.2-Acceso a redes y a servicios en red	2	4,0	4,0			4,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	4	4	4	12	12	12	12	12	A9.1.1-Política de control de acceso	4	3,0	3,0	3,0	3,0	3,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	3		4			6		8			A12.3.1-Respaldo de la información	3	2,0		2,7		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software SIIGO contable	Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	2	3	3	4	4	4	6	6	8	8	8	A9.4.4-Uso de programas utilitarios privilegiados	3	2,0	2,0	2,7	2,7	2,7
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	2	3	3	4		3	6	6	8		6	A11.2.4-Mantenimiento de los equipos.	4	1,5	1,5	2,0		1,5
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	3	4	3	3		3	12	9	9		9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,0	2,3	2,3		2,3
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	2	3	3	4			6	6	8			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	2,0		
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	3	3				3	3				A9.4.2-Procedimiento de ingreso seguro	1	3,0	3,0			
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	2	3	3			3	6	6			6	A9.2.5-Revisión de los derechos de acceso de usuarios	2	3,0	3,0			3,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	3	3	4			9	9	12			A12.2.1-Controles contra códigos maliciosos	4	2,3	2,3	3,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	1	3	3	4			3	3	4			A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	1	3,0	3,0	4,0		
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	3	4	4	3			12	12	9			A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,0	2,3		
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	3	3	3	4		3	9	9	12		9	A9.4.1-Restricción de acceso a la información	4	2,3	2,3	3,0		2,3
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	3	3	3				9	9				A9.2.6-Retiro o ajuste de los derechos de acceso	4	2,3	2,3			
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	3	3	3			9	9	9			A12.6.1-Gestión de las vulnerabilidades técnicas	4	2,3	2,3	2,3		
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3		4	4				12	12			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4		3,0	3,0		
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	2	4	4			4	8	8			8	A12.4.3-Registros del administrador y del operador	2	4,0	4,0			4,0
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	2	3	3	4			6	6	8			A6.1.2-Separación de deberes	2	3,0	3,0	4,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	5	5		4		15	15		12		A8.3.2-Disposición de los medios	4	3,8	3,8		3,0	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	4	4	4			12	12	12			A9.4.2-Procedimiento de ingreso seguro	4	3,0	3,0	3,0		
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	2	4	3	3			8	6	6			A8.1.3-Uso aceptable de los activos	2	4,0	3,0	3,0		
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	3	3	4		3	9	9	12		9	A12.2.1-Controles contra códigos maliciosos	4	2,3	2,3	3,0		2,3
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	2	3	3				6	6				A13.2.1-Políticas y procedimientos de transferencia de acción	3	2,0	2,0			
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1		3	3		4		3	3		4	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	1		3,0	3,0		4,0
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	4	4	4			12	12	12			A9.2.3-Gestión de derechos de acceso privilegiado	4	3,0	3,0	3,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Software de aplicación SART	Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	3		4	12	12	9		12	A9.1.1-Política de control de acceso	4	3,0	3,0	2,3		3,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	3	4	4	5		4	12	12	15		12	A12.3.1-Respaldo de la información	4	3,0	3,0	3,8		3,0
		Divulgación de información [A]	Revelación de información.	4	4	4	4		4	16	16	16		16	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	4,0	4,0	4,0		4,0
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	2	3	3	5	4	3	6	6	10	8	6	A9.4.4-Uso de programas utilitarios privilegiados	3	2,0	2,0	3,3	2,7	2,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	3	4	4	5		4	12	12	15		12	A11.2.4-Mantenimiento de los equipos.	4	3,0	3,0	3,8		3,0
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	3	3	3	3		3	9	9	9		9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	2,3		2,3
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	3	3	4		3	9	9	12		9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0		2,3
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	4	4	3			4	4	3			A9.4.2-Procedimiento de ingreso seguro	2	2,0	2,0	1,5		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	2	4	4	3		3	8	8	6		6	A9.2.5-Revisión de los derechos de acceso de usuarios	3	2,7	2,7	2,0		2,0
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	3	4	4	5			12	12	15			A12.2.1-Controles contra códigos maliciosos	4	3,0	3,0	3,8		
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	2	4	3	3			8	6	6			A13.2.1-Políticas y procedimientos de transferencia de acción	4	2,0	1,5	1,5		
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	2	4	4			4	8	8			8	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	2,7	2,7			2,7
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	2	3	3	4			6	6	8			A9.2.3-Gestión de derechos de acceso privilegiado	4	1,5	1,5	2,0		
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	2	5	5	4		4	10	10	8		8	A9.4.1-Restricción de acceso a la información	4	2,5	2,5	2,0		2,0
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	2	4	4				8	8				A9.2.6-Retiro o ajuste de los derechos de acceso	4	2,0	2,0			
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	4	3	4			12	9	12			A12.6.1-Gestión de las vulnerabilidades técnicas	3	4,0	3,0	4,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3	4	4	5			12	12	15			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	3,0	3,0	3,8		
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	1	4	4	4		4	4	4	4		4	A12.4.3-Registros del administrador y del operador	2	2,0	2,0	2,0		2,0
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	2	4	4	5			8	8	10			A6.1.2-Separación de deberes	4	2,0	2,0	2,5		
		Suplantación de la identidad del usuario [A]	el atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	4	4	3	3	4	12	12	9	9	12	A8.3.2-Disposición de los medios	4	3,0	3,0	2,3	2,3	3,0
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	2	4	4	4		4	8	8	8		8	A9.4.2-Procedimiento de ingreso seguro	3	2,7	2,7	2,7		2,7
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	2	3	3	4			6	6	8			A8.1.3-Uso aceptable de los activos	3	2,0	2,0	2,7		
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	3	4	4	5			12	12	15			A12.2.1-Controles contra códigos maliciosos	4	3,0	3,0	3,8		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros				Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1	3	3	4		3	3	3	4		3	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	1,5	1,5	2,0		1,5
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	3	3				6	6				A9.2.3-Gestión de derechos de acceso privilegiado	4	1,5	1,5			
		Repudio [A]	negación de origen, recepción y entrega de mensajes	3	4	4			4	12	12			12	A9.1.2-Acceso a redes y a servicios en red	3	4,0	4,0			4,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	4	4	5	5	4	8	8	10	10	8	A9.1.1-Política de control de acceso	4	2,0	2,0	2,5	2,5	2,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2	4	4	5			8	8	10			A12.3.1-Respaldo de la información	4	2,0	2,0	2,5		
		Divulgación de información [A]	Revelación de información.	2	4	4			4	8	8			8	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	2,0	2,0			2,0
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	3	4	4	5	4	4	12	12	15	12	12	A9.4.4-Uso de programas utilitarios privilegiados	4	3,0	3,0	3,8	3,0	3,0
	Antivirus Avast	Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	1	4	4	5			4	4	5			A11.2.4-Mantenimiento de los equipos.	4	1,0	1,0	1,3		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros														Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual								
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad			
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	2	5	5	3			10	10	6			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,5	2,5	1,5					
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	5	5	3		3	15	15	9		9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,8	3,8	2,3		2,3			
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	5	5				10	10				A9.4.2-Procedimiento de ingreso seguro	3	3,3	3,3						
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	3	4	4			4	12	12			12	A9.2.5-Revisión de los derechos de acceso de usuarios	4	3,0	3,0			3,0			
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	4	5	5	5			20	20	20			A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0					
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	1	4	4			4	4	4			4	A13.2.1-Políticas y procedimientos de transferencia de acción	4	1,0	1,0			1,0			
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	1	4	4			4	4	4			4	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	2,0	2,0			2,0			

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	1	4	4	3		4	4	4	3		4	A9.4.1-Restricción de acceso a la información	3	1,3	1,3	1,0		1,3
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	1	4	4			4	4	4			4	A9.2.6-Retiro o ajuste de los derechos de acceso	3	1,3	1,3			1,3
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	4	5	4	4			20	16	16			A12.6.1-Gestión de las vulnerabilidades técnicas	4	5,0	4,0	4,0		
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	4	3	3	4			12	12	16			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4	3,0	3,0	4,0		
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	1	4	4			4	4	4			4	A12.4.3-Registros del administrador y del operador	3	1,3	1,3			1,3
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	2	4	4	5			8	8	10			A6.1.2-Separación de deberes	3	2,7	2,7	3,3		
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	1	4	4		4		4	4		4		A8.3.2-Disposición de los medios	3	1,3	1,3		1,3	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	1	4	3	3			4	3	3			A9.4.2-Procedimiento de ingreso seguro	3	1,3	1,0	1,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	1	4	4	3			4	4	3			A8.1.3-Uso aceptable de los activos	2	2,0	2,0	1,5		
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	4	5	5	5			20	20	20			A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0		
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	1	4	4				4	4				A13.2.1-Políticas y procedimientos de transferencia de acción	3	1,3	1,3			
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1	4	4	4			4	4	4			A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	2,0	2,0	2,0		
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	5	5				5	5				A9.2.3-Gestión de derechos de acceso privilegiado	3	1,7	1,7			
		Repudio [A]	negación de origen, recepción y entrega de mensajes	1	4	4			4	4	4			4	A9.1.2-Acceso a redes y a servicios en red	2	2,0	2,0			2,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	1	3	3	4	4	4	3	3	4	4	4	A9.1.1-Política de control de acceso	4	0,8	0,8	1,0	1,0	1,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control							
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual						
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Antivirus Kaspersky	Divulgación de información [A]	Revelación de información.	1	5	5	4			5	5	4			A13.2.4-Acuerdos de confidencialidad o de no divulgación	3	1,7	1,7	1,3		
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	3	3	3	4	3	4	9	9	12	9	12	A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	3,0	2,3	3,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	1	4	4	5			4	4	5			A11.2.4-Mantenimiento de los equipos.	4	1,0	1,0	1,3		
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	2	5	5	3		3	10	10	6		6	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,5	2,5	1,5		1,5
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	5	5	3			15	15	9			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	3	5,0	5,0	3,0		
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	5	5				10	10				A9.4.2-Procedimiento de ingreso seguro	3	3,3	3,3			
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	3	4	4			3	12	12			9	A9.2.5-Revisión de los derechos de acceso de usuarios	4	3,0	3,0			2,3

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	1	4	4			4	4	4			4	A13.2.1-Políticas y procedimientos de transferencia de acción	4	1,0	1,0			1,0
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	1	4	4				4	4				A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	2,0	2,0			
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	1	4	4	4			4	4	4			A9.2.3-Gestión de derechos de acceso privilegiado	4	1,0	1,0	1,0		
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	1	4	4	3			4	4	3			A9.4.1-Restricción de acceso a la información	3	1,3	1,3	1,0		
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	1	4	4				4	4				A9.2.6-Retiro o ajuste de los derechos de acceso	3	1,3	1,3			
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	4	5	4	4			20	16	16			A12.6.1-Gestión de las vulnerabilidades técnicas	4	5,0	4,0	4,0		
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	4		4	4				16	16			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4		4,0	4,0		
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	1	4	4			4	4	4			4	A12.4.3-Registros del administrador y del operador	3	1,3	1,3			1,3

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	2	4	4	5			8	8	10			A6.1.2-Separación de deberes	3	2,7	2,7	3,3		
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	1	4	4		4		4	4		4		A8.3.2-Disposición de los medios	3	1,3	1,3		1,3	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	1	4	3	3			4	3	3			A9.4.2-Procedimiento de ingreso seguro	3	1,3	1,0	1,0		
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	1	4	4	3			4	4	3			A8.1.3-Uso aceptable de los activos	2	2,0	2,0	1,5		
		Difusión de software dañino [A]	Propagación intencionada de virus, gusanos, troyanos, bombas lógicas.	4	5	5	5			20	20	20			A12.2.1-Controles contra códigos maliciosos	4	5,0	5,0	5,0		
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	1	4	4				4	4				A13.2.1-Políticas y procedimientos de transferencia de acción	3	1,3	1,3			
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1		4	4				4	4			A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2		2,0	2,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control									
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual					
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Navegador Internet Explorer	Repudio [A]	negación de origen, recepción y entrega de mensajes	1	4	4			4	4	4			4	A9.1.2-Acceso a redes y a servicios en red	2	2,0	2,0			2,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	1	3	3	4	4	4	3	3	4	4	4	A9.1.1-Política de control de acceso	4	0,8	0,8	1,0	1,0	1,0
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	1	4	4	5			4	4	5			A12.3.1-Respaldo de la información	3	1,3	1,3	1,7		
		Divulgación de información [A]	Revelación de información.	1	5	5	4			5	5	4			A13.2.4-Acuerdos de confidencialidad o de no divulgación	3	1,7	1,7	1,3		
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	3	3	3	4	3	4	9	9	12	9	12	A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	3,0	2,3	3,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	2	4	4	5			8	8	10			A11.2.4-Mantenimiento de los equipos.	3	2,7	2,7	3,3		
		Errores de los usuarios [E]	Equivocaciones de usuarios con el uso de servicios y datos.	3	3	3	4			9	9	12			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0		
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	2	3	3	5			6	6	10			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	2,5		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores de monitorización (log) [E]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	4	4				8	8				A9.4.2-Procedimiento de ingreso seguro	3	2,7	2,7			
		Errores de configuración [E]	Los activos dependen de su configuración, el administrador es quien determina privilegios de acceso, flujo y registro de actividades y encaminamiento.	2	3	3			3	6	6			6	A9.2.5-Revisión de los derechos de acceso de usuarios	4	1,5	1,5			1,5
		Difusión de software dañino [E]	Propagación inocente de virus, gusanos, troyanos, bombas lógicas.	4	5	4	4			20	16	16			A12.2.1-Controles contra códigos maliciosos	4	5,0	4,0	4,0		
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	2	4	4	3			8	8	6			A13.2.1-Políticas y procedimientos de transferencia de acción	4	2,0	2,0	1,5		
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	2	3	4				6	8				A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	2	3,0	4,0			
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	2	4	4	4			8	8	8			A9.2.3-Gestión de derechos de acceso privilegiado	3	2,7	2,7	2,7		
		Destrucción de la información [E]	Perdida accidental de información, se identifica sobre los datos en general.	2		4	4		3		8	8		6	A9.4.1-Restricción de acceso a la información	3		2,7	2,7		2,0
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	2	4	4	4			8	8	8			A9.2.6-Retiro o ajuste de los derechos de acceso	3	2,7	2,7	2,7		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Vulnerabilidades de los programas (software) [E]	defectos del código que dan pie a una operación defectuosa sin intensión por parte del usuario	3	3	3	4			9	9	12			A12.6.1-Gestión de las vulnerabilidades técnicas	4	2,3	2,3	3,0		
		Errores de mantenimiento / actualización de programas (software) [E]	defectos de procedimientos o controles de actualización de código que permiten el uso de programas con defectos conocidos y reportados	3		3	3				9	9			A.14.2.5-Principio de Construcción de los Sistemas Seguros.	4		2,3	2,3		
		Manipulación de los registros de actividad (log) [A]	Manipulación a las evidencias del comportamiento del sistema.	2	3	3			3	6	6			6	A12.4.3-Registros del administrador y del operador	2	3,0	3,0			3,0
		Manipulación de la configuración [A]	Registro de actividad de configuración de administrador: privilegios de acceso, flujo, registro de actividades y encaminamiento.	2	3	3	4			6	6	8			A6.1.2-Separación de deberes	3	2,0	2,0	2,7		
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	4	4		4		12	12		12		A8.3.2-Disposición de los medios	4	3,0	3,0		3,0	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	5	5	4			15	15	12			A9.4.2-Procedimiento de ingreso seguro	3	5,0	5,0	4,0		
		Uso no previsto [A]	Utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos.	3	5	5	5			15	15	15			A8.1.3-Uso aceptable de los activos	4	3,8	3,8	3,8		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	2	4	4	3			8	8	6			A13.2.1-Políticas y procedimientos de transferencia de acción	3	2,7	2,7	2,0		
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	2	3	5	3			6	10	6			A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	2,0	3,3	2,0		
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	4	4				12	12				A9.2.3-Gestión de derechos de acceso privilegiado	3	4,0	4,0			
		Repudio [A]	negación de origen, recepción y entrega de mensajes	2	4	4			4	8	8			8	A9.1.2-Acceso a redes y a servicios en red	2	4,0	4,0			4,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	4	4	4	4	3	8	8	8	8	6	A9.1.1-Política de control de acceso	4	2,0	2,0	2,0	2,0	1,5
		Destrucción de la información [A]	Eliminación intencional de la información, con fines propios y causar perjuicio.	2		4	5				8	10			A12.3.1-Respaldo de la información	3		2,7	3,3		
		Divulgación de información [A]	Revelación de información.	3	4	4	3		3	12	12	9		9	A13.2.4-Acuerdos de confidencialidad o de no divulgación	4	3,0	3,0	2,3		2,3
		Manipulación de programas [A]	Alteración intencionada del funcionamiento de programas por personas autorizadas para su uso.	3	3	3	5	4	4	9	9	15	12	12	A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	3,8	3,0	3,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
Equipamiento informático [HW]	Computadores de escritorio directores técnicos y calidad	Fuego [N]	incendios: posibilidad que acabe con los recursos del sistema	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		1,5
		Daños por agua [N]	inundaciones: posibilidad de que el agua acabe con recursos del sistema	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		1,5
		Desastres naturales [N]	Desastres sin intención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		1,5
		Fuego [I]	incendio: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		1,5
		Daño por agua [I]	escapes, fugas, inundaciones: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		1,5
		Desastres industriales [I]	otros desastres debidos de la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga, fluctuaciones eléctricas, accidentes de tráfico (accidental o deliberado)	1	3	3	4		3	3	3	4		3	A16.1.2-Reporte de eventos de seguridad de la información	2	1,5	1,5	2,0		1,5
		Contaminación mecánica [I]	vibraciones, polvo, suciedad	2	2		3			4		6			A11.1.3-Seguridad de oficinas, recintos e instalaciones.	2	2,0		3,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Contaminación electromagnética [I]	interferencias de radio, campo magnético, luz ultravioleta (accidental o deliberado)	1	3	3	4			3	3	4			A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	2	3	3	4		3	6	6	8		6	A11.2.4-Mantenimiento de los equipos.	4	1,5	1,5	2,0		1,5
		Corte del suministro eléctrico [I]	cese de la alimentación de potencia (accidental o deliberado)	2	3	4	4			6	8	8			A11.2.2-Servicios de suministro	2	3,0	4,0	4,0		
		Condiciones inadecuadas de temperatura o humedad [I]	Deficiencias en la aclimatación de los locales, excediendo márgenes de trabajo de los equipos: exceso de calor, frio, humedad (accidental o deliberado)	1	3		3			3		3			A11.1.1-Perímetro de seguridad física	1	3,0		3,0		
		Emanaciones electromagnéticas [I]	Hecho de poner vía radio datos internos a disposición de terceros. Amenaza donde el emisor es víctima pasiva del atacante (accidental o deliberado)	1	2	2				2	2				A13.2.2-Acuerdos sobre transferencia de información	1	2,0	2,0			
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	2	3	3	4		4	6	6	8		8	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	2,0		2,0
		Errores de mantenimiento / actualización de equipos (hardware) [E]	Defectos en los procedimientos o controles de actualización de los equipos que se utilizan más allá del tiempo de uso	2		3	3				6	6			A.14.2.2-Procedimientos de control de cambios en sistemas	3		2,0	2,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Caída del sistema por agotamiento de recursos [E]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2	2	2	3			4	4	6			A16.1.3-Reporte de debilidades de seguridad de la información	3	1,3	1,3	2,0		
		Pérdida de equipos [E]	La pérdida de equipos provoca directamente la carencia de un medio para prestar el servicio, es decir indisponibilidad.	2		3	4				6	8			A11.2.4-Mantenimiento de los equipos.	4		1,5	2,0		
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	2	4	4	3			8	8	6			A9.4.2-Procedimiento de ingreso seguro	3	2,7	2,7	2,0		
		Uso no previsto [A]	utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	3	4	4	3			12	12	9			A8.1.3-Uso aceptable de los activos	3	4,0	4,0	3,0		
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	3	3				6	6				A9.2.3-Gestión de derechos de acceso privilegiado	3	2,0	2,0			
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	3	3	4	4	3	9	9	12	12	9	A9.1.1-Política de control de acceso	4	2,3	2,3	3,0	3,0	2,3
		Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en si misma se vea alterada.	3	4	4	3			12	12	9			A9.1.2-Acceso a redes y a servicios en red	4	3,0	3,0	2,3		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Computadores de escritorio inspección de pista	Manipulación de los equipos [A]	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	3	4		4	3	3	12		12	9	9	A9.4.4-Uso de programas utilitarios privilegiados	4	3,0		3,0	2,3	2,3
		Denegación de servicio [A]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	3	4	4	5			12	12	15			A13.1.2-Seguridad de los servicios de red	4	3,0	3,0	3,8		
		Robo [A]	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar servicios, es decir indisponibilidad	2	4	4	5			8	8	10			A11.1.3-Seguridad de oficinas, recintos e instalaciones.	3	2,7	2,7	3,3		
		Ataque destructivo [A]	Vandalismo, terrorismo, acción militar, la amenaza puede ser perpetrada por personal interno, externo o contratadas.	1	3	3	4			3	3	4			A12.3.1-Respaldo de la información	4	0,8	0,8	1,0		
		Fuego [N]	incendios: posibilidad que acabe con los recursos del sistema	1	4	4	4		4	4	4	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	2,0	2,0	2,0		2,0
		Daños por agua [N]	inundaciones: posibilidad de que el agua acabe con recursos del sistema	2		3	3				6	6			A11.1.4-Protección contra amenazas externas y ambientales.	3		2,0	2,0		
		Desastres naturales [N]	Desastres sin intención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.	2	3	3	3		3	6	6	6		6	A11.1.4-Protección contra amenazas externas y ambientales.	3	2,0	2,0	2,0		2,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Fuego [I]	incendio: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	4	4			3	4	4			3	A11.1.4-Protección contra amenazas externas y ambientales.	2	2,0	2,0			1,5
		Daño por agua [I]	escapes, fugas, inundaciones: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	2		3	3				6	6			A11.1.4-Protección contra amenazas externas y ambientales.	3		2,0	2,0		
		Desastres industriales [I]	otros desastres debidos de la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga, fluctuaciones eléctricas, accidentes de tráfico (accidental o deliberado)	1		3	3				3	3			A16.1.2-Reporte de eventos de seguridad de la información	2		1,5	1,5		
		Contaminación mecánica [I]	vibraciones, polvo, suciedad	3		3	4				9	12			A11.1.3-Seguridad de oficinas, recintos e instalaciones.	3		3,0	4,0		
		Contaminación electromagnética [I]	interferencias de radio, campo magnético, luz ultravioleta (accidental o deliberado)	1	3	3	4			3	3	4			A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	3	3	4	4			9	12	12			A11.2.4-Mantenimiento de los equipos.	3	3,0	4,0	4,0		
		Corte del suministro eléctrico [I]	cese de la alimentación de potencia (accidental o deliberado)	1	3	3	4			3	3	4			A11.2.2-Servicios de suministro	2	1,5	1,5	2,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Condiciones inadecuadas de temperatura o humedad [I]	Deficiencias en la aclimatación de los locales, excediendo márgenes de trabajo de los equipos: exceso de calor, frio, humedad (accidental o deliberado)	1		3	3				3	3			A11.1.1-Perímetro de seguridad física	2		1,5	1,5		
		Emanaciones electromagnéticas [I]	Hecho de poner vía radio datos internos a disposición de terceros. Amenaza donde el emisor es víctima pasiva del atacante (accidental o deliberado)	1	3	3				3	3				A13.2.2-Acuerdos sobre transferencia de información	2	1,5	1,5			
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	2	3	3	4			6	6	8			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	2,0		
		Errores de mantenimiento / actualización de equipos (hardware) [E]	Defectos en los procedimientos o controles de actualización de los equipos que se utilizan más allá del tiempo de uso	2		3	4				6	8			A.14.2.2-Procedimientos de control de cambios en sistemas	4		1,5	2,0		
		Caída del sistema por agotamiento de recursos [E]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2	3	3	3			6	6	6			A16.1.3-Reporte de debilidades de seguridad de la información	3	2,0	2,0	2,0		
		Pérdida de equipos [E]	La pérdida de equipos provoca directamente la carencia de un medio para prestar el servicio, es decir indisponibilidad.	2	3		3			6		6			A11.2.4-Mantenimiento de los equipos.	4	1,5		1,5		
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	4	4	3			12	12	9			A9.4.2-Procedimiento de ingreso seguro	4	3,0	3,0	2,3		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	3	3				6	6				A9.2.3-Gestión de derechos de acceso privilegiado	4	1,5	1,5			
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	4	3	3	12	12	12	9	9	A9.1.1-Política de control de acceso	4	3,0	3,0	3,0	2,3	2,3
		Interceptación de información (escucha)	el atacante llega a tener acceso a información que no le corresponde, sin que la información en si misma se vea alterada.	2	4	4	4		4	8	8	8		8	A9.1.2-Acceso a redes y a servicios en red	3	2,7	2,7	2,7		2,7
		Manipulación de los equipos [A]	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	3	4	3	4	3	4	12	9	12	9	12	A9.4.4-Uso de programas utilitarios privilegiados	4	3,0	2,3	3,0	2,3	3,0
		Denegación de servicio [A]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2	4	3	4			8	6	8			A13.1.2-Seguridad de los servicios de red	3	2,7	2,0	2,7		
		Robo [A]	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar servicios, es decir indisponibilidad	1	3		5			3		5			A11.1.3-Seguridad de oficinas, recintos e instalaciones.	3	1,0		1,7		
		Ataque destructivo [A]	Vandalismo, terrorismo, acción militar, la amenaza puede ser perpetrada por personal interno, externo o contratadas.	1		3	5				3	5			A12.3.1-Respaldo de la información	3		1,0	1,7		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Daños por agua [N]	inundaciones: posibilidad de que el agua acabe con recursos del sistema	1		3	3		3		3	3		3	A11.1.4-Protección contra amenazas externas y ambientales.	2		1,5	1,5		1,5
		Desastres naturales [N]	Desastres sin intención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.	1		3	3		3		3	3		3	A11.1.4-Protección contra amenazas externas y ambientales.	2		1,5	1,5		1,5
		Fuego [I]	incendio: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1		3	3		3		3	3		3	A11.1.4-Protección contra amenazas externas y ambientales.	2		1,5	1,5		1,5
		Daño por agua [I]	escapes, fugas, inundaciones: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1		3	3		3		3	3		3	A11.1.4-Protección contra amenazas externas y ambientales.	2		1,5	1,5		1,5
		Desastres industriales [I]	otros desastres debidos de la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga, fluctuaciones eléctricas, accidentes de tráfico (accidental o deliberado)	2		3	3		3		6	6		6	A16.1.2-Reporte de eventos de seguridad de la información	2		3,0	3,0		3,0
		Contaminación mecánica [I]	vibraciones, polvo, suciedad	1		3	3				3	3			A11.1.3-Seguridad de oficinas, recintos e instalaciones.	2		1,5	1,5		
		Contaminación electromagnética [I]	interferencias de radio, campo magnético, luz ultravioleta (accidental o deliberado)	1	3	3	4			3	3	4			A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Corte del suministro eléctrico [I]	cese de la alimentación de potencia (accidental o deliberado)	1	3	3	4			3	3	4			A11.2.2-Servicios de suministro	2	1,5	1,5	2,0		
		Condiciones inadecuadas de temperatura o humedad [I]	Deficiencias en la aclimatación de los locales, excediendo márgenes de trabajo de los equipos: exceso de calor, frio, humedad (accidental o deliberado)	1		3	3				3	3			A11.1.1-Perímetro de seguridad física	2		1,5	1,5		
		Emanaciones electromagnéticas [I]	Hecho de poner vía radio datos internos a disposición de terceros. Amenaza donde el emisor es víctima pasiva del atacante (accidental o deliberado)	1	3					3					A13.2.2-Acuerdos sobre transferencia de información	1	3,0				
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	3	3	4		3	9	9	12		9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0		2,3
		Errores de mantenimiento / actualización de equipos (hardware) [E]	Defectos en los procedimientos o controles de actualización de los equipos que se utilizan más allá del tiempo de uso	3	3	3	4			9	9	12			A.14.2.2-Procedimientos de control de cambios en sistemas	4	2,3	2,3	3,0		
		Caída del sistema por agotamiento de recursos [E]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2	4	4	4			8	8	8			A16.1.3-Reporte de debilidades de seguridad de la información	3	2,7	2,7	2,7		
		Pérdida de equipos [E]	La pérdida de equipos provoca directamente la carencia de un medio para prestar el servicio, es decir indisponibilidad.	2	4	3	4			8	6	8			A11.2.4-Mantenimiento de los equipos.	4	2,0	1,5	2,0		

Continúa…

ATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Uso no previsto [A]	utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	4	5	4	4			20	16	16			A8.1.3-Uso aceptable de los activos	4	5,0	4,0	4,0		
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	3	3	3				9	9				A9.2.3-Gestión de derechos de acceso privilegiado	3	3,0	3,0			
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	3	4	4	3	4	9	12	12	9	12	A9.1.1-Política de control de acceso	4	2,3	3,0	3,0	2,3	3,0
		Interceptación de información (escucha)	el atacante llega a tener acceso a información que no le corresponde, sin que la información en si misma se vea alterada.	3	4	4		3		12	12		9		A9.1.2-Acceso a redes y a servicios en red	3	4,0	4,0		3,0	
		Manipulación de los equipos [A]	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	3	3	3	3	4	3	9	9	9	12	9	A9.4.4-Uso de programas utilitarios privilegiados	4	2,3	2,3	2,3	3,0	2,3
		Denegación de servicio [A]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	3	3	3	3			9	9	9			A13.1.2-Seguridad de los servicios de red	4	2,3	2,3	2,3		
		Robo [A]	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar servicios, es decir indisponibilidad	1	3	3	3			3	3	3			A11.1.3-Seguridad de oficinas, recintos e instalaciones.	3	1,0	1,0	1,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Computador Servidor SART	Fuego [N]	incendios: posibilidad que acabe con los recursos del sistema	1	4	4	5		4	4	4	5		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	2,0	2,0	2,5		2,0
		Daños por agua [N]	inundaciones: posibilidad de que el agua acabe con recursos del sistema	1	4	4	5		4	4	4	5		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	2,0	2,0	2,5		2,0
		Desastres naturales [N]	Desastres sin intención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.	1	4	4	5		4	4	4	5		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	2,0	2,0	2,5		2,0
		Fuego [I]	incendio: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	4	4	5		4	4	4	5		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	2,0	2,0	2,5		2,0
		Daño por agua [I]	escapes, fugas, inundaciones: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	4	4	5		4	4	4	5		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	2,0	2,0	2,5		2,0
		Desastres industriales [I]	otros desastres debidos de la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga, fluctuaciones eléctricas, accidentes de tráfico (accidental o deliberado)	1	4	4	4		4	4	4	4		4	A16.1.2-Reporte de eventos de seguridad de la información	2	2,0	2,0	2,0		2,0
		Contaminación mecánica [I]	vibraciones, polvo, suciedad	1	4	4	5			4	4	5			A11.1.3-Seguridad de oficinas, recintos e instalaciones.	2	2,0	2,0	2,5		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	2	4	4	5			8	8	10			A11.2.4-Mantenimiento de los equipos.	4	2,0	2,0	2,5		
		Corte del suministro eléctrico [I]	cese de la alimentación de potencia (accidental o deliberado)	2	3	3	5		4	6	6	10		8	A11.2.2-Servicios de suministro	2	3,0	3,0	5,0		4,0
		Condiciones inadecuadas de temperatura o humedad [I]	Deficiencias en la aclimatación de los locales, excediendo márgenes de trabajo de los equipos: exceso de calor, frio, humedad (accidental o deliberado)	2	4	4	5			8	8	10			A11.1.1-Perímetro de seguridad física	2	4,0	4,0	5,0		
		Emanaciones electromagnéticas [I]	Hecho de poner vía radio datos internos a disposición de terceros. Amenaza donde el emisor es víctima pasiva del atacante (accidental o deliberado)	1	4	4	4			4	4	4			A13.2.2-Acuerdos sobre transferencia de información	2	2,0	2,0	2,0		
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	3	4	4	5	4	4	12	12	15	12	12	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	3,0	3,0	3,8	3,0	3,0
		Errores de mantenimiento / actualización de equipos (hardware) [E]	Defectos en los procedimientos o controles de actualización de los equipos que se utilizan más allá del tiempo de uso	3		4	5		4		12	15		12	A.14.2.2-Procedimientos de control de cambios en sistemas	4		3,0	3,8		3,0
		Caída del sistema por agotamiento de recursos [E]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2		4	4		4		8	8		8	A16.1.3-Reporte de debilidades de seguridad de la información	3		2,7	2,7		2,7

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control							
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual						
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
Redes de comunicaciones [COM]	Router	Manipulación de los equipos [A]	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	2	5	5	5	4	4	10	10	10	8	8	A9.4.4-Uso de programas utilitarios privilegiados	3	3,3	3,3	3,3	2,7	2,7
		Denegación de servicio [A]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2	4	4	5			8	8	10			A13.1.2-Seguridad de los servicios de red	3	2,7	2,7	3,3		
		Robo [A]	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar servicios, es decir indisponibilidad	1	4	4	5			4	4	5			A11.1.3-Seguridad de oficinas, recintos e instalaciones.	2	2,0	2,0	2,5		
		Ataque destructivo [A]	Vandalismo, terrorismo, acción militar, la amenaza puede ser perpetrada por personal interno, externo o contratadas.	1	4	4	5			4	4	5			A12.3.1-Respaldo de la información	3	1,3	1,3	1,7		
		Fallo de servicios de comunicaciones [I]	cese de la capacidad de datos de un sitio a otro, destrucción de medios físicos de transporte, conmutación (accidental o deliberado)	2		3	3				6	6			A12.6.1-Gestión de las vulnerabilidades técnicas	4		1,5	1,5		
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	2	3	3	4		3	6	6	8		6	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	2,0		1,5
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	2	3	3	4		3	6	6	8		6	A13.2.1-Políticas y procedimientos de transferencia de acción	3	2,0	2,0	2,7		2,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	2	4	4	4		3	8	8	8		6	A9.2.3-Gestión de derechos de acceso privilegiado	2	4,0	4,0	4,0		3,0
		Destrucción de la información [E]	Amenaza identificada sobre los datos en general.	2	5	5	4		3	10	10	8		6	A12.3.1-Respaldo de la información	3	3,3	3,3	2,7		2,0
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	2	4	4	3			8	8	6			A9.2.6-Retiro o ajuste de los derechos de acceso	3	2,7	2,7	2,0		
		Caída del sistema por agotamiento de recursos [E]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2		3	3				6	6			A11.2.4-Mantenimiento de los equipos.	3		2,0	2,0		
		Suplantación de la identidad del usuario [A]	El atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	3	4	4	3	4		12	12	9	12		A8.3.2-Disposición de los medios	4	3,0	3,0	2,3	3,0	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	3	3	3	4			9	9	12			A9.4.2-Procedimiento de ingreso seguro	4	2,3	2,3	3,0		
		Uso no previsto [A]	utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	3	3	3	3			9	9	9			A8.1.3-Uso aceptable de los activos	4	2,3	2,3	2,3		
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	2	3	3				6	6				A13.2.1-Políticas y procedimientos de transferencia de acción	3	2,0	2,0			

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	2	3	3		3		6	6		6		A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	2,0	2,0		2,0	
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	4	4				8	8				A9.2.3-Gestión de derechos de acceso privilegiado	4	2,0	2,0			
		Análisis de tráfico [A]	el atacante sin análisis de comunicaciones, extrae análisis de origen, destino, volumen y frecuencia de los intercambios	2	4	4			4	8	8			8	A13.2.1-Políticas y procedimientos de transferencia de acción	4	2,0	2,0			2,0
		Interceptación de información (escucha) [A]	El atacante llega a tener acceso a información que no le corresponde, sin que la información en si misma se vea alterada.	2	4	4			4	8	8			8	A9.1.2-Acceso a redes y a servicios en red	4	2,0	2,0			2,0
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	3	4	4	5	4	4	12	12	15	12	12	A9.1.1-Política de control de acceso	4	3,0	3,0	3,8	3,0	3,0
		Divulgación de información [A]	Revelación de información.	3	3	3				9	9				A13.2.4-Acuerdos de confidencialidad o de no divulgación	3	3,0	3,0			
		Denegación de servicio [A]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2	4	4	4			8	8	8			A13.1.2-Seguridad de los servicios de red	4	2,0	2,0	2,0		
	Switch	Fallo de servicios de comunicaciones [I]	cese de la capacidad de datos de un sitio a otro, destrucción de medios físicos de transporte, conmutación (accidental o deliberado)	1	3	3	4		4	3	3	4		4	A12.6.1-Gestión de las vulnerabilidades técnicas	3	1,0	1,0	1,3		1,3

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Errores del administrador [E]	Equivocaciones generadas por responsables de proceso de instalación y operación.	2	3	3	3		3	6	6	6		6	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5	1,5	1,5		1,5
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	1	3	3			3	3	3			3	A13.2.1-Políticas y procedimientos de transferencia de acción	4	0,8	0,8			0,8
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	1	3	3			3	3	3			3	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	4	0,8	0,8			0,8
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	1	4	4	3		4	4	4	3		4	A9.2.3-Gestión de derechos de acceso privilegiado	4	1,0	1,0	0,8		1,0
		Destrucción de la información [E]	Amenaza identificada sobre los datos en general.	1	5	5	4		3	5	5	4		3	A12.3.1-Respaldo de la información	4	1,3	1,3	1,0		0,8
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	1	4	4				4	4				A9.2.6-Retiro o ajuste de los derechos de acceso	3	1,3	1,3			
		Caída del sistema por agotamiento de recursos [E]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	1			4		4			4		4	A11.2.4-Mantenimiento de los equipos.	2			2,0		2,0
		Suplantación de la identidad del usuario [A]	el atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	1	5	5	5	5		5	5	5	5		A8.3.2-Disposición de los medios	4	1,3	1,3	1,3	1,3	

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	1	5	5	4			5	5	4			A9.4.2-Procedimiento de ingreso seguro	2	2,5	2,5	2,0		
		Uso no previsto [A]	utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	1	5	5	4			5	5	4			A8.1.3-Uso aceptable de los activos	2	2,5	2,5	2,0		
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	1	4	4				4	4				A13.2.1-Políticas y procedimientos de transferencia de acción	3	1,3	1,3			
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1	3	4			4	3	4			4	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	1,0	1,3			1,3
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	4	4	3			4	4	3			A9.2.3-Gestión de derechos de acceso privilegiado	4	1,0	1,0	0,8		
		Análisis de tráfico [A]	el atacante sin análisis de comunicaciones, extrae análisis de origen, destino, volumen y frecuencia de los intercambios	1	5	5	4	4	4	5	5	4	4	4	A13.2.1-Políticas y procedimientos de transferencia de acción	4	1,3	1,3	1,0	1,0	1,0
		Interceptación de información (escucha) [A]	el atacante llega a tener acceso a información que no le corresponde, sin que la información en si misma se vea alterada.	1	5	5	3	3	4	5	5	3	3	4	A9.1.2-Acceso a redes y a servicios en red	4	1,3	1,3	0,8	0,8	1,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual							
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad		
	Cableado estructurado - red LAN	Divulgación de información [A]	Revelación de información.	1	4	4	3		3	4	4	3		3	A13.2.4-Acuerdos de confidencialidad o de no divulgación	3	1,3	1,3	1,0		1,0		
		Denegación de servicio [A]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	1	4	4	5			4	4	5			A13.1.2-Seguridad de los servicios de red	3	1,3	1,3	1,7				
		Fallo de servicios de comunicaciones [I]	cese de la capacidad de datos de un sitio a otro, destrucción de medios físicos de transporte, conmutación	2	3		4	4	4	6		8	8	8	A12.6.1-Gestión de las vulnerabilidades técnicas	3	2,0		2,7	2,7	2,7		
		Errores del administrador [E]	(accidental o deliberado) Equivocaciones generadas por responsables de proceso de instalación y operación.	3	3	3	4	3	3	9	9	12	9	9	A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0	2,3	2,3		
		Errores de (re) encaminamiento [E]	Envió de información destino incorrecto por medio del sistema o de la red, la información llega al destinatario incorrecto.	1	4	4		3	4	4	4		3	4	A13.2.1-Políticas y procedimientos de transferencia de acción	3	1,3	1,3		1,0	1,3		
		Errores de secuencia [E]	Alteración accidental del orden de los mensajes transmitidos.	1	4	4			4	4	4			4	A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	1,3	1,3			1,3		
		Alteración accidental de la información [E]	Amenaza identificada sobre los datos en general.	2	4	4	3		3	8	8	6		6	A9.2.3-Gestión de derechos de acceso privilegiado	2	4,0	4,0	3,0		3,0		
		Destrucción de la información [E]	Amenaza identificada sobre los datos en general.	2	4	3	4		3	8	6	8		6	A12.3.1-Respaldo de la información	4	2,0	1,5	2,0		1,5		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	2	4	3		3		8	6		6		A9.2.6-Retiro o ajuste de los derechos de acceso	3	2,7	2,0		2,0	
		Caída del sistema por agotamiento de recursos [E]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2	4		4			8		8			A11.2.4-Mantenimiento de los equipos.	3	2,7		2,7		
		Suplantación de la identidad del usuario [A]	el atacante usa datos de un usuario autorizado, pueden ser ataques por personal interno o externo.	1	4	4		4		4	4		4		A8.3.2-Disposición de los medios	4	1,0	1,0		1,0	
		Abuso de privilegios de acceso [A]	Usuario que abusa de los privilegios en el sistema para realizar actividades fuera de su alcance.	2	3	3	4		3	6	6	8		6	A9.4.2-Procedimiento de ingreso seguro	4	1,5	1,5	2,0		1,5
		Uso no previsto [A]	utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	1	4	3	4		4	4	3	4		4	A8.1.3-Uso aceptable de los activos	3	1,3	1,0	1,3		1,3
		(re) encaminamiento de mensajes [A]	Envió de información destino incorrecto por medio del sistema o de la red, un atacante puede forzar la circulación de mensajes.	1	4	4			4	4	4			4	A13.2.1-Políticas y procedimientos de transferencia de acción	3	1,3	1,3			1,3
		Alteración de secuencia [A]	Alteración de mensajes transmitidos, con intensión de alterar y perjudicar la integridad de datos.	1	4	4				4	4				A.14.1.3-Protección de transacciones de los servicios de las aplicaciones.	3	1,3	1,3			

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros														Evaluación del control									
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual									
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad				
Equipamiento auxiliar [AUX]	Instalaciones Eléctricas	Análisis de tráfico [A]	el atacante sin análisis de comunicaciones, extrae análisis de origen, destino, volumen y frecuencia de los intercambios	1	4	4			4	4	4			4	A13.2.1-Políticas y procedimientos de transferencia de acción	4	1,0	1,0			1,0				
		Interceptación de información (escucha) [A]	el atacante llega a tener acceso a información que no le corresponde, sin que la información en si misma se vea alterada.	1	4	4	5		4	4	4	5		4	A9.1.2-Acceso a redes y a servicios en red	4	1,0	1,0	1,3		1,0				
		Modificación deliberada de la información [A]	Alteración de la información, con fines propios y causar perjuicio.	2	4	4	5	4	4	8	8	10	8	8	A9.1.1-Política de control de acceso	4	2,0	2,0	2,5	2,0	2,0				
		Divulgación de información [A]	Revelación de información.	2	5	5	4		4	10	10	8		8	A13.2.4-Acuerdos de confidencialidad o de no divulgación	3	3,3	3,3	2,7		2,7				
		Denegación de servicio [A]	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	2	3	3	4			6	6	8			A13.1.2-Seguridad de los servicios de red	4	1,5	1,5	2,0						
		Fuego [N]	incendios: posibilidad que acabe con los recursos del sistema	1	3	3	4		4	3	3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		2,0				
		Daños por agua [N]	inundaciones: posibilidad de que el agua acabe con recursos del sistema	1	3	3	4		4	3	3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		2,0				
		Desastres naturales [N]	Desastres sin intención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.	1	3	3	4		4	3	3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	3	1,0	1,0	1,3		1,3				

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros				Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Fuego [I]	incendio: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	3	3	4		4	3	3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		2,0
		Daño por agua [I]	escapes, fugas, inundaciones: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	3	3	4		4	3	3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		2,0
		Desastres industriales [I]	otros desastres debidos de la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga, fluctuaciones eléctricas, accidentes de tráfico (accidental o deliberado)	1	3	4	4		4	3	4	4		4	A16.1.2-Reporte de eventos de seguridad de la información	3	1,0	1,3	1,3		1,3
		Contaminación mecánica [I]	vibraciones, polvo, suciedad	1		4	5		4		4	5		4	A11.1.3-Seguridad de oficinas, recintos e instalaciones.	3		1,3	1,7		1,3
		Contaminación electromagnética [I]	interferencias de radio, campo magnético, luz ultravioleta (accidental o deliberado)	1	4	4	5		4	4	4	5		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	2,0	2,0	2,5		2,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	2	4	4	4		4	8	8	8		8	A11.2.4-Mantenimiento de los equipos.	4	2,0	2,0	2,0		2,0
		Corte del suministro eléctrico [I]	cese de la alimentación de potencia (accidental o deliberado)	1	3	4	5		3	3	4	5		3	A11.2.2-Servicios de suministro	4	0,8	1,0	1,3		0,8

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Interrupción de otros servicios o suministros esenciales [I]	Servicios o recursos de los que depende la operación de equipos: papel para impresoras, tóner, refrigerante (accidental o deliberado)	2	3	3	3			6	6	6			A12.6.1-Gestión de las vulnerabilidades técnicas	3	2,0	2,0	2,0		
		Emanaciones electromagnéticas [I]	Hecho de poner vía radio datos internos a disposición de terceros. Amenaza donde el emisor es víctima pasiva del atacante (accidental o deliberado)	1	4		4			4		4			A13.2.2-Acuerdos sobre transferencia de información	2	2,0		2,0		
		Errores de mantenimiento / actualización de equipos (hardware) [E]	Defectos en los procedimientos o controles de actualización de los equipos que se utilizan más allá del tiempo de uso	2	3	3	4			6	6	8			A.14.2.2-Procedimientos de control de cambios en sistemas	4	1,5	1,5	2,0		
		Pérdida de equipos [E]	La pérdida de equipos provoca directamente la carencia de un medio para prestar el servicio, es decir indisponibilidad.	1		3	4		4		3	4		4	A11.2.4-Mantenimiento de los equipos.	4		0,8	1,0		1,0
		Uso no previsto [A]	utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	1	3	4	4		3	3	4	4		3	A8.1.3-Uso aceptable de los activos	3	1,0	1,3	1,3		1,0
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	4	4	3			4	4	3			A9.2.3-Gestión de derechos de acceso privilegiado	3	1,3	1,3	1,0		
		Manipulación de los equipos [A]	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	1	4		4			4		4			A9.4.4-Uso de programas utilitarios privilegiados	4	1,0		1,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Internet de claro por fibra optica16 megas	Ataque destructivo [A]	Vandalismo, terrorismo, acción militar, la amenaza puede ser perpetrada por personal interno, externo o contratadas.	1		3	4				3	4			A12.3.1-Respaldo de la información	3		1,0	1,3		
		Fuego [N]	incendios: posibilidad que acabe con los recursos del sistema	1	3	3	4		4	3	3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		2,0
		Daños por agua [N]	inundaciones: posibilidad de que el agua acabe con recursos del sistema	1	3	3	4		4	3	3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		2,0
		Desastres naturales [N]	Desastres sin intención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.	2	3	4	4		4	6	8	8		8	A11.1.4-Protección contra amenazas externas y ambientales.	3	2,0	2,7	2,7		2,7
		Fuego [I]	incendio: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	3	3	4		4	3	3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		2,0
		Daño por agua [I]	escapes, fugas, inundaciones: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	3	3	4		4	3	3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		2,0
		Desastres industriales [I]	otros desastres debidos de la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga, fluctuaciones eléctricas, accidentes de tráfico (accidental o deliberado)	2		4	4		4		8	8		8	A16.1.2-Reporte de eventos de seguridad de la información	2		4,0	4,0		4,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Contaminación electromagnética [I]	interferencias de radio, campo magnético, luz ultravioleta (accidental o deliberado)	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	3	1,0	1,0	1,3		1,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	1	4	4	5		3	4	4	5		3	A11.2.4-Mantenimiento de los equipos.	4	1,0	1,0	1,3		0,8
		Corte del suministro eléctrico [I]	cese de la alimentación de potencia (accidental o deliberado)	1	4	4	5		3	4	4	5		3	A11.2.2-Servicios de suministro	4	1,0	1,0	1,3		0,8
		Condiciones inadecuadas de temperatura o humedad [I]	Deficiencias en la aclimatación de los locales, excediendo márgenes de trabajo de los equipos: exceso de calor, frio, humedad (accidental o deliberado)	1	3	3	4			3	3	4			A11.1.1-Perímetro de seguridad física	3	1,0	1,0	1,3		
		Interrupción de otros servicios o suministros esenciales [I]	Servicios o recursos de los que depende la operación de equipos: papel para impresoras, tóner, refrigerante (accidental o deliberado)	1		3	4				3	4			A12.6.1-Gestión de las vulnerabilidades técnicas	3		1,0	1,3		
		Emanaciones electromagnéticas [I]	Hecho de poner vía radio datos internos a disposición de terceros. Amenaza donde el emisor es víctima pasiva del atacante (accidental o deliberado)	1	4	4	3			4	4	3			A13.2.2-Acuerdos sobre transferencia de información	2	2,0	2,0	1,5		
		Errores de mantenimiento / actualización de equipos (hardware) [E]	Defectos en los procedimientos o controles de actualización de los equipos que se utilizan más allá del tiempo de uso	1	3	3	4			3	3	4			A.14.2.2-Procedimientos de control de cambios en sistemas	3	1,0	1,0	1,3		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual					
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	dispositivo de identificación de huella digital	Uso no previsto [A]	utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	2	3	3	4			6	6	8			A8.1.3-Uso aceptable de los activos	4	1,5	1,5	2,0		
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	2	4	4	4		4	8	8	8		8	A9.2.3-Gestión de derechos de acceso privilegiado	3	2,7	2,7	2,7		2,7
		Manipulación de los equipos [A]	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	1	4	3	5		3	4	3	5		3	A9.4.4-Uso de programas utilitarios privilegiados	4	1,0	0,8	1,3		0,8
		Robo [A]	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar servicios, es decir indisponibilidad	1	4	3	4			4	3	4			A11.1.3-Seguridad de oficinas, recintos e instalaciones.	3	1,3	1,0	1,3		
		Ataque destructivo [A]	Vandalismo, terrorismo, acción militar, la amenaza puede ser perpetrada por personal interno, externo o contratadas.	1	3	3	4		3	3	3	4		3	A12.3.1-Respaldo de la información	3	1,0	1,0	1,3		1,0
		Fuego [N]	incendios: posibilidad que acabe con los recursos del sistema	1		3	4		4		3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2		1,5	2,0		2,0
		Daños por agua [N]	inundaciones: posibilidad de que el agua acabe con recursos del sistema	1		3	4		4		3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2		1,5	2,0		2,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros											Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Fuego [I]	incendio: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1		3	4		4		3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2		1,5	2,0		2,0
		Daño por agua [I]	escapes, fugas, inundaciones: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1		3	4		4		3	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2		1,5	2,0		2,0
		Desastres industriales [I]	otros desastres debidos de la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga, fluctuaciones eléctricas, accidentes de tráfico (accidental o deliberado)	1		3	4		3		3	4		3	A16.1.2-Reporte de eventos de seguridad de la información	2		1,5	2,0		1,5
		Contaminación mecánica [I]	vibraciones, polvo, suciedad	2			5		4			10		8	A11.1.3-Seguridad de oficinas, recintos e instalaciones.	2			5,0		4,0
		Contaminación electromagnética [I]	interferencias de radio, campo magnético, luz ultravioleta (accidental o deliberado)	1	3	4	4		4	3	4	4		4	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	2,0	2,0		2,0
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	2	3	3	4		4	6	6	8		8	A11.2.4-Mantenimiento de los equipos.	3	2,0	2,0	2,7		2,7
		Corte del suministro eléctrico [I]	cese de la alimentación de potencia (accidental o deliberado)	1	3	3	4		4	3	3	4		4	A11.2.2-Servicios de suministro	2	1,5	1,5	2,0		2,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Interrupción de otros servicios o suministros esenciales [I]	Servicios o recursos de los que depende la operación de equipos: papel para impresoras, tóner, refrigerante (accidental o deliberado)	1		3	3		3		3	3		3	A12.6.1-Gestión de las vulnerabilidades técnicas	2		1,5	1,5		1,5
		Emanaciones electromagnéticas [I]	Hecho de poner vía radio datos internos a disposición de terceros. Amenaza donde el emisor es víctima pasiva del atacante (accidental o deliberado)	1	3	3	4			3	3	4			A13.2.2-Acuerdos sobre transferencia de información	2	1,5	1,5	2,0		
		Errores de mantenimiento / actualización de equipos (hardware) [E]	Defectos en los procedimientos o controles de actualización de los equipos que se utilizan más allá del tiempo de uso	1	3	3	4		3	3	3	4		3	A.14.2.2-Procedimientos de control de cambios en sistemas	2	1,5	1,5	2,0		1,5
		Pérdida de equipos [E]	La pérdida de equipos provoca directamente la carencia de un medio para prestar el servicio, es decir indisponibilidad.	4	3	3	5		4	12	12	20		16	A11.2.4-Mantenimiento de los equipos.	4	3,0	3,0	5,0		4,0
		Uso no previsto [A]	utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	1	3	3	4			3	3	4			A8.1.3-Uso aceptable de los activos	3	1,0	1,0	1,3		
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	4	4	4		4	4	4	4		4	A9.2.3-Gestión de derechos de acceso privilegiado	3	1,3	1,3	1,3		1,3

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control						
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	Energía eléctrica UPS	Ataque destructivo [A]	Vandalismo, terrorismo, acción militar, la amenaza puede ser perpetrada por personal interno, externo o contratadas.	4	3	3	5	4	4	12	12	20	16	16	A12.3.1-Respaldo de la información	4	3,0	3,0	5,0	4,0	4,0
		Fuego [N]	incendios: posibilidad que acabe con los recursos del sistema	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	1	3,0	3,0	4,0		3,0
		Daños por agua [N]	inundaciones: posibilidad de que el agua acabe con recursos del sistema	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	1	3,0	3,0	4,0		3,0
		Desastres naturales [N]	Desastres sin intención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		1,5
		Fuego [I]	incendio: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	1	3,0	3,0	4,0		3,0
		Daño por agua [I]	escapes, fugas, inundaciones: posibilidad que acabe con los recursos del sistema (accidental o deliberado)	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	1	3,0	3,0	4,0		3,0
		Desastres industriales [I]	otros desastres debidos de la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga, fluctuaciones eléctricas, accidentes de tráfico (accidental o deliberado)	1	3	3	3		3	3	3	3		3	A16.1.2-Reporte de eventos de seguridad de la información	2	1,5	1,5	1,5		1,5

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros												Evaluación del control								
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual					
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Contaminación electromagnética [I]	interferencias de radio, campo magnético, luz ultravioleta (accidental o deliberado)	1	3	3	4		3	3	3	4		3	A11.1.4-Protección contra amenazas externas y ambientales.	2	1,5	1,5	2,0		1,5
		Avería de origen físico o lógico [I]	fallos en los equipos y/o programas, por defectos de origen o sobrevenida durante el funcionamiento del sistema (accidental o deliberado)	1	3	3	4		3	3	3	4		3	A11.2.4-Mantenimiento de los equipos.	3	1,0	1,0	1,3		1,0
		Corte del suministro eléctrico [I]	cese de la alimentación de potencia (accidental o deliberado)	1	3	3	5			3	3	5			A11.2.2-Servicios de suministro	2	1,5	1,5	2,5		
		Condiciones inadecuadas de temperatura o humedad [I]	Deficiencias en la aclimatación de los locales, excediendo márgenes de trabajo de los equipos: exceso de calor, frio, humedad (accidental o deliberado)	1	3	3	4	3	4	3	3	4	3	4	A11.1.1-Perímetro de seguridad física	3	1,0	1,0	1,3	1,0	1,3
		Interrupción de otros servicios o suministros esenciales [I]	Servicios o recursos de los que depende la operación de equipos: papel para impresoras, tóner, refrigerante (accidental o deliberado)	1	3	3	3			3	3	3			A12.6.1-Gestión de las vulnerabilidades técnicas	2	1,5	1,5	1,5		
		Emanaciones electromagnéticas [I]	Hecho de poner vía radio datos internos a disposición de terceros. Amenaza donde el emisor es víctima pasiva del atacante (accidental o deliberado)	1	4	4	3			4	4	3			A13.2.2-Acuerdos sobre transferencia de información	2	2,0	2,0	1,5		
		Errores de mantenimiento / actualización de equipos (hardware) [E]	Defectos en los procedimientos o controles de actualización de los equipos que se utilizan más allá del tiempo de uso	2	3	3	4		4	6	6	8		8	A.14.2.2-Procedimientos de control de cambios en sistemas	4	1,5	1,5	2,0		2,0

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros													Evaluación del control							
					Valor del impacto potencial					Valor del riesgo potencial							Valor del riesgo residual						
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
Personas [P]	proveedor de mantenimiento instalaciones físicas y eléctricas	Uso no previsto [A]	utilización de recursos del sistema no previstos de interés personal: juegos, consultas, bases de datos personales, programas personales y almacenamiento de datos	1	3	3	4			3	3	4			A8.1.3-Uso aceptable de los activos	3	1,0	1,0	1,3		
		Acceso no autorizado [A]	Atacante accede a los recursos del sistema sin autorización, aprovecha fallos del sistema como identificación y autorización.	1	4	4	3			4	4	3			A9.2.3-Gestión de derechos de acceso privilegiado	3	1,3	1,3	1,0		
		Manipulación de los equipos [A]	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	1	4	3	4		3	4	3	4		3	A9.4.4-Uso de programas utilitarios privilegiados	3	1,3	1,0	1,3		1,0
		Deficiencias en la organización [E]	Cuando no está claro las actividades quien las debe desarrollar sobre los activos e informar a la jerarquía de gestión.	2	3	3	3			6	6	6			A6.1.1-Roles y responsabilidades para la seguridad de la información	3	2,0	2,0	2,0		
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	2	4	4				8	8				A9.2.6-Retiro o ajuste de los derechos de acceso	3	2,7	2,7			
		Indisponibilidad del personal [E]	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones de orden público.	3	3	3	4			9	9	12			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	3,0		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
	proveedor de mantenimiento de equipos informáticos	Indisponibilidad del personal [A]	Ausencia deliberada del puesto de trabajo: huelga, absentismo laboral, bajas no justificadas, bloqueo de accesos	1		3	3				3	3			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4		0,8	0,8		
		Extorsión [A]	Presión, mediante amenazas, se ejercen sobre alguien para obligarle a obrar en determinado sentido.	1	3	3	3			3	3	3			A6.1.3-Contacto con las autoridades	1	3,0	3,0	3,0		
		Ingeniería social (picaresca) [A]	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	2	4	4	4	4		8	8	8	8		A8.1.3-Uso aceptable de los activos	3	2,7	2,7	2,7	2,7	
		Deficiencias en la organización [E]	Cuando no está claro las actividades quien las debe desarrollar sobre los activos e informar a la jerarquía de gestión.	2		3	3				6	6			A6.1.1-Roles y responsabilidades para la seguridad de la información	3		2,0	2,0		
		Fugas de información [E]	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel	2	4	4				8	8				A9.2.6-Retiro o ajuste de los derechos de acceso	3	2,7	2,7			
		Indisponibilidad del personal [E]	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones de orden público.	3	3	3	3			9	9	9			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4	2,3	2,3	2,3		
		Indisponibilidad del personal [A]	Ausencia deliberada del puesto de trabajo: huelga, absentismo laboral, bajas no justificadas, bloqueo de accesos	1		3	3				3	3			A7.2.2-Toma de conciencia, educación y formación en la seguridad de la información.	4		0,8	0,8		

Continúa…

MATRIZ DE RIESGOS CENTRO DE DIAGNOSTICO AUTOMOTOR CORPOTRANS CDA

IDENTIFICACIÓN DE ACTIVOS		identificación y valoración de peligros			Valor del impacto potencial					Valor del riesgo potencial					Evaluación del control		Valor del riesgo residual				
CLASIFICACIÓN DE ACTIVO	NOMBRE DEL ACTIVO	Amenazas	Descripción de la Amenaza	Frecuencia	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Controles NTC ISO/IEC 27001-27002	Eficacia del control	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
		Extorsión [A]	Presión, mediante amenazas, se ejercen sobre alguien para obligarle a obrar en determinado sentido.	1	4	4	3			4	4	3			A6.1.3-Contacto con las autoridades	1	4,0	4,0	3,0		
		Ingeniería social (picaresca) [A]	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	3	4	4	4			12	12	12			A8.1.3-Uso aceptable de los activos	4	3,0	3,0	3,0		

Elaboración: propia.