



Centro De Diagnóstico Automotor De Caldas Limitada

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Manizales 2021



1.Introducción

La Seguridad de la Información en el Centro de Diagnóstico Automotor de Caldas tiene como objetivo principal la protección y conservación de todos y cada uno de los activos de información en cualquiera de sus estados, ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y disponibilidad.

Lo anterior mediante la implementación de medidas de control de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta.

Para conseguir que la información de la entidad sea confidencial, íntegra y disponible, se deberá manejar un ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

- **Confidencialidad:** Propiedad que la información sea concedida únicamente a quien esté autorizado.
- **Integridad:** Propiedad que la información se mantenga exacta y completa.
- **Disponibilidad:** propiedad que la información sea accesible y utilizable en el momento que se requiera.



2. Objetivo

Proveer una infraestructura a la entidad, que proporcione herramientas adecuadas para desarrollar y fortalecer la conservación e integridad de la información gestionada y almacenada por cada área, mitigando así los riesgos ocasionados por la vulneración externa de la seguridad informática; permitiendo además un mejoramiento continuo del Centro de Diagnóstico Automotor de Caldas Limitada.

3. Alcance

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso del Centro de Diagnóstico Automotor de Caldas Limitada, a cualquier sistema de información o aspecto particular de control de la Entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.



4. Objetivos Específicos

- Brindar lineamientos y principios que propendan por la unificación de criterios para la administración de los riesgos de seguridad de la información.
- Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la Entidad.
- Proteger el valor de los activos de información mediante la implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas
- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.
- Reducir toda posibilidad de que una brecha o evento produzca determinado impacto en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.
- Lograr y mantener a través de la implementación de medidas de control el nivel de probabilidad e impacto residual de los riesgos a el nivel aceptable por parte de la Alta Gerencia.



5. Definiciones

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Control: Medida que modifica el riesgo.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.



Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.



Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.

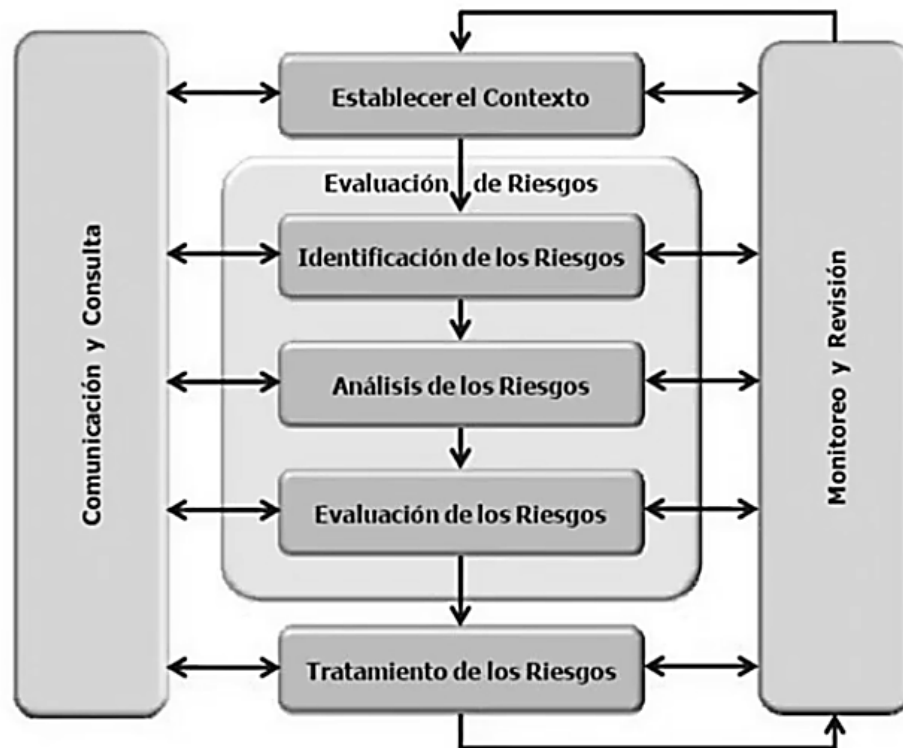
Tratamiento del Riesgo: Proceso para modificar el riesgo” (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información.

6. Proceso de gestión de riesgo en la seguridad de la información

El Centro de Diagnóstico Automotor de Caldas Limitada presenta el modelo de gestión estimado para la mitigación de los riesgos en la seguridad de la información:





6.1 Establecimiento del contexto

Definición de los parámetros externos e internos a tener en cuenta cuando se gestiona el riesgo, y se establecen el alcance y los criterios de riesgo para la política de gestión del riesgo. Comprende establecer los contextos estratégicos, organizacional y de gestión en los cuales tendrá lugar el Proceso de Gestión de Riesgos. Deben establecerse los objetivos de la evaluación del riesgo, los criterios contra los cuales se evaluarán los riesgos, el programa de evaluación del riesgo y definirse la estructura de análisis, los roles y responsabilidades

6.2 Evaluación del riesgo

La evaluación del riesgo es el proceso global de identificación del riesgo, de análisis del riesgo y de valoración del riesgo

- **Identificación del Riesgo:** Proceso de búsqueda, reconocimiento y descripción de riesgos. Comprende identificar los riesgos que podrían impedir, degradar o demorar el cumplimiento de los objetivos estratégicos y operativos de la organización, así como las oportunidades que puedan contribuir al logro de los referidos objetivos
- **Análisis del Riesgo:** Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis el riesgo proporciona las bases para la valoración del riesgo y para tomar las decisiones relativas al tratamiento del riesgo. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que los riesgos puedan ocurrir. Consecuencia y probabilidad se combinan para producir un nivel estimado de riesgo según la definición de la organización. Adicionalmente se debe identificar y analizar los controles mitigantes existentes

- **Valoración del Riesgo:** Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable. Comprende comparar los niveles de riesgo encontrados contra los criterios de riesgo aceptado preestablecidos por la organización, considerando el balance entre beneficios potenciales y resultados adversos. Ordenar y priorizar mediante un ranking los riesgos analizados.

6.2 Tratamiento del riesgo

Una vez completada la valuación del riesgo, el tratamiento del riesgo involucra la selección y el acuerdo para aplicar una o varias opciones pertinentes para cambiar la probabilidad de que los riesgos ocurran, los efectos de los riesgos, o ambas, y la implementación de estas opciones. A continuación de esto, sigue un proceso crítico de reevaluación del nuevo nivel de riesgo, con la intención de determinar su tolerancia con respecto a los criterios previamente establecidos, para decidir si se requiere tratamiento adicional. De acuerdo al ranking de riesgos y al nivel de riesgo aceptado preestablecido por la organización, definir su tratamiento y/o monitoreo, desarrollando e implementando estrategias y planes de acción específicos, que mantengan el riesgo dentro de los niveles aceptados por la organización.

COSTO - BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	Evitar el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	Transferir o compartir el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	Reducir o Mitigar el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	Retener o aceptar el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa



6.2 Monitoreo y Revisión

Como parte del proceso de gestión del riesgo, los riesgos y los controles se deben monitorear y revisar de manera regular. Comprende definir y utilizar mecanismos para la verificación, supervisión, observación crítica o determinación del estado de los riesgos y controles con objeto de identificar de una manera continua los cambios que se puedan producir en el nivel de desempeño requerido o esperado y dar cuenta de la evolución del nivel del riesgo en procesos críticos para la administración. desarrollando e implementando estrategias y planes de acción específicos, que mantengan el riesgo dentro de los niveles aceptados por la organización.

6.3 Comunicación y consulta

Los procesos continuos e iterativos que realiza una organización para proporcionar, compartir u obtener información y para comprometer el diálogo con las partes interesadas en relación con la gestión del riesgo. Comprende definir y utilizar mecanismos para comunicar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del Proceso de Gestión de Riesgos. Dichos mecanismos deben permitir a las autoridades tomar decisiones en forma oportuna respecto de los riesgos con mayores desviaciones en relación a los niveles aceptados.