PLAN DE SEGURIDAD DE LA INFORMACION

1. INTRODUCCION

El Centro de diagnóstico automotor de Cúcuta limitada-CEDAC determina que toda la información que maneja (financiera, del personal, contratistas, procesos de contratación y por supuesto revisiones técnico mecánicas) son de suma importancia para poder cumplir con la misión y objetivo de la entidad por lo cual se hace necesario implementar unas políticas de seguridad de la información que permitan mitigar los riesgos y proteger la confidencialidad, integridad y disponibilidad de la información.

En el presente manual se establecen las políticas de seguridad de la información, las cuales deben ser adoptadas por los funcionarios, contratistas, proveedores o pasantes que presten sus servicios o tengan algún tipo de relación con la entidad; estas se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001:2013.

OBJETIVO

Mantener unas políticas que permita mitigar los riesgos en seguridad de la información permitiendo de esta forma que la información generada día a día producto de las actividades diarias de la empresa se resguarde de forma segura.

DEFINICIONES

Amenaza. en seguridad de la información se define como toda situación, circunstancia o persona ya sea interna o externa en una entidad, organización, red pública o privada, que pueda causar daño a la información de un sistema como robo, divulgación de datos confidenciales, alteración de datos, borrado total de datos, negación de un servicio, entre otros[1].

Autorización: Acción de otorgar el acceso a usuarios o grupo de usuarios con el fin de que puedan usar los recursos de un sistema como aplicaciones, internet, descarga de datos entre otros[1].

[1] ARAYA, D. Glosario de términos de Seguridad Informática. [En línea]. [Consultado 20 de noviembre 2016]. Disponible en Internet: (http://safemode-cl.blogspot.com.co/2006/07/glosario-de-terminos-de-seguridad.html).

Control de acceso. Limitar el acceso a objetos de acuerdo a los permisos de acceso del sujeto, es decir, se puede otorgar una autorización para acceder al sistema, pero sus permisos son limitados ejemplo poder acceder a una determinada información para consultarla, pero no poner ni modificarla, descárgala o borrarla[2].

Cortafuego. Herramienta de seguridad que proporciona un límite entre redes de distinta confianza o nivel de seguridad mediante el uso de políticas de control de acceso de nivel de red, esta herramienta viene integrada con algunos sistemas operativos y su configuración es modificable por el administrador del equipo con el fin de establecer hasta qué punto pueda otorgar un determinado acceso[1].

Disponibilidad. Acceso y utilización de la información y los sistemas en los que la misma es procesada por parte de los individuos, entidades o procesos que se encuentran autorizados para ello[2].

Ethernet. Sistema de red de área local de alta velocidad en los que se pueden conectar un grupo determinado de equipos[1].

Gestión de redes. Controlar diversos aspectos de una red para optimizar su eficiencia como por ejemplo monitorizar, probar, configurar, analizar y evaluar los recursos de una red[3].

Gestión de seguridad. Proceso de establecer y mantener la seguridad en un sistema o red de sistemas informáticos. Las etapas de este proceso incluyen la prevención de problemas de seguridad, detección de intrusiones, investigación de intrusiones, y resolución[3].

Integridad. Hace referencia a la exactitud y completitud que posee la información, es decir, que la misma no le falten datos o tenga datos que no corresponden a dicha información[4].

Paquete. Estructura de datos con una cabecera que puede estar o no lógicamente completa, es decir, es cada uno de los tramos en el que se divide la información que se va a enviar a través del nivel de red[3].

Política de seguridad. Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos, todas estas componen

[2] GOMEZ, Á. Enciclopedia de la Seguridad Informática. México: Alfaomega; 2007.
[3] ARAYA, Op cit. p1.
[4] GOMEZ. Op cit. p.4-25.

unas reglas que la empresa seguirá para minimizar riesgos y amenazas en sus sistemas de información[4].

Ransomware: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

Riesgo: es aquella probabilidad que tienen los activos ya sean de hardware o software de sufrir algún daño debido a las vulnerabilidades y amenazas que estos puedan tener[4].

Seguridad de la información: Según [ISO IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

SGSI: Sistema de gestión de seguridad de la información.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

Vulnerabilidades. Hace referencia a las debilidades que puede tener un sistema las cuales podrían ser aprovechadas por un pirata informático para realizar un ataque, estas debilidades pueden ser a nivel de hardware o software[5]

Anualmente el encargado de sistemas programará el mantenimiento preventivo a las cámaras de la entidad dicho mantenimiento deberá ser entregado junto con un informe de actividades realizadas y registro fotográfico.

[5] SUAREZ, S. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Tesis de Especialización. Bogotá: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería; 2015.

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del CENTRO DE DIAGNOSTICO AUTOMOTOR DE CUCUTA - CEDAC con respecto a la protección de los activos de información (la información , los funcionarios, contratistas y terceros, los procesos, las tecnologías de información incluido el hardware y el software, entre otros), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

El CENTRO DE DIAGNOSTICO AUTOMOTOR DE CUCUTA - CEDAC, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos que la entidad lleva a cabo para el cumplimiento de su razón social.
- Mantener la confianza de los empleados de planta, contratistas y terceros.
- Apoyar la innovación tecnológica y la mejora continua.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger uno de los activos más importantes para la empresa como lo es la información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de los procesos administrativos.
- Fortalecer la cultura de seguridad de la información en los empleados de planta, terceros, aprendices, practicantes y clientes del **CENTRO DE DIAGNSTICO AUTOMOTOR DE CUCUTA - CEDAC**
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros que tengan un vínculo con el CENTRO DE DIAGNOSTICO AUTOMOTOR DE CUCUTA - CEDAC.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento de un 100% de la política.

A continuación, se establecen las políticas de seguridad que soportan el SGSI del CENTRO DE DIAGNOSTICO AUTOMOTOR DE CUCUTA - CEDAC

- **El CENTRO DE DIAGNOSTICO AUTOMOTOR DE CUCUTA - CEDAC** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros que tengan algún vínculo con la entidad y requieran del uso de información o de sus plataformas tecnológicas.
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA - CEDAC** protegerá la información generada, procesada o resguardada por los procesos llevados a cabo en la entidad (revisión técnico mecánica y de emisiones contaminantes, procesos contractuales, contables entre otros) y activos de información que se deriven o produzcan a partir de los mismos.
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA - CEDAC** protegerá la información creada, procesada, transmitida o resguardada por sus procesos en todas sus actividades, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de la misma. Para ello es primordial la aplicación de controles de acuerdo con la clasificación que se le dé a la información y total compromiso del propietario que tenga su custodia.
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA - CEDAC** protegerá por medio de la implementación de controles basados en la ISO/IEC 27001:2013 toda la información de las posibles amenazas originadas por parte del personal (borrado, alteración o robo).
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA - CEDAC** protegerá las instalaciones y la infraestructura tecnológica que soporta sus procesos críticos con

diferentes controles ya sean físicos o tecnológicos que garantices su buen funcionamiento (acceso restringido, UPS, Cámaras de seguridad entre otros).

- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA - CEDAC** monitoreara la operación de todos sus procesos, garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA - CEDAC** implementará control de acceso a la información, sistemas y recursos de red, mediante restricciones físicas y lógicas como usuarios y contraseñas con diferentes privilegios según el cargo y la información a la que se necesite acceso
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA - CEDAC** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA - CEDAC** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora continua que minimice los riesgos y fortalezcan la seguridad e la información.
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA - CEDAC** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA – CEDAC** realizara diariamente copias de seguridad de las Revisiones técnico mecánicas y semanalmente de toda la información de los equipos de la entidad.
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA – CEDAC** mantendrá una conexión mantendrá resguardada en tiempo real la información y copias de seguridad en un espacio en nube 24/7.
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA – CEDAC** establecerá una política de privacidad y protección de información de datos personales, la cual publicará en su página web y dará a conocer a todos los empleados, contratistas, terceros y clientes de la entidad.
- **El CENTRO DE DIAGNOSTICO AUOTMOTOR DE CUCUTA - CEDAC** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la Política General de Seguridad y Privacidad de la Información, traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad y la misma aplicará lo contemplado en el manual de proceso disciplinario, así como también recaerá lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

ELABORÓ:	REVISÓ:		APROBÓ:
			
MARTIN JAVIER DIEZ D.T. SUPLENTE	JULIETH SALCEDO ASESORA PLANEACION Y GESTION	MARTHA JAIMES ASESORA CONTROL INTERNO	MAIRA ALEJANDRA LOPEZ GERENTE
FECHA: 15/01/2024	**FECHA: 16/01/2024**	**FECHA: 24/01/2024**	**FECHA: 26/01/2024**